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 Red Hat OpenShift Service on AWS? ... 1
Fonctionnalités ... 1
Accès ROSA ... 1
Comment démarrer avec ROSA ... 2
Tarification ... 3
ROSA frais de service ... 3
AWS frais d'infrastructure ... 4
Responsabilités ... 4
Présentation ... 4
Tâches à responsabilités partagées par domaine ... 7
Responsabilités du client à l'égard des données et des applications ... 31
Modèles d'architecture ... 34
Comparaison ROSA avec HCP et ROSA classique ... 35
Commencez avec ROSA ... 37
Configuration ... 37
Prérequis ... 37
Activer ROSA et configurer les AWS prérequis ... 38
Créez un ROSA HCPcluster - CLI ... 39
Prérequis ... 40
Création Amazon VPC application ... 40
Créez le requis IAM rôles et configuration d'OpenID Connect ... 47
Créez un HCP cluster ROSA avec à l'aide du ROSA CLIet AWS STS ... 48
Configuration d'un fournisseur d'identité et autorisation cluster accès ... 49
Accorder à l'utilisateur l'accès à un cluster ... 51
Configuration `cluster-admin` des autorisations ... 52
Configuration `dedicated-admin` des autorisations ... 52
Accédez à un cluster via la console Red Hat Hybrid Cloud ... 52
Déployer une application depuis le catalogue des développeurs ... 53
Révoquer `cluster-admin` les autorisations d'un utilisateur ... 54
Révoquer `dedicated-admin` les autorisations d'un utilisateur ... 54
Révoquer l'accès d'un utilisateur à un cluster ... 55
Supprimer un cluster et AWS STS resources ... 55
Créez un cluster ROSA classique - CLI ... 56
Prérequis ... 57

Créez un cluster ROSA classique à l'aide du ROSA CLIet AWS STS ..... 57
Configuration d'un fournisseur d'identité et autorisation cluster accès ..... 59
Accorder à l'utilisateur l'accès à un cluster ..... 61
Configuration `cluster-admin` des autorisations ..... 62
Configuration `dedicated-admin` des autorisations ..... 62
Accédez à un cluster via la console Red Hat Hybrid Cloud ..... 62
Déployer une application depuis le catalogue des développeurs ..... 63
Révoquer `cluster-admin` les autorisations d'un utilisateur ..... 64
Révoquer `dedicated-admin` les autorisations d'un utilisateur ..... 64
Révoquer l'accès d'un utilisateur à un cluster ..... 65
Supprimer un cluster et AWS STS resources ..... 65
Créez un cluster ROSA classique - AWS PrivateLink ..... 66
Prérequis ..... 67
Création Amazon VPC application ..... 40
Créez un cluster ROSA classique à l'aide du ROSA CLIet AWS PrivateLink ..... 72
Configuration AWS PrivateLink DNStransfert ..... 74
Configuration d'un fournisseur d'identité et autorisation cluster accès ..... 76
Accorder à l'utilisateur l'accès à un cluster ..... 78
Configuration `cluster-admin` des autorisations ..... 78
Configuration `dedicated-admin` des autorisations ..... 78
Accédez à un cluster via la console Red Hat Hybrid Cloud ..... 79
Déployer une application à partir du catalogue pour développeurs ..... 79
Révoquer `cluster-admin` les autorisations d'un utilisateur ..... 80
Révoquer `dedicated-admin` les autorisations d'un utilisateur ..... 81
Révoquer l'accès d'un utilisateur à un cluster ..... 81
Supprimer un cluster et AWS STS resources ..... 81
Sécurité ..... 84
Protection des données ..... 84
Chiffrement des données ..... 86
Gestion des identités et des accès ..... 89
Public ciblé ..... 90
Authentification par des identités ..... 91
Gestion des accès à l’aide de politiques ..... 95
ROSA exemples de politiques basées sur l'identité ..... 97
AWS stratégies gérées ..... 118
Résolution des problèmes ..... 137

Résilience ... 139
AWS résilience des infrastructures mondiales ... 139
ROSA résilience des clusters ... 140
Résilience des applications déployées par le client ... 140
Sécurité de l’infrastructure ... 141
Isolation du réseau en cluster ... 141
Isolation du réseau de pods ... 142
Quotas de service ... 143
Utilisation avec d'autres services ... 144
ROSA et AWS Marketplace ... 144
Terminologie ... 144
ROSA paiements et facturation ... 145
Abonnement aux listings ROSA Marketplace via la console ... 146
Acheter un ROSA contrat ... 146
Private Marketplace ... 152
Résolution des problèmes ... 153
Accédez aux journaux ROSA de débogage du cluster ... 153
ROSA le cluster échoue à la vérification des quotas de AWS service lors de cluster la création ... 153
Résoudre les problèmes liés aux ROSA CLI jetons d'accès hors ligne expirés ... 154
Impossible de créer un fichier cluster avec une osdCcsAdmin erreur ... 154
Étapes suivantes ... 155
Obtention de support ... 155
Ouvrez un AWS Support étui ... 155
Ouvrez un dossier Red Hat Support ... 156
Historique de la documentation ... 157
... clxii

# Qu'est-ce que 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 Kubernetes OpenShift d'entreprise Red Hat sur AWS. ROSA rationalise le transfert des charges de travail Red Hat OpenShift sur site vers AWS, et offre une intégration étroite avec d'autres Services AWS.

## Fonctionnalités

ROSA est soutenu et géré conjointement par AWS et Red Hat. Chaque ROSA Le cluster est doté d'une assistance 24 heures sur 24 par un ingénieur responsable de la fiabilité des sites Red Hat (SRE) pour la gestion du cluster, conformément au contrat de niveau de service de 99,95 % de Red Hat (). SLA 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 SRE clusters, maintenance de clusters et mises à niveau de clusters prises en charge par Red Hat.
- Service AWS les intégrations incluent AWS calcul, base de données, analyse, apprentissage automatique, mise en réseau et mobile.
- Exécutez et dimensionnez le plan de contrôle Kubernetes sur plusieurs AWS Zones de 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 votre ROSA déploiements de services à l'aide des interfaces suivantes.

AWS

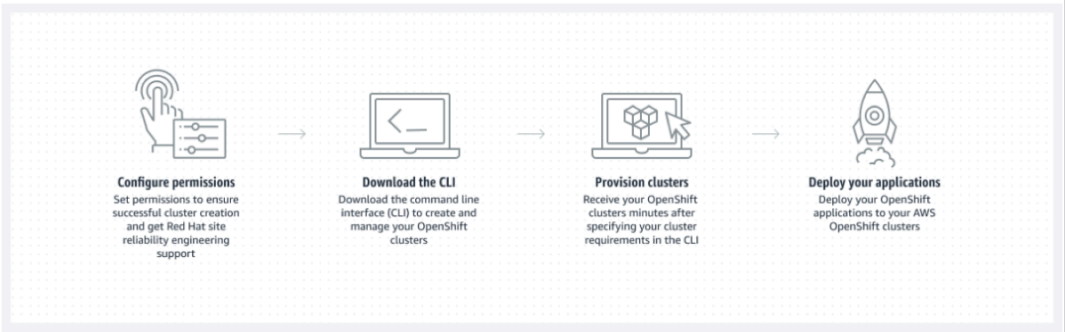
- ROSA console — Fournit une interface Web pour activer ROSA abonnement et achat d'un ROSA contrat de logiciel.

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

Chapeau rouge OpenShift

- Red Hat Hybrid Cloud Console : fournit une interface Web pour créer, mettre à jour et gérer ROSA clusters, installez des modules complémentaires pour clusters et créez et déployez des applications sur un ROSA grappe.
- ROSA CLI(rosa) — Fournit des commandes pour créer, mettre à jour et gérer ROSA clusters.
- OpenShift CLI(oc) — Fournit des commandes pour créer des applications et gérer des projets OpenShift Container Platform.
- Knative CLI (kn) - Fournit des commandes qui peuvent être utilisées pour interagir avec des composants OpenShift sans serveur, tels que Knative Serving et Eventing.
- Pipelines CLI (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.
- Opérateur SDK CLI : 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 démarrage détaillées, voirCommencez avec ROSA .

AWS Management Console/AWS CLI

1. Configurer les autorisations pour Services AWS that ROSA s'appuie sur pour fournir des fonctionnalités de service. Pour de plus amples informations, veuillez consulter the section called “Prérequis”.
2. Installation et configuration de la dernière version AWS CLI outil. Pour plus d'informations, voir Installation ou mise à jour de la dernière version du AWS CLIdans le AWS CLI Guide de l'utilisateur.
3. Enable ROSA dans le ROSA console.

Console de cloud hybride Red Hat/ROSA CLI

1. Téléchargez la dernière version du ROSA CLIet OpenShift CLI depuis la console Red Hat Hybrid Cloud. Pour plus d'informations, voir Commencer avec le ROSA CLIdans la documentation Red Hat.
2. Création ROSA clusters dans la console Red Hat Hybrid Cloud ou avec 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 regroupez de la même manière que vous le feriez avec n'importe quel autre OpenShift environnement.

# Tarification

Le coût total de ROSA se compose de deux éléments : ROSA frais de service et AWS frais d'infrastructure. Pour plus d'informations sur les tarifs, voir Red Hat OpenShift Service on AWS Tarification.

## ROSA frais de service

Par défaut, ROSA les frais de service s'accumulent sur demande à un taux horaire par 4 v CPU utilisés par les nœuds de travail. Les frais de service sont uniformes pour tous les services pris en charge AWS Régions standard. Outre les frais de service du nœud de travail, les clusters hébergés ROSA avec des plans de contrôle (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 AWS infrastructure 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), Red Hat et les clients du Red Hat OpenShift Service on AWS (ROSA) service géré. Pour plus d'informations sur ROSA et ses composants, voir Politiques et définition du service dans la documentation Red Hat.

L'interface AWS le modèle de responsabilité partagée définit 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, le réseau et les installations qui fonctionnent AWS Cloud services. Cette AWS la responsabilité est communément appelée « sécurité du cloud ». Pour opérer ROSA en tant que service entièrement géré, Red Hat et le client sont responsables des éléments du service que le AWS Le modèle de responsabilité se définit comme « la sécurité dans le cloud ».

Red Hat est responsable de la gestion et de la sécurité continues du ROSA l'infrastructure du cluster, la plate-forme d'application sous-jacente et le système d'exploitation. Tandis que ROSA les clusters sont hébergés sur AWS ressources chez le client Comptes AWS, ils sont accessibles à distance par ROSA composants de service et ingénieurs de fiabilité des sites Red Hat (SREs) via IAM 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 ROSA gestion du réseau, journalisation des clusters, gestion des versions des clusters et gestion des capacités. Alors que Red Hat gère ROSA service, le client est entièrement responsable de la gestion et de la sécurisation des applications, des charges de travail et des données déployées sur ROSA.

## Présentation

Le tableau suivant donne un aperçu des AWS, Red Hat et les responsabilités des clients pour 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 sur les clients | 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/AWS infrastructure mondiale | 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 de ROSA composants. Cette documentation définit ROSA responsabilités 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<br>• Surveillez OpenShift le service natif du routeur et répondez aux alertes. | Client<br>• Surveillez l'état des routes applicatives et des points de terminaison qui les sous-tendent.<br>• Signalez les pannes à AWS et Red Hat. |
| Gestion des réseaux virtuels | Chapeau rouge<br>• Surveiller AWS équilibre urs de charge, Amazon VPC des sous-réseaux, et Service AWS composant s nécessaires à la mise en réseau de la plate-forme par défaut. Répondez aux alertes. | Client<br>• Surveillez l'état de santé de AWS points de terminaison de l'équilibreur de charge.<br>• Surveillez le trafic réseau éventuellement configuré via Amazon VPC VPCconnexion -à-, AWS VPN connexion, ou AWS Direct Connect pour des problèmes potentiels ou des menaces de sécurité. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| Gestion du stockage virtuel | Chapeau rouge<br>• Surveiller Amazon EBS les volumes utilisés pour les nœuds du cluster, et Amazon S3 seaux utilisés pour le ROSA registre d'images de conteneur intégré au service. Répondez aux alertes. | Client<br>• Surveillez l'état des données des applications.<br>• Si le client a géré AWS KMS keys sont utilisés, créent et contrôlent le cycle de vie des clés et les politique s clés pour Amazon EBS chiffrement. |
| AWS logiciel (public) Services AWS) | AWS<br>• Pour plus d'informations sur AWS gestion des incidents et des opérations, voir Comment AWS assure la résilience opérationnelle et la continuité du service dans le AWS livre blanc. | Client<br>• Surveillez l'état de santé de AWS ressources du compte client.<br>• Utiliser IAM outils pour appliquer les autorisat ions appropriées à AWS ressources du compte client. |
| Matériel/AWS infrastructure mondiale | AWS<br>• Pour plus d'informations sur AWS gestion des incidents et des opérations, voir Comment AWS assure la résilience opérationnelle et la continuité du service dans le AWS livre blanc. | Client<br>• 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<br>• Agrégez et surveillez de manière centralisée les journaux d'audit de la plateforme.<br>• Fournir et gérer un opérateur de journalis ation pour permettre au client de déployer une pile de journalisation pour la journalisation des applicati ons par défaut.<br>• Fournissez des journaux d'audit à la demande du client. | Client<br>• Installez l'opérateur optionnel de journalisation des applications par défaut sur le cluster.<br>• Installez, configurez et gérez toutes les solutions de journalisation d'applications facultatives, telles que la journalisation de conteneur s annexes ou d'applications de journalisation tierces.<br>• 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.<br>• Demandez les journaux d'audit de la plateforme via un dossier d'assistance pour |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| | | rechercher des incidents spécifiques. |
| Mise en réseau d'applications | Chapeau rouge<br>• 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.<br>• 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.<br>• Installez, configurez et gérez les OpenShift SDN composants pour le trafic interne par défaut des pods.<br>• Donnez au client la possibilité de gérer `NetworkPolicy` et `EgressNetworkPolicy` (de protéger) des objets. | Client<br>• 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`<br>• Utilisez OpenShift Cluster Manager pour demander un équilibreur de charge privé pour les itinéraires d'application par défaut.<br>• Utilisez OpenShift Cluster Manager pour configurer jusqu'à une partition de routeur publique ou privée supplémentaire et l'équilibreur de charge correspondant.<br>• Demandez et configurez tout équilibreur de charge de service supplémentaire pour des services spécifiques.<br>• Configurez les règles DNS de transfert nécessaires. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| Mise en réseau de clusters | Chapeau rouge<br>• 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 composants.<br>• 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<br>• Fournissez des plages d'adresses IP facultatives autres que celles par défaut pour la machine CIDRCIDR, le service et le pod CIDR si nécessaire via OpenShift Cluster Manager lors du provisionnement du cluster.<br>• Demandez que le point de terminaison du API service 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<br>• Installation et configuration 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<br>• Permettre au client de gérer AWS VPN connectivité avec les ressources sur site, Amazon VPC VPCconnectivité -vers-, et AWS Direct Connect selon les besoins via OpenShift Cluster Manager.<br>• Permettre aux clients de créer et de déployer AWS équilibreurs de charge à utiliser avec les équilibreurs de charge de service. | Client<br>• Configuration et maintenance facultatives Amazon VPC composants, tels que Amazon VPC VPCconnexion -à-, AWS VPN connexion, ou AWS Direct Connect.<br>• 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<br>• Configurez et configurez le ROSA plan de contrôle et plan de données à utiliser Amazon EC2 instances pour le calcul en cluster.<br>• Surveillez et gérez le déploiement de Amazon EC2 plan de contrôle et nœuds d'infrastructure du cluster. | Client<br>• Surveiller et gérer Amazon EC2 nœuds de travail en créant un pool de machines à l'aide du gestionnaire de OpenShift clusters ou ROSA CLI.<br>• Gérez les modifications apportées aux applications déployées par les clients et aux données des applications. |
| Version du cluster | Chapeau rouge<br>• Activez le processus de planification des mises à niveau.<br>• Surveillez la progression de la mise à niveau et corrigez les éventuels problèmes rencontrés.<br>• Publiez des journaux des modifications et des notes de version pour les mises à niveau mineures et les mises à niveau de maintenance. | Client<br>• Planifiez les mises à niveau des versions de maintenance immédiatement, pour le futur, ou optez pour des mises à niveau automatiques.<br>• Reconnaissez et planifiez les mises à niveau des versions mineures.<br>• Assurez-vous que la version du cluster reste une version secondaire prise en charge.<br>• Testez les applications des clients sur les versions mineures et de maintenance pour garantir la compatibilité. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| Gestion des capacités | Chapeau rouge<br>• Surveillez l'utilisation du plan de contrôle. Les plans de contrôle incluent les nœuds du plan de contrôle et les nœuds d'infrast ructure.<br>• Faites évoluer et redimensi onnez les nœuds du plan de contrôle pour maintenir la qualité de service. | Client<br>• Surveillez l'utilisation des nœuds de travail et, le cas échéant, activez la fonction de dimension nement automatique.<br>• Déterminez la stratégie de mise à l'échelle du cluster.<br>• Utilisez les commandes du gestionnaire de OpenShift clusters fournies pour ajouter ou supprimer des nœuds de travail supplémen taires selon les besoins.<br>• 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<br>• Installation et configuration Amazon EBS pour fournir un stockage sur nœud local et un stockage de volume persistant pour le cluster.<br>• Configurez et configure z le registre d'images intégré à utiliser Amazon S3 rangement par seau.<br>• Élaguez régulièrement les ressources du registre d'images dans Amazon S3 pour optimiser Amazon S3 utilisation et performances du cluster. | Client<br>• Configurez éventuellement Amazon EBS CSIchauffeur ou Amazon EFS CSIpilote pour approvisionner des volumes persistants sur le cluster. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| AWS logiciel (public) AWS services) | AWS<br><br>Calcul<br><br>• Fournissez le Amazon EC2 service, utilisé pour ROSA plan de contrôle, infrastru cture et nœuds de travail.<br><br>Stockage<br><br>• Fournir Amazon EBS pour permettre le ROSA service permettant de fournir un stockage sur nœud local et un stockage de volume persistant pour le cluster.<br><br>Réseaux<br><br>• Fournissez les informati ons suivantes AWS Cloud des services pour satisfaire ROSA besoins en infrastru cture de réseau virtuel :<br>  • Amazon VPC<br>  • Elastic Load Balancing<br>  • IAM<br>• Fournissez les informati ons facultatives suivantes Service AWS intégrations pour ROSA:<br>  • AWS VPN | Client<br><br>• Signez les demandes à l'aide d'un identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal ou AWS STS informations d'identif ication de sécurité temporair es.<br>• Spécifiez VPC les sous-réseaux que le cluster doit utiliser lors de sa création.<br>• Configurez éventuellement un système géré par le client VPC pour l'utiliser avec ROSA clusters. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| | • AWS Direct Connect<br>• AWS PrivateLink<br>• AWS Transit Gateway | |
| Matériel/AWS infrastructure mondiale | AWS<br>• Pour plus d'informations sur les contrôles de gestion pour AWS centres de données, voir Nos contrôles sur le AWS Cloud Page de sécurité.<br>• Pour plus d'informations sur les meilleures pratiques en matière de gestion du changement, voir le Guide pour la gestion du changement sur AWSdans le AWS Bibliothèque de solutions. | Client<br>• 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 des accès autorisés 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 hiérarchi sé basé sur les normes du secteur pour les journaux d'audit de la plateforme.<br>• Fournissez des OpenShift RBAC fonctionnalités natives. | • Configurez OpenShift RBAC pour contrôler l'accès aux projets et, par extension, aux journaux des applicati ons d'un projet.<br>• 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<br>• Fournissez OpenShift RBAC des `dedicated-admin` fonctionnalités natives. | Client<br>• Configurez OpenShift `dedicated-admin` et RBAC contrôlez l'accès à la configuration des itinéraires selon les besoins.<br>• 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<br>• Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager. Fournissez OpenShift RBAC des `dedicated-admin` fonctionnalités natives. | Client<br>• Configurez OpenShift `dedicated-admin` et RBAC contrôlez l'accès à la configuration des itinéraires selon les besoins.<br>• Gérez l'adhésion des organisations Red Hat aux comptes Red Hat.<br>• Gérez les administrateurs de l'organisation pour que Red Hat accorde l'accès à OpenShift Cluster Manager. |
| Gestion des réseaux virtuels | Chapeau rouge<br>• Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager. | Client<br>• Gérez l'accès utilisateur facultatif à AWS composant s via OpenShift Cluster Manager. |
| Gestion du calcul virtuel | Chapeau rouge<br>• Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager. | Client<br>• Gérez l'accès utilisateur facultatif à AWS composant s via OpenShift Cluster Manager.<br>• Création IAM rôles et politiques associées nécessaires pour activer ROSA accès au service. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| Gestion du stockage virtuel | Chapeau rouge<br>• Fournissez des contrôles d'accès aux clients via OpenShift Cluster Manager. | Client<br>• Gérez l'accès utilisateur facultatif à AWS composant s via OpenShift Cluster Manager.<br>• Création IAM rôles et politiques associées nécessaires pour activer ROSA accès au service. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| AWS logiciel (public) AWS services) | AWS<br><br>Calcul<br><br>• Fournissez le Amazon EC2 service, utilisé pour ROSA plan de contrôle, infrastru cture et nœuds de travail.<br><br>Stockage<br><br>• Fournir Amazon EBS, utilisé pour permettre ROSA pour fournir un stockage sur nœud local et un stockage de volume persistant pour le cluster.<br>• Fournir Amazon S3, utilisé pour le registre d'images intégré au service.<br><br>Réseaux<br><br>• Fournir AWS Identity and Access Management (IAM), utilisé par les clients pour contrôler l'accès à ROSA ressources exécutées sur les comptes clients. | Client<br><br>• Création IAM rôles et politiques associées nécessaires pour activer ROSA accès au service.<br>• Utiliser IAM outils pour appliquer les autorisat ions appropriées à AWS ressources du compte client.<br>• Pour activer ROSA à travers votre AWS organisation, le client est responsable de la gestion AWS Organizations administrateurs.<br>• Pour activer ROSA à travers votre AWS organisation, le client est responsable de la distribution du ROSA allocation d'admissibilité en utilisant AWS License Manager. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| Matériel/AWS infrastructure mondiale | AWS<br>• Pour plus d'informations sur les contrôles d'accès physiques pour AWS centres de données, voir Nos contrôles sur le AWS Cloud Page de sécurité. | Client<br>• Le client n'est pas responsable de AWS infrastructure 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<br>• Envoyez les journaux d'audit du cluster à un Red Hat SIEM 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<br>• Analysez les journaux des applications pour détecter les événements de sécurité.<br>• Envoyez les journaux des applications à un point de terminaison externe via des conteneurs annexes ou des applications de journalisation tierces si une 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 composants du réseau virtuel pour détecter les problèmes potentiels et les menaces de sécurité.<br>• Utilisation publique AWS des outils pour une surveillance et une protection supplémentaires. | • Surveillez les composants réseau virtuels configurés en option pour détecter les problèmes potentiels et les menaces de sécurité.<br>• Configurez les règles de pare-feu ou les protections du centre de données client nécessaires selon les besoins. |
| Gestion du calcul virtuel | Chapeau rouge<br>• Surveillez les composants informatiques virtuels pour détecter les problèmes potentiels et les menaces de sécurité.<br>• Utilisation publique AWS des outils pour une surveillance et une protection supplémentaires. | Client<br>• Surveillez les composants réseau virtuels configurés en option pour détecter les problèmes potentiels et les menaces de sécurité.<br>• Configurez les règles de pare-feu ou les protections du centre de données client nécessaires selon les besoins. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| Gestion du stockage virtuel | Chapeau rouge<br>• Surveillez les composant s de stockage virtuel pour détecter les problèmes potentiels et les menaces de sécurité.<br>• Utilisation publique AWS des outils pour une surveilla nce et une protection supplémentaires.<br>• Configurez le ROSA service permettant de chiffrer par défaut les données du plan de contrôle, de l'infrast ructure et du volume des nœuds de travail à l'aide du AWS KMSclé gérée qui Amazon EBS fournit.<br>• Configurez le ROSA service permettant de chiffrer les volumes persistants des clients qui utilisent la classe de stockage par défaut avec AWS KMSclé gérée qui Amazon EBS fournit.<br>• Permettre au client d'utiliser un service géré par le client KMS key pour chiffrer les volumes persistants.<br>• Configurer le registre d'images du conteneur pour chiffrer les données du | Client<br>• Disposition Amazon EBS volumes.<br>• Gérer Amazon EBS stockage en volume pour garantir que suffisamment de stockage est disponible pour le montage en tant que volume dans ROSA.<br>• Créez la réclamation de volume persistant et générez un volume persistant via OpenShift Cluster Manager. |

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

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| AWS logiciel (public) AWS services) | AWS<br><br>Calcul<br><br>• Fournir Amazon EC2, utilisé pour ROSA plan de contrôle, infrastructure et nœuds de travail. Pour plus d'informations, consultez la section Sécurité de l'infrastructure dans Amazon EC2dans le Amazon EC2 Guide de l'utilisateur.<br><br>Stockage<br><br>• Fournir Amazon EBS, utilisé pour ROSA les volumes du plan de contrôle, de l'infrastructure et des nœuds de travail, ainsi que les volumes persistants de Kubernetes. Pour plus d'informations, consultez la section Protection des données dans Amazon EC2dans le Amazon EC2 Guide de l'utilisateur.<br>• Fournir AWS KMS, qui ROSA utilise pour chiffrer les volumes du plan de contrôle, de l'infrastructure, des nœuds de travail et des volumes persistants. | Client<br><br>• Assurez-vous que les meilleures pratiques de sécurité et le principe du moindre privilège sont respectés pour protéger les données sur le Amazon EC2 instance. Pour plus d'informations, consultez la section Sécurité de l'infrastructure dans Amazon EC2et protection des données dans Amazon EC2.<br>• Surveillez les composants réseau virtuels configurés en option pour détecter les problèmes potentiels et les menaces de sécurité.<br>• Configurez les règles de pare-feu ou les protections du centre de données client nécessaires selon les besoins.<br>• Créez une KMS clé optionnelle gérée par le client et chiffrez le Amazon EBS volume persistant à l'aide de la KMS clé.<br>• Surveillez les données des clients dans le stockage virtuel pour détecter les problèmes potentiels et les |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| | Pour plus d'informations, consultez .Amazon EBS chiffrement dans le Amazon EC2 Guide de l'utilisateur.<br>• Fournir Amazon S3, utilisé pour le registre d'images de conteneur intégré au ROSA service. Pour plus d'informations, consultez .Amazon S3 sécurité dans le Amazon S3 Guide de l'utilisateur.<br><br>Réseaux<br><br>• Fournir des fonctionnalités et des services de sécurité pour renforcer la confidentialité et contrôler l'accès au réseau sur AWS infrastructure mondiale, y compris les pare-feux réseau intégrés Amazon VPC, des connexions réseau privées ou dédiées et le chiffrement automatique de tout le trafic sur le AWS réseaux mondiaux et régionaux entre AWS installations sécurisées. Pour de plus amples informations, veuillez consulter le .AWS Modèle de responsabilité partagée et sécurité de l'infrastructure | menaces de sécurité. Pour de plus amples informations, veuillez consulter le .AWS Modèle de responsabilité partagée. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
|---|---|---|
| | dans l'introduction à AWS Livre blanc sur la sécurité. | |
| Matériel/AWS infrastructure mondiale | AWS<br>• Fournissez le AWS une infrastructure mondiale qui ROSA utilise pour fournir des fonctionnalités de service. Pour plus d'informations sur AWS contrôles de sécurité, voir Sécurité du AWS Infrastructure dans le AWS livre blanc.<br>• Fournir de la documentation au client pour gérer les besoins de conformité et vérifier son état de sécurité dans AWS en utilisant des outils tels que AWS Artifact and AWS Security Hub. | Client<br>• 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.<br>• Utiliser IAM outils pour appliquer les autorisations appropriées à 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 | Client |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| | • Restaurez ou recréez les composants réseau virtuels concernés qui sont nécessaires au fonctionnement de la plate-forme. | • Configurez des connexions réseau virtuelles avec plusieurs tunnels dans la mesure du possible pour vous protéger contre les pannes.<br>• Maintenez le basculement DNS et l'équilibrage de charge si vous utilisez un équilibreur de charge global avec plusieurs clusters. |
| Gestion du calcul virtuel | Chapeau rouge<br>• La surveillance du cluster et le remplacement ont échoué Amazon EC2 plan de contrôle ou nœuds d'infrastructure.<br>• Donnez au client la possibilité de remplacer manuellement ou automatiquement les nœuds de travail défaillants. | Client<br>• Le remplacement a échoué Amazon EC2 nœuds de travail en modifiant la configuration du pool de machines via OpenShift Cluster Manager ou le ROSA CLI. |
| Gestion du stockage virtuel | Chapeau rouge<br>• Dans ROSA clusters créés avec AWS IAM informations d'identification utilisateur, sauvegardez tous les objets Kubernetes du cluster via des instantanés de volume horaires, quotidiens et hebdomadaires. | Client<br>• Sauvegardez les applications clients et les données des applications. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
| --- | --- | --- |
| AWS logiciel (public) AWS services) | AWS<br><br>Calcul<br><br>• Fournir Amazon EC2 fonctionnalités qui favorisen t la résilience des données, telles que Amazon EBS instantanés et Amazon EC2 Auto Scaling. Pour plus d'informations, voir Résilience dans Amazon EC2dans le Amazon EC2 Guide de l'utilisateur.<br><br>Stockage<br><br>• Fournir la capacité de ROSA service et clients pour sauvegarder le Amazon EBS volume sur le cluster via Amazon EBS instantanés de volume.<br>• Pour plus d'informations sur Amazon S3 fonctionnalités qui favorisent la résilience des données, voir Résilienc e dans Amazon S3.<br><br>Réseaux<br><br>• Pour plus d'informations sur Amazon VPC fonctionn alités qui favorisent la | Client<br><br>• Configuration ROSA Des clusters multi-AZ pour améliorer la tolérance aux pannes et la disponibilité des clusters.<br>• Provisionnez des volumes persistants à l'aide du Amazon EBS CSIpilote pour activer les instantanés de volume.<br>• Créez des instantanés de CSI volumes de Amazon EBS volumes persistants. |

| Ressource | Responsabilités liées au service | Responsabilités du client |
|---|---|---|
| | résilience des données, voir Résilience dans Amazon Virtual Private Clouddans le Amazon VPC Guide de l'utilisateur. | |
| Matériel/AWS infrastructure mondiale | AWS<br>• Fournir AWS une infrastructure mondiale qui permet ROSA pour faire évoluer le plan de contrôle, l'infrastructure et les nœuds de travail entre les zones de disponibilité. Cette fonctionnalité permet ROSA pour orchestrer le basculement automatique entre les zones sans interruption.<br>• 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 Framework Well-Architected. | Client<br>• Configuration ROSA Des clusters 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 déploie Red Hat OpenShift Service on AWS. Cependant, AWS et Red Hat fournissent divers outils pour aider le client à gérer les données et les applications sur la plateforme.

| Ressource | Comment AWS et Red Hat vous aide | Responsabilités du client |
| --- | --- | --- |
| Données sur les clients | Chapeau rouge<br>• 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.<br>• Fournissez OpenShift des composants pour aider à gérer les données des applications, telles que les secrets.<br>• Facilitez l'intégration avec des services de données tels que Amazon RDS pour stocker et gérer des données en dehors du cluster et/ou AWS.<br><br>AWS<br>• Fournir Amazon RDS pour permettre aux clients de stocker et de gérer des données en dehors du cluster. | Client<br>• 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<br>• Provisionnez des clusters avec OpenShift des composants installés afin que les clients puissent | Client<br>• Assumez la responsabilité des applications clients et tierces, des données et du |

| Ressource | Comment AWS et Red Hat vous aide | Responsabilités du client |
| --- | --- | --- |
| | accéder à Kubernetes OpenShift et APIs pour déployer et gérer des applications conteneurisées.<br>• 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.<br>• Fournir un accès OpenShift APIs qu'un client peut utiliser pour configurer les opérateurs afin d'ajouter une communauté, un tiers, AWS, et les services Red Hat destinés au cluster.<br>• Fournissez des classes de stockage et des plug-ins pour prendre en charge les volumes persistants à utiliser avec les applications des clients.<br>• 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. | cycle de vie complet des applications.<br>• 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.<br>• 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 applications, configurer les autorisations, 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 vous aide | Responsabilités du client |
| --- | --- | --- |
| | AWS<br>• Fournir Amazon EBS pour prendre en charge les volumes persistants à utiliser avec les applications des clients.<br>• Fournir Amazon S3 pour prendre en charge le provisionnement par Red Hat du registre d'images de conteneurs. | hautement disponibles et résilientes.<br>• Assumer la responsab ilité de la surveillance des applications exécutées sur Red Hat OpenShift Service on AWS, y compris l'install ation et l'exploitation de logiciels permettant de recueillir des métriques , de créer des alertes et de protéger les secrets de l'application. |

# Modèles d'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 dans 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.

ROSAavec 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. La version ROSA avec HCP et la ROSA version classique peuvent être activées 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 du ROSA CLI.

> **Note**
>
> ROSAavec des plans de contrôle hébergés (HCP) n'offre pas les certifications de conformité Fed RAMP High et HIPAA Qualified. Pour plus d'informations, consultez la section Conformité dans la documentation Red Hat.

> **Note**
>
> ROSAavec des plans de contrôle hébergés (HCP) ne propose pas de points de terminaison Federal Information Processing Standard (FIPS).

## Comparaison ROSA avec HCP et ROSA classique

Le tableau suivant ROSA compare HCP les modèles d'architecture ROSA classiques.

| | ROSAavec HCP | ROSAclassique |
|---|---|---|
| Hébergement d'infrastructures de clusters | Les composants du plan de contrôle, tels que etcd, API server et oauth, sont hébergés dans un environnement appartenant à Red Hat. Compte AWS | Les composants du plan de contrôle, tels que etcd, API server et oauth, sont hébergés dans un établissement 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 chez le clientVPC. |
| AWS Identity and Access Management | 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 |

| | ROSAavec HCP | ROSAclassique |
|---|---|---|
| | | zone d'exploitation ou sur plusieurs zonesAZs. |
| Nœuds d'infrastructure | N'utilise pas de nœuds d'infrastructure dédiés. Les composants de la plate-forme sont déployés sur les nœuds de travail. | Utilise deux nœuds dédiés mono-AZ ou trois nœuds dédiés multi-AZ pour héberger les composants de la plate-for me. |
| 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 “Créez un ROSA HCPcluster - CLI”- Créez votre premier ROSA avec un HCP cluster en utilisant AWS STS et le ROSA CLI.
- the section called “Créez un cluster ROSA classique - AWS PrivateLink ”- Créez votre premier cluster ROSA classique en utilisant AWS PrivateLink.
- the section called “Créez un cluster ROSA classique - CLI”- Créez votre premier cluster ROSA classique en utilisant AWS STS et le ROSA CLI.

# Configurer pour utiliser ROSA

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

## Prérequis

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 la dernière version ROSA CLI de OpenShift Container PlatformCLI. 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 plus d'informations, consultez the section called "Obtention de support". Pour l'activer AWS Support, consultez la AWS Support page.
- Si vous utilisez AWS Organizations pour gérer le service Comptes AWS qui héberge le ROSA service, la politique de contrôle des services de l'organisation (SCP) doit être configurée pour permettre à Red Hat d'exécuter les actions politiques répertoriées dans le SCP sans restriction. Pour plus d'informations, consultez le the section called "AWS Organizations politique de contrôle des services refuse d'être requise AWS Marketplace des autorisations". Pour plus d'informationsSCPs, 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, voir link: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, des quotas de service nécessaires et du rôle Elastic Load Balancing (ELB) lié au service nommé. `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 ELB lié au service est créé, ouvrez une nouvelle session de terminal pour créer votre première ROSA cluster session en utilisant le. ROSA CLI

# Créez un HCP cluster ROSA avec à l'aide du ROSA CLI

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

Le ROSA CLIutilise `auto` le mode ou `manual` le mode pour créer le IAM ressources et configuration OpenID Connect (OIDC) requises pour créer un ROSA cluster. `auto`le mode crée automatiquement le requis IAM rôles, politiques et OIDC fournisseur. `manual`le mode affiche le AWS CLI commandes nécessaires pour créer le IAM ressources manuellement. En utilisant `manual` le mode, vous pouvez consulter les AWS CLI commandes 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 ROSA CLIpour créer le nécessaire IAM ressources et OIDC configuration pour ROSA withHCP. Pour plus d'options de démarrage, consultezCommencez avec ROSA .

Rubriques


- Prérequis
- Création Amazon VPC application
- Créez le requis IAM rôles et configuration d'OpenID Connect
- Créez un HCP cluster ROSA avec à l'aide du ROSA CLIet AWS STS
- Configuration d'un fournisseur d'identité et autorisation cluster accès
- Accorder à l'utilisateur l'accès à un cluster
- Configuration cluster-admin des autorisations
- Configuration dedicated-admin des autorisations
- Accédez à un cluster via la console Red Hat Hybrid Cloud
- Déployer une application depuis le catalogue des développeurs
- Révoquer cluster-admin les autorisations d'un utilisateur
- Révoquer dedicated-admin les autorisations d'un utilisateur
- Révoquer l'accès d'un utilisateur à un cluster
- Supprimer un cluster et AWS STS resources

## Prérequis

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

## Création Amazon VPC application

La procédure suivante crée Amazon VPC architecture pouvant être utilisée pour héberger un cluster. Tous cluster les ressources sont hébergées dans le sous-réseau privé. Le sous-réseau public achemine le trafic sortant depuis le sous-réseau privé via une NAT passerelle vers l'Internet public. Cet exemple utilise le CIDR bloc `10.0.0.0/16` pour Amazon VPC. Vous pouvez toutefois choisir un autre CIDR bloc. Pour plus d'informations, consultez la section VPCDimensionnement.

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

Example

Terraform

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

   ```
   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, le 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 du VPC référentiel Terraform. README

6. Appliquez le fichier de plan pour créer leVPC.

```
terraform apply rosa.tfplan
```

Une fois terminé, ils ont CLI renvoyé un message de réussite qui vérifie les ressources ajoutées.

a. (Facultatif) Créez des variables d'environnement pour le sous-réseau IDs privé, public et machinepool approvisionné par Terraform à utiliser lors de la création de votre cluster with. ROSA 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 le fichier Amazon VPC console.
2. Sur le VPC tableau de bord, choisissez Create VPC.
3. Pour que Resources crée, choisissez VPCet plus encore.
4. Conservez l'option Génération automatique de balises de nom sélectionnée pour créer des balises de nom pour les VPC ressources, ou désactivez-la pour fournir vos propres balises de nom pour les VPC ressources.
5. Pour le IPv4CIDRbloc, entrez une plage d'IPv4adresses pour leVPC. A VPC doit avoir une plage d'IPv4adresses.

6. (Facultatif) Pour prendre en charge IPv6 le trafic, choisissez IPv6CIDRBloquer, bloc fourni par Amazon IPv6 CIDR.
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 nécessite trois zones de disponibilité. Pour choisir le AZs pour vos sous-réseaux, développez Personnaliser AZs.

> **Note**
>
> Momentanée ROSA les types d'instance ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser le plugin ROSA CLI`rosa list instance-types`commande pour tout lister ROSA types d'instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez 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 les blocs Personnaliser les sous-réseaux CIDR.

> **Note**
>
> ROSAavec 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 viaIPv4, pour les passerelles, choisissez le nombre de NATpasserelles AZs dans lesquelles vous souhaitez créer NAT des passerelles. En production, nous vous recommandons de déployer une NAT passerelle dans chaque AZ avec des ressources nécessitant un accès à l'Internet public.
11. (Facultatif) Si vous devez accéder Amazon S3 directement depuis votre passerelle S3VPC, choisissez les VPC points de terminaison.
12. Laissez les DNS options par défaut sélectionnées. ROSA nécessite la prise en charge DNS du nom d'hôte 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. Choisissez Créer VPC.

AWS CLI

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

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

   La commande précédente renvoie l'VPCID. Voici un exemple de sortie.

```
vpc-1234567890abcdef0
```

2. Stockez l'VPCID dans une variable d'environnement.

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

3. Créez une `Name` balise pour leVPC, 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 DNS noms d'hôte sur le. VPC

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

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

> **Important**
>
> ROSAavec 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**
>
> Momentanée ROSA les types d'instance ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser le plugin ROSA CLI`rosa list instance-types`commande pour tout lister ROSA types d'instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez 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 VPC sous-réseaux. 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 auVPC.

```
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 NAT passerelle 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 NAT passerelle.

```
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 le requis IAM rôles et configuration d'OpenID Connect

Avant de créer un HCP cluster ROSA with, vous devez créer le nécessaire IAM les rôles et les politiques et la configuration d'OpenID Connect (OIDC). Pour plus d'informations sur IAM rôles et politiques pour ROSA withHCP, voirthe section called “ AWS stratégies gérées”.

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

1. Créez le requis IAM rôles et politiques du compte. 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, le ROSA CLIaffiche 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 ROSA CLI jetons d'accès hors ligne expirés”.

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

   ```
   rosa list oidc-config
   ```

5. Créez le requis IAM rôles d'opérateur, en les `<OIDC_CONFIG_ID>` remplaçant par l'ID de OIDC configuration 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 IAM les rôles d'opérateur ont été créés, exécutez la commande suivante :

```
rosa list operator-roles
```

## Créez un HCP cluster ROSA avec à l'aide du ROSA CLIet AWS STS

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

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

La procédure suivante utilise la `rosa create cluster --hosted-cp` commande pour créer un mono-AZ ROSA 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 HCP cluster ROSA with à l'aide de l'une des commandes suivantes.
   - Créez un HCP cluster ROSA avec un cluster public API et une entrée, en spécifiant le nom du cluster, le préfixe du rôle d'opérateur, l'ID de OIDC configuration 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 HCP cluster ROSA with avec un private API et une entrée, en spécifiant le nom du cluster, le préfixe du rôle d'opérateur, l'ID de OIDC configuration 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 AWS Support ou le support Red Hat pour obtenir de l'aide, consultezthe section called “Obtention de support”.

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

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

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

ROSA inclut un OAuth serveur intégré. Après votre cluster est 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, GoogleLDAP, 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. HTPasswdn'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, voir 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 le provisionnement des identités pour votre cluster, créez-en un. Pour plus d'informations, consultez les étapes décrites dans la GitHub documentation.
3. Utilisation de ROSA CLIen mode interactif, configurez un fournisseur d'identité pour votre cluster.

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

4. Suivez les instructions de configuration dans la sortie pour restreindre cluster 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 le URL dans la sortie, en le `<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 en les 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. Inviter les utilisateurs qui ont besoin cluster accès à votre GitHub organisation. Pour plus d'informations, consultez la section Inviter des utilisateurs à rejoindre votre organisation dans la GitHub documentation.

## Configuration **`cluster-admin`** des autorisations

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>
```

## Configuration **`dedicated-admin`** des autorisations

1. Accordez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre utilisateur et 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 cluster via la console Red Hat Hybrid Cloud.

1. Procurez-vous la console URL pour votre 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 la console URL 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 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 choisissez Create Application pour ouvrir la page Create Source-to-Image 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. Sélectionnez Create (Créer).

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

13. Lorsque le déploiement est terminé, choisissez l'itinéraire URL de 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 utilisateur et 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 utilisateur et 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 accès pour 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 accès pour 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 AWS STS resources

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

> **Note**
>
> IAM rôles et politiques créés par ROSA pourrait être utilisé par d'autres ROSA clusters dans le même compte.

1. Supprimez les photos ou les vidéos cluster et regardez 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 le cluster à supprimer complètement avant de supprimer le IAM rôles, politiques et OIDC fournisseur. Les IAM rôles de compte sont nécessaires pour supprimer les ressources créées par le programme d'installation. Les IAM rôles d'opérateur sont nécessaires pour nettoyer les ressources créées par les OpenShift opérateurs. Les opérateurs utilisent le OIDC fournisseur pour s'authentifier.

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

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

3. Supprimer l'opérateur spécifique au cluster IAM rôles.

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

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

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

5. Supprimez les photos ou les vidéos IAM politiques créées par ROSA.
   a. Connectez-vous au IAM console.
   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 IAM politiques du cluster.

# Créez un cluster ROSA classique à l'aide du ROSA CLI

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

Le ROSA CLIutilise `auto` le mode ou `manual` le mode pour créer le IAM ressources nécessaires pour fournir un ROSA cluster. `auto`le mode crée immédiatement le requis IAM rôles et politiques et un fournisseur OpenID Connect (OIDC). `manual`le mode affiche le AWS CLI commandes nécessaires pour créer le IAM ressources. En utilisant `manual` le mode, vous pouvez consulter les AWS CLI commandes 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


- Prérequis
- Créez un cluster ROSA classique à l'aide du ROSA CLIet AWS STS
- Configuration d'un fournisseur d'identité et autorisation cluster accès
- Accorder à l'utilisateur l'accès à un cluster
- Configuration cluster-admin des autorisations
- Configuration dedicated-admin des autorisations
- Accédez à un cluster via la console Red Hat Hybrid Cloud
- Déployer une application depuis le catalogue des développeurs
- Révoquer cluster-admin les autorisations d'un utilisateur
- Révoquer dedicated-admin les autorisations d'un utilisateur
- Révoquer l'accès d'un utilisateur à un cluster
- Supprimer un cluster et AWS STS resources


## Prérequis

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

## Créez un cluster ROSA classique à l'aide du ROSA CLIet AWS STS

Vous pouvez créer un ROSA classique cluster en utilisant le ROSA CLIet AWS STS.

1. Créez le requis IAM rôles et politiques de compte utilisant `--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, le ROSA CLIaffiche 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 ROSA CLI jetons d'accès hors ligne expirés”.

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 spécifiez`--mode auto`, la `rosa create cluster` commande crée l'opérateur spécifique au cluster IAM les rôles et le OIDC fournisseur automatiquement. Les opérateurs utilisent le OIDC fournisseur 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 EBS chiffrement Amazon par défaut qui chiffre les volumes etcd.

> **Note**
>
> Après avoir exécuté le `manual` mode pour créer le cluster, vous devez créer manuellement les IAM rôles d'opérateur 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 AWS Support ou le support Red Hat pour obtenir de l'aide, consultezthe section called “Obtention de support”.

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

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

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

ROSA inclut un OAuth serveur intégré. Après votre cluster est 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, GoogleLDAP, 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. HTPasswdn'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, voir 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 le provisionnement des identités pour votre cluster, créez-en un. Pour plus d'informations, consultez les étapes décrites dans la GitHub documentation.
3. Utilisation de ROSA CLIen mode interactif, configurez un fournisseur d'identité pour votre cluster.

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

4. Suivez les instructions de configuration dans la sortie pour restreindre cluster 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 le URL dans la sortie, en le `<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 en les 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. Inviter les utilisateurs qui ont besoin cluster accès à votre GitHub organisation. Pour plus d'informations, consultez la section Inviter des utilisateurs à rejoindre votre organisation dans la GitHub documentation.

## Configuration **`cluster-admin`** des autorisations

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>
```

## Configuration **`dedicated-admin`** des autorisations

1. Accordez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre utilisateur et 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 cluster utilisateur administrateur ou vous avez ajouté un utilisateur à votre fournisseur d'identité configuré, vous pouvez vous connecter à votre cluster via la console Red Hat Hybrid Cloud.

1. Procurez-vous la console URL pour votre 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 la console URL 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 votre 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 choisissez Create Application pour ouvrir la page Create Source-to-Image 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. Sélectionnez Create (Créer).

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

13. Lorsque le déploiement est terminé, choisissez l'itinéraire URL de 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 utilisateur et 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 utilisateur et 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 accès pour 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 accès pour 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 AWS STS resources

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

> **Important**
>
> IAM rôles et politiques créés par ROSA pourrait être utilisé par d'autres ROSA clusters dans le même compte.

1. Supprimez les photos ou les vidéos cluster et regardez 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 le cluster à supprimer complètement avant de supprimer le IAM rôles, politiques et OIDC fournisseur. Les IAM rôles de compte sont nécessaires pour supprimer

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

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

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

3. Supprimer l'opérateur spécifique au cluster IAM rôles.

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

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

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

5. Supprimez les photos ou les vidéos IAM politiques créées par ROSA.
   a. Connectez-vous au IAM console.
   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 IAM politiques du cluster.

# Créez un cluster ROSA classique qui utilise AWS PrivateLink

ROSAles clusters classiques peuvent être déployés de différentes manières : public, privé ou privé avec AWS PrivateLink. Pour plus d'informations sur la ROSA version classique, consultezthe section called “Modèles d'architecture”. Pour le public comme pour le privé cluster configurations, les OpenShift cluster a accès à Internet, et la confidentialité est définie sur les charges de travail des applications au niveau de la couche application.

Si vous avez besoin des deux cluster et les charges de travail des applications doivent être privées, vous pouvez configurer AWS PrivateLink avec du ROSA classique. AWS PrivateLink est une technologie hautement disponible et évolutive qui ROSA utilise pour créer une connexion privée entre

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

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

Rubriques


- Prérequis
- Création Amazon VPC application
- Créez un cluster ROSA classique à l'aide du ROSA CLIet AWS PrivateLink
- Configuration AWS PrivateLink DNStransfert
- Configuration d'un fournisseur d'identité et autorisation cluster accès
- Accorder à l'utilisateur l'accès à un cluster
- Configuration cluster-admin des autorisations
- Configuration dedicated-admin des autorisations
- Accédez à un cluster via la console Red Hat Hybrid Cloud
- Déployer une application à partir du catalogue pour développeurs
- Révoquer cluster-admin les autorisations d'un utilisateur
- Révoquer dedicated-admin les autorisations d'un utilisateur
- Révoquer l'accès d'un utilisateur à un cluster
- Supprimer un cluster et AWS STS resources


## Prérequis

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

## Création Amazon VPC application

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

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

Example

Amazon VPC console

1. Ouvrez le fichier Amazon VPC console.
2. Sur le VPC tableau de bord, choisissez Create VPC.
3. Pour que Resources crée, choisissez VPCet plus encore.
4. Conservez l'option Génération automatique de balises de nom sélectionnée pour créer des balises de nom pour les VPC ressources, ou désactivez-la pour fournir vos propres balises de nom pour les VPC ressources.
5. Pour le IPv4CIDRbloc, entrez une plage d'IPv4adresses pourVPC. A VPC doit avoir une plage d'IPv4adresses.
6. (Facultatif) Pour prendre en charge IPv6 le trafic, choisissez IPv6CIDRBloquer, bloc fourni par Amazon IPv6 CIDR.
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 nécessite trois zones de disponibilité. Pour choisir le AZs pour vos sous-réseaux, développez Personnaliser AZs.

> **Note**
>
> Momentanée ROSA les types d'instance ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser le plugin ROSA CLI`rosa list instance-types`commande pour tout lister ROSA types d'instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez 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 les blocs Personnaliser les sous-réseaux CIDR.

> **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 publicIPv4, pour les passerelles, choisissez le nombre de NATpasserelles AZs dans lesquelles vous souhaitez créer NAT des passerelles. En production, nous vous recommandons de déployer une NAT passerelle dans chaque AZ avec des ressources nécessitant un accès à l'Internet public.
11. (Facultatif) Si vous devez accéder Amazon S3 directement depuis votre passerelle S3VPC, choisissez les VPC points de terminaison.
12. Laissez les DNS options par défaut sélectionnées. ROSA nécessite la prise en charge DNS du nom d'hôte sur le. VPC
13. Choisissez Create VPC.

AWS CLI

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

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

La commande précédente renvoie l'VPCID. Voici un exemple de sortie.

```
vpc-1234567890abcdef0
```

2. Stockez l'VPCID dans une variable d'environnement.

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

3. Créez une `Name` balise pour leVPC, 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 DNS noms d'hôte sur le. VPC

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

5. Créez un sous-réseau public et privé dans leVPC, 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 conditions ne sont pas remplies, la création du cluster échoue.

> **Note**
>
> Momentanée ROSA les types d'instance ne sont disponibles que dans certaines zones de disponibilité. Vous pouvez utiliser le plugin ROSA CLI`rosa list instance-types`commande pour tout lister ROSA types d'instances disponibles. Pour vérifier si un type d'instance est disponible pour une zone de disponibilité donnée, utilisez 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. Reliez la passerelle Internet auVPC.

```
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 NAT passerelle 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 NAT passerelle.

```
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 classique à l'aide du ROSA CLIet AWS PrivateLink

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

La procédure suivante utilise la `rosa create cluster` commande pour créer un ROSA classique cluster. Pour créer un Multi-AZ cluster, spécifiez `--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 telle sorte que ROSA peut accéder aux sites dont il a besoin pour fonctionner.
> Pour plus d'informations, consultez .AWS les prérequis en matière de pare-feu sont décrits dans la OpenShift documentation Red Hat.

1. Créez le requis IAM rôles et politiques de compte utilisant `--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, ROSA CLIaffiche 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 ROSA CLI jetons d'accès hors ligne expirés".
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 AWS PrivateLink avec AWS Security Token Service (AWS STS) informations d'identification de courte durée, à ajouter `--sts --mode auto` ou `--sts --mode manual` à la fin de la `rosa create cluster` commande.

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

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

4. Créez le fournisseur OpenID Connect (OIDC) cluster les 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**
>
> Cela peut prendre jusqu'à 40 minutes pour cluster `Statechamp` pour afficher le `ready` statut. Si le provisionnement échoue ou ne s'affiche pas au `ready` bout de 40 minutes, consultezRésolution des problèmes. Pour contacter AWS Support ou le support Red Hat pour obtenir de l'aide, consultezthe section called “Obtention de support”.

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

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

## Configuration AWS PrivateLink DNStransfert

Clusters qui utilisent AWS PrivateLink créer une zone hébergée publique et une zone hébergée privée dans Route 53. Enregistrements au sein du Route 53 les zones hébergées privées ne peuvent être résolues qu'à partir de VPC celle à laquelle elles sont assignées.

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

## Configurez un Route 53 Resolver point de terminaison entrant

1. Pour autoriser des enregistrements tels que `api.<cluster_domain>` et `*.apps.<cluster_domain>` pour les résoudre en dehors deVPC, configurez un Route 53 Resolver point de terminaison 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 les sous-réseaux VPC et les sous-réseaux privés utilisés lors de la création du cluster.

## Configurer DNS le transfert pour le cluster

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

1. Configurez votre réseau d'entreprise pour transférer les DNS requêtes vers les adresses IP du domaine de premier niveau, telles que`drow-pl-01.htno.p1.openshiftapps.com`.
2. Si vous transférez DNS des requêtes de l'un VPC à l'autreVPC, suivez les instructions de la section Gestion des règles de transfert.

3. Si vous configurez votre DNS serveur réseau distant, consultez la documentation de votre DNS serveur spécifique pour configurer le DNS transfert sélectif pour le domaine de cluster installé.

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

ROSA inclut un OAuth serveur intégré. Après votre ROSA cluster est 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 GitLab, GoogleLDAP, 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. HTPasswdn'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, voir 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 le provisionnement des identités pour votre ROSA cluster, créez-en un. Pour plus d'informations, consultez les étapes décrites dans la GitHub documentation.
3. Utilisation de ROSA CLIen mode interactif, 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 dans la sortie pour restreindre cluster 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 le URL dans la sortie, en le `<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 en les 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. Inviter les utilisateurs qui ont besoin cluster accès à votre GitHub organisation. Pour plus d'informations, consultez la section Inviter des utilisateurs à rejoindre votre organisation dans la GitHub documentation.

## Configuration **`cluster-admin`** des autorisations

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>
```

## Configuration **`dedicated-admin`** des autorisations

1. Accordez les `dedicated-admin` autorisations à l'aide de la commande suivante. Remplacez `<IDP_USER_NAME>` et `<CLUSTER_NAME>` par votre utilisateur et 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 cluster utilisateur administrateur ou vous avez ajouté un utilisateur à votre fournisseur d'identité configuré, vous pouvez vous connecter à votre cluster via la console Red Hat Hybrid Cloud.

1. Procurez-vous la console URL pour votre 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 la console URL 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 votre cluster, choisissez le nom du fournisseur d'identité dans la boîte de dialogue Se connecter avec... et répondez aux demandes d'autorisation présentées par votre fournisseur.

## Déployer une application à partir du catalogue pour 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 choisissez Create Application pour ouvrir la page Create Source-to-Image 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. Sélectionnez Create (Créer).

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

13. Lorsque le déploiement est terminé, choisissez l'itinéraire URL de 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 utilisateur et 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 utilisateur et 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 accès pour 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 accès pour 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 AWS STS resources

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

> **Important**
> IAM rôles et politiques créés par ROSA pourrait être utilisé par d'autres ROSA clusters dans le même compte.

1. Supprimez les photos ou les vidéos cluster et regardez 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 le cluster à supprimer complètement avant de supprimer le IAM rôles, politiques et OIDC fournisseur. Les IAM rôles de compte sont nécessaires pour supprimer les ressources créées par le programme d'installation. Les IAM rôles d'opérateur sont nécessaires pour nettoyer les ressources créées par les OpenShift opérateurs. Les opérateurs utilisent le OIDC fournisseur pour s'authentifier.

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

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

3. Supprimer l'opérateur spécifique au cluster IAM rôles.

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

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

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

5. Supprimez les photos ou les vidéos IAM politiques créées par ROSA.
   a. Connectez-vous au IAM console.
   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 IAM politiques du cluster.

# Sécurité dans ROSA

Sécurité du cloud chez AWS est la plus haute priorité. 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 AWS et toi. Le modèle de responsabilité partagée décrit ceci en tant que sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud — AWS est chargé de protéger l'infrastructure qui fonctionne 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 du AWS Programmes de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à ROSA, voir Services AWS dans le champ d'application du programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le Service AWS que tu utilises. 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 l'utilisation ROSA. Il vous montre comment configurer ROSA pour atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres Services AWS qui vous aident à surveiller et à sécuriser votre ROSA ressources.

Table des matières


- Protection des données dans ROSA
- Gestion des identités et des accès pour ROSA
- Résilience dans ROSA
- Sécurité de l'infrastructure dans ROSA


## Protection des données dans ROSA

La the section called “Responsabilités” documentation et AWS modèle de responsabilité partagée : définissez 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 les tâches de configuration et de gestion de la sécurité pour le Services AWS que tu utilises. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le AWS Modèle de responsabilité partagée et article de GDPR blog sur AWS Blog sur la sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger Compte AWS informations d'identification et configuration des utilisateurs individuels avec AWS Identity and Access Management (IAM). De cette façon, chaque utilisateur ne reçoit que les autorisations nécessaires pour accomplir ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et enregistrement de l'activité des utilisateurs avec AWS CloudTrail.
- Utiliser AWS solutions de chiffrement, ainsi que tous les contrôles de sécurité par défaut intégrés Services AWS.
- Utilisez des services de sécurité gérés avancés tels que Amazon Macie, qui aide à découvrir et à sécuriser les données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 2 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un FIPS point de terminaison. Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-2.

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 Nom. Cela inclut lorsque vous travaillez avec ROSA ou autre Services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez ROSA ou d'autres services peuvent être sélectionnés pour être inclus dans les journaux de diagnostic. Lorsque vous fournissez un URL à un serveur externe, n'incluez pas d'informations d'identification dans le URL pour valider votre demande auprès de ce serveur.

Rubriques

- Protection des données à l'aide du chiffrement

# Protection des données à l'aide du chiffrement

La protection des données fait référence à la protection des données pendant leur transit (lors de leur trajet à destination et en provenance) ROSA) et au repos (pendant qu'il est stocké sur des disques dans AWS centres de données).

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

> **Important**
>
> Parce que ROSA est un service géré, AWS et Red Hat gèrent l'infrastructure qui ROSA utilise. Les clients ne doivent pas essayer de désactiver manuellement le Amazon EC2 des instances qui ROSA utilisations depuis le AWS console ouCLI. Cette action peut entraîner une perte de données client.

## Chiffrement des données pour 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) volumes de stockage attachés à Amazon EC2 instances.

Dans ROSA volumes et nœuds persistants soutenus par Amazon EBS, les opérations de chiffrement ont lieu sur les serveurs EC2 hébergeant les instances, garantissant ainsi la sécurité des données au repos et des données en transit entre une instance et le stockage qui lui est rattaché. Pour plus d'informations, consultez .Amazon EBS chiffrement dans le Amazon EC2 Guide de l'utilisateur.

Chiffrement des données pour Amazon EBS CSIchauffeur et Amazon EFS CSIchauffeur

ROSA utilise par défaut le Amazon EBS CSIdu chauffeur à l'approvisionnement Amazon EBS rangement. Le Amazon EBS CSIchauffeur et Amazon EBS CSILes opérateurs de pilotes sont

installés sur le cluster par défaut dans l'espace de `openshift-cluster-csi-drivers` noms. Le Amazon EBS CSIle pilote et l'opérateur 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 Amazon EFS CSIchauffeur et Amazon EFS CSIChauffeur-opérateur. Le Amazon EFS le pilote et l'opérateur vous permettent également de partager les données du système de fichiers entre les pods ou avec d'autres applications au sein ou en dehors de Kubernetes.

Les données de volume sont sécurisées en transit pour les deux Amazon EBS CSIchauffeur et Amazon EFS CSIchauffeur. Pour plus d'informations, consultez Using Container Storage Interface (CSI) dans la documentation Red Hat.

> **Important**
>
> Lors du provisionnement dynamique ROSA volumes persistants à l'aide du Amazon EFS CSIchauffeur, Amazon EFS prend en compte l'ID utilisateur, l'ID de groupe (GID) et le groupe secondaire du point IDs 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 NFS clientIDs. En conséquence, Amazon EFS ignore `fsGroup` silencieusement les paramètres. ROSA n'est pas en mesure GIDs de remplacer les fichiers en utilisant`fsGroup`. Tout module pouvant accéder à un Amazon EFS un point d'accès peut accéder à n'importe quel fichier du volume. Pour plus d'informations, voir Travailler avec Amazon EFS points d'accès dans le Amazon EFS Guide de 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 sur le chiffrement etcd dans le ROSA définition du service.

Gestion des clés

ROSA les usages KMS keys pour 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 valeur par défaut AWS gérés KMS key fourni par Amazon EBS, ou en spécifiant 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 Amazon S3 rangement par seau. 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 en plus 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 inactives de votre registre, ROSA utilise le chiffrement côté serveur par défaut avec Amazon S3 clés gérées (SSE-S3). Cela ne nécessite aucune action de votre part et est proposé sans frais supplémentaires. Pour plus d'informations, voir Protection des données à l'aide du chiffrement côté serveur avec Amazon S3 clés de chiffrement gérées (SSE-S3) dans le Amazon S3 Guide de l'utilisateur.

ROSA utilise le protocole Transport Layer Security (TLS) 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 les usages Amazon Virtual Private Cloud (Amazon VPC) pour créer des limites entre les ressources de votre ROSA regroupez et contrôlez le trafic entre eux, votre réseau local et Internet. Pour plus d'informations sur Amazon VPC sécurité, voir Confidentialité du trafic interréseau dans Amazon VPC dans le . Amazon VPC Guide de l'utilisateur.

Dans leVPC, vous pouvez configurer votre ROSA des clusters pour utiliser un serveur HTTPS proxy HTTP ou un serveur proxy pour refuser l'accès direct à Internet. Si vous êtes administrateur de cluster, vous pouvez également définir des politiques réseau au niveau du module qui limitent le trafic interréseau aux pods de votre ROSA grappe. Pour de plus amples informations, veuillez consulter the section called “Sécurité de l’infrastructure”.

### Chiffrement des données avec KMS

ROSA les usages AWS KMS pour gérer en toute sécurité les clés des données chiffrées. Les volumes du plan de contrôle, de l'infrastructure et des nœuds de travail sont chiffrés par défaut à l'aide du AWS gérés KMS key fourni par Amazon EBS. Ce KMS key possède 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.

Nouvellement créé ROSA les clusters 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 ROSA classes de stockage prédéfinies, voir 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 en utilisant la valeur par défaut Amazon EBS-clé fournie, ou spécifiez votre propre système symétrique géré par le client KMS key. Pour plus d'informations sur la création de clés, consultez la section Création de KMS clés de chiffrement symétriques dans le AWS KMS Guide du 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 Chiffrement des volumes persistants de conteneurs sur AWS avec un KMS keydans la documentation Red Hat.

Les points suivants doivent être pris en compte lorsque vous cryptez des volumes persistants à l'aide de vos propres KMS keys:

- Lorsque vous utilisez KMS le chiffrement avec le vôtre KMS key, la clé doit exister dans le même Région AWS en tant que cluster.
- Il y a un coût associé à la création et à l'utilisation de vos propres KMS keys Pour de plus amples informations, veuillez consulter .AWS Key Management Service tarification.

## Gestion des identités et des accès pour ROSA

AWS Identity and Access Management (IAM) est un Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès à AWS ressources. IAM les administrateurs contrôlent qui peut être

authentifié (connecté) et autorisé (autorisé) à utiliser ROSA ressources. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques


- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- ROSA exemples de politiques basées sur l'identité
- AWS politiques gérées pour ROSA
- Résolution des problèmes ROSA identité et accès


## Public ciblé

Comment utilisez-vous AWS Identity and Access Management (IAM) diffère en fonction du travail que vous effectuez dans ROSA.

Utilisateur du service - Si vous utilisez le ROSA service pour faire votre travail, puis votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous en utilisez ROSA fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans ROSA, voir the section called “Résolution des problèmes”.

Administrateur du service - Si vous êtes responsable de ROSA ressources de votre entreprise, vous avez probablement un accès complet à ROSA. C'est à vous de déterminer lequel ROSA fonctionnalités et ressources auxquelles les utilisateurs de vos services devraient avoir accès. Vous devez ensuite soumettre 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 voir un exemple ROSA politiques basées sur l'identité que vous pouvez utiliser dans IAM, voir 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 en utilisant vos informations d'identification. Vous devez être authentifié (connecté) à AWS) en tant que Compte AWS utilisateur root, un Utilisateur IAM, ou en supposant un IAM rôle.

Vous pouvez vous connecter à AWS en 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 AWS en utilisant la fédération, vous assumez indirectement un rôle.

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

Si vous accédez AWS programmatiquement, 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 AWS outils, vous devez signer les demandes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, voir Signature AWS APIdemandes dans le IAM Guide de 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, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez la section Authentification multifactorielle dans le AWS IAMIdentity Center (successeur de AWS Guide de l'utilisateur (authentification unique) et utilisation de l'authentification multifactorielle () MFA dans AWS dans le guide de l'utilisateur IAM.

### Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une identité de connexion unique offrant un accès complet à tous Services AWS et les ressources du compte. Cette identité s'appelle le Compte AWS utilisateur 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 root pour vos tâches quotidiennes. Protégez vos informations d’identification d’utilisateur

root 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 d'utilisateur root dans le IAM Guide de l'utilisateur.

## Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris les utilisateurs nécessitant un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, le AWS Directory Service, le répertoire Identity Center ou tout utilisateur accédant Services AWS en utilisant les informations d'identification fournies par le biais d'une source d'identité. Lorsque les identités fédérées accèdent Comptes AWS, ils assument des rôles, et les rôles fournissent des informations d'identification temporaires.

Pour une gestion centralisée des accès, 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 tous vos Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le AWS IAMIdentity Center (successeur de AWS Guide de l'utilisateur (Authentification unique).

## Utilisateurs IAM et groupes

Un Utilisateur IAMest une identité au sein de votre Compte AWS qui dispose d'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 Utilisateurs IAM qui possèdent 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 avec Utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAM un 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 pourriez avoir un groupe nommé IAMAdminset lui donner les autorisations d'administration IAM 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, voir Quand créer un Utilisateur IAM (au lieu d'un rôle) dans le guide de IAM l'utilisateur.

## IAM roles

Un IAM le rôle est une identité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Il est similaire à un Utilisateur IAM, mais n'est pas associé à une personne en particulier. Vous pouvez temporairement assumer un IAM rôle dans le AWS Management Console en changeant de rôle. Vous pouvez assumer un rôle en appelant un AWS CLI or AWS APIopération ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, voir Utilisation IAM rôles dans le guide de IAM l'utilisateur.

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 plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans IAM. Pour plus d'informations sur les ensembles d'autorisations, voir Ensembles d'autorisations dans le AWS IAMIdentity Center (successeur de AWS Guide de l'utilisateur (Authentification unique).
- Temporaire Utilisateur IAM autorisations - Un Utilisateur IAM peut supposer un IAM rôle permettant d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes - Vous pouvez utiliser un IAM rôle permettant à une personne (un mandant fiable) d'un autre compte d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Cependant, avec certains Services AWS, 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 Comment IAM les rôles diffèrent des politiques basées sur les ressources décrites dans le Guide de l'IAMutilisateur.

- Accès multiservices - Certains Services AWS utiliser 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 dans Amazon EC2 ou stockez des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations du principal appelant, en utilisant un rôle de service ou en utilisant un rôle lié à un service.
  - Transférer les sessions d'accès (FAS) - Lorsque vous utilisez un Utilisateur IAM ou rôle pour effectuer des actions dans AWS, vous êtes considéré comme un directeur. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant un Service AWS, combiné à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, voir Transférer les sessions d'accès.
  - Rôle de service - Un rôle de service est IAM rôle qu'un service assume pour effectuer des actions en votre nom. Un IAM l'administrateur peut créer, modifier et supprimer un rôle de service depuis l'intérieur IAM. Pour plus d'informations, voir Création d'un rôle pour déléguer des 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 lié à un service Service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre IAM et sont détenus par le service. Un IAM l'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 un Amazon EC2 instance et fabrication AWS CLI or AWS APIdemandes. Cela est préférable au stockage des clés d'accès dans Amazon EC2 instance. Pour attribuer un AWS rôle pour un Amazon EC2 instance et la mettez à la disposition de toutes ses applications, vous créez un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et active les programmes qui s'exécutent sur Amazon EC2 instance pour obtenir des informations d'identification temporaires. Pour plus d'informations, voir Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur Amazon EC2 instances dans le guide de IAM l'utilisateur.

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

## Gestion des accès à l'aide de politiques

Vous contrôlez l'accès dans AWS en créant des politiques et en les associant à AWS identités ou ressources. Une politique est un objet dans AWS qui, lorsqu'elle est associée 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 dans AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSONpolitiques 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 l'administrateur peut créer IAM politiques. L'administrateur peut ensuite ajouter IAM politiques relatives 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 auprès du AWS Management Console, le AWS CLI, ou le AWS API.

### Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, comme un Utilisateur IAM, rôle ou 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, voir Création IAM politiques décrites dans le guide de IAM l'utilisateur.

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 dans votre Compte AWS. Les politiques gérées incluent AWS politiques

gérées et politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

## Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Voici des exemples de politiques basées sur les ressources : IAM les politiques de confiance dans les rôles et Amazon S3 politiques relatives aux compartiments. 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 AWS politiques gérées à partir de IAM dans une politique 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. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3, AWS WAF, et Amazon VPC sont des exemples de services qui soutiennentACLs. Pour en savoir plusACLs, 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 un IAM entité (Utilisateur IAM ou 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 des autorisations, consultez la section Limites des autorisations pour IAM entités du guide de IAM l'utilisateur.

- Politiques de contrôle des services (SCPs) : SCPs sont des JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service de regroupement et de gestion centralisée de plusieurs Comptes AWS que votre entreprise possède. 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. Les SCP limites d'autorisations pour les entités figurant dans les comptes des membres, y compris chaque Compte AWS utilisateur root. Pour plus d'informations sur les Organizations et SCPs voir Politiques de contrôle des services (SCPs) dans le AWS Organizations Guide de 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 la section Politiques de session dans le guide de IAM l'utilisateur.

### 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 détermine s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, voir la logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

## ROSA exemples de politiques basées sur l'identité

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

Pour savoir comment créer un IAM stratégie basée sur l'identité À l'aide de ces exemples JSON de documents de stratégie, voir Création de politiques dans l'JSONonglet du Guide de l'IAMutilisateur.

## Utilisation de ROSA console

Pour vous abonner à ROSA depuis la console, votre IAM principal doit disposer des informations requises AWS Marketplace autorisations. Les autorisations permettent au directeur de s'abonner et de se désabonner du ROSA liste de produits dans AWS Marketplace et voir AWS Marketplace abonnements. Pour ajouter les autorisations requises, rendez-vous sur ROSA console et fixez le AWS politique gérée `ROSAManageSubscription` pour votre IAM principal. Pour plus d'informations sur `ROSAManageSubscription`, consultez the section called “AWS politique gérée : ROSAManageSubscription”.

## Autoriser ROSA avec HCP pour gérer AWS resources

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

Pour de plus amples informations, veuillez consulter the section called “ AWS stratégies gérées”.

## Autoriser ROSA Classic à gérer AWS resources

ROSAclassic utilise des IAM politiques gérées par le client avec des autorisations prédéfinies par le service. Vous utilisez le ROSA CLIpour créer ces politiques et les associer aux 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 ROSA classiques sans d'abord consulter Red Hat. Cela pourrait annuler le contrat de niveau de service de 99,95 % de disponibilité du cluster conclu par Red Hat. ROSAavec des plans de contrôle hébergés, utilise AWS politiques gérées avec un ensemble d'autorisations plus limité. Pour de plus amples informations, veuillez consulter the section called “ AWS stratégies gérées”.

Il existe deux types de politiques gérées par le client pour ROSA: politiques relatives aux comptes et politiques des opérateurs. Les politiques relatives aux comptes sont jointes à IAM rôles que le service utilise pour établir une relation de confiance avec Red Hat pour le support de l'ingénieur de fiabilité du

site (SRE), la création de clusters et les fonctionnalités de calcul. Les politiques de l'opérateur sont jointes à IAM rôles utilisés par les OpenShift opérateurs 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 Compte AWS, tandis que les politiques d'opérateur sont créées une fois par cluster.

Pour plus d'informations, consultez the section called "ROSApolitiques de compte classiques" et the section called "ROSApolitiques classiques pour les opérateurs".

## Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment vous pouvez créer une politique qui permet Utilisateurs IAM pour consulter les politiques intégrées et gérées associées à leur identité 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": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
```

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

## ROSApolitiques de compte classiques

Cette section fournit des détails sur les politiques de compte requises pour ROSA Classic. Ces autorisations sont nécessaires pour que ROSA Classic puisse gérer le AWS ressources sur lesquelles les clusters s'exécutent et permettent aux ingénieurs 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 les joindre `[Prefix]-Installer-Role-Policy` à vos IAM entités. Avant de créer un cluster ROSA classique, vous devez d'abord associer cette politique à un IAM rôle nommé`[Prefix]-Installer-Role`. Cette politique accorde les autorisations requises qui permettent ROSA programme d'installation pour gérer le AWS ressources nécessaires à la création de clusters.

#### 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:PassRole",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:SimulatePrincipalPolicy",
                "iam:TagRole",
                "iam:UntagRole",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone",
```

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

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

[Préfixe] - ControlPlane -Role-Policy

Vous pouvez les joindre `[Prefix]-ControlPlane-Role-Policy` à vos IAM entités. Avant de créer un cluster ROSA classique, vous devez d'abord associer cette politique à un IAM rôle nommé`[Prefix]-ControlPlane-Role`. Cette politique accorde les autorisations requises à ROSA Classic pour gérer Amazon EC2 and Elastic Load Balancing ressources hébergeant le ROSA plan de contrôle, ainsi que lecture 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 les joindre `[Prefix]-Worker-Role-Policy` à vos IAM entités. Avant de créer un cluster ROSA classique, vous devez d'abord associer cette politique à un IAM rôle nommé`[Prefix]-Worker-Role`. Cette politique accorde les autorisations requises à ROSA Classic pour décrire les EC2 instances 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 les joindre `[Prefix]-Support-Role-Policy` à vos IAM entités. Avant de créer un cluster ROSA classique, vous devez d'abord associer cette politique à un IAM rôle nommé`[Prefix]-Support-Role`. Cette politique accorde les autorisations nécessaires à l'ingénierie de fiabilité des sites Red Hat pour observer, diagnostiquer et prendre en charge les AWS les ressources utilisées par les clusters ROSA classiques, 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*"
            ]
        }
    ]
```

```
}
```

## ROSApolitiques classiques pour les opérateurs

Cette section fournit des détails sur les politiques d'opérateur requises pour la ROSA version classique. Avant de créer un cluster ROSA classique, 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 classiques. 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 les joindre `[Prefix]-openshift-ingress-operator-cloud-credentials` à vos IAM entités. Cette politique accorde les autorisations requises à l'opérateur d'entrée pour provisionner et gérer les équilibreurs de charge et les DNS configurations pour l'accès au cluster externe. La politique permet également à l'opérateur d'entrée de lire et de filtrer Route 53 valeurs des balises de ressources pour 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 les joindre `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` à vos IAM entités. Cette politique accorde les autorisations requises à Amazon EBS CSIChauffeur-opérateur chargé de l'installation et de la maintenance du Amazon EBS CSIpilote sur un cluster ROSA classique. 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 les joindre `[Prefix]-openshift-machine-api-aws-cloud-credentials` à vos IAM entités. Cette politique accorde les autorisations requises à l'opérateur de configuration de la machine pour décrire, exécuter et arrêter 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 à l'aide de 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:PassRole",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

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

Vous pouvez les joindre `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` à vos IAM entités. Cette politique accorde les autorisations requises à l'opérateur d'identification du cloud pour récupérer Utilisateur IAM détails, y compris la clé d'accèsIDs, les documents de politique intégrés joints, la date de création de l'utilisateur, le chemin, l'ID utilisateur et le nom de la 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 les joindre `[Prefix]-openshift-image-registry-installer-cloud-credentials` à vos IAM entités. Cette politique accorde les autorisations requises à l'opérateur de registre d'images pour fournir et gérer les ressources pour le registre d'images intégré au cluster de ROSA Classic et les services dépendants, notamment Amazon S3. Cela est nécessaire pour que l'opérateur puisse installer et gérer le registre interne d'un cluster ROSA classique. 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 les joindre `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` à vos IAM entités. 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 classique. L'opérateur utilise ces autorisations pour gérer les adresses IP privées pour Amazon EC2 instances dans le cadre du cluster ROSA classique. 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

Un AWS une politique 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.

Gardez à l'esprit que AWS les politiques gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous AWS clients à utiliser. 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 AWS politiques gérées. If AWS met à jour les autorisations définies dans un AWS stratégie gérée, 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 un AWS politique gérée lorsqu'un nouveau Service AWS est lancé ou de nouvelles API opérations deviennent disponibles pour les services existants. Pour plus d'informations, consultez .AWS politiques gérées dans le IAM Guide de l'utilisateur.

### AWS politique gérée : ROSAManageSubscription

Vous pouvez joindre la `ROSAManageSubscription` politique à votre IAM entités. Avant d'activer ROSA dans le AWS ROSA console, vous devez d'abord associer cette politique à un rôle de console.

Cette politique accorde le AWS Marketplace autorisations requises pour que vous puissiez gérer le 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 mandants de supprimer les abonnements à AWS Marketplace produits.
- `aws-marketplace:ViewSubscriptions`- Permet aux principaux de consulter les abonnements depuis AWS Marketplace. Cela est nécessaire pour que IAM le principal peut consulter les informations disponibles AWS Marketplace abonnements.

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

## ROSAavec les politiques relatives aux HCP comptes

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

> **Note**
>
> AWS les politiques gérées sont destinées à être utilisées ROSA avec des plans de contrôle hébergés (HCP). ROSAles clusters classiques utilisent des IAM politiques gérées par le client. Pour plus d'informations sur les politiques ROSA classiques, reportez-vous the section called "ROSApolitiques de compte classiques" aux sections etthe section called "ROSApolitiques classiques pour les opérateurs".

AWS politique gérée : ROSAWorkerInstancePolicy

Vous pouvez joindre `ROSAWorkerInstancePolicy` à votre IAM entités. Avant de créer un cluster ROSA avec des plans de contrôle hébergés, vous devez d'abord associer cette politique à un IAM rôle de travailleur.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes qui permettent ROSA service pour effectuer les tâches suivantes :

- `ec2`— Révision Région AWS and Amazon EC2 détails de l'instance dans le cadre de la gestion du cycle de vie des nœuds de travail dans un ROSA grappe.

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

AWS politique gérée : ROSASRESupportPolicy

Vous pouvez les joindre `ROSASRESupportPolicy` à vos IAM entités.

Avant de créer un cluster ROSA avec des plans de contrôle hébergés, vous devez d'abord associer cette politique à un IAM rôle de support. Cette politique accorde les autorisations requises aux ingénieurs de fiabilité des sites Red Hat (SREs) pour observer, diagnostiquer et prendre directement en charge AWS ressources associées à ROSA clusters, y compris la capacité de changer ROSA état du nœud du 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 événements et sentiers pertinents pour le cluster.
- `cloudwatch`— Lisez Amazon CloudWatch métriques pertinentes pour le cluster.
- `ec2`— Lisez, décrivez et révisez Amazon EC2 les composants liés à l'état du cluster, tels que les groupes de sécurité, les connexions aux VPC terminaux et l'état des volumes. Lancer, arrêter, redémarrer et arrêter Amazon EC2 instances.
- `elasticloadbalancing`— Lisez, décrivez et révisez Elastic Load Balancing paramètres liés à l'état de santé du cluster.
- `iam`— Évaluer IAM rôles liés à l'état de santé du cluster.
- `route53`— Vérifiez DNS les paramètres liés à l'état de santé du cluster.
- `sts`— `DecodeAuthorizationMessage` — Lisez IAM messages à des fins de débogage.

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

AWS politique gérée : ROSAInstallerPolicy

Vous pouvez joindre `ROSAInstallerPolicy` à votre IAM entités.

Avant de créer un cluster ROSA avec des plans de contrôle hébergés, vous devez d'abord associer cette politique à un IAM rôle 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 AWS ressources qui soutiennent ROSA installation du cluster.

Détails de l'autorisation

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

- `ec2`— Courir Amazon EC2 instances utilisant AMIs Hosted in Comptes AWS détenu et géré par Red Hat. Describe Amazon EC2 instances, volumes et ressources réseau associés à 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 dans Amazon VPC. Marquez 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.
- `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 un AWS KMS attribuer, créer et gérer des subventions pour Amazon EC2, et renvoient 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 IAM les rôles et les politiques. Approvisionnement et gestion dynamiques Amazon EC2 profils d'instance pertinents pour le cluster. Ajoutez des balises à un profil d'IAMinstance 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 de cluster OIDC spécifié par le client.

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

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

## ROSAavec les politiques des HCP opérateurs

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

> **Note**
>
> AWS les politiques gérées sont destinées à être utilisées ROSA avec des plans de contrôle hébergés (HCP). ROSAles clusters classiques utilisent des IAM politiques gérées par le client. Pour plus d'informations sur les politiques ROSA classiques, reportez-vous the section called “ROSApolitiques de compte classiques” aux sections etthe section called “ROSApolitiques classiques pour les opérateurs”.

AWS politique gérée : ROSAAmazonEBSCSIDriverOperatorPolicy

Vous pouvez joindre `ROSAAmazonEBSCSIDriverOperatorPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des 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 Amazon EBS CSIChauffeur-opérateur chargé de l'installation et de la maintenance du Amazon EBS CSIchauffeur sur un ROSA grappe. Pour plus d'informations sur l'opérateur, consultez la section aws-ebs-csi-driver opérateur dans la OpenShift GitHub documentation.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes qui permettent Amazon EBS Chauffeur-opérateur pour effectuer les tâches suivantes :

- `ec2`— Créez, modifiez, attachez, détachez et supprimez Amazon EBS volumes attachés à Amazon EC2 instances. Création et suppression Amazon EBS instantanés et liste des volumes Amazon EC2 instances, volumes et instantanés.

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

AWS politique gérée : ROSAIngressOperatorPolicy

Vous pouvez joindre `ROSAIngressOperatorPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des 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 fournir et gérer les équilibreurs de charge et DNS les configurations pour ROSA clusters. La politique autorise l'accès en lecture aux valeurs des balises. L'opérateur filtre ensuite les valeurs des balises pour Route 53 des ressources pour 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` – List (liste) Route 53 zones hébergées et modification des enregistrements qui gèrent les zones DNS contrôlées par le ROSA cluster.
- `tag`— Gérez les ressources étiquetées en utilisant l'`tag:GetResources`autorisation.

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

AWS politique gérée : ROSAImageRegistryOperatorPolicy

Vous pouvez joindre `ROSAImageRegistryOperatorPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des 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 registre d'images pour fournir et gérer les ressources pour le ROSA registre d'images intégré au cluster et services dépendants, notamment S3. Cela est nécessaire pour que l'opérateur puisse installer et maintenir le registre interne d'un ROSA grappe. 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`— Gérer et évaluer Amazon S3 des compartiments servant de stockage persistant pour le contenu des images du conteneur et les métadonnées du cluster.

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

AWS politique gérée : ROSACloudNetworkConfigOperatorPolicy

Vous pouvez joindre `ROSACloudNetworkConfigOperatorPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des 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 fournir et gérer les ressources réseau pour le ROSA superposition de réseau en cluster. L'opérateur utilise ces autorisations pour gérer les adresses IP privées pour Amazon EC2 instances dans le cadre du ROSA grappe. 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 de connexion Amazon EC2 des instances, Amazon VPC des sous-réseaux et des interfaces réseau élastiques dans un ROSA grappe.

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

AWS politique gérée : ROSAKubeControllerPolicy

Vous pouvez joindre `ROSAKubeControllerPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des 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 AWS KMS ressources pour 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 à Amazon EC2 groupes de sécurité d'instance. Ajoutez des règles de trafic entrant aux groupes de sécurité. Décrire les zones de disponibilité, Amazon EC2 instances, tables de routageVPCs, groupes de sécurité et sous-réseaux.
- `elasticloadbalancing`— Créez et gérez les équilibreurs de charge et leurs politiques. Créez et gérez des écouteurs d'équilibrage de charge. Enregistrez les cibles auprès des groupes cibles et gérez les groupes cibles. S'inscrire et se désinscrire Amazon EC2 instances avec un équilibreur de charge, et ajoutez des balises aux équilibreurs de charge.
- `kms`— Récupère des informations détaillées sur un 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 JSON de politique complet, consultez ROSAKubeControllerPolicyle AWS Guide de référence des politiques gérées.

AWS politique gérée : ROSANodePoolManagementPolicy

Vous pouvez joindre `ROSANodePoolManagementPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des plans de contrôle hébergés de passer des appels à 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 arrêter 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 à l'aide de AWS KMS clés. 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`— Courir Amazon EC2 instances utilisant AMIs Hosted in Comptes AWS détenu et géré par Red Hat. Gérez les EC2 cycles de vie dans ROSA grappe. Créez et intégrez dynamiquement des nœuds de travail avec Elastic Load Balancing, Amazon VPC, Route 53, Amazon EBS, et Amazon EC2.
- `iam`— Utilisation Elastic Load Balancing via le rôle lié au service nommé. `AWSServiceRoleForElasticLoadBalancing` Attribuez des rôles à Amazon EC2 profils d'instance.
- `kms`— Lisez un AWS KMS attribuer, créer et gérer des subventions pour Amazon EC2, et renvoient 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 JSON de politique complet, consultez ROSANodePoolManagementPolicyle AWS Guide de référence des politiques gérées.

AWS politique gérée : ROSAKMSProviderPolicy

Vous pouvez joindre `ROSAKMSProviderPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des 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 système intégré AWS Fournisseur de chiffrement à gérer AWS KMS clés qui prennent en charge le chiffrement `etcd` des données. Cette politique permet Amazon EC2 pour utiliser KMS des touches qui AWS Le fournisseur de chiffrement permet de chiffrer et de `etcd` déchiffrer les données. Pour plus d'informations sur ce fournisseur, voir AWS Fournisseur de chiffrement dans la documentation de Kubernetes GitHub .

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent AWS Fournisseur de chiffrement pour effectuer les tâches suivantes :

- `kms`— Chiffrer, déchiffrer et récupérer un 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 JSON de politique complet, consultez ROSAKMSProviderPolicyle AWS Guide de référence des politiques gérées.

AWS politique gérée : ROSAControlPlaneOperatorPolicy

Vous pouvez joindre `ROSAControlPlaneOperatorPolicy` à votre IAM entités. Vous devez associer cette politique à un IAM rôle d'opérateur pour permettre à un cluster ROSA avec des 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 and Route 53 ressources pour les clusters ROSA 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`— Création et gestion Amazon VPC points de terminaison.
- `route53`— Répertorier et modifier Route 53 ensembles d'enregistrements et listes de zones hébergées.

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

## ROSA mises à jour de AWS stratégies gérées

Afficher les détails des mises à jour de AWS politiques gérées pour ROSA depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS fil d'actualité de la Historique de la documentation page.

| Modification | Description | Date |
| --- | --- | --- |
| ROSANodePoolManagementPolicy— Politique mise à jour | ROSA a mis à jour la politique pour permettre ROSA gestionnaire de pool de nœuds pour décrire les ensembles d'DHCPoptions afin de définir les DNS noms privés appropriés. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSANodePoolManagementPolicy”. | 2 mai 2024 |
| ROSAInstallerPolicy— Politique mise à jour | ROSA a mis à jour la politique pour permettre ROSA programme d'installation pour ajouter des balises aux sous-réseaux en utilisant la correspondance `"kubernetes.io/cluster/*"` des clés de balise. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAInstallerPolicy”. | 24 avril 2024 |
| ROSASRESupportPolicy— Politique mise à jour | ROSA a mis à jour la politique pour permettre au SRE rôle | 10 avril 2024 |

| Modification | Description | Date |
| --- | --- | --- |
| | de récupérer des informati ons sur les profils d'instance qui ont été balisés par ROSA commered-hat-managed . Pour en savoir plus, consultez the section called “AWS politique gérée : ROSASRESupportPolicy”. | |
| ROSAInstallerPolicy— Politique mise à jour | ROSA a mis à jour la politique pour permettre ROSA installat eur pour le valider AWS politiques gérées pour ROSA sont attachés à 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 à ROSA rôles. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAInstallerPolicy”. | 10 avril 2024 |

| Modification | Description | Date |
| --- | --- | --- |
| ROSAInstallerPolicy—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 de cluster OIDC spécifié par le client. Cette mise à jour permet également au service de récupérer les serveurs de DNS noms existants afin que les opérations de provisionnement de clusters soient idempotentes. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAInstallerPolicy”. | 26 janvier 2024 |
| ROSASRESupportPolicy—Politique mise à jour | ROSA a mis à jour la politique pour autoriser le service à effectuer des opérations de lecture sur les groupes de sécurité à l'aide du DescribeSecurityGroups API. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSASRESupportPolicy”. | 22 janvier 2024 |

| Modification | Description | Date |
| --- | --- | --- |
| ROSAImageRegistryOperatorPolicy— Politique mise à jour | ROSA a mis à jour la politique pour permettre à l'opérateur du registre d'images de prendre des mesures sur Amazon S3 compartiments dans les régions avec des noms à 14 caractères. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAImageRegistryOperatorPolicy”. | 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 instances, tables de routageVPCs, groupes de sécurité et sous-réseaux. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAKubeControllerPolicy”. | 16 octobre 2023 |
| ROSAManageSubscription— 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, consultez the section called “AWS politique gérée : ROSAManageSubscription”. | 1er août 2023 |

| Modification | 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, consultez the section called “AWS politique gérée : ROSAKubeControllerPolicy”. | 13 juillet 2023 |
| ROSANodePoolManagementPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour permettre au NodePool contrôleur de décrire, exécuter et arrêter 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, consultez the section called “AWS politique gérée : ROSANodePoolManagementPolicy”. | 8 juin 2023 |

| Modification | Description | Date |
| --- | --- | --- |
| ROSAInstallerPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour permettre au programme d'installation de gérer AWS ressources qui prennent en charge l'install ation du cluster. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAInstallerPolicy”. | 6 juin 2023 |
| ROSASRESupportPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour permettre à Red Hat SREs d'observer, de diagnostiquer et de soutenir directement AWS ressource s associées à ROSA clusters, y compris la capacité de changer ROSA état du nœud du cluster. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSASRESupportPolicy”. | 1er juin 2023 |
| ROSAKMSProviderPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour autoriser le AWS Fournisseur de chiffreme nt à gérer AWS KMS clés pour prendre en charge le cryptage des données etcd. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAKMSProviderPol icy”. | 27 avril 2023 |

| Modification | Description | Date |
| --- | --- | --- |
| ROSAKubeControllerPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour permettre au contrôleur Kube de gérer Amazon EC2, Elastic Load Balancing, et AWS KMS ressources pour ROSA avec des clusters de plans de contrôle hébergés. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAKubeController Policy”. | 27 avril 2023 |
| ROSAImageRegistryOperatorPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique permettant à l'opérateur du registre d'images de fournir et de gérer les ressources pour le ROSA registre d'images intégré au cluster et services dépendants, notamment S3. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAImageRegistryOperatorPolicy”. | 27 avril 2023 |

| Modification | Description | Date |
| --- | --- | --- |
| ROSAControlPlaneOperatorPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour permettre à l'opérateur du plan de contrôle de gérer Amazon EC2 and Route 53 ressources pour ROSA avec des clusters de plans de contrôle hébergés. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAControlPlaneOperatorPolicy”. | 24 avril 2023 |
| 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 le ROSA superposition de réseau en cluster. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSACloudNetworkConfigOperatorPolicy”. | 20 avril 2023 |
| ROSAIngressOperatorPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique permettant à l'opérateur d'entrée de fournir et de gérer des équilibreurs de charge et DNS des configurations pour ROSA clusters. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAIngressOperatorPolicy”. | 20 avril 2023 |

| Modification | Description | Date |
| --- | --- | --- |
| ROSAAmazonEBSCSIDriverOperatorPolicy— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour permettre Amazon EBS CSIChauffeur-opérateur chargé de l'installation et de la maintenance du Amazon EBS CSIchauffeur sur un ROSA grappe. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAAmazonEBSCSIDriverOperatorPolicy”. | 20 avril 2023 |
| 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, consultez the section called “AWS politique gérée : ROSAWorkerInstancePolicy”. | 20 avril 2023 |
| ROSAManageSubscription— Ajout d'une nouvelle politique | ROSA a ajouté une nouvelle politique pour accorder le AWS Marketplace autorisations requises pour gérer le ROSA abonnement. Pour en savoir plus, consultez the section called “AWS politique gérée : ROSAManageSubscription”. | 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 à son AWS politiques gérées. | 2 mars 2022 |

# Résolution des problèmes ROSA identité et 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 and IAM.

## AWS Organizations politique de contrôle des services refuse d'être requise AWS Marketplace des autorisations

Si vos recettes AWS Organizations la politique de contrôle des services (SCP) n'autorise pas les AWS Marketplace autorisations d'abonnement lorsque vous tentez d'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 les SCP pour autoriser `aws-marketplace:Subscribeaws-marketplace:Unsubscribe`, et `aws-marketplace:ViewSubscriptions` les autorisations. Pour plus d'informations, voir Mettre à jour un SCP  AWS Organizations Guide de l'utilisateur.
2. Enable ROSA dans le compte de gestion de l'organisation.
3. Partagez le ROSA abonnement à des comptes de membres nécessitant un accès au sein de l'organisation. Pour plus d'informations, voir Partage d'abonnements au sein d'une organisation dans le  AWS Marketplace Guide de l'acheteur.

## L'utilisateur ou le rôle ne possède pas les éléments requis AWS Marketplace des autorisations

Si vos recettes IAM le directeur n'a pas les éléments requis AWS Marketplace autorisations d'abonnement lorsque vous tentez d'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 au IAM console et fixez le AWS politique gérée relative `ROSAManageSubscription` à votre IAM identité. Pour plus d'informations, consultez ROSAManageSubscriptionle AWS Guide de référence des politiques 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 dans IAM ou si vous recevez un message d'erreur, vous devez contacter votre administrateur pour obtenir de l'aide. Demandez à cette personne de joindre `ROSAManageSubscription` à votre IAM identifiez-vous et suivez la procédure dansthe section called “Activer ROSA et configurer les AWS prérequis”. Lorsqu'un administrateur exécute cette action, il active ROSA en mettant à jour l'ensemble d'autorisations pour tous IAM identités en vertu de la Compte AWS.

## Obligatoire AWS Marketplace autorisations bloquées par un administrateur

Si l'administrateur de votre compte a bloqué le AWS Marketplace autorisations d'abonnement, l'erreur de console suivante se produit lorsque vous tentez d'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 au ROSA console et fixez le AWS politique gérée relative `ROSAManageSubscription` à votre IAM identité. Pour plus d'informations, consultez ROSAManageSubscriptionle AWS Guide de référence des politiques gérées.
2. Suivez la procédure the section called “Activer ROSA et configurer les AWS prérequis” pour activer ROSA. Cette procédure permet ROSA en mettant à jour l'ensemble d'autorisations pour tous IAM identités en vertu de la 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 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  Elastic Load Balancing Guide de l'utilisateur.

# Résilience dans ROSA

## AWS résilience des infrastructures mondiales

Le AWS l'infrastructure mondiale est construite autour de Régions AWS et 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 en une seule fois AWS Zone de disponibilité, ou entre 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 Régions AWS et zones de disponibilité, voir AWS Infrastructure mondiale.

## ROSA résilience des clusters

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

Le ROSA un plan de 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 SREs de manière proactive les ROSA cluster, et sont chargés de remplacer les nœuds du plan de contrôle et les nœuds d'infrastructure défaillants. Pour de plus amples informations, veuillez consulter the section called “Responsabilités”.

> **Important**
>
> Parce que ROSA est un service géré, Red Hat est responsable de la gestion du service sous-jacent AWS une infrastructure qui ROSA utilise. Les clients ne doivent pas essayer de désactiver manuellement le Amazon EC2 des instances qui ROSA utilisations depuis le 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 que ROSA fournit de nombreuses protections pour garantir la haute disponibilité du service, les clients sont responsables 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, voir À propos de la disponibilité de ROSAdans la documentation Red Hat.

# Sécurité de l'infrastructure dans ROSA

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

Vous utilisez AWS APIappels d'accès publiés ROSA par le biais du AWS réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE 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 identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Ou vous pouvez utiliser AWS Security Token Service (AWS STS) pour générer des informations de sécurité temporaires pour 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, voir the section called “Responsabilités”.

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

L'accès au API serveur Kubernetes est sécurisé à l'aide d'une combinaison de AWS Identity and Access Management (IAM) et le contrôle d'accès natif basé sur les rôles de Kubernetes (). RBAC Pour plus d'informations sur KubernetesRBAC, consultez la section Utilisation de l'RBACautorisation dans la documentation de Kubernetes.

ROSA vous permet de créer des itinéraires d'application sécurisés en utilisant plusieurs types de TLS terminaison 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 dans un cluster existantVPC, vous spécifiez les VPC sous-réseaux et les zones de disponibilité que votre cluster doit utiliser. Vous définissez également les CIDR plages que le réseau de clusters doit utiliser et vous associez ces CIDR plages aux VPC sous-réseaux. Pour plus d'informations, consultez les définitions des CIDR plages dans la documentation Red Hat.

Pour les clusters qui utilisent le point de API terminaison public, ROSA nécessite que vous VPC soyez 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 API terminaison privé, seuls les sous-réseaux privés sont requis.

Si vous utilisez un appareil existantVPC, vous pouvez configurer votre ROSA clusters destinés à utiliser un HTTP serveur HTTPS proxy pendant ou après la création du cluster pour 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 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 module qui limitent le trafic aux modules de votre ROSA grappe.

# 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. ROSAle standard est mesuré et facturé via un produit basé sur AWS Marketplace Amazon Machine Image (AMI), tandis que les plans de contrôle ROSA hébergés (HCP) sont mesurés et facturés 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 ROSA de l'intégration avec AWS Marketplace.

Image de machine Amazon (AMI)

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

AMIabonnement

Dans AWS Marketplace, AMI les produits logiciels 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, notamment 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. ROSAles frais HCP de service s'accumulant par défaut sur demande à un taux horaire fixe basé sur le nombre de clusters en cours d'exécution et de nœuds de travail vCPUs exécutés dans ces clusters. ROSAles frais de service classiques s'accumulent sur demande en fonction du nombre de nœuds de travailleursvCPUs. ROSAclassic 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 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 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 à la ROSA version classique et ROSA les HCP listes sont activées AWS Marketplace. L'activation des ROSA abonnements est gratuite.

Pour AWS Organizations les utilisateurs, vous ROSA permet de partager des abonnements ROSA classiques 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 with 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 la ROSA version classique et ROSA avec HCP depuis la ROSA console.

> **Note**
> ROSAClassic 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 classique de 12 mois

Lorsque vous souscrivez un contrat ROSA classique 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**
> ROSAles contrats classiques de 12 mois ne se renouvellent pas automatiquement.

Pour acheter un contrat de 12 mois pour Classic ROSA

> **Note**
> Si vous utilisez la ROSA console dans une région qui n'est pas encore compatible ROSA avecHCP, ce flux de travail n'est pas encore disponible. Pour obtenir la liste des régions compatibles ROSA avecHCP, voirthe section called “Comparaison ROSA avec HCP et ROSA classique”.

Pour acheter des contrats ROSA classiques dans les régions ROSA sans HCP assistance, 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 pour la ROSA version classique.
4. Choisissez Contrat d'achat.
5. Sélectionnez le type d'EC2instance 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 AWS Support Centre et ouvrez un dossier d'assistance.

Acheter un contrat ROSA de HCP 12 mois

Lorsque vous activez ROSA with HCP dans la console, un HCP contrat gratuit de 12 mois ROSA est initialement créé sur votre compte pour faciliter la facturation à la demande. Si vous choisissez d'acheter un HCP contrat ROSA avec 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 vCPUs et des plans de contrôle que vous spécifiez.

Lorsque vous achetez un contrat ROSA de HCP 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 vCPUs et les plans de contrôle couverts. Le coût du contrat est basé sur le nombre de nœuds de travail vCPUs et de plans de contrôle que vous sélectionnez. Le contrat couvre uniquement le nœud de travail vCPUs 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 prépayés vCPUs et de contrôle sont convertis en un quota d'utilisation mensuel. Les taux d'utilisation horaires à la demande s'appliquent pour l'utilisation du v CPU et du plan de contrôle qui dépasse le quota mensuel. ROSAwith HCP utilise les formules suivantes pour calculer le quota mensuel associé au contrat :

- Nœud de travail vCPUs : nombre de vCPUs 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 vCPUs et de 8 plans de contrôle se traduirait par un quota mensuel de 2 920 000 heures par nœud de travail et de 5 840 CPU heures de plan de contrôle consommables par mois.

Pour acheter un contrat ROSA de HCP 12 mois

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

1. Accédez à la console ROSA.
2. Dans le volet de navigation de gauche, sélectionnez Contracts.
3. Choisissez Contrats pour ROSA avec HCP.
4. Choisissez Contrat d'achat.
5. Entrez le numéro vCPUs 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 AWS Support Centre et ouvrez un dossier d'assistance.

Mise à niveau d'ROSAun contrat HCP de 12 mois

Vous pouvez à tout moment améliorer votre contrat actif ROSA de HCP 12 mois avec un nœud de travail vCPUs et des plans de contrôle supplémentaires. Lorsque vous passez ROSA à un contrat de HCP 12 mois, vous effectuez un paiement initial au prorata des 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 vCPUs 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 ajoutés vCPUs et de contrôle 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 du v CPU et du plan de contrôle qui dépasse le quota mensuel. Pour plus d’informations, consultez the section called “Quota d'utilisation mensuel”.

Pour mettre à niveau un ROSA contrat de HCP 12 mois

1. Accédez à la console ROSA.
2. Dans le volet de navigation de gauche, sélectionnez Contracts.
3. Choisissez Contrats pour ROSA avec HCP.
4. Choisissez Upgrade (Mise à niveau).
5. Entrez le nombre de vCPUs 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**
> ROSAles contrats classiques de 12 mois ne peuvent pas être revalorisés. Des contrats ROSA classiques supplémentaires de 12 mois peuvent être achetés à tout moment à l'aide de la ROSA console.

## Obtenir 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 classique émise uniquement 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 termes et conditions.
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 un site de vente privé, un administrateur doit ajouter les AWS Marketplace listes ROSA pour le marché privé 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
- ROSA le cluster échoue à la vérification des quotas de AWS service lors de cluster la création
- Résoudre les problèmes liés aux ROSA CLI jetons d'accès hors ligne expirés
- Impossible de créer un fichier cluster avec une osdCcsAdmin erreur
- Étapes suivantes
- Obtenir de ROSA l'aide


## 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 ROSA CLI débogage 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 ROSA CLI commande 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 ROSA CLI jetons d'accès hors ligne expirés

Si vous utilisez le jeton d'accès hors ligne api.openshift.com ROSA CLI et que celui-ci 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 STS méthode non utilisée pour provisionner des ROSA clusters. Pour éviter ce problème, provisionnez vos ROSA clusters à l'aide de AWS STS. Pour plus d'informations, consultez the section called “Créez un cluster ROSA classique - 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 AWS 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 ROSA le modèle de support, consultezthe section called “Obtention de support”.

# Obtenir de ROSA l'aide

Avec ROSA, vous pouvez bénéficier de l'assistance de la part AWS 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 transmis à l'équipe appropriée pour résoudre votre problème.

## Ouvrez un AWS 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 le AWS 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 AWS Support les forfaits, consultez AWS Support.

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

Pour plus d'informations sur la création d'un AWS 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 être informé des mises à jour de cette documentation, vous pouvez vous abonner à un RSS flux.

| Modification | Description | Date |
| --- | --- | --- |
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible au Moyen-Orient (UAE) Région AWS. | 13 mai 2024 |
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible en Europe (Paris) Région AWS. | 6 mai 2024 |
| Mis à jour ROSANodePoolManagementPolicy | Mise à jour de l'outil de ligne de commande AWS politique géréeROSANodePoolManagementPolicy. | 2 mai 2024 |
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible en Europe (Espagne) Région AWS. | 29 avril 2024 |
| Mis à jour ROSAInstallerPolicy | Mise à jour de l'outil de ligne de commande AWS politique géréeROSAInstallerPolicy. | 24 avril 2024 |
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible en Europe (Zurich) Région AWS. | 19 avril 2024 |

| | | |
|---|---|---|
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible en Asie-Pacifique (Osaka) Région AWS. | 17 avril 2024 |
| Mis à jour ROSAInstallerPolicy et ROSASRESupportPolicy | Mise à jour de l'outil de ligne de commande AWS politique s gérées ROSAInstallerPolicy etROSASRESupportPolicy. | 10 avril 2024 |
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible en Asie-Pacifique (Hong Kong) Région AWS. | 8 avril 2024 |
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible en Amérique du Sud (São Paulo) Région AWS. | 1er avril 2024 |
| ROSAavec HCP Région AWS expansion | ROSAavec des avions de contrôle hébergés (HCP) est désormais disponible au Moyen-Orient (Bahreïn) Région AWS. | 25 mars 2024 |
| ROSAavec HCP Région AWS expansion | ROSAavec des plans de contrôle hébergés (HCP) est désormais disponible en Asie-Pacifique (Séoul) Région AWS. | 14 mars 2024 |

| | | |
|---|---|---|
| ROSAavec HCP Région AWS expansion | ROSAavec des avions de contrôle hébergés (HCP) est désormais disponible en Afrique (Cape Town) Région AWS. | 5 mars 2024 |
| Mis à jour ROSAInstallerPolicy | Mise à jour de l'outil de ligne de commande AWS politique géréeROSAInstallerPolicy. | 26 janvier 2024 |
| Mis à jour ROSASRESupportPolicy | Mise à jour de l'outil de ligne de commande AWS politique géréeROSASRESupportPolicy. | 22 janvier 2024 |
| Mis à jour ROSAImageRegistryOperatorPolicy | Mise à jour de l'outil de ligne de commande AWS politique géréeROSAImageRegistryOperatorPolicy. | 12 décembre 2023 |
| Mis à jour ROSAKubeControllerPolicy | Mise à jour de l'outil de ligne de commande AWS politique géréeROSAKubeControllerPolicy. | 16 octobre 2023 |
| Mis à jour ROSAManageSubscription | Mise à jour de l'outil de ligne de commande AWS politique géréeROSAManageSubscription. | 1er août 2023 |
| Mis à jour ROSAKubeControllerPolicy | Mise à jour de l'outil de ligne de commande AWS politique géréeROSAKubeControllerPolicy. | 13 juillet 2023 |

| | | |
|---|---|---|
| Pages ROSA de sécurité ajoutées | La résilienceROSA, la sécurité de l'infrastructure et la protection des données dans les ROSA pages ont été ajoutées. ROSA | 30 juin 2023 |
| Ajout de la page des options de déploiement | La page des options de déploiement a été ajoutée. | 9 juin 2023 |
| Nouveau ajouté AWS politique gérée ROSANodePoolManagementPolicy | New AWS une politique gérée ROSANodePoolManagementPolicy a été ajoutée. | 8 juin 2023 |
| Nouveau ajouté AWS politique gérée ROSAInstallerPolicy | New AWS une politique gérée ROSAInstallerPolicy a été ajoutée. | 6 juin 2023 |
| Nouveau ajouté AWS politique gérée ROSASRESupportPolicy | New AWS une politique gérée ROSASRESupportPolicy a été ajoutée. | 1er juin 2023 |
| Ajout d'un aperçu des responsabilités pour ROSA | Ajout d'un aperçu des responsabilités pour ROSA la page. | 26 mai 2023 |
| Mise à jour de ce qui est Red Hat OpenShift Service on AWS? | Mise à jour du What is Red Hat OpenShift Service on AWS page. | 24 mai 2023 |
| Nouveau ajouté AWS politiques gérées pour les rôles des ROSA opérateurs | New AWS politiques gérées ROSAImageRegistryOperatorPolicyROSAKubeControllerPolicy, et ROSAKMSProviderPolicy ont été ajoutées. | 27 avril 2023 |

| | | |
|---|---|---|
| Nouveau ajouté AWS politique gérée ROSAControlPlaneOperatorPolicy | New AWS une politique gérée ROSAControlPlaneOperatorPolicy a été ajoutée. | 24 avril 2023 |
| Nouveau ajouté AWS politiques gérées pour les rôles de ROSA compte | New AWS des pages de politique gérées pour le ROSA compte et la page des rôles des opérateurs ont été ajoutées. | 20 avril 2023 |
| Ajout de la page des quotas de ROSA service | La page des quotas de ROSA service 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 |
| Nouveau ajouté AWS politique gérée ROSAManageSubscription | New AWS une politique gérée ROSAManageSubscription a été ajoutée. | 11 avril 2022 |
| Première version | La version initiale du Red Hat OpenShift Service on AWS Guide de l'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.