OpenShift Dedicated 4

Clusters dédiés à OpenShift sur AWS

Installation de clusters dédiés OpenShift sur AWS

Last Updated: 2025-05-27

OpenShift Dedicated 4 Clusters dédiés à OpenShift sur AWS

Installation de clusters dédiés OpenShift sur AWS

Notice légale

Résumé

Ce document fournit des informations sur la façon d’installer OpenShift Dedicated clusters sur AWS. Le document fournit également des détails sur la configuration des clusters.

Table des matières

CHAPITRE 1. CRÉATION D'UN CLUSTER SUR AWS

Il est possible de déployer OpenShift Dedicated sur Amazon Web Services (AWS) en utilisant votre propre compte AWS via le modèle Customer Cloud Subscription (CCS) ou en utilisant un compte d'infrastructure AWS appartenant à Red Hat.

1.1. CONDITIONS PRÉALABLES

- Découvrez l'introduction à OpenShift Dedicated et la documentation sur les concepts d'architecture.
- Les options de déploiement de cloud dédiés à OpenShift ont été revues.

1.2. CRÉATION D'UN CLUSTER SUR AWS

En utilisant le modèle de facturation Customer Cloud Subscription (CCS), vous pouvez créer un cluster OpenShift dédié dans un compte Amazon Web Services (AWS) existant que vous possédez.

Il est également possible de sélectionner le type d'infrastructure de compte cloud Red Hat pour déployer OpenShift Dedicated dans un compte de fournisseur de cloud appartenant à Red Hat.

Complétez les conditions préalables suivantes pour utiliser le modèle CCS pour déployer et gérer OpenShift Dedicated dans votre compte AWS.

Conditions préalables

- Avec OpenShift Dedicated, vous avez configuré votre compte AWS.
- Aucun service n'a été déployé sur votre compte AWS.
- Les quotas et les limites de compte AWS sont configurés pour prendre en charge la taille du cluster souhaitée.
- Il y a un utilisateur de gestion de l'identité et de l'accès (IAM) d'AWSAdmin (OSdCcsAdmin) avec la politique AdministratorAccess jointe.
- Dans votre organisation AWS, vous avez mis en place une stratégie de contrôle des services (SCP). Consultez la politique minimale de contrôle du service (SCP) pour plus d'informations.
- Envisagez d'avoir un support commercial ou supérieur à partir d'AWS.
- Lorsque vous configurez un proxy à l'échelle du cluster, vous avez vérifié que le proxy est accessible depuis le VPC dans lequel le cluster est installé. Le proxy doit également être accessible depuis les sous-réseaux privés du VPC.

Procédure

1. Connectez-vous à OpenShift Cluster Manager.
2. Dans la page Aperçu, sélectionnez Créer un cluster dans la carte Red Hat OpenShift dédiée.
3. Dans le modèle de facturation, configurez le type d'abonnement et le type d'infrastructure:

a. Choisissez un type d'abonnement. En ce qui concerne les options d'abonnement dédiées à OpenShift, consultez les abonnements Cluster et l'inscription dans la documentation OpenShift Cluster Manager.

NOTE

Les types d'abonnement qui vous sont disponibles dépendent de vos abonnements OpenShift dédiés et des quotas de ressources. Contactez votre représentant commercial ou votre support Red Hat pour plus d'informations.

b. Choisissez le type d'infrastructure d'abonnement cloud client pour déployer OpenShift Dedicated dans un compte de fournisseur de cloud existant que vous possédez ou sélectionnez le type d'infrastructure de compte cloud Red Hat pour déployer OpenShift Dedicated dans un compte fournisseur de cloud appartenant à Red Hat.

c. Cliquez sur **Next**.

4. Choisissez Exécuter sur Amazon Web Services. Lorsque vous provisionnez votre cluster dans un compte AWS, remplissez les sous-étapes suivantes:

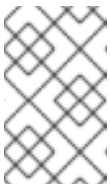
a. Examinez et complétez les Prérequis listés.

b. Choisissez la case à cocher pour reconnaître que vous avez lu et rempli toutes les conditions préalables.

c. Fournissez les détails de votre compte AWS:

i. Entrez votre identifiant de compte AWS.

ii. Entrez votre ID de clé d'accès AWS et votre clé d'accès secret AWS pour votre compte utilisateur AWS IAM.



NOTE

La révocation de ces informations d'identification dans AWS entraîne une perte d'accès à n'importe quel cluster créé avec ces informations d'identification.

iii. Facultatif : Vous pouvez sélectionner Bypass AWS Service Control Policy (SCP) pour désactiver les vérifications SCP.

NOTE

Certains SCP AWS peuvent faire échouer l'installation, même si vous avez les autorisations requises. La désactivation des contrôles SCP permet à une installation de procéder. Le SCP est toujours appliqué même si les contrôles sont contournés.

5. Cliquez sur Suivant pour valider votre compte de fournisseur de cloud et accédez à la page Détails du cluster.

6. Dans la page Détails du cluster, fournissez un nom pour votre cluster et spécifiez les détails du cluster:

a. Ajoutez un nom de cluster.

b. Facultatif: Création de cluster génère un préfixe de domaine en tant que sous-domaine pour votre cluster provisionné sur openshiftapps.com. Lorsque le nom du cluster est inférieur ou égal à 15 caractères, ce nom est utilisé pour le préfixe de domaine. Lorsque le nom du cluster est supérieur à 15 caractères, le préfixe de domaine est généré au hasard sur une chaîne de 15 caractères.
Afin de personnaliser le sous-domaine, sélectionnez la case à cocher Créer un préfixe de domaine, puis entrez le nom de préfixe de domaine dans le champ Préfixe de domaine. Le préfixe de domaine ne peut pas dépasser 15 caractères, doit être unique au sein de votre organisation et ne peut pas être modifié après la création de clusters.

c. Choisissez une version de cluster dans le menu déroulant Version.

d. Choisissez une région fournisseur de cloud dans le menu déroulant Région.

e. Choisissez une configuration de zone unique ou multi-zone.

f. Laissez activer la surveillance de la charge de travail de l'utilisateur sélectionnée pour surveiller vos propres projets indépendamment des métriques de la plate-forme Red Hat Site Reliability Engineer (SRE). Cette option est activée par défaut.

g. Facultatif: Expandez le chiffrement avancé pour apporter des modifications aux paramètres de chiffrement.

    i. Acceptez le paramètre par défaut Utilisez les clés KMS par défaut pour utiliser votre clé AWS KMS par défaut, ou sélectionnez Utilisez les touches KMS personnalisées pour utiliser une clé KMS personnalisée.

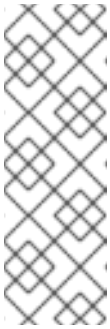
        A. Avec les touches KMS personnalisées sélectionnées, saisissez l'ARN ARN de la clé personnalisée Amazon Resource Name (ARN) d'AWS Key Management Service (KMS) dans le champ Key ARN. La clé est utilisée pour chiffrer tous les plans de contrôle, l'infrastructure, les volumes racine des nœuds de travail et les volumes persistants de votre cluster.

    ii. Facultatif: Sélectionnez Activer la cryptographie FIPS si vous exigez que votre cluster soit validé FIPS.

NOTE

Lorsque la cryptographie FIPS est sélectionnée, Activer le chiffrement etcd supplémentaire est activé par défaut et ne peut pas être désactivé. Activez le chiffrement supplémentaire etcd sans sélectionner Activer la cryptographie FIPS.

    iii. Facultatif: Sélectionnez Activer le chiffrement supplémentaire etcd si vous avez besoin d'un cryptage de valeur clé etcd. Avec cette option, les valeurs de clé etcd sont cryptées, mais les clés ne le sont pas. Cette option s'ajoute au chiffrement de stockage de plan de contrôle qui chiffre les volumes etcd dans les clusters dédiés OpenShift par défaut.



NOTE

En activant le chiffrement etcd pour les valeurs clés dans etcd, vous subirez un surcharge de performance d'environ 20%. Les frais généraux sont le résultat de l'introduction de cette deuxième couche de chiffrement, en plus du chiffrement de stockage de plan de contrôle par défaut qui crypte les volumes etcd. Envisagez d'activer le chiffrement etcd seulement si vous en avez spécifiquement besoin pour votre cas d'utilisation.

h. Cliquez sur **Next**.

7. Dans la page de pool machine par défaut, sélectionnez un type d'instance de nœud de calcul dans le menu déroulant.

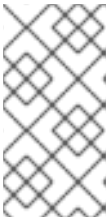
8. Facultatif: Sélectionnez la case à cocher Autoscaling pour activer l'autoscaling.

   a. Cliquez sur Modifier les paramètres d'autoscaling du cluster pour apporter des modifications aux paramètres de mise à l'échelle automatique.

   b. Lorsque vous avez apporté vos modifications souhaitées, cliquez sur Fermer.

   c. Choisissez un nombre minimum et maximum de nœuds. Les nombres de nœuds peuvent être sélectionnés en engageant les signes plus et moins disponibles ou en entrant le nombre de nœuds souhaité dans le champ d'entrée du nombre.

9. Choisissez un nombre de nœuds de calcul dans le menu déroulant.

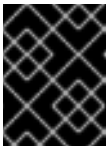


NOTE

Après la création de votre cluster, vous pouvez modifier le nombre de nœuds de calcul dans votre cluster, mais vous ne pouvez pas modifier le type d'instance de nœud de calcul dans un pool de machines. Le nombre et les types de nœuds à votre disposition dépendent de votre abonnement OpenShift dédié.

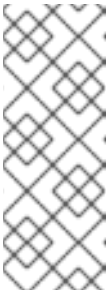
10. Choisissez votre préférence pour le type de service de métadonnées d'instance (IMDS), soit en utilisant à la fois les types IMDSv1 et IMDSv2, soit en exigeant que vos instances EC2 utilisent uniquement IMDSv2. Les métadonnées d'instance peuvent être consultées à partir d'une instance en cours d'exécution de deux manières:

    - Instance Metadata Service Version 1 (IMDSv1) - une méthode de requête/réponse
    - Instance Metadata Service Version 2 (IMDSv2) - une méthode orientée session



IMPORTANT

Les paramètres du service de métadonnées d'instance ne peuvent pas être modifiés après la création de votre cluster.



NOTE

IMDSv2 utilise des requêtes orientées session. Avec les requêtes axées sur la session, vous créez un jeton de session qui définit la durée de la session, qui peut aller d'un minimum d'une seconde à un maximum de six heures. Au cours de la durée spécifiée, vous pouvez utiliser le même jeton de session pour les demandes ultérieures. Après l'expiration de la durée spécifiée, vous devez créer un nouveau jeton de session à utiliser pour les demandes futures.

Consultez les métadonnées de l'instance et les données de l'utilisateur dans la documentation AWS.

11. En option: Expandez les étiquettes de nœuds pour ajouter des étiquettes à vos nœuds. Cliquez sur Ajouter une étiquette pour ajouter d'autres étiquettes de nœuds et sélectionnez Suivant.

12. Dans la page de configuration réseau, sélectionnez Public ou Privé pour utiliser des points de terminaison API publics ou privés et des itinéraires d'application pour votre cluster.

IMPORTANT

Lorsque vous utilisez des points de terminaison d'API privés, vous ne pouvez pas accéder à votre cluster tant que vous n'avez pas mis à jour les paramètres réseau de votre compte fournisseur de cloud.

13. Facultatif: Pour installer le cluster dans un cloud privé virtuel AWS (VPC) existant:

    a. Choisissez Installer dans un VPC existant.

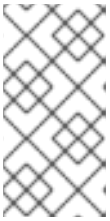
    b. Lorsque vous installez dans un VPC existant et que vous avez choisi d'utiliser des points de terminaison d'API privés, vous pouvez sélectionner Utiliser un PrivateLink. Cette option permet des connexions au cluster par Red Hat Site Reliability Engineering (SRE) en utilisant uniquement les points de terminaison AWS PrivateLink.

NOTE

L'option Utiliser un PrivateLink ne peut pas être modifiée après la création d'un cluster.

    c. Lorsque vous installez dans un VPC existant et que vous souhaitez activer un proxy HTTP ou HTTPS pour votre cluster, sélectionnez Configurer un proxy à l'échelle du cluster.

14. Lorsque vous avez choisi d'installer le cluster dans un VPC AWS existant, fournissez vos paramètres de sous-réseau Virtual Private Cloud (VPC) et sélectionnez Suivant. Il faut avoir créé la traduction d'adresse réseau Cloud (NAT) et un routeur Cloud. Consultez la section « Ressources supplémentaires » pour obtenir des informations sur les NAT Cloud et les VPC Google.



NOTE

Assurez-vous que votre VPC est configuré avec un sous-réseau public et privé pour chaque zone de disponibilité dans laquelle vous souhaitez installer le cluster. Lorsque vous avez choisi d'utiliser PrivateLink, seuls les sous-réseaux privés sont requis.

a. Facultatif: Expandez des groupes de sécurité supplémentaires et sélectionnez des groupes de sécurité personnalisés supplémentaires à appliquer aux nœuds dans les pools de machines créés par défaut. Il faut déjà avoir créé les groupes de sécurité et les associer au VPC que vous avez sélectionné pour ce cluster. Après avoir créé le cluster, vous ne pouvez pas ajouter ou modifier des groupes de sécurité dans les pools de machines par défaut. Les groupes de sécurité que vous spécifiez sont ajoutés par défaut pour tous les types de nœuds. Effacer la case Appliquer les mêmes groupes de sécurité à tous les types de nœuds pour appliquer différents groupes de sécurité pour chaque type de nœud.

   Consultez les exigences relatives aux groupes de sécurité au titre des ressources supplémentaires.

15. Acceptez les paramètres d'entrée de l'application par défaut, ou pour créer vos propres paramètres personnalisés, sélectionnez Paramètres personnalisés.

    a. Facultatif: Fournir le sélecteur d'itinéraire.

    b. Facultatif: Fournir des espaces de noms exclus.

    c. Choisissez une politique de propriété d'espace de noms.

    d. Choisissez une politique de wildcard.
    Cliquez sur l'icône d'information fournie pour chaque paramètre.

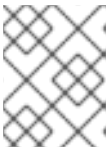
16. Lorsque vous avez choisi de configurer un proxy à l'échelle du cluster, fournissez les détails de la configuration de votre proxy sur la page proxy à l'échelle du cluster:

    a. Entrez une valeur dans au moins un des champs suivants:

       - Indiquez une URL proxy HTTP valide.
       - Indiquez une URL proxy HTTPS valide.
       - Dans le champ Autres paquets de confiance, fournissez un paquet de certificats X.509 codé PEM. Le paquet est ajouté au magasin de certificats de confiance pour les nœuds de cluster. Il est nécessaire d'obtenir un fichier de groupe de confiance supplémentaire si vous utilisez un proxy d'inspection TLS à moins que le certificat d'identité du proxy ne soit signé par une autorité du groupe de confiance Red Hat Enterprise Linux CoreOS (RHCOS). Cette exigence s'applique indépendamment du fait que le proxy soit transparent ou nécessite une configuration explicite en utilisant les arguments http-proxy et https-proxy.

    b. Cliquez sur **Next**.
    De plus amples informations sur la configuration d'un proxy avec OpenShift Dedicated, voir Configuration d'un proxy à l'échelle du cluster.

17. Dans la boîte de dialogue des plages CIDR, configurez des gammes de routage interdomaine sans classe (CIDR) ou utilisez les valeurs par défaut fournies.



NOTE

Lorsque vous installez dans un VPC, la gamme Machine CIDR doit correspondre aux sous-réseaux VPC.

IMPORTANT

Les configurations CIDR ne peuvent pas être modifiées ultérieurement. Confirmez vos sélections avec votre administrateur réseau avant de procéder.

18. Dans la page Stratégie de mise à jour Cluster, configurez vos préférences de mise à jour:

    a. Choisissez une méthode de mise à jour de cluster:

    - Choisissez des mises à jour individuelles si vous souhaitez planifier chaque mise à jour individuellement. C'est l'option par défaut.
    - Choisissez les mises à jour récurrentes pour mettre à jour votre cluster le jour de votre choix et l'heure de début, lorsque des mises à jour sont disponibles.

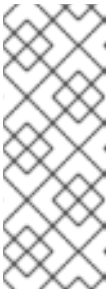
NOTE

Consultez les dates de fin de vie dans la documentation du cycle de vie de la mise à jour pour OpenShift Dedicated. Consultez OpenShift Dedicated cycle de vie pour plus d'informations.

    b. Lorsque vous avez opté pour des mises à jour récurrentes, sélectionnez un jour préféré de la semaine et mettez à niveau l'heure de début en UTC dans les menus déroulants.

    c. Facultatif: Vous pouvez définir un délai de grâce pour le drainage des nœuds pendant les mises à niveau de cluster. Le délai de grâce d'une heure est fixé par défaut.

    d. Cliquez sur **Next**.



NOTE

En cas de problèmes de sécurité critiques qui ont un impact significatif sur la sécurité ou la stabilité d'un cluster, Red Hat Site Reliability Engineering (SRE) pourrait programmer des mises à jour automatiques de la dernière version z-stream qui n'est pas affectée. Les mises à jour sont appliquées dans les 48 heures suivant la notification des clients. La description de la cote de sécurité d'impact critique, voir Comprendre les cotes de sécurité Red Hat.

19. Examinez le résumé de vos sélections et cliquez sur Créer un cluster pour démarrer l'installation du cluster. L'installation prend environ 30 à 40 minutes à compléter.

20. Facultatif: Dans l'onglet Aperçu, vous pouvez activer la fonction de protection de suppression en sélectionnant Activer, qui est situé directement sous Supprimer Protection: Désactiver. Cela empêchera votre cluster d'être supprimé. Afin de désactiver la protection, sélectionnez Désactiver. Les clusters sont créés par défaut avec la fonction de protection de suppression désactivée.

La vérification

- Dans la page Aperçu de votre cluster, vous pouvez suivre l'avancement de l'installation. Les journaux d'installation sont affichés sur la même page. Le cluster est prêt lorsque l'état dans la section Détails de la page est listé comme prêt.

1.3. RESSOURCES SUPPLÉMENTAIRES

- Afin d'obtenir des informations sur la configuration d'un proxy avec OpenShift Dedicated, consultez Configurer un proxy à l'échelle du cluster.
- En ce qui concerne les stratégies de contrôle de service AWS requises pour les déploiements CCS, consultez la politique de contrôle du service minimum (SCP).
- En ce qui concerne le stockage persistant d'OpenShift Dedicated, consultez la section Stockage dans la définition du service dédié OpenShift.
- En ce qui concerne les équilibreurs de charge pour OpenShift Dedicated, consultez la section Balanceurs de charge dans la définition du service dédié OpenShift.
- Consultez la définition du service de cryptage etcd pour plus d'informations sur le chiffrement etc.
- En ce qui concerne les dates de fin de vie pour les versions dédiées à OpenShift, consultez le cycle de vie de la mise à jour de OpenShift Dedicated.
- Afin d'obtenir des informations sur les exigences relatives aux groupes de sécurité supplémentaires personnalisés, consultez les groupes de sécurité personnalisés supplémentaires.
- Afin d'obtenir des informations sur la configuration des fournisseurs d'identité, consultez Configuring Identity Provider.
- Afin d'obtenir de l'information sur la révocation des privilèges de cluster, consultez les privilèges Revoking et l'accès à un cluster dédié OpenShift.

CHAPITRE 2. LA SUPPRESSION D'UN CLUSTER DÉDIÉ OPENSHIFT SUR AWS

En tant que propriétaire de clusters, vous pouvez supprimer vos clusters dédiés OpenShift.

2.1. LA SUPPRESSION DE VOTRE CLUSTER

Dans Red Hat OpenShift Cluster Manager, vous pouvez supprimer votre cluster OpenShift Dedicated.

Conditions préalables

- Connectez-vous à OpenShift Cluster Manager.
- Création d'un cluster OpenShift dédié.

Procédure

1. À partir d'OpenShift Cluster Manager, cliquez sur le cluster que vous souhaitez supprimer.
2. Choisissez Supprimer le cluster dans le menu déroulant Actions.
3. Entrez le nom du cluster en gras, puis cliquez sur Supprimer. La suppression de cluster se produit automatiquement.