OpenShift Container Platform 4.12

Notes de mise à jour

Aperçu des nouveautés et des changements apportés par cette version d'OpenShift Container Platform

Last Updated: 2023-05-02

OpenShift Container Platform 4.12 Notes de mise à jour

Aperçu des nouveautés et des changements apportés par cette version d'OpenShift Container Platform

Notice légale

Résumé

Les notes de version d'OpenShift Container Platform résument toutes les nouvelles fonctionnalités et améliorations, les changements techniques notables, les corrections majeures par rapport à la version précédente et tous les bogues connus au moment de la disponibilité générale.

Table des matières

CHAPITRE 1. NOTES DE VERSION DE OPENSHIFT CONTAINER PLATFORM 4.12 3
1.1. À PROPOS DE CETTE VERSION 3
1.2. PRISE EN CHARGE ET COMPATIBILITÉ DES COMPOSANTS EN COUCHES ET DÉPENDANTS D'OPENSHIFT CONTAINER PLATFORM 3
1.3. NOUVELLES FONCTIONNALITÉS ET AMÉLIORATIONS 3
1.4. CHANGEMENTS TECHNIQUES NOTABLES 39
1.5. FONCTIONNALITÉS OBSOLÈTES ET SUPPRIMÉES 41
1.6. BUG FIXES 48
1.7. CARACTÉRISTIQUES DE L'APERÇU TECHNOLOGIQUE 66
1.8. PROBLÈMES CONNUS 77
1.9. MISES À JOUR ASYNCHRONES DE L'ERRATA 85

CHAPITRE 1. NOTES DE VERSION DE OPENSHIFT CONTAINER PLATFORM 4.12

Red Hat OpenShift Container Platform offre aux développeurs et aux organisations informatiques une plateforme d'application cloud hybride pour le déploiement d'applications nouvelles et existantes sur des ressources sécurisées et évolutives, avec un minimum de configuration et de frais de gestion. OpenShift Container Platform prend en charge une large sélection de langages de programmation et de frameworks, tels que Java, JavaScript, Python, Ruby et PHP.

Construite sur Red Hat Enterprise Linux (RHEL) et Kubernetes, OpenShift Container Platform fournit un système d'exploitation multitenant plus sûr et plus évolutif pour les applications d'entreprise d'aujourd'hui, tout en offrant des runtimes et des bibliothèques d'applications intégrées. OpenShift Container Platform permet aux organisations de répondre aux exigences en matière de sécurité, de confidentialité, de conformité et de gouvernance.

1.1. À PROPOS DE CETTE VERSION

OpenShift Container Platform(RHSA-2022:7399) est désormais disponible. Cette version utilise Kubernetes 1.25 avec le runtime CRI-O. Les nouvelles fonctionnalités, les changements et les problèmes connus qui concernent OpenShift Container Platform 4.12 sont inclus dans cette rubrique.

Les clusters OpenShift Container Platform 4.12 sont disponibles sur https://console.redhat.com/openshift. Avec l'application Red Hat OpenShift Cluster Manager pour OpenShift Container Platform, vous pouvez déployer des clusters OpenShift dans des environnements sur site ou dans le cloud.

OpenShift Container Platform 4.12 est prise en charge sur Red Hat Enterprise Linux (RHEL) 8.6 ainsi que sur Red Hat Enterprise Linux CoreOS (RHCOS) 4.12.

Vous devez utiliser des machines RHCOS pour le plan de contrôle, et vous pouvez utiliser RHCOS ou RHEL pour les machines de calcul.

À partir d'OpenShift Container Platform 4.12, une phase supplémentaire de six mois d'Extended Update Support (EUS) sur les versions paires de 18 mois à deux ans. Pour plus d'informations, consultez la politique de cycle de vie de Red Hat OpenShift Container Platform .

OpenShift Container Platform 4.8 est une version Extended Update Support (EUS). Plus d'informations sur Red Hat OpenShift EUS sont disponibles dans OpenShift Life Cycle et OpenShift EUS Overview.

Le support de maintenance se termine pour la version 4.8 en janvier 2023 et passe à la phase de vie étendue. Pour plus d'informations, consultez la politique de cycle de vie de Red Hat OpenShift Container Platform.

1.2. PRISE EN CHARGE ET COMPATIBILITÉ DES COMPOSANTS EN COUCHES ET DÉPENDANTS D'OPENSHIFT CONTAINER PLATFORM

L'étendue du support pour les composants en couches et dépendants d'OpenShift Container Platform change indépendamment de la version d'OpenShift Container Platform. Pour déterminer l'état actuel de l'assistance et la compatibilité d'un module complémentaire, reportez-vous à ses notes de version. Pour plus d'informations, consultez la politique de cycle de vie de Red Hat OpenShift Container Platform .

1.3. NOUVELLES FONCTIONNALITÉS ET AMÉLIORATIONS

Cette version apporte des améliorations concernant les composants et concepts suivants.

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. Les consoles par défaut pour les nouveaux clusters sont désormais déterminées par la plateforme d'installation

Les nœuds Red Hat Enterprise Linux CoreOS (RHCOS) installés à partir d'une image de démarrage OpenShift Container Platform 4.12 utilisent désormais une console par défaut spécifique à la plateforme. Les consoles par défaut sur les plateformes cloud correspondent aux consoles système spécifiques attendues par ce fournisseur de cloud. Les images VMware et OpenStack utilisent désormais une console graphique principale et une console série secondaire. Les autres installations bare metal n'utilisent plus que la console graphique par défaut et n'activent pas de console série. Les installations réalisées à l'aide de **coreos-installer** peuvent remplacer les valeurs par défaut existantes et activer la console série.

Les nœuds existants ne sont pas concernés. Les nouveaux nœuds des clusters existants ne sont pas susceptibles d'être affectés car ils sont généralement installés à partir de l'image de démarrage utilisée à l'origine pour l'installation du cluster.

Pour plus d'informations sur l'activation de la console série, voir la documentation suivante :

- Configuration par défaut de la console .
- Modification d'une image ISO d'installation en direct pour activer la console série .
- Modifier un environnement PXE d'installation en direct pour activer la console série .

1.3.1.2. IBM Secure Execution sur IBM zSystems et LinuxONE (aperçu technologique)

OpenShift Container Platform prend désormais en charge la configuration des nœuds Red Hat Enterprise Linux CoreOS (RHCOS) pour IBM Secure Execution sur IBM zSystems et LinuxONE (architecture s390x) en tant que fonctionnalité Technology Preview. IBM Secure Execution est une amélioration matérielle qui protège les limites de la mémoire pour les invités KVM. IBM Secure Execution fournit le plus haut niveau d'isolation et de sécurité pour les charges de travail en cluster, et vous pouvez l'activer en utilisant une image de démarrage QCOW2 prête pour IBM Secure Execution.

Pour utiliser IBM Secure Execution, vous devez disposer de clés hôte pour votre (vos) machine(s) hôte(s) et les spécifier dans votre fichier de configuration Ignition. IBM Secure Execution chiffre automatiquement vos volumes de démarrage à l'aide du chiffrement LUKS.

Pour plus d'informations, voir Installation de RHCOS à l'aide d'IBM Secure Execution .

1.3.1.3. RHCOS utilise désormais RHEL 8.6

RHCOS utilise désormais les paquets Red Hat Enterprise Linux (RHEL) 8.6 dans OpenShift Container Platform 4.12. Cela vous permet de bénéficier des derniers correctifs, fonctionnalités et améliorations, ainsi que des dernières mises à jour de la prise en charge matérielle et des pilotes. OpenShift Container Platform 4.10 est une version Extended Update Support (EUS) qui continuera à utiliser les paquets RHEL 8.4 EUS pendant toute la durée de son cycle de vie.

1.3.2. Installation et mise à niveau

1.3.2.1. Assisted Installer SaaS fournit un support d'intégration de plateforme pour Nutanix

Assisted Installer SaaS sur console.redhat.com prend en charge l'installation d'OpenShift Container Platform sur la plateforme Nutanix avec l'intégration Machine API en utilisant soit l'interface utilisateur

Assisted Installer, soit l'API REST. L'intégration permet aux utilisateurs de Nutanix Prism de gérer leur infrastructure à partir d'une interface unique, et permet l'auto-scaling. Il y a quelques étapes d'installation supplémentaires pour permettre l'intégration de Nutanix avec Assisted Installer SaaS. Voir la documentation Assisted Installer pour plus de détails.

1.3.2.2. Spécifier le type d'équilibreur de charge dans AWS lors de l'installation

À partir d'OpenShift Container Platform 4.12, vous pouvez spécifier soit Network Load Balancer (NLB) soit Classic comme type d'équilibreur de charge persistant dans AWS lors de l'installation. Par la suite, si un contrôleur d'entrée est supprimé, le type d'équilibreur de charge persiste avec le lbType configuré lors de l'installation.

Pour plus d'informations, voir Installation d'un cluster sur AWS avec personnalisation du réseau .

1.3.2.3. Étendre les nœuds de travail à la périphérie d'AWS lors de l'installation dans un nuage privé virtuel (VPC) existant avec des sous-réseaux de zone locale.

Avec cette mise à jour, vous pouvez installer OpenShift Container Platform sur un VPC existant avec une infrastructure fournie par l'installateur, en étendant les nœuds de travail aux sous-réseaux des zones locales. Le programme d'installation fournira des nœuds de travail à la périphérie du réseau AWS qui sont spécifiquement désignés pour les applications utilisateur en utilisant les taches NoSchedule. Les applications déployées dans les zones locales offrent une faible latence aux utilisateurs finaux.

Pour plus d'informations, voir Installation d'un cluster à l'aide des zones locales AWS .

1.3.2.4. L'offre de Google Cloud Platform Marketplace

OpenShift Container Platform est désormais disponible sur le GCP Marketplace. L'installation d'OpenShift Container Platform avec une image GCP Marketplace vous permet de créer des déploiements de clusters autogérés qui sont facturés sur la base d'un paiement à l'utilisation (à l'heure, par cœur) via GCP, tout en continuant à être pris en charge directement par Red Hat.

Pour plus d'informations sur l'installation à l'aide d'une infrastructure fournie par l'installateur, voir Utilisation d'une image GCP Marketplace . Pour plus d'informations sur l'installation à l'aide d'une infrastructure fournie par l'utilisateur, voir Création de machines de travail supplémentaires dans GCP .

1.3.2.5. Dépannage des échecs de démarrage lors de l'installation sur GCP et Azure

Le programme d'installation recueille désormais les journaux de la console série des hôtes bootstrap et control plane sur GCP et Azure. Ces données sont ajoutées au paquet de logs bootstrap standard.

Pour plus d'informations, voir Résolution des problèmes d'installation.

1.3.2.6. Disponibilité générale d'IBM Cloud VPC

IBM Cloud VPC est désormais disponible dans OpenShift Container Platform 4.12.

Pour plus d'informations sur l'installation d'un cluster, voir Préparation de l'installation sur IBM Cloud VPC.

1.3.2.7. Confirmation requise de l'administrateur lors de la mise à niveau d'OpenShift Container Platform 4.11 vers 4.12

OpenShift Container Platform 4.12 utilise Kubernetes 1.25, qui a supprimé plusieurs API obsolètes.

Un administrateur de cluster doit fournir un accusé de réception manuel avant que le cluster puisse être mis à niveau d'OpenShift Container Platform 4.11 à 4.12. Cela permet d'éviter les problèmes après la mise à niveau vers OpenShift Container Platform 4.12, lorsque les API qui ont été supprimées sont encore utilisées par des charges de travail, des outils ou d'autres composants fonctionnant sur le cluster ou interagissant avec lui. Les administrateurs doivent évaluer leur cluster pour déterminer si des API utilisées seront supprimées et migrer les composants concernés pour qu'ils utilisent la nouvelle version appropriée de l'API. Une fois cette opération effectuée, l'administrateur peut fournir l'accusé de réception de l'administrateur.

Tous les clusters OpenShift Container Platform 4.11 nécessitent cette reconnaissance de l'administrateur avant de pouvoir être mis à niveau vers OpenShift Container Platform 4.12.

Pour plus d'informations, voir Préparation de la mise à jour vers OpenShift Container Platform 4.12 .

1.3.2.8. Activation d'un jeu de fonctionnalités lors de l'installation d'un cluster

À partir d'OpenShift Container Platform 4.12, vous pouvez activer un ensemble de fonctionnalités dans le cadre du processus d'installation. Un ensemble de fonctionnalités est une collection de fonctionnalités d'OpenShift Container Platform qui ne sont pas activées par défaut.

Pour plus d'informations sur l'activation d'un ensemble de fonctionnalités lors de l'installation, voir Activation des fonctionnalités d'OpenShift Container Platform à l'aide des portes de fonctionnalités .

1.3.2.9. OpenShift Container Platform sur ARM

OpenShift Container Platform 4.12 est désormais pris en charge sur les infrastructures Azure provisionnées par l'installateur et basées sur l'architecture ARM. Les processeurs AWS Graviton 3 sont désormais disponibles pour les déploiements de clusters et sont également pris en charge par OpenShift Container Platform 4.11. Pour plus d'informations sur la disponibilité des instances et la documentation d'installation, voir Méthodes d'installation prises en charge pour différentes plateformes

1.3.2.10. Mise en miroir d'images d'opérateurs de catalogues basés sur des fichiers au format OCI avec le plugin CLI oc-mirror (aperçu technologique)

L'utilisation du plugin CLI oc-mirror pour mettre en miroir des images d'opérateurs de catalogue basées sur des fichiers au format OCI au lieu du format Docker v2 est désormais disponible en tant qu'aperçu technologique.

Pour plus d'informations, voir Mise en miroir d'images d'opérateurs de catalogues basés sur des fichiers au format OCI.

1.3.2.11. Installer un cluster OpenShift Container Platform sur GCP dans un VPC partagé (Technology Preview)

Dans OpenShift Container Platform 4.12, vous pouvez installer un cluster sur GCP dans un VPC partagé en tant qu'aperçu technologique. Dans cette méthode d'installation, le cluster est configuré pour utiliser un VPC d'un projet GCP différent. Un VPC partagé permet à une organisation de connecter les ressources de plusieurs projets à un réseau VPC commun. Vous pouvez communiquer au sein de l'organisation de manière sécurisée et efficace en utilisant les adresses IP internes de ce réseau.

Pour plus d'informations, voir Installer un cluster sur GCP dans un VPC partagé .

1.3.2.12. Adresse IP cohérente pour l'API Ironic dans les installations bare-metal sans réseau de provisionnement

Avec cette mise à jour, dans les installations bare-metal sans réseau de provisionnement, le service Ironic API est accessible via un serveur proxy. Ce serveur proxy fournit une adresse IP cohérente pour le service Ironic API. Si le pod Metal3 qui contient **metal3-ironic** est déplacé vers un autre pod, l'adresse proxy cohérente assure une communication constante avec le service Ironic API.

1.3.2.13. Installer OpenShift Container Platform sur GCP en utilisant l'authentification du compte de service

Dans OpenShift Container Platform 4.12, vous pouvez installer un cluster sur GCP en utilisant une machine virtuelle à laquelle est attaché un compte de service. Cela vous permet d'effectuer une installation sans avoir besoin d'utiliser un fichier JSON de compte de service.

Pour plus d'informations, voir Création d'un compte de service GCP .

1.3.2.14. **propagateUserTags** paramètre pour les ressources AWS fournies par le cluster OpenShift Container Platform

Dans OpenShift Container Platform 4.12, le paramètre **propagateUserTags** est un drapeau qui indique aux opérateurs en cluster d'inclure les balises utilisateur spécifiées dans les balises des ressources AWS que les opérateurs créent.

Pour plus d'informations, voir Paramètres de configuration optionnels.

1.3.2.15. Les images de conteneurs ironiques utilisent l'image de base de RHEL 9

Dans les versions antérieures d'OpenShift Container Platform, les images de conteneurs Ironic utilisaient Red Hat Enterprise Linux (RHEL) 8 comme image de base. À partir de la version 4.12 d'OpenShift Container Platform, les images de conteneurs Ironic utilisent RHEL 9 comme image de base. L'image de base RHEL 9 ajoute la prise en charge de CentOS Stream 9, Python 3.8 et Python 3.9 dans les composants Ironic.

Pour plus d'informations sur le service de provisionnement Ironic, voir Déployer des clusters provisionnés par l'installateur sur du métal nu.

1.3.2.16. Mises à jour de la configuration des fournisseurs de cloud pour les clusters fonctionnant sous RHOSP

Dans OpenShift Container Platform 4.12, les clusters qui s'exécutent sur Red Hat OpenStack Platform (RHOSP) passent du fournisseur de cloud OpenStack hérité au Cloud Controller Manager (CCM) externe. Ce changement fait suite à l'évolution de Kubernetes, qui est passé de fournisseurs de clouds traditionnels à des fournisseurs de clouds externes mis en œuvre à l'aide du gestionnaire de contrôleur de clouds.

Pour plus d'informations, voir OpenStack Cloud Controller Manager.

1.3.2.17. Prise en charge des charges de travail sur les nœuds de calcul distribués RHOSP

Dans OpenShift Container Platform 4.12, les déploiements de clusters vers les clouds Red Hat OpenStack Platform (RHOSP) qui ont une architecture de nœuds de calcul distribués (DCN) ont été validés. Une architecture de référence pour ces déploiements est à venir.

Pour un bref aperçu de ce type de déploiement, consultez l'article de blog Déployer votre cluster à la périphérie avec OpenStack.

1.3.2.18. OpenShift Container Platform sur AWS Outposts (aperçu technologique)

OpenShift Container Platform 4.12 est maintenant supporté sur la plateforme AWS Outposts en tant que Technology Preview. Avec AWS Outposts, vous pouvez déployer des nœuds de travailleurs en périphérie, tout en utilisant AWS Regions pour les nœuds du plan de contrôle. Pour plus d'informations, voir Installer un cluster sur AWS avec des travailleurs distants sur AWS Outposts .

1.3.2.19. L'installation basée sur un agent prend en charge deux modes d'entrée

L'installation basée sur l'agent prend en charge deux modes de saisie :

- **install-config.yaml** fichier
- **agent-config.yaml** fichier

En option

- Manifestes ZTP (Zero Touch Provisioning)

Avec le mode préféré, vous pouvez configurer le fichier **install-config.yaml** et spécifier les paramètres spécifiques à l'agent dans le fichier **agent-config.yaml**. Pour plus d'informations, voir À propos de l'installateur OpenShift Container Platform basé sur l'agent.

1.3.2.20. L'installation basée sur un agent prend en charge l'installation des clusters OpenShift Container Platform en mode conforme aux normes FIPS

L'installateur OpenShift Container Platform basé sur un agent prend en charge les clusters OpenShift Container Platform en mode conforme aux normes fédérales de traitement de l'information (FIPS). Vous devez définir la valeur du champ **fips** sur **True** dans le fichier **install-config.yaml**. Pour plus d'informations, voir À propos de la conformité FIPS .

1.3.2.21. Déployer un cluster OpenShift Container Platform basé sur un agent dans un environnement déconnecté

Vous pouvez effectuer une installation basée sur l'agent dans un environnement déconnecté. Pour créer une image utilisée dans un environnement déconnecté, la section **imageContentSources** du fichier **install-config.yaml** doit contenir les informations sur le miroir ou le fichier **registries.conf** si vous utilisez des manifestes ZTP. Les paramètres de configuration à utiliser dans ces fichiers sont fournis par la commande **oc adm release mirror** ou **oc mirror**. Pour plus d'informations, voir Comprendre la mise en miroir d'une installation déconnectée.

1.3.2.22. L'installation basée sur un agent prend en charge les réseaux à une ou deux piles

Vous pouvez créer l'image ISO de l'agent avec les configurations d'adresses IP suivantes :

- IPv4
- IPv6
- IPv4 and IPv6 in parallel (dual-stack)

NOTE

IPv6 is supported only on bare metal platforms.

Pour plus d'informations, voir Clusters de piles IP simples et doubles .

1.3.2.23. Le cluster OpenShift Container Platform déployé par l'agent peut être utilisé en tant que hub cluster

Vous pouvez installer le moteur multicluster pour Kubernetes Operator et déployer un hub cluster avec l'installateur OpenShift Container Platform basé sur l'agent. Pour plus d'informations, voir Préparation d'un cluster installé à l'aide d'un agent pour le moteur multicluster de Kubernetes Operator.

1.3.2.24. L'installation basée sur un agent effectue des validations d'installation

L'installateur de la plateforme OpenShift Container basé sur un agent effectue des validations sur :

- Génération de l'image d'installation : La validité et la compatibilité des manifestes fournis par l'utilisateur sont vérifiées.
- Installation : Le service d'installation vérifie le matériel disponible pour l'installation et émet des événements de validation qui peuvent être récupérés à l'aide des sous-commandes **openshift-install agent wait-for**.

Pour plus d'informations, voir les validations d'installation.

1.3.2.25. Configurer un réseau statique dans une installation basée sur un agent

Avec l'installateur OpenShift Container Platform basé sur l'agent, vous pouvez configurer des adresses IP statiques pour IPv4, IPv6, ou dual-stack (à la fois IPv4 et IPv6) pour tous les hôtes avant de créer l'image ISO de l'agent. Vous pouvez ajouter les adresses statiques à la section **hosts** du fichier **agent-config.yaml** ou au fichier **NMStateConfig.yaml** si vous utilisez les manifestes ZTP. Notez que la configuration des adresses doit suivre les règles de syntaxe pour NMState comme décrit dans les exemples d'état de NMState .

NOTE

IPv6 is supported only on bare metal platforms.

Pour plus d'informations, voir À propos de la mise en réseau .

1.3.2.26. Déploiement automatisé basé sur le CLI dans une installation basée sur un agent

Avec l'installateur OpenShift Container Platform basé sur un agent, vous pouvez définir vos configurations d'installation, générer une ISO pour tous les nœuds, puis effectuer une installation sans surveillance en démarrant les systèmes cibles avec l'ISO générée. Pour plus d'informations, voir Installation d'un cluster OpenShift Container Platform avec l'installateur OpenShift Container Platform basé sur un agent.

1.3.2.27. L'installation basée sur un agent permet une configuration spécifique de l'hôte au moment de l'installation

Vous pouvez configurer le nom d'hôte, la configuration du réseau au format NMState, les indices du périphérique racine et le rôle dans une installation basée sur un agent.

Pour plus d'informations, voir À propos des conseils sur le périphérique racine .

1.3.2.28. L'installation basée sur un agent prend en charge le protocole DHCP

Avec l'installateur OpenShift Container Platform basé sur un agent, vous pouvez déployer dans des environnements où vous comptez sur DHCP pour configurer le réseau pour tous les nœuds, à condition que vous connaissiez l'IP qu'au moins l'un des systèmes recevra. Cette IP est nécessaire pour que tous les nœuds l'utilisent comme point de rencontre. Pour plus d'informations, voir DHCP.

1.3.3. Configuration post-installation

1.3.3.1. Installation du pilote CSI sur les clusters vSphere

Pour installer un pilote CSI sur un cluster fonctionnant sous vSphere, les conditions suivantes doivent être remplies :

- Virtual machines of hardware version 15 or later
- VMware vSphere version 7.0 Update 2 ou ultérieure, jusqu'à la version 8 incluse. vSphere 8 n'est pas pris en charge.
- vCenter 7.0 Update 2 ou ultérieur, jusqu'à la version 8 incluse. vCenter 8 n'est pas pris en charge.
- No third-party CSI driver already installed in the cluster
  Si un pilote CSI tiers est présent dans le cluster, OpenShift Container Platform ne l'écrase pas.

Les composants dont les versions sont antérieures à celles mentionnées ci-dessus sont toujours pris en charge, mais sont obsolètes. Ces versions sont toujours entièrement prises en charge, mais la version 4.12 d'OpenShift Container Platform nécessite la version 15 ou ultérieure du matériel virtuel vSphere. Pour plus d'informations, voir Fonctionnalités obsolètes et supprimées.

Le non-respect des exigences ci-dessus empêche la mise à niveau d'OpenShift Container Platform vers OpenShift Container Platform 4.13 ou une version ultérieure.

1.3.3.2. Capacités des grappes d'entreprises

Les nouvelles capacités suivantes ont été ajoutées :

- Console
- Perspectives
- Stockage
- CSISnapshot

Un nouvel ensemble prédéfini de capacités de cluster, **v4.12**, a été ajouté. Il comprend toutes les fonctionnalités de **v4.11**, ainsi que les nouvelles fonctionnalités ajoutées dans la version actuelle.

Pour plus d'informations, voir le lien : Activation des capacités des clusters.

1.3.3.3. OpenShift Container Platform avec des machines de calcul multi-architectures (Technology Preview)

OpenShift Container Platform 4.12 avec des machines de calcul multi-architecture prend désormais en charge les images listées dans le manifeste sur les flux d'images. Pour plus d'informations sur les images de la liste de manifeste, voir Configuration des machines de calcul multi-architecture sur un cluster OpenShift Container Platform.

Sur un cluster avec des machines de calcul multi-architectures, vous pouvez désormais remplacer l'affinité de nœud dans l'objet **Subscription** de l'opérateur pour planifier des pods sur des nœuds avec des architectures prises en charge par l'opérateur. Pour plus d'informations, voir Utilisation de l'affinité de nœud pour contrôler l'emplacement d'installation d'un opérateur.

1.3.4. Console web

1.3.4.1. Le point de vue de l'administrateur

Cette version comporte plusieurs mises à jour de la perspective **Administrator** de la console web.

- La console web d'OpenShift Container Platform affiche un **ConsoleNotification** si le cluster est en train d'être mis à niveau. Une fois la mise à niveau effectuée, la notification est supprimée.
- A ***restart rollout*** pour la ressource **Deployment** et une option ***retry rollouts*** pour la ressource **DeploymentConfig** sont disponibles dans les menus **Action** et **Kebab**.

1.3.4.1.1. Machines de calcul multi-architecture sur la console web de OpenShift Container Platform

L'application **console-operator** analyse maintenant tous les nœuds et construit un ensemble de tous les types d'architecture sur lesquels les nœuds du cluster fonctionnent et le transmet à l'application **console-config.yaml**. L'application **console-operator** peut être installée sur des nœuds dont les architectures ont les valeurs **amd64**, **arm64**, **ppc64le**, ou **s390x**.

Pour plus d'informations sur les machines de calcul à architecture multiple, voir Configurer une machine de calcul à architecture multiple sur un cluster OpenShift.

1.3.4.1.2. Le plugin dynamique est généralement disponible

Cette fonctionnalité a déjà été introduite en tant qu'aperçu technologique dans OpenShift Container Platform 4.10 et est maintenant disponible de manière générale dans OpenShift Container Platform 4.12. Avec le plugin dynamique, vous pouvez construire des expériences utilisateur uniques et de haute qualité nativement dans la console web. Vous pouvez :

- Ajouter des pages personnalisées.
- Ajouter des perspectives au-delà de l'administrateur et du développeur.
- Ajouter des éléments de navigation.
- Ajouter des onglets et des actions aux pages de ressources.
- Étendre les pages existantes.

Pour plus d'informations, voir Vue d'ensemble des plugins dynamiques.

1.3.4.2. Le point de vue du développeur

Cette version comporte plusieurs mises à jour de la perspective **Developer** de la console web. Vous pouvez effectuer les actions suivantes :

- Exportez votre application au format ZIP vers un autre projet ou cluster en utilisant l'option **Export application** sur la page **Add**.

- Créer un puits d'événements Kafka pour recevoir des événements d'une source particulière et les envoyer à un sujet Kafka.
- Définissez la préférence de ressource par défaut dans la page **User Preferences → Applications**. En outre, vous pouvez sélectionner un autre type de ressource par défaut.
    - Vous pouvez également définir un autre type de ressource à partir de la page **Add** en cliquant sur **Import from Git → Advanced options → Resource type** et en sélectionnant la ressource dans la liste déroulante.
- Rendre visible l'adresse IP du nœud **status.HostIP** pour les pods dans l'onglet **Details** de la page **Pods**.
- L'étiquette d'alerte relative au quota de ressources est affichée sur les pages **Topology** et **Add** chaque fois qu'une ressource atteint le quota. Le lien de l'étiquette d'alerte vous renvoie à la page de la liste **ResourceQuotas**. Si le lien de l'étiquette d'alerte concerne un seul quota de ressources, il vous renvoie à la page **ResourceQuota details**.
    - Pour les déploiements, une alerte s'affiche dans le panneau latéral du nœud de topologie si des erreurs sont associées aux quotas de ressources. En outre, une bordure jaune s'affiche autour des nœuds de déploiement lorsque le quota de ressources est dépassé.
- Personnalisez les éléments suivants de l'interface utilisateur à l'aide du formulaire ou de la vue YAML :
    - Perspectives visibles par les utilisateurs
    - Démarrage rapide visible par les utilisateurs
    - Rôles des clusters accessibles à un projet
    - Actions visibles sur la page **Add**
    - Les types d'articles dans le **Developer Catalog**
- Consultez les mises à jour communes de la visualisation des pages **Pipeline details** et **PipelineRun details** en effectuant les actions suivantes :
    - Utilisez la molette de la souris pour modifier le facteur de zoom.
    - Survolez les tâches pour en voir les détails.
    - Les icônes standard permettent d'effectuer un zoom avant, un zoom arrière, de s'adapter à l'écran et de réinitialiser l'affichage.
    - **PipelineRun details** uniquement : À certains facteurs de zoom, la couleur d'arrière-plan des tâches change pour indiquer l'état d'erreur ou d'avertissement. Vous pouvez survoler l'insigne des tâches pour voir le nombre total de tâches et les tâches terminées.

1.3.4.2.1. Amélioration de la page de pilotage

Dans OpenShift Container Platform 4.12, vous pouvez effectuer les opérations suivantes à partir de la page **Helm**:

- Créez des versions et des dépôts Helm en utilisant le bouton **Create**.
- Créer, mettre à jour ou supprimer un référentiel graphique Helm à l'échelle d'un cluster ou d'un espace de noms.

- Voir la liste des référentiels graphiques Helm existants avec leur portée dans la page **Repositories**.
- Voir la nouvelle version de Helm sur la page **Helm Releases**.

1.3.4.2.2. Correspondants négatifs dans l'Alertmanager

Avec cette mise à jour, Alertmanager supporte désormais l'option **Negative matcher**. En utilisant **Negative matcher**, vous pouvez mettre à jour le **Label value** en le remplaçant par une option "Pas égal". La case à cocher de la correspondance négative transforme **=** (valeur égale) en **!=** (valeur non égale) et transforme **=~** (valeur correspondant à une expression régulière) en **!~**(valeur ne correspondant pas à une expression régulière). En outre, l'étiquette de la case à cocher **Use RegEx** est renommée **RegEx**.

1.3.5. OpenShift CLI (oc)

1.3.5.1. Gérer les plugins pour la CLI d'OpenShift avec Krew (Technology Preview)

L'utilisation de Krew pour installer et gérer des plugins pour l'OpenShift CLI (**oc**) est maintenant disponible en tant que Technology Preview.

Pour plus d'informations, voir Gérer les plugins CLI avec Krew .

1.3.6. IBM Z et LinuxONE

Avec cette version, IBM Z et LinuxONE sont désormais compatibles avec OpenShift Container Platform 4.12. L'installation peut être effectuée avec z/VM ou RHEL KVM. Pour les instructions d'installation, voir la documentation suivante :

- Installation d'un cluster avec z/VM sur IBM Z et LinuxONE
- Installation d'un cluster avec z/VM sur IBM Z et LinuxONE dans un réseau restreint
- Installation d'un cluster avec RHEL KVM sur IBM Z et LinuxONE
- Installation d'un cluster avec RHEL KVM sur IBM Z et LinuxONE dans un réseau restreint

Améliorations notables
Les nouvelles fonctionnalités suivantes sont prises en charge sur IBM Z et LinuxONE avec OpenShift Container Platform 4.12 :

- Emplois Cron
- Déscheduler
- IPv6
- PodDisruptionBudget
- Profils du planificateur
- Protocole de transmission de contrôle de flux (SCTP)

IBM Secure Execution (aperçu technologique)
OpenShift Container Platform prend désormais en charge la configuration des nœuds Red Hat Enterprise Linux CoreOS (RHCOS) pour IBM Secure Execution sur IBM zSystems et LinuxONE (architecture s390x) en tant que fonctionnalité d'aperçu technologique.

Pour les instructions d'installation, voir la documentation suivante :

- Installation de RHCOS à l'aide d'IBM Secure Execution

Caractéristiques prises en charge
Les fonctionnalités suivantes sont également prises en charge sur IBM Z et LinuxONE :

- Actuellement, les opérateurs suivants sont pris en charge :
  - Opérateur de journalisation des clusters
  - Opérateur de conformité
  - Opérateur d'intégrité des fichiers
  - Opérateur de stockage local
  - Opérateur NFD
  - NMState Opérateur
  - Opérateur OpenShift Elasticsearch
  - Opérateur de liaison de service
  - Opérateur de détartreur de nacelles verticales
- Les plugins CNI de Multus suivants sont pris en charge :
  - Pont
  - Appareil hôte
  - IPAM
  - IPVLAN
- Autres fournisseurs d'authentification
- Découverte automatique des appareils avec l'opérateur de stockage local
- Volumes CSI
  - Clonage
  - Expansion
  - Aperçu
- Chiffrement des données stockées dans etcd
- Tige
- Mise à l'échelle horizontale des pods
- Suivi des projets définis par l'utilisateur
- Multipathing

- Opérateur API
- Plugins OC CLI
- Stockage persistant à l'aide d'iSCSI
- Stockage persistant à l'aide de volumes locaux (Opérateur de stockage local)
- Stockage persistant à l'aide de hostPath
- Stockage persistant à l'aide de Fibre Channel
- Stockage persistant à l'aide de blocs bruts
- OVN-Kubernetes, y compris le cryptage IPsec
- Prise en charge de plusieurs interfaces réseau
- Prise en charge d'un cluster à trois nœuds
- périphériques FBA émulés z/VM sur disques SCSI
- dispositif bloc FCP 4K

Ces fonctionnalités sont disponibles uniquement pour OpenShift Container Platform on IBM Z et LinuxONE pour la version 4.12 :

- HyperPAV activé sur IBM Z et LinuxONE pour les machines virtuelles pour le stockage ECKD attaché à FICON

Restrictions
Les restrictions suivantes ont un impact sur OpenShift Container Platform sur IBM Z et LinuxONE :

- Réparation automatique des machines endommagées avec contrôle de l'état des machines
- Red Hat OpenShift Local
- Contrôle de l'overcommit et gestion de la densité des conteneurs sur les nœuds
- NVMe
- OpenShift Metering
- Virtualisation OpenShift
- Matériel pour le protocole de temps de précision (PTP)
- Chiffrement des disques en mode Tang lors du déploiement d'OpenShift Container Platform
- Les nœuds de calcul doivent fonctionner sous Red Hat Enterprise Linux CoreOS (RHCOS)
- Le stockage partagé persistant doit être approvisionné en utilisant Red Hat OpenShift Data Foundation ou d'autres protocoles de stockage pris en charge
- Le stockage persistant non partagé doit être approvisionné en utilisant le stockage local, comme iSCSI, FC, ou en utilisant LSO avec DASD, FCP, ou EDEV/FBA

1.3.7. IBM Power

Avec cette version, IBM Power est désormais compatible avec OpenShift Container Platform 4.12. Pour les instructions d'installation, voir la documentation suivante :

- Installation d'un cluster sur IBM Power
- Installation d'un cluster sur IBM Power dans un réseau restreint

Améliorations notables
Les nouvelles fonctionnalités suivantes sont prises en charge sur IBM Power avec OpenShift Container Platform 4.12 :

- Gestionnaire de contrôleur cloud pour IBM Cloud
- Emplois Cron
- Désceduler
- PodDisruptionBudget
- Profils du planificateur
- Protocole de transmission de contrôle de flux (SCTP)
- Gestionnaire de topologie

Caractéristiques prises en charge
Les fonctionnalités suivantes sont également prises en charge sur IBM Power :

- Actuellement, les opérateurs suivants sont pris en charge :
  - Opérateur de journalisation des clusters
  - Opérateur de conformité
  - Opérateur d'intégrité des fichiers
  - Opérateur de stockage local
  - Opérateur NFD
  - NMState Opérateur
  - Opérateur OpenShift Elasticsearch
  - Opérateur de réseau SR-IOV
  - Opérateur de liaison de service
  - Opérateur de détartreur de nacelles verticales
- Les plugins CNI de Multus suivants sont pris en charge :
  - Pont
  - Appareil hôte

    - IPAM
    - IPVLAN
- Autres fournisseurs d'authentification
- Volumes CSI
    - Clonage
    - Expansion
    - Aperçu
- Chiffrement des données stockées dans etcd
- Tige
- Mise à l'échelle horizontale des pods
- IPv6
- Suivi des projets définis par l'utilisateur
- Multipathing
- Multus SR-IOV
- Opérateur API
- Plugins OC CLI
- OVN-Kubernetes, y compris le cryptage IPsec
- Stockage persistant à l'aide d'iSCSI
- Stockage persistant à l'aide de volumes locaux (Opérateur de stockage local)
- Stockage persistant à l'aide de hostPath
- Stockage persistant à l'aide de Fibre Channel
- Stockage persistant à l'aide de blocs bruts
- Prise en charge de plusieurs interfaces réseau
- Support pour Power10
- Prise en charge d'un cluster à trois nœuds
- prise en charge des disques 4K

Restrictions
Les restrictions suivantes ont un impact sur OpenShift Container Platform on IBM Power :

- Réparation automatique des machines endommagées avec contrôle de l'état des machines
- Red Hat OpenShift Local

- Contrôle de l'overcommit et gestion de la densité des conteneurs sur les nœuds
- OpenShift Metering
- Virtualisation OpenShift
- Matériel pour le protocole de temps de précision (PTP)
- Chiffrement des disques en mode Tang lors du déploiement d'OpenShift Container Platform
- Les nœuds de calcul doivent fonctionner sous Red Hat Enterprise Linux CoreOS (RHCOS)
- Le stockage persistant doit être du type Système de fichiers qui utilise des volumes locaux, Red Hat OpenShift Data Foundation, Network File System (NFS), ou Container Storage Interface (CSI)

1.3.8. Images

Une nouvelle valeur d'importation, **importMode**, a été ajoutée au paramètre **importPolicy** des flux d'images. Les champs suivants sont disponibles pour cette valeur :

- **Legacy Legacy** est la valeur par défaut de . Lorsqu'elle est active, la liste des manifestes est rejetée et un seul sous-manifeste est importé. La plate-forme est choisie dans l'ordre de priorité suivant : **importMode**
    1. Annotations d'étiquettes
    2. Architecture du plan de contrôle
    3. Linux/AMD64
    4. Le premier manifeste de la liste
- **PreserveOriginal**: Lorsqu'il est actif, le manifeste original est préservé. Pour les listes de manifestes, la liste de manifestes et tous ses sous-manifestes sont importés.

1.3.9. Sécurité et conformité

1.3.9.1. Opérateur de profils de sécurité

L'opérateur de profils de sécurité (SPO) est désormais disponible pour OpenShift Container Platform 4.12 et les versions ultérieures.

Le SPO permet de définir des profils informatiques sécurisés(seccomp) et des profils SELinux en tant que ressources personnalisées, en synchronisant les profils avec chaque nœud d'un espace de noms donné.

Pour plus d'informations, voir Profils de sécurité - Présentation de l'opérateur .

1.3.10. Mise en réseau

1.3.10.1. Prise en charge de l'adressage à double pile pour l'API VIP et l'Ingress VIP

Assisted Installer prend en charge l'installation d'OpenShift Container Platform 4.12 et des versions ultérieures avec un réseau à double pile pour l'API VIP et l'Ingress VIP sur le métal nu uniquement. Cette

prise en charge introduit deux nouveaux paramètres de configuration : **api_vips** et **ingress_vips**, qui peuvent prendre une liste d'adresses IP. Les anciens paramètres, **api_vip** et **ingress_vip**, doivent également être définis dans OpenShift Container Platform 4.12 ; cependant, comme ils ne prennent qu'une seule adresse IP, vous devez définir l'adresse IPv4 lors de la configuration de la mise en réseau à double pile pour l'API VIP et l'Ingress VIP à l'aide des anciens paramètres de configuration **api_vip** et **ingress_vip**.

L'adresse VIP API et l'adresse VIP Ingress doivent appartenir à la famille d'adresses IP primaire lors de l'utilisation d'un réseau à double pile. Actuellement, Red Hat ne prend pas en charge les VIP à double pile ou la mise en réseau à double pile avec IPv6 comme famille d'adresses IP primaire. Cependant, Red Hat prend en charge la mise en réseau à double pile avec IPv4 comme famille d'adresses IP primaire. Par conséquent, vous devez placer les entrées IPv4 avant les entrées IPv6. Pour plus d'informations, consultez la documentation d'Assisted Installer.

1.3.10.2. Red Hat OpenShift Networking

Red Hat OpenShift Networking est un écosystème de fonctionnalités, de plugins et de capacités de mise en réseau avancées qui étendent la mise en réseau de Kubernetes au-delà du plugin CNI de Kubernetes avec les fonctionnalités avancées liées à la mise en réseau dont votre cluster a besoin pour gérer son trafic réseau pour un ou plusieurs clusters hybrides. Cet écosystème de capacités de mise en réseau intègre l'entrée, la sortie, l'équilibrage de charge, le débit haute performance, la sécurité et la gestion du trafic inter- et intra-cluster et fournit un outil d'observabilité basé sur les rôles pour réduire ses complexités naturelles.

Pour plus d'informations, voir À propos de la mise en réseau .

1.3.10.3. OVN-Kubernetes est désormais le plugin réseau par défaut

Lors de l'installation d'un nouveau cluster, le plugin réseau OVN-Kubernetes est le plugin réseau par défaut. Pour toutes les versions antérieures d'OpenShift Container Platform, OpenShift SDN reste le plugin réseau par défaut.

Le plugin réseau OVN-Kubernetes comprend un plus large éventail de fonctionnalités qu'OpenShift SDN, notamment :

- Prise en charge de toutes les fonctionnalités existantes d'OpenShift SDN
- Prise en charge des réseaux IPv6
- Prise en charge de la configuration du cryptage IPsec
- Prise en charge complète de l'API**NetworkPolicy**
- Prise en charge de l'enregistrement d'audit des événements liés à la politique de réseau
- Prise en charge du suivi des flux réseau aux formats NetFlow, sFlow et IPFIX
- Prise en charge des réseaux hybrides pour les conteneurs Windows
- Prise en charge du délestage matériel vers des cartes réseau compatibles

OpenShift Container Platform 4.12 présente également d'énormes améliorations en termes d'échelle, de performances et de stabilité par rapport aux versions précédentes.

Si vous utilisez le plugin réseau OpenShift SDN, notez que :

- Les déploiements existants et futurs utilisant OpenShift SDN continuent d'être pris en charge.

- OpenShift SDN reste la solution par défaut sur les versions d'OpenShift Container Platform antérieures à la version 4.12.
- Depuis OpenShift Container Platform 4.12, OpenShift SDN est une option d'installation prise en charge.
- OpenShift SDN reste figé dans ses fonctionnalités.

Pour plus d'informations sur OVN-Kubernetes, y compris une matrice de comparaison des fonctionnalités avec OpenShift SDN, voir À propos du plugin réseau OVN-Kubernetes.

Pour plus d'informations sur la migration vers OVN-Kubernetes depuis OpenShift SDN, voir Migrations depuis le plugin réseau OpenShift SDN.

1.3.10.4. Opérateur du pare-feu du nœud d'entrée

Cette mise à jour introduit un nouvel opérateur de pare-feu sans état pour les nœuds d'entrée. Vous pouvez désormais configurer des règles de pare-feu au niveau du nœud. Pour plus d'informations, voir Opérateur de pare-feu de nœud d'entrée .

1.3.10.5. Amélioration des mesures de mise en réseau

Les métriques suivantes sont désormais disponibles pour le plugin réseau OVN-Kubernetes :

- **ovn_controller_southbound_database_connected**
- **ovnkube_master_libovsdb_monitors**
- **ovnkube_master_network_programming_duration_seconds**
- **ovnkube_master_network_programming_ovn_duration_seconds**
- **ovnkube_master_egress_routing_via_host**
- **ovs_vswitchd_interface_resets_total**
- **ovs_vswitchd_interface_rx_dropped_total**
- **ovs_vswitchd_interface_tx_dropped_total**
- **ovs_vswitchd_interface_rx_errors_total**
- **ovs_vswitchd_interface_tx_errors_total**
- **ovs_vswitchd_interface_collisions_total**

La métrique suivante a été supprimée :

- **ovnkube_master_skipped_nbctl_daemon_total**

1.3.10.6. Installation de l'installateur multizone de l'infrastructure provisionnée VMware vSphere (aperçu technologique)

À partir d'OpenShift Container Platform 4.12, la possibilité de configurer plusieurs centres de données vCenter et plusieurs clusters vCenter dans une seule installation vCenter en utilisant l'infrastructure fournie par l'installateur est maintenant disponible en tant que fonctionnalité de l'aperçu technologique.

En utilisant les balises vCenter, vous pouvez utiliser cette fonctionnalité pour associer les centres de données vCenter et les clusters de calcul avec des régions et des zones openshift. Ces associations définissent des domaines de défaillance pour permettre aux charges de travail des applications d'être associées à des emplacements et à des domaines de défaillance spécifiques.

1.3.10.7. Kubernetes NMState dans VMware vSphere désormais pris en charge

À partir d'OpenShift Container Platform 4.12, vous pouvez configurer les paramètres de mise en réseau tels que les serveurs DNS ou les domaines de recherche, les VLAN, les ponts et le collage d'interface à l'aide de l'opérateur Kubernetes NMState sur votre instance VMware vSphere.

Pour plus d'informations, voir À propos de l'opérateur NMState de Kubernetes .

1.3.10.8. Kubernetes NMState dans OpenStack désormais pris en charge

À partir d'OpenShift Container Platform 4.12, vous pouvez configurer les paramètres de mise en réseau tels que les serveurs DNS ou les domaines de recherche, les VLAN, les ponts et le collage d'interface à l'aide de l'opérateur Kubernetes NMState sur votre instance OpenStack.

Pour plus d'informations, voir À propos de l'opérateur NMState de Kubernetes .

1.3.10.9. Opérateur DNS externe

Dans OpenShift Container Platform 4.12, l'Opérateur DNS Externe modifie le format des enregistrements TXT wildcard ExternalDNS sur AzureDNS. L'Opérateur DNS externe remplace l'astérisque par **any** dans les enregistrements TXT wildcard ExternalDNS. Vous devez éviter que les enregistrements Wildcard A et CNAME de ExternalDNS aient **any** comme sous-domaine le plus à gauche car cela pourrait causer un conflit.

La version amont de **ExternalDNS** pour OpenShift Container Platform 4.12 est v0.13.1.

1.3.10.10. Capturer les métriques et la télémétrie associées à l'utilisation des itinéraires et des ensembles de données (shards)

Dans OpenShift Container Platform 4.12, le Cluster Ingress Operator exporte une nouvelle métrique nommée **route_metrics_controller_routes_per_shard**. L'étiquette **shard_name** de la métrique spécifie le nom des tessons. Cette métrique indique le nombre total d'itinéraires admis par chaque shard.

Les mesures suivantes sont envoyées par télémétrie.

Tableau 1.1. Mesures envoyées par télémétrie

Nom	Expression de la règle d'enregistrement	Description
cluster:route_metrics_controller_routes_per_shard:min	**min(route_metrics_controller_routes_per_shard)**	Suivi du nombre minimum d'itinéraires admis par l'un ou l'autre des shards
cluster:route_metrics_controller_routes_per_shard:max	**max(route_metrics_controller_routes_per_shard)**	Suivi du nombre maximum d'itinéraires admis par l'un quelconque des shards

Nom	Expression de la règle d'enregistrement	Description
cluster:route_metrics_controller_routes_per_shard:avg	**avg(route_metrics_controller_routes_per_shard)**	Suivi de la valeur moyenne de la métrique **route_metrics_controller_routes_per_shard**
cluster:route_metrics_controller_routes_per_shard:median	**quantile(0.5, route_metrics_controller_routes_per_shard)**	Suivi de la valeur médiane de la métrique **route_metrics_controller_routes_per_shard**
cluster:openshift_route_info:tls_termination:sum	**sum (openshift_route_info) by (tls_termination)**	Indique le nombre d'itinéraires pour chaque valeur de **tls_termination**. Les valeurs possibles pour **tls_termination** sont **edge**, **passthrough** et **reencrypt**

1.3.10.11. Opérateur d'équilibreur de charge AWS

Dans OpenShift Container Platform 4.12, le contrôleur AWS Load Balancer implémente désormais la spécification Kubernetes Ingress pour les correspondances multiples. Si plusieurs chemins au sein d'un Ingress correspondent à une demande, le chemin le plus long est prioritaire. Si deux chemins correspondent encore, les chemins avec un type de chemin exact sont prioritaires sur un type de chemin préfixe.

L'opérateur de l'équilibreur de charge AWS définit la porte de fonctionnalité **EnableIPTargetType** sur **false**. Le contrôleur de l'équilibreur de charge AWS désactive la prise en charge des services et des ressources d'entrée pour **target-type ip** .

La version amont de **aws-load-balancer-controller** pour OpenShift Container Platform 4.12 est v2.4.4.

1.3.10.12. Mise à l'échelle automatique du contrôleur d'entrée (aperçu technologique)

Vous pouvez maintenant utiliser l'opérateur Custom Metrics Autoscaler d'OpenShift Container Platform pour mettre à l'échelle dynamiquement le contrôleur d'ingestion par défaut en fonction des métriques de votre cluster déployé, telles que le nombre de nœuds de travail disponibles. Le Custom Metrics Autoscaler est disponible en tant que fonctionnalité Technology Preview.

Pour plus d'informations, voir Autoscaling an Ingress Controller (Mise à l'échelle automatique d'un contrôleur d'entrée).

1.3.10.13. La valeur par défaut de HAProxy maxConnections est désormais de 50 000

Dans OpenShift Container Platform 4.12, la valeur par défaut du paramètre **maxConnections** est désormais 50000. Auparavant, à partir d'OpenShift Container Platform 4.11, la valeur par défaut du paramètre **maxConnections** était 20000.

Pour plus d'informations, voir les paramètres de configuration du contrôleur d'entrée .

1.3.10.14. Configuration d'un contrôleur d'entrée pour la gestion manuelle du DNS

Vous pouvez maintenant configurer un contrôleur d'entrée pour arrêter la gestion automatique du DNS et démarrer la gestion manuelle du DNS. Définissez le paramètre **dnsManagementPolicy** pour spécifier la gestion automatique ou manuelle du DNS.

Pour plus d'informations, voir Configuration d'un contrôleur d'entrée pour gérer manuellement le DNS .

1.3.10.15. Matériel pris en charge pour SR-IOV (Single Root I/O Virtualization)

OpenShift Container Platform 4.12 ajoute la prise en charge des périphériques SR-IOV suivants :

- Famille MT2892 [ConnectX-6 Dx]
- Famille MT2894 [ConnectX-6 Lx]
- MT42822 BlueField-2 en mode NIC ConnectX-6
- Famille Silicom STS

Pour plus d'informations, voir Dispositifs pris en charge.

1.3.10.16. Matériel pris en charge pour OvS (Open vSwitch) Hardware Offload

OpenShift Container Platform 4.12 ajoute la prise en charge OvS Hardware Offload pour les périphériques suivants :

- Famille MT2892 [ConnectX-6 Dx]
- Famille MT2894 [ConnectX-6 Lx]
- MT42822 BlueField-2 en mode NIC ConnectX-6

Pour plus d'informations, voir Dispositifs pris en charge.

1.3.10.17. Prise en charge de politiques multi-réseaux pour SR-IOV (aperçu technologique)

OpenShift Container Platform 4.12 ajoute la prise en charge de la configuration de la politique multiréseau pour les périphériques SR-IOV.

Vous pouvez désormais configurer le multiréseau pour les réseaux supplémentaires SR-IOV. La configuration des réseaux supplémentaires SR-IOV est une fonctionnalité de l'aperçu technologique et n'est prise en charge qu'avec les cartes d'interface réseau (NIC) du noyau.

Pour plus d'informations, voir Configuration de la politique multi-réseaux.

1.3.10.18. Passer d'un type d'équilibreur de charge AWS à un autre sans supprimer le contrôleur d'entrée

Vous pouvez mettre à jour le contrôleur d'entrée pour passer d'un équilibreur de charge classique AWS (CLB) à un équilibreur de charge réseau AWS (NLB) sans supprimer le contrôleur d'entrée.

Pour plus d'informations, voir Configuration du trafic d'entrée des clusters sur AWS.

1.3.10.19. Les annonces non sollicitées de voisins IPv6 et le protocole de résolution gratuite d'adresses IPv4 sont désormais par défaut sur le plugin CNI SR-IOV

Les pods créés avec le plugin CNI SR-IOV (Single Root I/O Virtualization), auxquels le plugin CNI de gestion des adresses IP a attribué des IP, envoient désormais par défaut sur le réseau des annonces de voisinage non sollicitées IPv6 et/ou un protocole de résolution d'adresse gratuit IPv4. Cette amélioration notifie aux hôtes l'adresse MAC du nouveau pod pour une IP particulière afin de rafraîchir les caches ARP/NDP avec les informations correctes.

Pour plus d'informations, voir Dispositifs pris en charge .

1.3.10.20. Prise en charge de l'optimisation du cache CoreDNS

Vous pouvez maintenant configurer la durée de vie (TTL) des requêtes DNS réussies et non réussies mises en cache par CoreDNS.

Pour plus d'informations, voir Optimisation du cache CoreDNS.

1.3.10.21. OVN-Kubernetes prend en charge la configuration du sous-réseau interne

Auparavant, le sous-réseau utilisé en interne par OVN-Kubernetes était **100.64.0.0/16** pour IPv4 et **fd98::/48** pour IPv6 et ne pouvait pas être modifié. Pour prendre en charge les cas où ces sous-réseaux se chevauchent avec des sous-réseaux existants dans votre infrastructure, vous pouvez désormais modifier ces sous-réseaux internes pour éviter tout chevauchement.

Pour plus d'informations, voir l'objet de configuration Cluster Network Operator

1.3.10.22. Prise en charge de l'IP Egress sur Red Hat OpenStack Platform (RHOSP)

RHOSP, associé à OpenShift Container Platform, prend désormais en charge l'attachement et le détachement automatiques des adresses IP Egress. Le trafic provenant d'un ou plusieurs pods dans un nombre quelconque d'espaces de noms dispose d'une adresse IP source cohérente pour les services extérieurs au cluster. Cette prise en charge s'applique à OpenShift SDN et OVN-Kubernetes en tant que fournisseurs de réseau par défaut.

1.3.10.23. Prise en charge de la migration des fonctionnalités d'OpenShift SDN vers OVN-Kubernetes

Si vous prévoyez de migrer du plugin réseau OpenShift SDN vers le plugin réseau OVN-Kubernetes, vos configurations pour les capacités suivantes sont automatiquement converties pour fonctionner avec OVN-Kubernetes :

- Adresses IP de sortie
- Pare-feu de sortie
- Multidiffusion

Pour plus d'informations sur le fonctionnement de la migration vers OVN-Kubernetes, voir Migrations à partir du fournisseur de réseau de cluster SDN OpenShift.

1.3.10.24. Journalisation de l'audit du pare-feu de sortie

Pour le plugin réseau OVN-Kubernetes, les pare-feu de sortie prennent en charge la journalisation des audits à l'aide du même mécanisme que la journalisation des audits de stratégie réseau. Pour plus d'informations, voir Journalisation des règles de pare-feu de sortie et de stratégie réseau .

1.3.10.25. Annoncer MetalLB à partir d'un pool d'adresses donné à partir d'un sous-ensemble de nœuds

Avec cette mise à jour, en mode BGP, vous pouvez utiliser le sélecteur de nœuds pour annoncer le service MetalLB à partir d'un sous-ensemble de nœuds, en utilisant un pool spécifique d'adresses IP. Cette fonctionnalité a été introduite en tant qu'aperçu technologique dans OpenShift Container Platform 4.11 et est maintenant disponible dans OpenShift Container Platform 4.12 pour le mode BGP uniquement. Le mode L2 reste une fonctionnalité d'aperçu technologique.

Pour plus d'informations, voir Publicité d'un pool d'adresses IP à partir d'un sous-ensemble de nœuds .

1.3.10.26. Spécifications supplémentaires pour le déploiement de MetalLB

Cette mise à jour fournit des spécifications de déploiement supplémentaires pour MetalLB. Lorsque vous utilisez une ressource personnalisée pour déployer MetalLB, vous pouvez utiliser ces spécifications de déploiement supplémentaires pour gérer le déploiement et l'exécution des pods MetalLB **speaker** et **controller** dans votre cluster. Par exemple, vous pouvez utiliser les spécifications de déploiement MetalLB pour gérer l'endroit où les pods MetalLB sont déployés, définir des limites de CPU pour les pods MetalLB et attribuer des classes d'exécution aux pods MetalLB.

Pour plus d'informations sur les spécifications de déploiement pour MetalLB, voir Spécifications de déploiement pour MetalLB.

1.3.10.27. Amélioration de la sélection de l'IP du nœud

Auparavant, le service **nodeip-configuration** sur un hôte du cluster sélectionnait l'adresse IP de l'interface utilisée par la route par défaut. Si plusieurs routes étaient présentes, le service sélectionnait la route ayant la valeur métrique la plus faible. Par conséquent, le trafic réseau pouvait être distribué à partir de l'interface incorrecte.

Avec OpenShift Container Platform 4.12, une nouvelle interface a été ajoutée au service **nodeip-configuration**, qui permet aux utilisateurs de créer un fichier d'indices. Ce fichier contient une variable, **NODEIP_HINT**, qui remplace la logique de sélection IP par défaut et sélectionne une adresse IP de nœud spécifique à partir de la variable de sous-réseau **NODEIP_HINT**. L'utilisation de la variable **NODEIP_HINT** permet aux utilisateurs de spécifier l'adresse IP utilisée, ce qui garantit que le trafic réseau est distribué à partir de l'interface correcte.

Pour plus d'informations, voir Facultatif : Remplacer la logique de sélection de l'IP du nœud par défaut .

1.3.10.28. Mise à jour de CoreDNS vers la version 1.10.0

Dans OpenShift Container Platform 4.12, CoreDNS utilise la version 1.10.0, qui inclut les changements suivants :

- CoreDNS n'augmente pas la taille de la mémoire tampon UDP de la requête si elle a été précédemment fixée à une valeur inférieure.
- CoreDNS préfixe désormais chaque ligne de journal dans les journaux des clients Kubernetes avec le niveau de journal associé.
- CoreDNS se recharge désormais plus rapidement à une vitesse approximative de 20ms.

1.3.10.29. Prise en charge d'un intervalle de rechargement configurable dans HAProxy

Avec cette mise à jour, un administrateur de cluster peut configurer l'intervalle de rechargement pour forcer HAProxy à recharger sa configuration moins fréquemment en réponse aux mises à jour des routes

et des points d'extrémité. L'intervalle minimum de rechargement de HAProxy par défaut est de 5 secondes.

Pour plus d'informations, voir Configuration de l'intervalle de recharge de HAProxy .

1.3.10.30. Nouvel opérateur d'observabilité du réseau pour observer le flux de trafic du réseau

En tant qu'administrateur, vous pouvez maintenant installer le Network Observability Operator pour observer le trafic réseau du cluster OpenShift Container Platform dans la console. Vous pouvez visualiser et surveiller les données du trafic réseau dans différentes représentations graphiques. Le Network Observability Operator utilise la technologie eBPF pour créer les flux réseau. Les flux réseau sont enrichis avec les informations d'OpenShift Container Platform et stockés dans Loki. Vous pouvez utiliser les informations sur le trafic réseau pour un dépannage et une analyse détaillés.

Pour plus d'informations, voir Observabilité du réseau.

1.3.10.31. IPv6 pour les interfaces réseau secondaires sur RHOSP

IPv6 pour les interfaces réseau secondaires est désormais pris en charge dans les clusters fonctionnant sous RHOSP.

Pour plus d'informations, voir Activation de la connectivité IPv6 aux pods sur RHOSP .

1.3.10.32. Support UDP pour les équilibreurs de charge sur RHOSP

Suite au passage à un fournisseur externe de cloud OpenStack, UDP est désormais pris en charge pour les services **LoadBalancer** pour les clusters qui fonctionnent sur cette plateforme.

1.3.10.33. Déployer l'opérateur SR-IOV pour les plans de contrôle hébergés (aperçu technologique)

Si vous avez configuré et déployé votre cluster de services d'hébergement, vous pouvez maintenant déployer l'opérateur SR-IOV pour un cluster hébergé. Pour plus d'informations, voir Déploiement de l'opérateur SR-IOV pour les plans de contrôle hébergés.

1.3.10.34. Prise en charge des adresses IP virtuelles IPv6 (VIP) pour les services Ingress VIP et API VIP sur métal nu

Avec cette mise à jour, dans les clusters d'infrastructure fournis par l'installateur, les paramètres de configuration **ingressVIP** et **apiVIP** du fichier **install-config.yaml** sont obsolètes. Utilisez plutôt les paramètres de configuration **ingressVIPs** et **apiVIPs**. Ces paramètres prennent en charge la mise en réseau à double pile pour les applications sur métal nu qui nécessitent un accès IPv4 et IPv6 au cluster en utilisant les services Ingress VIP et API VIP. Les paramètres de configuration **ingressVIPs** et **apiVIPs** utilisent un format de liste pour spécifier une adresse IPv4, une adresse IPv6 ou les deux formats d'adresse IP. L'ordre de la liste indique l'adresse VIP primaire et secondaire pour chaque service. L'adresse IP primaire doit provenir du réseau IPv4 en cas d'utilisation d'un réseau à double pile.

1.3.10.35. Prise en charge du passage du périphérique réseau Bluefield-2 du mode unité de traitement des données (DPU) au mode contrôleur d'interface réseau (NIC) (aperçu technologique)

Avec cette mise à jour, vous pouvez faire passer le périphérique réseau BlueField-2 du mode unité de traitement des données (DPU) au mode contrôleur d'interface réseau (NIC).

Pour plus d'informations, voir Passer Bluefield-2 de DPU à NIC .

1.3.11. Stockage

1.3.11.1. Stockage persistant à l'aide de l'opérateur GCP Filestore Driver (aperçu technologique)

OpenShift Container Platform est capable de provisionner des volumes persistants (PV) en utilisant le pilote CSI (Container Storage Interface) pour Google Compute Platform (GCP) Filestore. L'opérateur du pilote CSI de GCP Filestore qui gère ce pilote est en avant-première technologique.

Pour plus d'informations, voir GCP Filestore CSI Driver Operator .

1.3.11.2. La migration automatique CSI pour la migration automatique AWS Elastic Block Storage est généralement disponible

À partir d'OpenShift Container Platform 4.8, la migration automatique pour les plugins de volume in-tree vers leurs pilotes équivalents Container Storage Interface (CSI) est devenue disponible en tant que fonctionnalité d'aperçu technologique. La prise en charge de l'Elastic Block Storage (EBS) d'Amazon Web Services (AWS) a été fournie dans cette fonctionnalité dans OpenShift Container Platform 4.8, et OpenShift Container Platform 4.12 prend désormais en charge la migration automatique pour AWS EBS en tant que disponibilité générale. La migration CSI pour AWS EBS est désormais activée par défaut et ne nécessite aucune action de la part d'un administrateur.

Cette fonction traduit automatiquement les objets de l'arborescence en leurs représentations CSI correspondantes et devrait être totalement transparente pour les utilisateurs. Les objets traduits ne sont pas stockés sur le disque et les données des utilisateurs ne sont pas migrées.

Bien que le référencement de la classe de stockage au plugin de stockage dans l'arborescence continue de fonctionner, il est recommandé de remplacer la classe de stockage par défaut par la classe de stockage CSI.

Pour plus d'informations, voir Migration automatique CSI .

1.3.11.3. Migration automatique de l'ICS pour les BPC La migration automatique de l'ICS est généralement disponible

À partir d'OpenShift Container Platform 4.8, la migration automatique pour les plugins de volume in-tree vers leurs pilotes équivalents Container Storage Interface (CSI) est devenue disponible en tant que fonctionnalité d'aperçu technologique. La prise en charge de Google Compute Engine Persistent Disk (GCP PD) a été fournie dans cette fonctionnalité dans OpenShift Container Platform 4.9, et OpenShift Container Platform 4.12 prend désormais en charge la migration automatique pour GCP PD en tant que fonctionnalité généralement disponible. La migration CSI pour GCP PD est désormais activée par défaut et ne nécessite aucune action de la part d'un administrateur.

Cette fonction traduit automatiquement les objets de l'arborescence en leurs représentations CSI correspondantes et devrait être totalement transparente pour les utilisateurs. Les objets traduits ne sont pas stockés sur le disque et les données des utilisateurs ne sont pas migrées.

Bien que le référencement de la classe de stockage au plugin de stockage dans l'arborescence continue de fonctionner, il est recommandé de remplacer la classe de stockage par défaut par la classe de stockage CSI.

Pour plus d'informations, voir Migration automatique CSI .

1.3.11.4. Le suivi des capacités de stockage pour l'ordonnancement des nacelles est généralement disponible

Cette nouvelle fonctionnalité expose la capacité de stockage actuellement disponible à l'aide d'objets **CSIStorageCapacity**, et améliore la planification des pods qui utilisent des volumes CSI (Container Storage Interface) avec une liaison tardive. Actuellement, le seul type de stockage d'OpenShift Container Platform qui supporte cette fonctionnalité est OpenShift Data Foundation.

1.3.11.5. La topologie VMware vSphere CSI est généralement disponible

OpenShift Container Platform offre la possibilité de déployer OpenShift Container Platform for vSphere sur différentes zones et régions, ce qui vous permet de déployer sur plusieurs clusters de calcul, contribuant ainsi à éviter un point de défaillance unique.

Pour plus d'informations, voir topologie vSphere CSI.

1.3.11.6. La gestion des ressources locales de stockage éphémère est généralement disponible

La fonctionnalité de gestion des ressources de stockage éphémère local est désormais disponible. Grâce à cette fonctionnalité, vous pouvez gérer le stockage éphémère local en spécifiant des demandes et des limites.

Pour plus d'informations, voir Gestion du stockage éphémère.

1.3.11.7. Populateurs de volume (Avant-première technologique)

Les populateurs de volumes utilisent **datasource** pour permettre la création de volumes pré-remplis.

La population de volume est actuellement activée et prise en charge en tant que fonctionnalité d'aperçu technologique. Cependant, OpenShift Container Platform n'est pas livré avec des populateurs de volume.

Pour plus d'informations, voir Populateurs de volume.

1.3.11.8. VMware vSphere CSI Driver Operator requirements

Pour OpenShift Container Platform 4.12, VMWare vSphere Container Storage Interface (CSI) Driver Operator nécessite l'installation des composants minimums suivants :

- VMware vSphere version 7.0 Update 2 ou ultérieure, jusqu'à la version 8 incluse. vSphere 8 n'est pas pris en charge.
- vCenter 7.0 Update 2 ou ultérieur, jusqu'à la version 8 incluse. vCenter 8 n'est pas pris en charge.
- Virtual machines of hardware version 15 or later
- No third-party CSI driver already installed in the cluster

If a third-party CSI driver is present in the cluster, OpenShift Container Platform does not overwrite it. The presence of a third-party CSI driver prevents OpenShift Container Platform from upgrading to OpenShift Container Platform 4.13 or later.

Pour plus d'informations, voir VMware vSphere CSI Driver Operator requirements.

1.3.12. Cycle de vie de l'opérateur

1.3.12.1. Opérateurs de plateforme (aperçu technologique)

À partir d'OpenShift Container Platform 4.12, Operator Lifecycle Manager (OLM) introduit le type *platform Operator* en tant que fonctionnalité d'aperçu technologique. Le mécanisme Operator de la plateforme s'appuie sur les ressources du composant RukPak, également introduit dans OpenShift Container Platform 4.12, pour sourcer et gérer le contenu.

Un opérateur de plateforme est un opérateur basé sur OLM qui peut être installé pendant ou après les opérations du jour 0 d'un cluster OpenShift Container Platform et qui participe au cycle de vie du cluster. En tant qu'administrateur de cluster, vous pouvez utiliser les opérateurs de plateforme pour personnaliser davantage votre installation OpenShift Container Platform afin de répondre à vos exigences et à vos cas d'utilisation.

Pour plus d'informations sur les opérateurs de plate-forme, voir Gestion des opérateurs de plate-forme . Pour plus d'informations sur RukPak et ses ressources, voir Operator Framework packaging format.

1.3.12.2. Contrôler l'endroit où un opérateur est installé

Par défaut, lorsque vous installez un Operator, OpenShift Container Platform installe aléatoirement le pod Operator sur l'un de vos worker nodes.

Dans OpenShift Container Platform 4.12, vous pouvez contrôler l'endroit où un pod Operator est installé en ajoutant des contraintes d'affinité à l'objet **Subscription** de l'Operator.

Pour plus d'informations, voir Contrôle de l'emplacement d'installation d'un opérateur .

1.3.12.3. Synchronisation de l'admission à la sécurité des pods pour les espaces de noms openshift-* créés par les utilisateurs

Dans OpenShift Container Platform 4.12, la synchronisation de l'admission à la sécurité des pods est activée par défaut si un opérateur est installé dans des espaces de noms créés par l'utilisateur qui ont un préfixe **openshift-**. La synchronisation est activée après la création d'une version de service de cluster (CSV) dans l'espace de noms. L'étiquette synchronisée hérite des autorisations des comptes de service dans l'espace de noms.

Pour plus d'informations, voir Synchronisation des contraintes de contexte de sécurité avec les normes de sécurité des pods.

1.3.13. Développement des opérateurs

1.3.13.1. Configuration du contexte de sécurité d'un module de catalogue

Vous pouvez configurer le contexte de sécurité d'un pod de catalogue en utilisant l'indicateur **--security-context-config** dans les sous-commandes **run bundle** et **bundle-upgrade**. Cet indicateur permet aux profils seccomp de se conformer à l'admission de sécurité du pod. L'indicateur accepte les valeurs **restricted** et **legacy**. Si vous ne spécifiez pas de valeur, le profil seccomp prend par défaut la valeur **restricted**. Si votre module de catalogue ne peut pas fonctionner avec des autorisations restreintes, définissez l'indicateur sur **legacy**, comme indiqué dans l'exemple suivant :

```
$ operator-sdk run bundle \
  --security-context-config=legacy
```

1.3.13.2. Validation des manifestes de bundle pour les API supprimées de Kubernetes 1.25

Vous pouvez désormais vérifier les manifestes de bundle pour les API obsolètes supprimées de Kubernetes 1.25 en utilisant la suite de tests Operator Framework avec la sous-commande **bundle validate**.

Par exemple :

```
$ operator-sdk bundle validate .<bundle_dir_or_image> \
  --select-optional suite=operatorframework \
  --optional-values=k8s-version=1.25
```

Si votre opérateur demande l'autorisation d'utiliser l'une des API supprimées de Kubernetes 1.25, la commande affiche un message d'avertissement.

Si l'une des versions d'API supprimées de Kubernetes 1.25 est incluse dans la version du service de cluster (CSV) de votre opérateur, la commande affiche un message d'erreur.

Voir Beta APIs removed from Kubernetes 1.25 and the Operator SDK CLI reference pour plus d'informations.

1.3.14. Machine API

1.3.14.1. Ensembles de machines à plans de contrôle

OpenShift Container Platform 4.12 introduit des ensembles de machines de plan de contrôle. Les ensembles de machines du plan de contrôle fournissent des capacités de gestion pour les machines du plan de contrôle qui sont similaires à ce que les ensembles de machines de calcul fournissent pour les machines de calcul. Pour plus d'informations, voir Gestion des machines du plan de contrôle .

1.3.14.2. Spécifier la verbosité du niveau de journalisation de l'autoscaler de cluster

OpenShift Container Platform prend désormais en charge la définition de la verbosité du niveau de journal du cluster autoscaler en définissant le paramètre **logVerbosity** dans la ressource personnalisée **ClusterAutoscaler**. Pour plus d'informations, voir la définition de la ressource **ClusterAutoscaler** .

1.3.14.3. Activation des diagnostics de démarrage Azure

OpenShift Container Platform prend désormais en charge l'activation des diagnostics de démarrage sur les machines Azure créées par votre jeu de machines. Pour plus d'informations, voir "Activation des diagnostics de démarrage Azure" pour les machines de calcul ou les machines de plan de contrôle .

1.3.15. Machine Config Operator

1.3.15.1. Superposition d'images RHCOS

La superposition d'images de Red Hat Enterprise Linux CoreOS (RHCOS) vous permet d'ajouter de nouvelles images au-dessus de l'image RHCOS de base. Cette stratification ne modifie pas l'image RHCOS de base. Au lieu de cela, elle crée un site *custom layered image* qui inclut toutes les fonctionnalités de RHCOS et ajoute des fonctionnalités supplémentaires à des nœuds spécifiques du cluster.

Actuellement, la stratification d'images RHCOS vous permet de travailler avec Customer Experience and Engagement (CEE) pour obtenir et appliquer des paquets Hotfix sur votre image RHCOS, sur la

base de la politique Hotfix de Red Hat . Il est prévu, dans les prochaines versions, que vous puissiez utiliser la stratification d'images RHCOS pour incorporer des logiciels tiers tels que Libreswan ou numactl.

Pour plus d'informations, voir RHCOS image layering .

1.3.16. Nœuds

1.3.16.1. Mise à jour de la liste de sécurité spécifique à l'interface (Technology Preview)

OpenShift Container Platform prend désormais en charge la mise à jour de la sécurité par défaut spécifique à l'interface **sysctls**.

Vous pouvez ajouter ou supprimer **sysctls** de la liste prédéfinie. Lorsque vous ajoutez des **sysctls**, ils peuvent être définis sur tous les nœuds. La mise à jour de la liste **sysctls** spécifique à l'interface est une fonctionnalité de l'aperçu technologique uniquement.

Pour plus d'informations, voir Mise à jour de la liste des sysctls sûrs spécifiques à l'interface .

1.3.16.2. Fuseaux horaires des tâches Cron (Technology Preview)

La définition d'un fuseau horaire pour la planification d'une tâche cron est désormais proposée en tant qu'aperçu technologique. Si aucun fuseau horaire n'est spécifié, le gestionnaire de contrôleur Kubernetes interprète la programmation en fonction de son fuseau horaire local.

Pour plus d'informations, voir Création de tâches cron .

1.3.16.3. La version 2 du groupe de contrôle Linux passe en avant-première technologique

La prise en charge par OpenShift Container Platform de Linux Control Group version 2 (cgroup v2) a été promue au rang d'aperçu technologique. cgroup v2 est la prochaine version des groupes de contrôle du noyau. cgroups v2 offre de multiples améliorations, notamment une hiérarchie unifiée, une délégation de sous-arbres plus sûre, de nouvelles fonctionnalités telles que Pressure Stall Information, ainsi qu'une gestion des ressources et une isolation améliorées. Pour plus d'informations, voir Enabling Linux Control Group version 2 (cgroup v2).

1.3.16.4. exécution d'un conteneur crun (aperçu technologique)

OpenShift Container Platform prend désormais en charge le runtime de conteneur crun dans l'aperçu technologique. Vous pouvez basculer entre le moteur d'exécution de conteneur crun et le moteur d'exécution de conteneur par défaut en utilisant une ressource personnalisée (CR) **ContainerRuntimeConfig**. Pour plus d'informations, voir À propos du moteur de conteneurs et de l'exécution des conteneurs.

1.3.16.5. Améliorations apportées par l'opérateur d'assainissement autonome des nœuds

OpenShift Container Platform prend désormais en charge la clôture du plan de contrôle par l'opérateur de remédiation des nœuds autonomes. En cas de défaillance d'un nœud, vous pouvez suivre des stratégies de remédiation à la fois sur les nœuds de travail et les nœuds du plan de contrôle. Pour plus d'informations, voir Control Plane Fencing.

1.3.16.6. Améliorations apportées par l'opérateur au bilan de santé du nœud

OpenShift Container Platform prend désormais en charge la clôture du plan de contrôle sur l'opérateur

de vérification de la santé des nœuds. En cas de défaillance d'un nœud, vous pouvez suivre des stratégies de remédiation sur les nœuds de travail et les nœuds du plan de contrôle. Pour plus d'informations, voir Control Plane Fencing.

L'opérateur de bilan de santé des nœuds inclut désormais un plugin de console web pour gérer les bilans de santé des nœuds. Pour plus d'informations, voir Création d'un bilan de santé d'un nœud .

Pour installer ou mettre à jour la dernière version du Node Health Check Operator, utilisez le canal d'abonnement **stable**. Pour plus d'informations, voir Installation de l'opérateur de contrôle de santé des nœuds à l'aide de l'interface CLI.

1.3.17. Contrôle

La pile de surveillance de cette version comprend les fonctionnalités nouvelles et modifiées suivantes.

1.3.17.1. Mises à jour des composants et des dépendances de la pile de surveillance

Cette version comprend les mises à jour de version suivantes pour les composants et dépendances de la pile de surveillance :

- kube-state-metrics vers 2.6.0
- node-exporter à 1.4.0
- prom-label-proxy à 0.5.0
- Prometheus à 2.39.1
- prometheus-adapter à 0.10.0
- prometheus-operator à 0.60.1
- Thanos à 0.28.1

1.3.17.2. Modifications des règles d'alerte

NOTE

Red Hat ne garantit pas la compatibilité ascendante pour les règles d'enregistrement ou les règles d'alerte.

- **New**
  - Ajout de l'alerte **TelemeterClientFailures**, qui se déclenche lorsqu'un cluster tente et échoue à soumettre des données de télémétrie à un certain taux sur une période de temps. L'alerte se déclenche lorsque le taux de demandes échouées atteint 20 % du taux total de demandes dans une fenêtre de 15 minutes.
- **Changed**
  - L'alerte **KubeAggregatedAPIDown** attend désormais 900 secondes au lieu de 300 secondes avant d'envoyer une notification.
  - Les alertes **NodeClockNotSynchronising** et **NodeClockSkewDetected** n'évaluent plus que les mesures du travail **node-exporter**.

- Les alertes **NodeRAIDDegraded** et **NodeRAIDDiskFailure** comprennent désormais un filtre d'étiquette de dispositif qui ne correspond qu'à la valeur renvoyée par **mmcblk.p.|nvme.|sd.|vd.|xvd.|dm-.|dasd.** .
- Les alertes **PrometheusHighQueryLoad** et **ThanosQueryOverload** se déclenchent désormais également lorsqu'une charge de requête élevée existe sur la couche de requête.

1.3.17.3. Nouvelle option permettant de spécifier les contraintes d'étalement de la topologie des pods pour les composants de surveillance

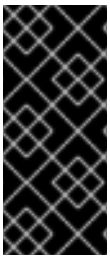
Vous pouvez désormais utiliser les contraintes de répartition de la topologie des pods pour contrôler la répartition des pods Prometheus, Thanos Ruler et Alertmanager sur une topologie de réseau lorsque les pods OpenShift Container Platform sont déployés dans plusieurs zones de disponibilité.

1.3.17.4. Nouvelle option pour améliorer la cohérence des données pour Prometheus Adapter

Vous pouvez désormais configurer un moniteur de service kubelet facultatif pour Prometheus Adapter (PA) qui améliore la cohérence des données entre plusieurs requêtes de mise à l'échelle automatique. L'activation de ce moniteur de service élimine la possibilité que deux requêtes envoyées en même temps à PA produisent des résultats différents parce que les requêtes PromQL sous-jacentes exécutées par PA peuvent se trouver sur des serveurs Prometheus différents.

1.3.17.5. Mise à jour de la configuration de l'Alertmanager pour les clés secrètes supplémentaires

Avec cette version, si vous configurez un secret Alertmanager pour contenir des clés supplémentaires et si la configuration Alertmanager fait référence à ces clés en tant que fichiers (tels que des modèles, des certificats TLS ou des jetons), vos paramètres de configuration doivent pointer vers ces clés en utilisant un chemin d'accès absolu plutôt qu'un chemin d'accès relatif. Ces clés sont disponibles dans le répertoire **/etc/alertmanager/config**. Dans les versions précédentes d'OpenShift Container Platform, vous pouviez utiliser des chemins relatifs dans votre configuration pour pointer vers ces clés car le fichier de configuration de l'Alertmanager était situé dans le même répertoire que les clés.



IMPORTANT

Si vous mettez à jour OpenShift Container Platform 4.12 et que vous avez spécifié des chemins relatifs pour des clés secrètes Alertmanager supplémentaires qui sont référencées en tant que fichiers, vous devez changer ces chemins relatifs en chemins absolus dans votre configuration Alertmanager. Dans le cas contraire, les récepteurs d'alertes qui utilisent ces fichiers ne parviendront pas à envoyer des notifications.

1.3.18. Évolutivité et performance

1.3.18.1. La désactivation du temps réel à l'aide des indices de charge de travail supprime le pilotage des paquets de réception du cluster

Au niveau du cluster, un service systemd définit par défaut un masque RPS (Receive Packet Steering) pour les interfaces réseau virtuelles. Le masque RPS achemine les demandes d'interruption des interfaces réseau virtuelles en fonction de la liste des unités centrales réservées définie dans le profil de performances. Au niveau du conteneur, un script hook **CRI-O** définit également un masque RPS pour tous les périphériques réseau virtuels.

Avec cette mise à jour, si vous définissez **spec.workloadHints.realTime** dans le profil de performance

sur **False**, le système désactive également le service systemd et le script hook **CRI-O** qui définissent le masque RPS. Le système désactive ces fonctions RPS parce que RPS est typiquement pertinent pour les cas d'utilisation nécessitant des charges de travail à faible latence et en temps réel uniquement.

Pour conserver les fonctions RPS même lorsque vous définissez **spec.workloadHints.realTime** sur **False**, consultez la section *RPS Settings* de la solution Performance addons operator advanced configuration de la base de connaissances de Red Hat.

Pour plus d'informations sur la configuration des indices de charge de travail, voir Comprendre les indices de charge de travail.

1.3.18.2. Profil accordé

Le profil **tuned** définit désormais la valeur **fs.aio-max-nr sysctl** par défaut, ce qui améliore les performances des E/S asynchrones pour les profils de nœuds par défaut.

1.3.18.3. Prise en charge des nouvelles fonctionnalités et options du noyau

Le réglage de la faible latence a été mis à jour pour utiliser les dernières fonctionnalités et options du noyau. Le correctif pour 2117780 a introduit un nouveau thread par CPU **kthread**, **ktimers**. Ce thread doit être épinglé aux cœurs de l'unité centrale appropriés. Avec cette mise à jour, il n'y a pas de changement fonctionnel ; l'isolation de la charge de travail est la même. Pour plus d'informations, voir 2102450.

1.3.18.4. Configurations d'économie d'énergie

Dans OpenShift Container Platform 4.12, en activant les C-states et les P-states contrôlés par le système d'exploitation, vous pouvez utiliser différentes configurations d'économie d'énergie pour les charges de travail critiques et non critiques. Vous pouvez appliquer les configurations via le nouvel indice de charge de travail **perPodPowerManagement** et les annotations CRI-O **cpu-c-states.crio.io** et **cpu-freq-governor.crio.io**. Pour plus d'informations sur cette fonctionnalité, voir Configurations d'économie d'énergie.

1.3.18.5. Extension des clusters OpenShift à un seul nœud avec des nœuds de travail à l'aide de GitOps ZTP (Avant-première technologique)

Dans OpenShift Container Platform 4.11, une fonctionnalité permettant d'ajouter manuellement des nœuds de travail aux clusters OpenShift à nœud unique a été introduite. Cette fonctionnalité est désormais également disponible dans GitOps ZTP.

Pour plus d'informations, voir Ajouter des nœuds de travail à des clusters OpenShift à nœud unique avec GitOps ZTP.

1.3.18.6. Outil Factory-precaching-cli pour réduire les temps de déploiement d'OpenShift Container Platform et d'Operator (Technology Preview)

Dans OpenShift Container Platform 4.12, vous pouvez utiliser l'outil factory-precaching-cli pour pré-cacher les images OpenShift Container Platform et Operator sur un serveur à l'usine, puis vous pouvez inclure le serveur pré-caché sur le site pour le déploiement. Pour plus d'informations sur l'outil factory-precaching-cli, voir Pre-caching images for single-node OpenShift deployments.

1.3.18.7. Intégration de l'outil factory-precaching-cli dans le Zero Touch Provisioning (ZTP) (aperçu technologique)

Dans OpenShift Container Platform 4.12, vous pouvez utiliser l'outil factory-precaching-cli dans le flux de travail GitOps ZTP. Pour plus d'informations, voir Pre-caching images for single-node OpenShift deployments.

1.3.18.8. Optimisation des nœuds dans un cluster hébergé (aperçu technologique)

Vous pouvez désormais configurer le réglage au niveau du système d'exploitation pour les nœuds d'un cluster hébergé à l'aide de l'opérateur de réglage des nœuds. Pour configurer l'optimisation des nœuds, vous pouvez créer des cartes de configuration dans le cluster de gestion qui contiennent des objets **Tuned**, et référencer ces cartes de configuration dans vos pools de nœuds. La configuration de l'optimisation définie dans les objets **Tuned** est appliquée aux nœuds du pool de nœuds. Pour plus d'informations, voir Configuration de l'optimisation des nœuds dans un cluster hébergé .

1.3.18.9. Gestion des modules du noyau Opérateur

L'opérateur de gestion des modules du noyau (KMM) remplace l'opérateur de ressources spéciales (SRO). KMM comprend les fonctionnalités suivantes pour les environnements connectés uniquement :

- Prise en charge des concentrateurs et des antennes pour les déploiements en périphérie
- Contrôles avant le vol pour le soutien à la mise à niveau
- Signature du module de démarrage sécurisé du noyau
- Doit collecter des journaux pour aider au dépannage
- Déploiement d'un micrologiciel binaire

1.3.18.10. Prise en charge des grappes en étoile (Avant-première technologique)

Pour les déploiements en étoile dans un environnement qui peut accéder à l'internet, vous pouvez utiliser l'opérateur de gestion des modules du noyau (KMM) déployé dans le cluster de l'étoile pour gérer le déploiement des modules du noyau requis vers un ou plusieurs clusters gérés.

1.3.18.11. Gestionnaire du cycle de vie tenant compte de la topologie (TALM)

Topology Aware Lifecycle Manager (TALM) fournit désormais des informations d'état et des messages plus détaillés, ainsi que des conditions redéfinies. Vous pouvez utiliser le champ **ClusterLabelSelector** pour une plus grande flexibilité dans la sélection des clusters à mettre à jour. Vous pouvez utiliser des paramètres de délai pour déterminer ce qui se passe si une mise à jour échoue pour un cluster, par exemple, ignorer le cluster défaillant et continuer à mettre à niveau d'autres clusters, ou arrêter la remédiation de la politique pour tous les clusters. Pour plus d'informations, voir Topology Aware Lifecycle Manager pour les mises à jour de clusters.

1.3.18.12. Encapsulation de l'espace de noms du mont (aperçu technologique)

L'encapsulation est le processus de déplacement de tous les points de montage spécifiques à Kubernetes vers un espace de noms alternatif afin de réduire la visibilité et l'impact sur les performances d'un grand nombre de points de montage dans l'espace de noms par défaut. Auparavant, l'encapsulation de l'espace de noms de montage a été déployée de manière transparente dans OpenShift Container Platform, spécifiquement pour les unités distribuées (DU) installées à l'aide de GitOps ZTP. Dans OpenShift Container Platform v4.12, cette fonctionnalité est désormais disponible en tant qu'option configurable.

Un système d'exploitation hôte standard utilise systemd pour analyser en permanence tous les espaces

de noms de montage : à la fois les montages Linux standard et les nombreux montages que Kubernetes utilise pour fonctionner. L'implémentation actuelle de Kubelet et de CRI-O utilise l'espace de noms de premier niveau pour tous les points de montage des conteneurs et de Kubelet. L'encapsulation de ces points de montage spécifiques aux conteneurs dans un espace de noms privé réduit la charge de travail de systemd et améliore les performances de l'unité centrale. L'encapsulation peut également améliorer la sécurité, en stockant les points de montage spécifiques à Kubernetes dans un emplacement à l'abri de l'inspection par des utilisateurs non privilégiés.

Pour plus d'informations, voir Optimiser l'utilisation de l'unité centrale avec l'encapsulation de l'espace de noms de montage.

1.3.18.13. Modifier l'ensemble de CPU de partitionnement de la charge de travail dans les clusters OpenShift à nœud unique qui sont déployés avec GitOps ZTP

Vous pouvez configurer l'ensemble de CPU de partitionnement de la charge de travail dans les clusters OpenShift à nœud unique que vous déployez avec GitOps ZTP. Pour ce faire, vous spécifiez les ressources CPU de gestion de cluster avec le champ **cpuset** de la ressource personnalisée (CR) **SiteConfig** et le champ **reserved** de la CR de groupe **PolicyGenTemplate**. La valeur que vous définissez pour **cpuset** doit correspondre à la valeur définie dans le champ cluster **PerformanceProfile** CR **.spec.cpu.reserved** pour le partitionnement de la charge de travail.

Pour plus d'informations, voir Partitionnement de la charge de travail .

1.3.18.14. Les fonctions du modèle de hub RHACM sont désormais disponibles pour une utilisation avec GitOps ZTP

Les fonctions de modèle de hub sont maintenant disponibles pour une utilisation avec GitOps ZTP en utilisant Red Hat Advanced Cluster Management (RHACM) et Topology Aware Lifecycle Manager (TALM). Les modèles de cluster côté hub réduisent le besoin de créer des politiques séparées pour de nombreux clusters avec des configurations similaires mais avec des valeurs différentes. Pour plus d'informations, voir Utilisation de modèles de concentrateur dans les CR PolicyGenTemplate .

1.3.18.15. Limites des clusters gérés par ArgoCD

Le RHACM utilise les CR **SiteConfig** pour générer les CR d'installation de cluster géré du jour 1 pour ArgoCD. Chaque application ArgoCD peut gérer un maximum de 300 CR **SiteConfig**. Pour plus d'informations, voir Configuration du cluster hub avec ArgoCD .

1.3.18.16. Prise en charge par GitOps ZTP de la configuration des délais d'évaluation de la conformité des politiques dans les CR de PolicyGenTemplate

Dans GitOps ZTP v4.11 , une valeur par défaut de délai d'évaluation de la conformité aux politiques est disponible pour une utilisation dans **PolicyGenTemplate** custom resources (CRs). Cette valeur indique la durée pendant laquelle la CR **ConfigurationPolicy** concernée peut se trouver dans un état de conformité ou de non-conformité aux politiques avant que RHACM ne réévalue les politiques de cluster appliquées.

En option, vous pouvez désormais remplacer les intervalles d'évaluation par défaut pour toutes les politiques dans les CR **PolicyGenTemplate**.

Pour plus d'informations, voir Configuration des délais d'évaluation de la conformité des politiques pour les CR PolicyGenTemplate.

1.3.18.17. Spécifier le type de plate-forme pour les clusters gérés

L'installateur assisté prend actuellement en charge les plateformes OpenShift Container Platform suivantes :

- **BareMetal**
- **VSphere**
- **None**

OpenShift à nœud unique ne prend pas en charge **VSphere**.

1.3.18.18. Configurer le hub cluster pour utiliser des registres non authentifiés

Cette version prend en charge l'utilisation de registres non authentifiés lors de la configuration du cluster hub. Les registres qui ne nécessitent pas d'authentification sont répertoriés sous **spec.unauthenticatedRegistries** dans la ressource **AgentServiceConfig**. Tout registre figurant sur cette liste n'est pas tenu d'avoir une entrée dans le secret d'extraction utilisé pour l'installation du cluster de rayons. **assisted-service** valide le secret d'extraction en s'assurant qu'il contient les informations d'authentification pour chaque registre d'image utilisé pour l'installation.

Pour plus d'informations, voir Configurer le cluster hub pour utiliser des registres non authentifiés .

1.3.18.19. Mise en miroir ironique d'agents dans des installations ZTP GitOps déconnectées

Pour les installations déconnectées utilisant GitOps ZTP, si vous déployez OpenShift Container Platform version 4.11 ou antérieure sur un cluster spoke avec converged flow activé, vous devez mettre en miroir l'image de l'agent Ironic par défaut dans le référentiel d'images local. Les images par défaut de l'agent Ironic sont les suivantes :

- AMD64 Image de l'agent ironique : **quay.io/openshift-release-dev/ocp-v4.0-art-dev@sha256:d3f1d4d3cd5fbcf1b9249dd71d01be4b901d337fdc5f8f66569eb71df4d9d446**
- AArch64 Image ironique de l'agent : **quay.io/openshift-release-dev/ocp-v4.0-art-dev@sha256:cb0edf19fffc17f542a7efae76939b1e9757dc75782d4727fb0aa77ed5809b43**

Pour plus d'informations sur la mise en miroir des images, voir Mise en miroir du référentiel d'images OpenShift Container Platform.

1.3.18.20. Configurer les arguments du noyau pour l'ISO Discovery en utilisant GitOps ZTP

OpenShift Container Platform prend désormais en charge la spécification d'arguments de noyau pour l'ISO de découverte dans les déploiements GitOps ZTP. Dans les déploiements GitOps ZTP manuels et automatisés, l'ISO de découverte fait partie du processus d'installation d'OpenShift Container Platform sur les hôtes bare-metal gérés. Vous pouvez maintenant éditer la ressource **InfraEnv** pour spécifier les arguments du noyau pour l'ISO de découverte. Ceci est utile pour les installations de clusters avec des exigences environnementales spécifiques. Par exemple, vous pouvez définir l'argument de noyau **rd.net.timeout.carrier** pour aider à configurer le cluster pour un réseau statique.

Pour plus d'informations sur la manière de spécifier les arguments du noyau, voir Configuration des arguments du noyau pour l'ISO de découverte à l'aide de GitOps ZTP et Configuration des arguments du noyau pour l'ISO de découverte pour les installations manuelles à l'aide de GitOps ZTP.

1.3.18.21. Déployer des clusters de rayons hétérogènes à partir d'un cluster hub

Avec cette mise à jour, vous pouvez créer des clusters à architecture mixte d'OpenShift Container Platform, également connus sous le nom de clusters hétérogènes, qui comprennent des hôtes avec des

architectures de CPU AMD64 et AArch64. Vous pouvez déployer un cluster hétérogène à partir d'un cluster hub géré par Red Hat Advanced Cluster Management (RHACM). Pour créer un cluster hétérogène, ajoutez un nœud de travail AArch64 à un cluster AMD64 déployé.

Pour ajouter un nœud de travail AArch64 à un cluster AMD64 déployé, vous pouvez spécifier l'architecture AArch64, l'image de version multi-architecture et le système d'exploitation requis pour le nœud à l'aide d'une ressource personnalisée (CR) **InfraEnv**. Vous pouvez ensuite intégrer le nœud de travailleur AArch64 au cluster AMD64 à l'aide de l'API Assisted Installer et de la CR **InfraEnv**.

1.3.19. Opérateur Insights

1.3.19.1. Alertes sur l'actualité

Dans OpenShift Container Platform 4.12, les recommandations actives d'Insights sont désormais présentées à l'utilisateur sous forme d'alertes. Vous pouvez visualiser et configurer ces alertes avec Alertmanager.

1.3.19.2. Insights Amélioration de la collecte de données par les opérateurs

Dans OpenShift Container Platform 4.12, l'opérateur Insights collecte désormais les métriques suivantes :

- **console_helm_uninstalls_total**
- **console_helm_upgrades_total**

1.3.20. Authentification et autorisation

1.3.20.1. Informations d'identification de l'application sur RHOSP

Vous pouvez désormais spécifier des identifiants d'application dans les fichiers **clouds.yaml** des clusters qui s'exécutent sur Red Hat OpenStack Platform (RHOSP). Les informations d'identification de l'application sont une alternative à l'intégration des détails du compte d'utilisateur dans les fichiers de configuration. À titre d'exemple, voir la section suivante d'un fichier **clouds.yaml** qui inclut des détails de compte d'utilisateur :

```
clouds:
  openstack:
    auth:
      auth_url: https://127.0.0.1:13000
      password: thepassword
      project_domain_name: Default
      project_name: theprojectname
      user_domain_name: Default
      username: theusername
    region_name: regionOne
```

Comparez cette section à une autre qui utilise les informations d'identification de l'application :

```
clouds:
  openstack:
    auth:
      auth_url: https://127.0.0.1:13000
      application_credential_id: '5dc185489adc4b0f854532e1af81ffe0'
```

```
        application_credential_secret:
'PDCTKans2bPBbaEqBLiT_IajG8e5J_nJB4kvQHjaAy6ufhod0Zl0NkNoBzjn_bWSYzk587ieIGSlT11c4pV
ehA'
      auth_type: "v3applicationcredential"
      region_name: regionOne
```

Pour utiliser les identifiants d'application avec votre cluster en tant qu'administrateur RHOSP, créez les identifiants. Utilisez-les ensuite dans un fichier **clouds.yaml** lors de l'installation d'un cluster. Vous pouvez également créer le fichier **clouds.yaml** et le faire pivoter dans un cluster existant.

1.3.21. Plans de contrôle hébergés (aperçu technologique)

1.3.21.1. La version bêta de l'API HyperShift est désormais disponible

La version par défaut de l'API **hypershift.openshift.io**, qui est l'API pour les plans de contrôle hébergés sur OpenShift Container Platform, est maintenant v1beta1. Actuellement, pour un cluster existant, le passage de la version alpha à la version bêta n'est pas pris en charge.

1.3.21.2. Versioning pour les plans de contrôle hébergés

Avec chaque version majeure, mineure ou corrective d'OpenShift Container Platform, l'HyperShift Operator est publié. L'interface de ligne de commande (CLI) HyperShift est publiée dans le cadre de chaque version de l'opérateur HyperShift.

Les ressources des API **HostedCluster** et **NodePool** sont disponibles dans la version bêta de l'API et suivent une politique similaire à celle d'OpenShift Container Platform et de Kubernetes.

1.3.21.3. Sauvegarde et restauration d'etcd sur un cluster hébergé

Si vous utilisez des plans de contrôle hébergés sur OpenShift Container Platform, vous pouvez sauvegarder et restaurer etcd en prenant un instantané d'etcd et en le téléchargeant vers un emplacement où vous pourrez le récupérer plus tard, tel qu'un seau S3. Plus tard, si nécessaire, vous pouvez restaurer l'instantané. Pour plus d'informations, voir Sauvegarde et restauration d'etcd sur un cluster hébergé.

1.3.21.4. Reprise après sinistre pour un cluster hébergé dans une région AWS

Si vous avez besoin d'une reprise après sinistre pour un cluster hébergé, vous pouvez récupérer le cluster hébergé dans la même région au sein d'AWS. Pour plus d'informations, voir Reprise après sinistre d'un cluster hébergé dans une région AWS.

1.3.22. Red Hat Virtualization (RHV)

Cette version fournit plusieurs mises à jour de Red Hat Virtualization (RHV). Avec cette version :

- La journalisation du pilote oVirt CSI a été révisée avec de nouveaux messages d'erreur pour améliorer la clarté et la lisibilité des journaux.
- Le fournisseur d'API de cluster met automatiquement à jour les informations d'identification oVirt et Red Hat Virtualization (RHV) lorsqu'elles sont modifiées dans OpenShift Container Platform.

1.4. CHANGEMENTS TECHNIQUES NOTABLES

OpenShift Container Platform 4.12 introduit les changements techniques notables suivants.

Points d'extrémité régionaux du service de jetons de sécurité AWS

L'utilitaire Cloud Credential Operator (**ccoctl**) crée désormais des secrets qui utilisent des points d'extrémité régionaux pour le service de jetons de sécurité AWS (AWS STS) . Cette approche est conforme aux meilleures pratiques recommandées par AWS.

Paramètre du répertoire des demandes d'informations d'identification pour la suppression des ressources GCP à l'aide de l'utilitaire Cloud Credential Operator

Avec cette version, lorsque vous supprimez des ressources GCP avec l'utilitaire Cloud Credential Operator, vous devez spécifier le répertoire contenant les fichiers des objets du composant **CredentialsRequest**.

Application restreinte à l'avenir pour l'admission à la sécurité des pods

Actuellement, les violations de la sécurité des pods sont affichées sous forme d'avertissements et enregistrées dans les journaux d'audit, mais n'entraînent pas le rejet du pod.

Une application restreinte globale pour l'admission de la sécurité des pods est actuellement prévue pour la prochaine version mineure d'OpenShift Container Platform. Lorsque cette application restreinte est activée, les pods présentant des violations de la sécurité des pods seront rejetés.

Pour vous préparer à ce changement, assurez-vous que vos charges de travail correspondent au profil d'admission de sécurité du pod qui s'applique à elles. Les charges de travail qui ne sont pas configurées conformément aux normes de sécurité appliquées définies globalement ou au niveau de l'espace de noms seront rejetées. Le SCC **restricted-v2** admet les charges de travail conformément à la définition de Kubernetes restreint.

Si vous recevez des violations de la sécurité des pods, consultez les ressources suivantes :

- Reportez-vous à la section Identification des violations de sécurité des pods pour savoir comment identifier les charges de travail à l'origine des violations de sécurité des pods.
- Voir Synchronisation des contraintes de contexte de sécurité avec les normes de sécurité des pod s pour comprendre quand la synchronisation des étiquettes d'admission à la sécurité des pods est effectuée. Les étiquettes d'admission à la sécurité des pods ne sont pas synchronisées dans certaines situations, notamment dans les cas suivants :
    - La charge de travail s'exécute dans un espace de noms créé par le système et préfixé par **openshift-**.
    - La charge de travail s'exécute sur un pod qui a été créé directement sans contrôleur de pod.
- Si nécessaire, vous pouvez définir un profil d'admission personnalisé pour l'espace de noms ou le pod en définissant l'étiquette **pod-security.kubernetes.io/enforce**.

Cataloguer les sources et les pods restreints, appliquer les règles d'admission à la sécurité

Les sources de catalogue construites en utilisant le format de catalogue basé sur SQLite et une version de l'outil CLI **opm** publiée avant OpenShift Container Platform 4.11 ne peuvent pas fonctionner sous l'application de la sécurité des pods restreints.

Dans OpenShift Container Platform 4.12, les espaces de noms n'ont pas de mise en œuvre de la sécurité restreinte des pods par défaut et le mode de sécurité de la source du catalogue par défaut est défini sur **legacy**.

Si vous ne souhaitez pas exécuter vos pods de source de catalogue basés sur SQLite dans le cadre d'une application restreinte de la sécurité des pods, vous n'avez pas besoin de mettre à jour votre source de catalogue dans OpenShift Container Platform 4.12. Cependant, pour garantir l'exécution de vos

sources de catalogue dans les futures versions d'OpenShift Container Platform, vous devez mettre à jour vos sources de catalogue pour qu'elles s'exécutent dans le cadre d'une application restreinte de la sécurité des pods.

En tant qu'auteur de catalogue, vous pouvez activer la compatibilité avec l'application de la sécurité des pods restreints en effectuant l'une des actions suivantes :

- Migrez votre catalogue vers le format de catalogue basé sur les fichiers.
- Mettez à jour votre image de catalogue avec une version de l'outil **opm** CLI publiée avec OpenShift Container Platform 4.11 ou une version ultérieure.

Si vous ne souhaitez pas mettre à jour l'image du catalogue de votre base de données SQLite ou migrer votre catalogue vers le format de catalogue basé sur des fichiers, vous pouvez configurer votre catalogue pour qu'il s'exécute avec des autorisations élevées.

Pour plus d'informations, voir Sources du catalogue et admission de la sécurité des pods .

Opérateur SDK 1.25.4

OpenShift Container Platform 4.12 supporte Operator SDK 1.25.4. Voir Installer l'Operator SDK CLI pour installer ou mettre à jour cette dernière version.

NOTE

Operator SDK 1.25.4 prend en charge Kubernetes 1.25.

Pour plus d'informations, voir Beta APIs removed from Kubernetes 1.25 et Validating bundle manifests for APIs removed from Kubernetes 1.25.

Si vous avez des projets Operator qui ont été précédemment créés ou maintenus avec Operator SDK 1.22.0, mettez à jour vos projets pour maintenir la compatibilité avec Operator SDK 1.25.4.

- Mise à jour des projets de l'opérateur Go-based
- Mise à jour des projets d'opérateurs basés sur Ansible
- Mise à jour des projets de l'opérateur basé sur le Helm
- Mise à jour des projets de l'opérateur hybride basé sur le gouvernail
- Mise à jour des projets d'opérateurs basés sur Java

L'opérateur LVM s'appelle désormais Logical Volume Manager Storage

L'opérateur LVM qui était précédemment livré avec Red Hat OpenShift Data Foundation nécessite une installation via OpenShift Data Foundation. Dans OpenShift Container Platform v4.12, l'opérateur LVM a été renommé *Logical Volume Manager Storage* . Désormais, vous l'installez en tant qu'opérateur autonome à partir du catalogue OpenShift Operator. Logical Volume Manager Storage permet le provisionnement dynamique du stockage en bloc sur un cluster OpenShift unique à nœud unique et à ressources limitées.

1.5. FONCTIONNALITÉS OBSOLÈTES ET SUPPRIMÉES

Certaines fonctionnalités disponibles dans les versions précédentes sont devenues obsolètes ou ont été supprimées.

Les fonctionnalités dépréciées sont toujours incluses dans OpenShift Container Platform et continuent

d'être prises en charge ; cependant, elles seront supprimées dans une prochaine version de ce produit et ne sont pas recommandées pour les nouveaux déploiements. Pour la liste la plus récente des principales fonctionnalités dépréciées et supprimées dans OpenShift Container Platform 4.12, reportez-vous au tableau ci-dessous. Des détails supplémentaires pour plus de fonctionnalités qui ont été dépréciées et supprimées sont répertoriés après le tableau.

Dans les tableaux suivants, les caractéristiques sont marquées par les statuts suivants :

- *General Availability*
- *Deprecated*
- *Removed*

Fonctionnalités obsolètes et supprimées de l'opérateur

Tableau 1.2. Opérateur obsolète et tracker supprimé

Fonctionnalité	4.10	4.11	4.12
Format de base de données SQLite pour les catalogues des opérateurs	Déclassé	Déclassé	Déclassé

Images des fonctionnalités obsolètes et supprimées

Tableau 1.3. Suivi des images dépréciées et supprimées

Fonctionnalité	4.10	4.11	4.12
ImageChangesInProgress condition pour l'opérateur d'échantillonnage en grappe	Déclassé	Déclassé	Déclassé
MigrationInProgress condition pour l'opérateur d'échantillonnage en grappe	Déclassé	Déclassé	Déclassé
Suppression des images Jenkins de la charge utile d'installation	Disponibilité générale	Supprimé	Supprimé

Surveillance des fonctionnalités obsolètes et supprimées

Tableau 1.4. Suivi des trackers obsolètes et supprimés

Fonctionnalité	4.10	4.11	4.12
Composant Grafana dans la pile de surveillance	Déclassé	Supprimé	Supprimé
Accès aux interfaces Prometheus et Grafana dans la pile de surveillance	Déclassé	Supprimé	Supprimé

Installation des fonctionnalités obsolètes et supprimées

Tableau 1.5. Installation d'un tracker obsolète et supprimé

Fonctionnalité	4.10	4.11	4.12
vSphere 6.7 Update 2 ou antérieur	Déclassé	Supprimé	Supprimé
vSphere 7.0 Update 1 ou antérieur	Disponibilité générale	Déclassé	Déclassé
VMware ESXi 6.7 Update 2 ou version antérieure	Déclassé	Supprimé	Supprimé
VMware ESXi 7.0 Update 1 ou version antérieure	Disponibilité générale	Déclassé	Déclassé
Requêtes CoreDNS pour le domaine **cluster.local**	Disponibilité générale	Disponibilité générale	Déclassé
ingressVIP et **apiVIP** dans le fichier **install-config.yaml** pour les clusters d'infrastructure fournis par le programme d'installation	Disponibilité générale	Disponibilité générale	Déclassé

Mise à jour des fonctionnalités obsolètes et supprimées des clusters

Tableau 1.6. Mise à jour du tracker des clusters dépréciés et supprimés

Fonctionnalité	4.10	4.11	4.12
Version 13 du matériel virtuel	Déclassé	Supprimé	Supprimé

Fonctionnalités de stockage obsolètes et supprimées

Tableau 1.7. Stockage d'un tracker obsolète et supprimé

Fonctionnalité	4.10	4.11	4.12
Snapshot.storage.k8s.io/v1beta1 Point de terminaison de l'API	Déclassé	Supprimé	Supprimé
Stockage persistant à l'aide de FlexVolume	Déclassé	Déclassé	Déclassé

Fonctionnalités d'authentification et d'autorisation dépréciées et supprimées

Tableau 1.8. Authentication and authorization deprecated and removed tracker (en anglais)

Fonctionnalité	4.10	4.11	4.12
Génération automatique de secrets de jetons de compte de service	Disponibilité générale	Supprimé	Supprimé

Activation de matériel spécialisé et de pilotes Fonctionnalités obsolètes et supprimées

Tableau 1.9. Matériel spécialisé et activation des pilotes : tracker déprécié et supprimé

Fonctionnalité	4.10	4.11	4.12
Opérateur spécial de ressources (OSR)	Avant-première technologique	Avant-première technologique	Supprimé

Fonctionnalités multiarchitectures dépréciées et supprimées

Tableau 1.10. Tracker multiarchitecture déprécié et supprimé

Fonctionnalité	4.10	4.11	4.12
IBM POWER8 tous les modèles (**ppc64le**)	Disponibilité générale	Disponibilité générale	Déclassé
IBM IBM POWER9 AC922 (**ppc64le**)	Disponibilité générale	Disponibilité générale	Déclassé
IBM IBM POWER9 IC922 (**ppc64le**)	Disponibilité générale	Disponibilité générale	Déclassé
IBM IBM POWER9 LC922 (**ppc64le**)	Disponibilité générale	Disponibilité générale	Déclassé
IBM z13 tous les modèles (**s390x**)	Disponibilité générale	Disponibilité générale	Déclassé
IBM LinuxONE Emperor (**s390x**)	Disponibilité générale	Disponibilité générale	Déclassé
IBM LinuxONE Rockhopper (**s390x**)	Disponibilité générale	Disponibilité générale	Déclassé
AMD64 (x86_64) v1 CPU	Disponibilité générale	Disponibilité générale	Déclassé

Mise en réseau des fonctionnalités obsolètes et supprimées

Tableau 1.11. Mise en réseau de trackers obsolètes et supprimés

Fonctionnalité	4.10	4.11	4.12
Kuryr sur RHOSP	Disponibilité générale	Disponibilité générale	Déclassé

Fonctionnalités obsolètes et supprimées de la console web

Tableau 1.12. Console web dépréciée et tracker supprimé

Fonctionnalité	4.10	4.11	4.12
Console multicluster (aperçu technologique)	REM	REM	REM

1.5.1. Fonctionnalités obsolètes

1.5.1.1. Red Hat Virtualization (RHV) en tant que plateforme hôte pour OpenShift Container Platform sera déprécié

Red Hat Virtualization (RHV) sera déprécié dans une prochaine version d'OpenShift Container Platform. La prise en charge d'OpenShift Container Platform sur RHV sera supprimée dans une prochaine version d'OpenShift Container Platform, actuellement prévue comme OpenShift Container Platform 4.14.

1.5.1.2. Les requêtes DNS Wildcard pour le domaine **cluster.local** sont obsolètes

CoreDNS arrêtera de supporter les requêtes DNS wildcard pour les noms sous le domaine **cluster.local**. Ces requêtes seront résolues dans OpenShift Container Platform 4.12 comme dans les versions antérieures, mais leur prise en charge sera supprimée dans une prochaine version d'OpenShift Container Platform.

1.5.1.3. Les modèles de matériel spécifiques sur les architectures de CPU **ppc64le, s390x, et x86_64 v1 sont obsolètes**

Dans OpenShift Container Platform 4.12, la prise en charge de la fonctionnalité RHCOS est obsolète pour :

- IBM POWER8 tous les modèles (ppc64le)
- IBM POWER9 AC922 (ppc64le)
- IBM POWER9 IC922 (ppc64le)
- IBM POWER9 LC922 (ppc64le)
- IBM z13 tous les modèles (s390x)
- LinuxONE Emperor (s390x)
- LinuxONE Rockhopper (s390x)
- AMD64 (x86_64) v1 CPU

Bien que ces modèles de matériel restent entièrement pris en charge dans OpenShift Container Platform 4.12, Red Hat vous recommande d'utiliser des modèles de matériel plus récents.

1.5.1.4. Prise en charge de Kuryr pour les clusters fonctionnant sous RHOSP

Dans OpenShift Container Platform 4.12, la prise en charge de Kuryr sur les clusters qui fonctionnent sur RHOSP est dépréciée. La prise en charge sera supprimée au plus tôt dans OpenShift Container Platform 4.14.

1.5.2. Fonctionnalités supprimées

1.5.2.1. Les API bêta supprimées de Kubernetes 1.25

Kubernetes 1.25 a supprimé les API dépréciées suivantes. Vous devez donc migrer les manifestes et les clients API pour utiliser la version appropriée de l'API. Pour plus d'informations sur la migration des API supprimées, consultez la documentation de Kubernetes .

Tableau 1.13. API supprimées de Kubernetes 1.25

Ressources	API supprimée	Migrer vers	Changements notables
CronJob	**batch/v1beta1**	**batch/v1**	Non
EndpointSlice	**discovery.k8s.io/v1beta1**	**discovery.k8s.io/v1**	Oui
Event	**events.k8s.io/v1beta1**	**events.k8s.io/v1**	Oui
HorizontalPodAutoscaler	**autoscaling/v2beta1**	**autoscaling/v2**	Non
PodDisruptionBudget	**policy/v1beta1**	**policy/v1**	Oui
PodSecurityPolicy	**policy/v1beta1**	Admission à la sécurité des pods [1]	Oui
RuntimeClass	**node.k8s.io/v1beta1**	**node.k8s.io/v1**	Non

1. Pour plus d'informations sur l'admission à la sécurité des pods dans OpenShift Container Platform, voir Comprendre et gérer l'admission à la sécurité des pods .

1.5.2.2. Prise en charge des fichiers vides et de la sortie standard pour la commande oc registry login

Les options **--registry-config** et **--to option** de la commande **oc registry login** n'acceptent plus les fichiers vides. Ces options continuent de fonctionner avec des fichiers qui n'existent pas. La possibilité d'écrire la sortie sur **-** (stdout) est également supprimée.

1.5.2.3. La prise en charge par RHEL 7 de l'OpenShift CLI (oc) a été supprimée

La prise en charge de l'utilisation de Red Hat Enterprise Linux (RHEL) 7 avec l'OpenShift CLI (**oc**) a été supprimée. Si vous utilisez l'OpenShift CLI (**oc**) avec RHEL, vous devez utiliser RHEL 8 ou une version ultérieure.

1.5.2.4. Les commandes OpenShift CLI (oc) ont été supprimées

Les commandes OpenShift CLI (**oc**) suivantes ont été supprimées avec cette version :

- **oc adm migrate etcd-ttl**
- **oc adm migrate image-references**
- **oc adm migrate legacy-hpa**
- **oc adm migrate storage**

1.5.2.5. Le composant Grafana est retiré de la pile de surveillance

Le composant Grafana ne fait plus partie de la pile de surveillance d'OpenShift Container Platform 4.12. En guise d'alternative, rendez-vous sur **Observe → Dashboards** dans la console web d'OpenShift Container Platform pour afficher les tableaux de bord de surveillance.

1.5.2.6. L'accès à l'interface utilisateur de Prometheus et Grafana a été supprimé de la pile de surveillance

L'accès aux interfaces utilisateur tierces Prometheus et Grafana a été supprimé de la pile de surveillance d'OpenShift Container Platform 4.12. Comme alternative, cliquez sur **Observe** dans la console web d'OpenShift Container Platform pour afficher les alertes, les métriques, les tableaux de bord et les cibles de métriques pour les composants de surveillance.

1.5.2.7. La prise en charge de la version 13 du matériel virtuel est supprimée

Dans OpenShift Container Platform 4.11, la prise en charge de la version 13 du matériel virtuel est supprimée. La prise en charge de la version 13 du matériel virtuel a été supprimée dans OpenShift Container Platform 4.9. Red Hat vous recommande d'utiliser la version 15 ou ultérieure du matériel virtuel.

1.5.2.8. La prise en charge du point de terminaison de l'API snapshot v1beta1 est supprimée

Dans OpenShift Container Platform 4.11, la prise en charge du point de terminaison de l'API **snapshot.storage.k8s.io/v1beta1** est supprimée. La prise en charge du point de terminaison de l'API **snapshot.storage.k8s.io/v1beta1** a été supprimée dans OpenShift Container Platform 4.7. Red Hat vous recommande d'utiliser **snapshot.storage.k8s.io/v1**. Tous les objets créés en tant que **v1beta1** sont disponibles via le point de terminaison v1.

1.5.2.9. La prise en charge du déploiement manuel d'un planificateur personnalisé a été supprimée

La prise en charge du déploiement manuel de planificateurs personnalisés a été supprimée avec cette version. Utilisez plutôt le Secondary Scheduler Operator for Red Hat OpenShift pour déployer un planificateur secondaire personnalisé dans OpenShift Container Platform.

1.5.2.10. La prise en charge du déploiement d'OpenShift à nœud unique avec OpenShiftSDN a été supprimée

La prise en charge du déploiement de clusters OpenShift à nœud unique avec OpenShiftSDN a été supprimée avec cette version. OVN-Kubernetes est la solution de mise en réseau par défaut pour les déploiements OpenShift à nœud unique.

1.5.2.11. Suppression des images Jenkins de la charge utile d'installation

- OpenShift Container Platform 4.11 déplace les images \N "OpenShift Jenkins" et \N "OpenShift Agent Base" vers le dépôt **ocp-tools-4** à l'adresse **registry.redhat.io** afin que Red Hat puisse produire et mettre à jour les images en dehors du cycle de vie d'OpenShift Container Platform. Auparavant, ces images se trouvaient dans la charge utile d'installation d'OpenShift Container Platform et dans le référentiel **openshift4** à l'adresse **registry.redhat.io**. Pour plus d'informations, voir OpenShift Jenkins.

- OpenShift Container Platform 4.11 supprime les images \N "OpenShift Jenkins Maven\N" et \N "NodeJS Agent\N" de son payload. Auparavant, OpenShift Container Platform 4.10 a déprécié ces images. Red Hat ne produit plus ces images et elles ne sont pas disponibles dans le dépôt **ocp-tools-4** à l'adresse **registry.redhat.io**.
  Cependant, la mise à niveau vers OpenShift Container Platform 4.11 ne supprime pas les images " OpenShift Jenkins Maven " et " NodeJS Agent " de la version 4.10 et des versions antérieures. Red Hat fournit des corrections de bugs et une assistance pour ces images jusqu'à la fin du cycle de vie de la version 4.10, conformément à la politique de cycle de vie d'OpenShift Container Platform.

  Pour plus d'informations, voir OpenShift Jenkins.

1.5.3. Futures suppressions d'API Kubernetes

La prochaine version mineure d'OpenShift Container Platform devrait utiliser Kubernetes 1.26. Actuellement, il est prévu que Kubernetes 1.26 supprime plusieurs API obsolètes.

Voir le Deprecated API Migration Guide dans la documentation Kubernetes en amont pour la liste des suppressions d'API Kubernetes prévues.

Voir Naviguer dans les dépréciations et suppressions d'API Kubernetes pour plus d'informations sur la façon de vérifier votre cluster pour les API Kubernetes dont la suppression est prévue.

1.6. BUG FIXES

Serveur API et authentification

- Auparavant, l'état de l'opérateur d'authentification de cluster était défini sur **progressing = false** après avoir reçu une erreur **workloadIsBeingUpdatedTooLong**. Dans le même temps, **degraded = false** était conservé pendant la durée de l'erreur **inertia**. Par conséquent, la réduction du temps de progression et l'augmentation du temps de dégradation créaient une situation où **progressing = false** et **degraded = false** étaient définis prématurément. Cela provoquait des tests OpenShift CI incohérents car un état sain était supposé, ce qui était incorrect. Ce problème a été corrigé en supprimant le paramètre **progressing = false** après le retour de l'erreur **workloadIsBeingUpdatedTooLong**. Maintenant, parce qu'il n'y a pas d'état **progressing = false**, les tests OpenShift CI sont plus cohérents. (BZ#2111842)

Provisionnement du matériel Bare Metal

- Dans les versions récentes du firmware du serveur, le temps entre les opérations du serveur a augmenté. Cela entraîne des dépassements de délais lors des installations d'infrastructures provisionnées par l'installateur, lorsque le programme d'installation d'OpenShift Container Platform attend une réponse du contrôleur de gestion de la carte mère (BMC). La nouvelle version **python3-sushy** augmente le nombre de tentatives côté serveur pour contacter le BMC. Cette mise à jour prend en compte le temps d'attente prolongé et évite les dépassements de délai pendant l'installation. (OCPBUGS-4097)

- Avant cette mise à jour, le service de provisionnement d'Ironic ne prenait pas en charge les contrôleurs de gestion de cartes de base (BMC) qui utilisent des eTags faibles combinés à une

validation stricte des eTags. Par conception, si le BMC fournit un eTag faible, Ironic renvoie deux eTags : l'eTag original et l'eTag original converti au format fort pour la compatibilité avec les BMC qui ne supportent pas les eTags faibles. Bien qu'Ironic puisse envoyer deux eTags, la BMC qui utilise une validation stricte des eTags rejette ces demandes en raison de la présence du second eTag. Par conséquent, sur certains serveurs plus anciens, le provisionnement bare-metal a échoué avec l'erreur suivante : **HTTP 412 Precondition Failed**. Dans OpenShift Container Platform 4.12 et plus, ce comportement change et Ironic ne tente plus d'envoyer deux eTags dans les cas où un eTag faible est fourni. Au lieu de cela, si une requête Redfish dépendant d'un eTag échoue avec une erreur de validation d'eTag, Ironic réessaie la requête avec des solutions de contournement connues. Cela minimise le risque d'échec du provisionnement bare-metal sur les machines avec une validation stricte de l'eTag. (OCPBUGS-3479)

- Avant cette mise à jour, lorsqu'un système Redfish comportait un URI de paramétrage, le service de provisionnement Ironic tentait toujours d'utiliser cet URI pour apporter des modifications aux paramètres du BIOS liés au démarrage. Cependant, le provisionnement bare-metal échoue si le contrôleur de gestion de la carte de base (BMC) présente un URI de paramètres mais ne prend pas en charge la modification d'un paramètre particulier du BIOS en utilisant cet URI de paramètres. Dans OpenShift Container Platform 4.12 et plus, si un système dispose d'un Settings URI, Ironic vérifie qu'il peut modifier un paramètre particulier du BIOS en utilisant le Settings URI avant de procéder. Dans le cas contraire, Ironic met en œuvre le changement en utilisant l'URI System. Cette logique supplémentaire garantit qu'Ironic peut appliquer les changements de paramètres du BIOS liés à l'amorçage et que l'approvisionnement en métal nu peut réussir. (OCPBUGS-2052)

Constructions

- Par défaut, Buildah imprime les étapes dans le fichier journal, y compris le contenu des variables d'environnement, qui peuvent inclure des secrets d'entrée de compilation. Bien que vous puissiez utiliser l'argument **--quiet** build pour supprimer l'impression de ces variables d'environnement, cet argument n'est pas disponible si vous utilisez la stratégie de compilation source-image (S2I). La version actuelle corrige ce problème. Pour supprimer l'impression des variables d'environnement, définissez la variable d'environnement **BUILDAH_QUIET** dans votre configuration de compilation :

```
sourceStrategy:
...
  env:
    - name: "BUILDAH_QUIET"
      value: "true"
```

(BZ#2099991)

Informatique en nuage

- Auparavant, les instances n'étaient pas configurées pour respecter l'option par défaut de l'infrastructure GCP pour les redémarrages automatiques. Par conséquent, des instances pouvaient être créées sans utiliser l'option par défaut de l'infrastructure pour les redémarrages automatiques. Cela signifiait parfois que les instances étaient terminées dans GCP mais que leurs machines associées étaient toujours listées dans l'état **Running** parce qu'elles n'avaient pas redémarré automatiquement. Avec cette version, le code de transmission de l'option de redémarrage automatique a été amélioré pour mieux détecter et transmettre la sélection de l'option par défaut par les utilisateurs. Les instances utilisent désormais correctement l'infrastructure par défaut et sont automatiquement redémarrées lorsque l'utilisateur demande la fonctionnalité par défaut. (OCPBUGS-4504)

- La version **v1beta1** de l'objet **PodDisruptionBudget** est désormais obsolète dans Kubernetes. Avec cette version, les références internes à **v1beta1** sont remplacées par **v1**. Ce changement

est interne à l'autoscaler du cluster et ne nécessite pas d'action de la part de l'utilisateur au-delà des conseils donnés dans l'article de la base de connaissances Red Hat Preparing to upgrade to OpenShift Container Platform 4.12. (**OCPBUGS-1484**)

- Auparavant, le contrôleur de machines GCP rapprochait l'état des machines toutes les 10 heures. D'autres fournisseurs fixent cette valeur à 10 minutes afin que les changements qui se produisent en dehors du système Machine API soient détectés dans un court laps de temps. La période de réconciliation plus longue pour GCP pouvait causer des problèmes inattendus tels que des approbations de demandes de signature de certificat (CSR) manquantes en raison d'une adresse IP externe ajoutée mais non détectée pendant une période prolongée. Avec cette version, le contrôleur de machine GCP est mis à jour pour effectuer une réconciliation toutes les 10 minutes afin d'être cohérent avec les autres plateformes et pour que les changements externes soient détectés plus tôt. (**OCPBUGS-4499**)

- Auparavant, en raison d'une mauvaise configuration du déploiement de l'opérateur d'approbation des machines en grappe, l'activation de l'ensemble de fonctionnalités **TechPreviewNoUpgrade** provoquait des erreurs et une dégradation sporadique de l'opérateur. Comme les clusters avec le jeu de fonctionnalités **TechPreviewNoUpgrade** activé utilisent deux instances de Cluster Machine Approver Operator et que les deux déploiements utilisent le même jeu de ports, il y avait un conflit qui entraînait des erreurs pour la topologie à nœud unique. Avec cette version, le déploiement de Cluster Machine Approver Operator est mis à jour pour utiliser un ensemble de ports différent pour les différents déploiements. (**OCPBUGS-2621**)

- Auparavant, la fonctionnalité de mise à l'échelle à partir de zéro dans Azure reposait sur une liste de types d'instance compilée de manière statique, associant le nom du type d'instance au nombre de CPU et à la quantité de mémoire allouée au type d'instance. Cette liste est devenue obsolète au fil du temps. Avec cette version, les informations sur les tailles des types d'instance sont collectées dynamiquement à partir de l'API Azure directement pour éviter que la liste ne devienne obsolète. (**OCPBUGS-2558**)

- Auparavant, les pods du gestionnaire de terminaison de l'API Machine ne démarraient pas sur les instances ponctuelles. Par conséquent, les pods qui s'exécutaient sur des instances ponctuelles entachées ne recevaient pas de signal de terminaison si l'instance était terminée. Cela pouvait entraîner une perte de données dans les applications de charge de travail. Avec cette version, le déploiement du gestionnaire de terminaison de l'API Machine est modifié pour tolérer les taints et les pods s'exécutant sur des instances ponctuelles avec des taints reçoivent maintenant des signaux de terminaison. (**OCPBUGS-1274**)

- Auparavant, les messages d'erreur pour les clusters Azure n'expliquaient pas qu'il n'était pas possible de créer de nouvelles machines avec des adresses IP publiques pour une installation déconnectée qui utilise uniquement la stratégie de publication interne. Avec cette version, le message d'erreur est mis à jour pour plus de clarté. (**OCPBUGS-519**)

- Auparavant, l'opérateur du gestionnaire de contrôleur cloud ne vérifiait pas le fichier de configuration **cloud-config** pour les clusters AWS. Par conséquent, il n'était pas possible de transmettre des paramètres supplémentaires au composant AWS cloud controller manager en utilisant le fichier de configuration. Avec cette version, le Cloud Controller Manager Operator vérifie la ressource d'infrastructure et analyse les références au fichier de configuration **cloud-config** afin que les utilisateurs puissent configurer des paramètres supplémentaires. (**BZ#2104373**)

- Auparavant, lorsqu'Azure ajoutait de nouveaux types d'instance et activait la prise en charge de la mise en réseau accélérée sur des types d'instance qui n'en disposaient pas auparavant, la liste des instances Azure dans le contrôleur de machine devenait obsolète. Par conséquent, le contrôleur de machine ne pouvait pas créer de machines avec des types d'instance qui ne prenaient pas auparavant en charge la mise en réseau accélérée, même s'ils prenaient en charge cette fonctionnalité sur Azure. Avec cette version, les informations requises sur le type

d'instance sont récupérées à partir de l'API Azure avant la création de la machine afin de les maintenir à jour pour que le contrôleur de machine puisse créer des machines avec des types d'instance nouveaux et mis à jour. Cette correction s'applique également à tous les types d'instance qui seront ajoutés à l'avenir. (BZ#2108647)

- Auparavant, l'autoscaler de cluster ne respectait pas les étiquettes de topologie AWS, IBM Cloud et Alibaba Cloud pour les pilotes CSI lors de l'utilisation du fournisseur Cluster API. Par conséquent, les nœuds avec l'étiquette de topologie n'étaient pas traités correctement par l'autoscaler lorsqu'il tentait d'équilibrer les nœuds au cours d'un événement de mise à l'échelle. Avec cette version, les processeurs personnalisés de l'autoscaler sont mis à jour afin de respecter ce label. L'autoscaler peut désormais équilibrer des groupes de nœuds similaires portant les étiquettes AWS, IBM Cloud ou Alibaba CSI. (BZ#2001027)

- Auparavant, les fournisseurs de cloud Power VS n'étaient pas en mesure de récupérer l'adresse IP de la machine à partir d'un serveur DHCP. La modification de l'adresse IP ne mettait pas à jour le nœud, ce qui entraînait certaines incohérences, telles que des demandes de signature de certificat en attente. Avec cette version, le fournisseur de cloud Power VS est mis à jour pour récupérer l'adresse IP de la machine à partir du serveur DHCP, de sorte que les adresses IP des nœuds sont cohérentes avec l'adresse IP de la machine. (BZ#2111474)

- Auparavant, les machines créées dans les premières versions d'OpenShift Container Platform avec des configurations invalides ne pouvaient pas être supprimées. Avec cette version, les webhooks qui empêchent la création de machines avec des configurations invalides n'empêchent plus la suppression des machines invalides existantes. Les utilisateurs peuvent désormais supprimer ces machines de leur cluster en supprimant manuellement les finaliseurs sur ces machines. (BZ#2101736)

- Auparavant, des baux DHCP de courte durée, causés par le fait que **NetworkManager** n'était pas exécuté en tant que démon ou en mode continu, entraînaient le blocage des machines lors du provisionnement initial et leur incapacité à devenir des nœuds dans le cluster. Avec cette version, des vérifications supplémentaires ont été ajoutées afin que si une machine reste bloquée dans cet état, elle soit supprimée et recréée automatiquement. Les machines affectées par cette condition de réseau peuvent devenir des nœuds après un redémarrage à partir du contrôleur Machine API. (BZ#2115090)

- Auparavant, lors de la création d'une nouvelle ressource **Machine** à l'aide d'un profil de machine qui n'existe pas dans IBM Cloud, les machines restaient bloquées dans la phase **Provisioning**. Avec cette version, la validation est ajoutée au fournisseur IBM Cloud Machine API pour s'assurer qu'un profil de machine existe, et les machines avec un profil de machine invalide sont rejetées par l'API Machine. (BZ#2062579)

- Auparavant, le fournisseur Machine API pour AWS ne vérifiait pas que le groupe de sécurité défini dans la spécification de la machine existait. Au lieu de renvoyer une erreur dans ce cas, il utilisait un groupe de sécurité par défaut, qui ne devrait pas être utilisé pour les machines OpenShift Container Platform, et créait avec succès une machine sans informer l'utilisateur que le groupe par défaut était utilisé. Avec cette version, l'API Machine renvoie une erreur lorsque les utilisateurs définissent des noms de groupes de sécurité incorrects ou vides dans la spécification de la machine. (BZ#2060068)

- Auparavant, le fournisseur de l'API Machine Azure ne traitait pas les valeurs fournies par l'utilisateur pour les types d'instance comme sensibles à la casse. Cela entraînait des erreurs fausses positives lorsque les types d'instance étaient corrects mais ne correspondaient pas à la casse. Avec cette version, les types d'instance sont convertis en caractères minuscules afin que les utilisateurs obtiennent des résultats corrects sans erreurs faussement positives dues à une mauvaise correspondance des majuscules et des minuscules. (BZ#2085390)

- Auparavant, il n'y avait pas de vérification des valeurs nulles dans les annotations d'un objet

machine avant de tenter d'accéder à l'objet. Cette situation était rare, mais provoquait la panique du contrôleur de machine lors de la réconciliation de la machine. Avec cette version, les valeurs nulles sont vérifiées et le contrôleur de machine est en mesure de réconcilier les machines sans annotations. (BZ#2106733)

- Auparavant, les mesures de l'autoscaler de cluster pour l'utilisation du CPU et de la mémoire du cluster n'atteignaient jamais, ou ne dépassaient jamais, les limites définies par la ressource **ClusterAutoscaler**. Par conséquent, aucune alerte n'était déclenchée lorsque l'autoscaler de cluster ne pouvait pas évoluer en raison des limitations de ressources. Avec cette version, une nouvelle métrique appelée **cluster_autoscaler_skipped_scale_events_count** est ajoutée à l'autoscaler de cluster pour détecter plus précisément lorsque les limites de ressources sont atteintes ou dépassées. Les alertes sont désormais déclenchées lorsque l'autoscaler de cluster n'est pas en mesure d'augmenter la taille du cluster parce qu'il a atteint les limites de ressources du cluster. (BZ#1997396)

- Auparavant, lorsque le fournisseur de l'API Machine ne parvenait pas à récupérer l'adresse IP de la machine, il ne définissait pas le nom DNS interne et les demandes de signature de certificat de la machine n'étaient pas automatiquement approuvées. Avec cette version, le fournisseur de machines Power VS est mis à jour pour définir le nom du serveur comme nom DNS interne même s'il ne parvient pas à récupérer l'adresse IP. (BZ#2111467)

- Auparavant, le contrôleur de machine vSphere Machine API définissait l'indicateur **PowerOn** lors du clonage d'une VM. Cela créait une tâche **PowerOn** dont le contrôleur de machine n'avait pas connaissance. Si cette tâche **PowerOn** échouait, les machines étaient bloquées dans la phase **Provisioned** mais n'étaient jamais mises sous tension. Avec cette version, la séquence de clonage est modifiée pour éviter ce problème. En outre, le contrôleur de machine tente à nouveau de mettre sous tension la VM en cas d'échec et signale correctement les échecs. (BZ#2087981, OCPBUGS-954)

- Avec cette version, les groupes de sécurité AWS sont marqués immédiatement au lieu d'être marqués après leur création. Cela signifie que moins de demandes sont envoyées à AWS et que les privilèges d'utilisateur requis sont réduits. (BZ#2098054, OCPBUGS-3094)

- Auparavant, un bogue dans le fournisseur de cloud hérité RHOSP entraînait un plantage si certaines opérations RHOSP étaient tentées après l'échec de l'authentification. Par exemple, l'arrêt d'un serveur entraîne le gestionnaire de contrôleur Kubernetes à récupérer des informations sur le serveur auprès de RHOSP, ce qui a déclenché ce bogue. Par conséquent, si l'authentification initiale dans le nuage a échoué ou a été configurée de manière incorrecte, l'arrêt d'un serveur a provoqué un plantage du gestionnaire de contrôleur Kubernetes. Avec cette version, le fournisseur de cloud hérité de RHOSP est mis à jour pour ne pas tenter d'appeler l'API RHOSP s'il ne s'est pas authentifié avec succès auparavant. Désormais, l'arrêt d'un serveur dont les informations d'identification ne sont pas valides n'entraîne plus le plantage du gestionnaire de contrôleur Kubernetes. (BZ#2102383)

Console du développeur

- Auparavant, l'espace de noms **openshift-config** était codé en dur pour la ressource personnalisée **HelmChartRepository**, qui était le même espace de noms pour la ressource personnalisée **ProjectHelmChartRepository**. Cela empêchait les utilisateurs d'ajouter des ressources personnalisées privées **ProjectHelmChartRepository** dans l'espace de noms de leur choix. Par conséquent, les utilisateurs ne pouvaient pas accéder aux secrets et aux cartes de configuration dans l'espace de noms **openshift-config**. Cette mise à jour corrige la définition de la ressource personnalisée **ProjectHelmChartRepository** avec un champ **namespace** qui peut lire le secret et les cartes de configuration d'un espace de noms choisi par un utilisateur disposant des autorisations correctes. En outre, l'utilisateur peut ajouter des secrets et des cartes de configuration à l'espace de noms accessible, et il peut ajouter des dépôts de cartes Helm privés dans l'espace de noms utilisé pour les ressources de création. (BZ#2071792)

Registre des images

- Auparavant, le contrôleur du déclencheur d'images n'avait pas le droit de modifier les objets. Par conséquent, les annotations de déclenchement d'images ne fonctionnaient pas sur certaines ressources. Cette mise à jour crée une liaison de rôle de cluster qui fournit au contrôleur les autorisations nécessaires pour mettre à jour les objets en fonction des annotations. (BZ#2055620)

- Auparavant, l'opérateur du registre des images n'avait pas de condition **progressing** pour l'ensemble de démons **node-ca** et utilisait **generation** à partir d'un objet incorrect. Par conséquent, le jeu de démons **node-ca** pouvait être marqué comme **degraded** alors que l'opérateur était toujours en cours d'exécution. Cette mise à jour ajoute la condition **progressing**, qui indique que l'installation n'est pas terminée. Par conséquent, l'opérateur de registre d'images installe avec succès le jeu de démons **node-ca** et le programme d'installation attend qu'il soit entièrement déployé. ([BZ#2093440)

Installateur

- Auparavant, le nombre de tags définis par l'utilisateur pris en charge était de 8, et les tags OpenShift Container Platform réservés étaient de 2 pour les ressources AWS. Avec cette version, le nombre de balises définies par l'utilisateur prises en charge est désormais de 25 et les balises OpenShift Container Platform réservées sont de 25 pour les ressources AWS. Vous pouvez désormais ajouter jusqu'à 25 balises utilisateur lors de l'installation. (CFE#592)

- Auparavant, l'installation d'un cluster sur Amazon Web Services démarrait puis échouait lorsque l'utilisateur administratif IAM ne disposait pas de l'autorisation **s3:GetBucketPolicy**. Cette mise à jour ajoute cette stratégie à la liste de contrôle que le programme d'installation utilise pour s'assurer que toutes les autorisations requises sont attribuées. Par conséquent, le programme d'installation arrête désormais l'installation en affichant un avertissement indiquant que l'utilisateur administratif IAM ne dispose pas de l'autorisation **s3:GetBucketPolicy**. (BZ#2109388)

- Auparavant, l'installation d'un cluster sur Microsoft Azure échouait lorsque les séries Azure DCasv5 ou DCadsv5 de VM confidentielles étaient spécifiées comme nœuds du plan de contrôle. Avec cette mise à jour, le programme d'installation arrête maintenant l'installation avec une erreur, qui indique que les VM confidentielles ne sont pas encore prises en charge. (BZ#2055247)

- Auparavant, la collecte des journaux de démarrage n'était pas possible tant que les machines du plan de contrôle ne fonctionnaient pas. Avec cette mise à jour, la collecte des journaux de démarrage ne nécessite plus que la disponibilité de la machine de démarrage. (BZ#2105341)

- Auparavant, si l'installation d'un cluster sur Google Cloud Platform échouait parce que le compte de service ne disposait pas d'autorisations suffisantes, le message d'erreur qui en résultait ne mentionnait pas cet élément comme cause de l'échec. Cette mise à jour améliore le message d'erreur, qui indique désormais aux utilisateurs de vérifier les autorisations attribuées au compte de service. (BZ#2103236)

- Auparavant, lorsqu'une installation sur Google Cloud provider (GCP) échouait parce qu'une région GCP non valide était spécifiée, le message d'erreur qui en résultait ne mentionnait pas cet élément comme cause de l'échec. Cette mise à jour améliore le message d'erreur, qui indique désormais que la région n'est pas valide. (BZ#2102324)

- Auparavant, les installations de clusters utilisant Hive pouvaient échouer si Hive utilisait une ancienne version du fichier install-config.yaml. Cette mise à jour permet au programme d'installation d'accepter les anciennes versions du fichier **install-config.yaml** fourni par Hive. (BZ#2098299)

- Auparavant, le programme d'installation autorisait à tort les paramètres **apiVIP** et **ingressVIP** à utiliser la même adresse IPv6 s'ils représentaient l'adresse différemment, par exemple en la listant dans un format abrégé. Dans cette mise à jour, le programme d'installation valide correctement ces deux paramètres indépendamment de leur formatage, en exigeant des adresses IP distinctes pour chaque paramètre. (BZ#2103144)

- Auparavant, la désinstallation d'un cluster à l'aide du programme d'installation ne supprimait pas toutes les ressources des clusters installés sur GCP si le nom du cluster comportait plus de 22 caractères. Dans cette mise à jour, la désinstallation d'un cluster à l'aide du programme d'installation localise et supprime correctement toutes les ressources des clusters GCP lorsque les noms des clusters sont longs. (BZ#2076646)

- Auparavant, lors de l'installation d'un cluster sur Red Hat OpenStack Platform (RHOSP) avec plusieurs réseaux définis dans le paramètre **machineNetwork**, le programme d'installation ne créait des règles de groupe de sécurité que pour le premier réseau. Avec cette mise à jour, le programme d'installation crée des règles de groupe de sécurité pour tous les réseaux définis dans le paramètre **machineNetwork** afin que les utilisateurs n'aient plus à modifier manuellement les règles de groupe de sécurité après l'installation. (BZ#2095323)

- Auparavant, les utilisateurs pouvaient définir manuellement les adresses IP virtuelles API et Ingress à des valeurs qui entraient en conflit avec le pool d'allocation du serveur DHCP lors de l'installation d'un cluster sur OpenStack. Cela pouvait amener le serveur DHCP à attribuer l'une des adresses VIP à une nouvelle machine, qui ne démarrait pas. Dans cette mise à jour, le programme d'installation valide les adresses VIP fournies par l'utilisateur pour s'assurer qu'elles n'entrent pas en conflit avec les pools DHCP. (BZ#1944365)

- Auparavant, lors de l'installation d'un cluster sur vSphere à l'aide d'un centre de données intégré dans un dossier, le programme d'installation ne pouvait pas localiser l'objet centre de données, ce qui entraînait l'échec de l'installation. Dans cette mise à jour, le programme d'installation peut traverser le répertoire qui contient l'objet centre de données, ce qui permet à l'installation de réussir. (BZ#2097691)

- Auparavant, lors de l'installation d'un cluster sur Azure utilisant l'architecture arm64 avec une infrastructure fournie par l'installateur, la ressource de définition d'image pour **hyperVGeneration** V1 avait une valeur d'architecture incorrecte de **x64**. Avec cette mise à jour, la ressource de définition d'image pour **hyperVGeneration** V1 a la valeur d'architecture correcte de **Arm64**. (OCPBUGS-3639)

- Auparavant, lors de l'installation d'un cluster sur VMware vSphere, l'installation pouvait échouer si l'utilisateur spécifiait un dossier défini par l'utilisateur dans la section **failureDomain** du fichier **install-config.yaml**. Avec cette mise à jour, le programme d'installation valide correctement les dossiers définis par l'utilisateur dans la section **failureDomain** du fichier **install-config.yaml**. (OCPBUGS-3343)

- Auparavant, lors de la destruction d'un cluster partiellement déployé après l'échec d'une installation sur VMware vSphere, certains dossiers de machines virtuelles n'étaient pas détruits. Cette erreur pouvait se produire dans les clusters configurés avec plusieurs centres de données vSphere ou plusieurs clusters vSphere. Avec cette mise à jour, toute l'infrastructure fournie par l'installateur est correctement supprimée lors de la destruction d'un cluster partiellement déployé après un échec de l'installation. (OCPBUGS-1489)

- Auparavant, lors de l'installation d'un cluster sur VMware vSphere, l'installation échouait si l'utilisateur spécifiait le paramètre **platform.vsphere.vcenters** sans spécifier le paramètre **platform.vsphere.failureDomains.topology.networks** dans le fichier **install-config.yaml**. Avec cette mise à jour, le programme d'installation avertit l'utilisateur que le champ **platform.vsphere.failureDomains.topology.networks** est requis lorsqu'il spécifie **platform.vsphere.vcenters**. (OCPBUGS-1698)

- Auparavant, lors de l'installation d'un cluster sur VMware vSphere, l'installation échouait si l'utilisateur définissait les paramètres **platform.vsphere.vcenters** et **platform.vsphere.failureDomains** mais ne définissait pas **platform.vsphere.defaultMachinePlatform.zones**, ou **compute.platform.vsphere.zones** et **controlPlane.platform.vsphere.zones**. Avec cette mise à jour, le programme d'installation valide que l'utilisateur a défini le paramètre **zones** dans les déploiements multi-régions ou multi-zones avant l'installation. (OCPBUGS-1490)

Gestionnaire de contrôleur Kubernetes

- Auparavant, l'opérateur du gestionnaire de contrôleur Kubernetes signalait **degraded** sur les environnements sans la présence d'une pile de surveillance. Avec cette mise à jour, l'opérateur du gestionnaire du contrôleur Kubernetes ne vérifie pas la surveillance pour les indices de dégradation lorsque la pile de surveillance n'est pas présente. (BZ#2118286)

- Avec cette mise à jour, les alertes de Kubernetes Controller Manager (**KubeControllerManagerDown**, **PodDisruptionBudgetAtLimit**, **PodDisruptionBudgetLimit**, et **GarbageCollectorSyncFailed**) ont des liens vers des runbooks Github. Les runbooks aident les utilisateurs à comprendre le débogage de ces alertes. (BZ#2001409)

Ordonnanceur Kubernetes

- Auparavant, le déploiement du planificateur secondaire n'était pas supprimé après la suppression d'une ressource personnalisée du planificateur secondaire. Par conséquent, l'opérateur et l'opérande de planification secondaire n'étaient pas complètement désinstallés. Avec cette mise à jour, la référence propriétaire correcte est définie dans la ressource personnalisée du planificateur secondaire de sorte qu'elle pointe vers le déploiement du planificateur secondaire. Par conséquent, les déploiements du planificateur secondaire sont supprimés lorsque la ressource personnalisée du planificateur secondaire est supprimée. (BZ#2100923)

- Pour la version 4.12 d'OpenShift Container Platform, le désarchiveur peut maintenant publier des événements à un groupe API parce que la version ajoute des règles supplémentaires de contrôle d'accès basé sur les rôles (RBAC) au profil du désarchiveur.(OCPBUGS-2330)

Machine Config Operator

- Auparavant, la ressource **ControllerConfig** de l'opérateur de configuration de machine (MCO), qui contient des certificats importants, n'était synchronisée que si la synchronisation du démon de l'opérateur réussissait. Par conception, les nœuds non prêts pendant la synchronisation d'un démon empêchent la synchronisation de ce démon, de sorte que les nœuds non prêts empêchent indirectement la synchronisation de la ressource **ControllerConfig**, et donc de ces certificats. Il en résultait une dégradation éventuelle de la grappe en cas de nœuds non prêts en raison de l'impossibilité d'effectuer la rotation des certificats contenus dans la ressource **ControllerConfig**. Avec cette version, la synchronisation de la ressource **ControllerConfig** ne dépend plus de la réussite de la synchronisation du démon, de sorte que la ressource **ControllerConfig** continue à se synchroniser si la synchronisation du démon échoue. Cela signifie que les nœuds non prêts n'empêchent plus la ressource **ControllerConfig** de se synchroniser, de sorte que les certificats continuent d'être mis à jour même lorsqu'il y a des nœuds non prêts. (BZ#2034883)

Console de gestion

- Auparavant, la page **Operator details** tentait d'afficher plusieurs messages d'erreur, mais le composant "message d'erreur" ne peut afficher qu'un seul message d'erreur à la fois. Par conséquent, les messages d'erreur pertinents n'étaient pas affichés. Avec cette mise à jour, la

page **Operator details** n'affiche que le premier message d'erreur, de sorte que l'utilisateur voit une erreur pertinente. (OCPBUGS-3927)

- Auparavant, le nom du produit pour Azure Red Hat OpenShift était incorrect dans la gestion des cas clients (CCM). Par conséquent, la console devait utiliser le même nom de produit incorrect pour remplir correctement les champs dans CCM. Une fois le nom du produit mis à jour dans CCM, la console a dû être mise à jour également. Avec cette mise à jour, le même nom de produit correct dans CCM est correctement rempli avec le nom de produit Azure correct lorsque l'on suit le lien depuis la console. (OCPBUGS-869)

- Auparavant, lorsqu'une page de plugin entraînait une erreur, celle-ci n'était pas réinitialisée lorsque l'utilisateur s'éloignait de la page d'erreur, et l'erreur persistait lorsqu'il naviguait vers une page qui n'était pas à l'origine de l'erreur. Avec cette mise à jour, l'état de l'erreur est réinitialisé à sa valeur par défaut lorsqu'un utilisateur navigue vers une nouvelle page, et l'erreur ne persiste plus après avoir navigué vers une nouvelle page. (BZ#2117738, OCPBUGS-523)

- Auparavant, le lien ***View it here*** dans le volet **Operator details** pour les opérateurs installés n'était pas correctement construit lorsque l'option ***All Namespaces*** était sélectionné. En conséquence, le lien tentait de naviguer vers la page **Operator details** pour une version de service de cluster (CSV) dans **All Projects**, ce qui est un itinéraire non valide. Avec cette mise à jour, le lien ***View it here*** pour utiliser l'espace de noms où le CSV est installé se construit maintenant correctement et le lien fonctionne comme prévu. (OCPBUGS-184)

- Auparavant, les numéros de ligne de plus de cinq chiffres posaient un problème esthétique : le numéro de ligne recouvrait la ligne de séparation verticale entre le numéro de ligne et le contenu de la ligne, ce qui rendait la lecture plus difficile. Avec cette mise à jour, l'espace disponible pour les numéros de ligne a été augmenté pour tenir compte des numéros de ligne plus longs, et le numéro de ligne ne recouvre plus la ligne de séparation verticale. (OCPBUGS-183)

- Auparavant, dans la perspective de l'administrateur de la console web, le lien vers ***Learn more about the OpenShift local update services*****Default update server** dans la fenêtre contextuelle de la page **Cluster Settings** produisait une erreur 404. Avec cette mise à jour, le lien fonctionne comme prévu. (BZ#2098234)

- Auparavant, le composant **MatchExpression** ne prenait pas en compte les valeurs de type tableau. Par conséquent, seules des valeurs uniques pouvaient être saisies dans les formulaires utilisant ce composant. Avec cette mise à jour, le composant **MatchExpression** accepte les valeurs séparées par des virgules comme un tableau. (BZ#207690)

- Auparavant, des vérifications redondantes du modèle entraînaient le rechargement des onglets, ce qui provoquait parfois un scintillement du contenu des onglets lorsqu'ils étaient rechargés. Avec cette mise à jour, la vérification redondante du modèle a été supprimée et le modèle n'est vérifié qu'une seule fois. Par conséquent, le contenu des onglets ne scintille plus et ne se réactualise plus. (BZ#2037329)

- Auparavant, lors de la sélection du label **edit** à partir de la liste d'actions sur la page du nœud OpenShift Dedicated, aucune réponse n'était obtenue et une erreur de web hook était renvoyée. Ce problème a été corrigé de sorte que le message d'erreur n'est renvoyé que lorsque l'édition échoue. (BZ#2102098)

- Auparavant, si des questions étaient en suspens, le fait de cliquer sur le lien **Insights** entraînait le blocage de la page. Pour contourner ce problème, vous pouvez attendre que la variable devienne **initialized** avant de cliquer sur le lien **Insights**. La page Insights s'ouvrira alors comme prévu. (BZ#2052662)

- Auparavant, lorsque la ressource **MachineConfigPool** était mise en pause, l'option de remise en pause indiquait **Resume rollouts**. La formulation a été mise à jour et indique désormais **Resume updates**. (BZ#2094240)

- Auparavant, la mauvaise méthode de calcul était utilisée pour compter les nœuds maîtres et les nœuds travailleurs. Avec cette mise à jour, les nœuds ouvriers corrects sont calculés lorsque les nœuds ont à la fois le rôle **master** et **worker**. (BZ#1951901)

- Auparavant, des itinéraires **react-router** conflictuels pour **ImageManifestVuln** entraînaient des tentatives d'affichage d'une page de détails pour **ImageManifestVuln** avec un nom **~new**. Le plugin de sécurité des conteneurs a été mis à jour pour supprimer les conflits d'itinéraires et s'assurer que les listes dynamiques et les extensions de pages de détails sont utilisées sur la page de détails de l'opérateur. Par conséquent, la console affiche correctement les pages de création, de liste et de détails pour **ImageManifestVuln**. (BZ#2080260)

- Auparavant, un YAML incomplet non synchronisé était occasionnellement affiché aux utilisateurs. Avec cette mise à jour, le YAML synchronisé s'affiche toujours. (BZ#2084453)

- Auparavant, lors de l'installation d'un opérateur nécessitant la création d'une ressource personnalisée (CR), le bouton **Create resource** pouvait ne pas installer la CR parce qu'il pointait vers l'espace de noms incorrect. Avec cette mise à jour, le bouton **Create resource** fonctionne comme prévu. (BZ#2094502)

- Auparavant, la fenêtre modale **Cluster update** n'affichait pas correctement les erreurs. Par conséquent, la fenêtre modale **Cluster update** n'affichait ni n'expliquait les erreurs lorsqu'elles se produisaient. Avec cette mise à jour, la fenêtre modale **Cluster update** affiche correctement les erreurs. (BZ#2096350)

Contrôle

- Avant cette mise à jour, les administrateurs de clusters ne pouvaient pas faire la distinction entre un pod qui n'était pas prêt à cause d'un problème de planification et un pod qui n'était pas prêt parce qu'il ne pouvait pas être démarré par le kubelet. Dans les deux cas, l'alerte **KubePodNotReady** était déclenchée. Avec cette mise à jour, l'alerte **KubePodNotScheduled** se déclenche désormais lorsqu'un module n'est pas prêt en raison d'un problème de programmation, et l'alerte **KubePodNotReady** se déclenche lorsqu'un module n'est pas prêt parce qu'il n'a pas pu être démarré par le kubelet. (OCPBUGS-4431)

- Avant cette mise à jour, **node_exporter** fournissait des données sur les interfaces réseau virtuelles telles que les interfaces **tun**, **br** et **ovn-k8s-mp**. Avec cette mise à jour, les mesures relatives à ces interfaces virtuelles ne sont plus collectées, ce qui réduit la consommation de ressources de surveillance. (OCPBUGS-1321)

- Avant cette mise à jour, le démarrage du pod Alertmanager pouvait être retardé en raison de la lenteur de la résolution DNS, et les pods Alertmanager ne démarraient pas. Avec cette version, la valeur du timeout a été augmentée à sept minutes, ce qui empêche le démarrage des pods. (BZ#2083226)

- Avant cette mise à jour, si Prometheus Operator ne parvenait pas à exécuter ou à planifier les pods Prometheus, le système ne fournissait aucune raison sous-jacente à l'échec. Avec cette mise à jour, si les pods Prometheus ne sont pas exécutés ou planifiés, l'opérateur de surveillance de cluster met à jour l'état de surveillance **clusterOperator** en indiquant la raison de l'échec, ce qui peut être utilisé pour résoudre le problème sous-jacent. (BZ#2043518)

- Avant cette mise à jour, si vous créiez une alerte silencieuse depuis la perspective **Developer** dans la console web d'OpenShift Container Platform, des étiquettes externes étaient incluses qui ne correspondaient pas à l'alerte. Par conséquent, l'alerte n'était pas réduite au silence. Avec

cette mise à jour, les étiquettes externes sont désormais exclues lorsque vous créez un silence dans la perspective **Developer**, de sorte que les silences nouvellement créés fonctionnent comme prévu. (BZ#2084504)

- Auparavant, si vous activiez une instance d'Alertmanager dédiée aux projets définis par l'utilisateur, une mauvaise configuration pouvait se produire dans certaines circonstances, et vous n'étiez pas informé que les paramètres de la carte de configuration d'Alertmanager pour les projets définis par l'utilisateur n'étaient pas chargés pour l'instance principale d'Alertmanager ou l'instance dédiée aux projets définis par l'utilisateur. Avec cette version, si cette erreur de configuration se produit, l'opérateur de surveillance des clusters affiche maintenant un message qui vous informe du problème et fournit les étapes de résolution. (BZ#2099939)

- Avant cette mise à jour, si l'opérateur de surveillance de cluster (CMO) ne parvenait pas à mettre à jour Prometheus, il ne vérifiait pas si un déploiement antérieur était en cours d'exécution et signalait que la surveillance de cluster était indisponible même si l'un des pods Prometheus était toujours en cours d'exécution. Avec cette mise à jour, le CMO vérifie désormais si des pods Prometheus sont en cours d'exécution dans cette situation et signale que la surveillance du cluster est indisponible uniquement si aucun pod Prometheus n'est en cours d'exécution. (BZ#2039411)

- Avant cette mise à jour, si vous configuriez OpsGenie comme récepteur d'alertes, un avertissement apparaissait dans le journal indiquant que **api_key** et **api_key_file** s'excluent mutuellement et que **api_key** est prioritaire. Cet avertissement apparaissait même si vous n'aviez pas défini **api_key_file**. Avec cette mise à jour, cet avertissement n'apparaît dans le journal que si vous avez défini à la fois **api_key** et **api_key_file**. (BZ#2093892)

- Avant cette mise à jour, le Telemeter Client (TC) ne chargeait les nouveaux secrets d'extraction que lorsqu'il était redémarré manuellement. Par conséquent, si un secret d'extraction avait été modifié ou mis à jour et que le TC n'avait pas été redémarré, le TC ne parvenait pas à s'authentifier auprès du serveur. Cette mise à jour résout le problème de sorte que lorsque le secret est modifié, le déploiement est automatiquement redémarré et utilise le jeton mis à jour pour s'authentifier. (BZ#2114721)

Mise en réseau

- Auparavant, les routeurs en état de terminaison retardaient la commande **oc cp**, ce qui retardait la commande **oc adm must-gather** jusqu'à ce que le pod soit terminé. Avec cette mise à jour, un délai d'attente pour chaque commande **oc cp** émise est défini pour éviter de retarder l'exécution de la commande **must-gather**. Par conséquent, les pods qui se terminent ne retardent plus les commandes **must-gather**. (BZ#2103283)

- Auparavant, un contrôleur d'entrée ne pouvait pas être configuré avec le type de stratégie de publication de point final **Private** et le protocole PROXY. Avec cette mise à jour, les utilisateurs peuvent désormais configurer un contrôleur d'entrée avec le type de stratégie de publication de point final **Private** et le protocole PROXY. (BZ#2104481)

- Auparavant, le paramètre **routeSelector** effaçait l'état de l'itinéraire du contrôleur d'entrée avant le déploiement du routeur. De ce fait, l'état de l'itinéraire se repeuplait de manière incorrecte. Pour éviter d'utiliser des données périmées, la détection de l'état de l'itinéraire a été mise à jour pour ne plus s'appuyer sur le cache d'objets Kubernetes. En outre, cette mise à jour inclut un correctif pour vérifier l'ID de génération sur le déploiement de la route pour déterminer l'état de la route. Par conséquent, l'état de la route est systématiquement effacé avec une mise à jour de **routeSelector**. (BZ#2101878)

- Auparavant, un cluster mis à niveau à partir d'une version d'OpenShift Container Platform antérieure à la version 4.8 pouvait avoir des objets **Route** orphelins. Cela était dû au fait que les

versions antérieures d'OpenShift Container Platform traduisaient les objets **Ingress** en objets **Route** sans tenir compte de l'indication **IngressClass** d'un objet **Ingress** donné. Avec cette mise à jour, une alerte est envoyée à l'administrateur du cluster concernant tous les objets Route orphelins encore présents dans le cluster après la traduction Ingress-to-Route. Cette mise à jour ajoute également une autre alerte qui notifie à l'administrateur du cluster tous les objets Ingress qui ne spécifient pas de **IngressClass**. (BZ#1962502)

- Auparavant, si un site **configmap** dont dépend le déploiement du routeur n'était pas créé, le déploiement du routeur ne progressait pas. Avec cette mise à jour, l'opérateur de cluster signale **ingress progressing=true** si le déploiement du contrôleur d'entrée par défaut progresse. Cela permet aux utilisateurs de déboguer les problèmes liés au contrôleur d'entrée à l'aide de la commande **oc get co**. (BZ#2066560)

- Auparavant, lorsqu'une politique réseau mal créée était ajoutée au cache d'OVN-Kubernetes, le leader d'OVN-Kubernetes entrait dans le statut **crashloopbackoff**. Avec cette mise à jour, le leader OVN-Kubernetes n'entre pas dans le statut **crashloopbackoff** en sautant la suppression des politiques nulles. (BZ#2091238)

- Auparavant, la recréation d'un pod EgressIP avec le même espace de noms ou le même nom dans les 60 secondes suivant la suppression d'un pod plus ancien avec le même espace de noms ou le même nom entraînait la configuration du mauvais SNAT. En conséquence, les paquets pouvaient sortir avec nodeIP au lieu de EgressIP SNAT. Avec cette mise à jour, le trafic quitte le pod avec EgressIP au lieu de nodeIP. (BZ#2097243).

- Auparavant, les anciennes listes de contrôle d'accès (ACL) avec **arp** produisaient des erreurs sur **unexpectedly found multiple equivalent ACLs (arp v/s arp||nd)** en raison d'un changement dans l'ACL de **arp** à **arp || nd**, ce qui empêchait la création correcte de stratégies de réseau. Avec cette mise à jour, les anciennes listes de contrôle d'accès (ACL) ne contenant que la correspondance **arp** ont été supprimées, de sorte que seules les ACL contenant la nouvelle correspondance **arp || nd** existent, de sorte que les stratégies de réseau peuvent être créées correctement et qu'aucune erreur ne sera observée sur **ovnkube-master**. REMARQUE : cette mise à jour concerne les clients qui mettent à jour leur système vers les versions 4.8.14, 4.9.32, 4.10.13 ou plus, à partir de versions antérieures. (BZ#2095852).

- Avec cette mise à jour, CoreDNS est passé à la version 1.10.0, qui est basée sur Kubernetes 1.25. Cela permet d'aligner à la fois la version de CoreDNS et celle d'OpenShift Container Platform 4.12, qui est également basée sur Kubernetes 1.25. (OCPBUGS-1731)

- Avec cette mise à jour, le routeur OpenShift Container Platform utilise désormais la version 1.25.2 de **k8s.io/client-go**, qui prend en charge Kubernetes 1.25. Ainsi, le site **openshift-router** et OpenShift Container Platform 4.12, qui est également basé sur Kubernetes 1.25, sont alignés l'un sur l'autre. (OCPBUGS-1730)

- Avec cette mise à jour, Ingress Operator utilise désormais la version 1.25.2 de **k8s.io/client-go**, qui prend en charge Kubernetes 1.25. Cela permet d'aligner à la fois Ingress Operator et OpenShift Container Platform 4.12, qui est également basé sur Kubernetes 1.25. (OCPBUGS-1554)

- Auparavant, l'opérateur DNS ne réconciliait pas l'espace de noms **openshift-dns**. Comme OpenShift Container Platform 4.12 exige que l'espace de noms **openshift-dns** ait des étiquettes de sécurité pour les pods, ces étiquettes manquaient à l'espace de noms lors de la mise à jour du cluster. Sans les étiquettes pod-security, les pods ne démarraient pas. Avec cette mise à jour, l'opérateur DNS réconcilie maintenant l'espace de noms **openshift-dns**, et les étiquettes de pod-sécurité sont maintenant présentes. Par conséquent, les pods démarrent comme prévu. (OCPBUGS-1549)

- Auparavant, le site **ingresscontroller.spec.tuniningOptions.reloadInterval** ne prenait pas en

charge les chiffres décimaux en tant que valeurs de paramètres valides, car l'opérateur d'entrée convertissait en interne la valeur spécifiée en millisecondes, qui n'était pas une unité de temps prise en charge. Cela empêchait la suppression d'un contrôleur d'entrée. Avec cette mise à jour, **ingresscontroller.spec.tuningOptions.reloadInterval** prend désormais en charge les chiffres décimaux et les utilisateurs peuvent supprimer des contrôleurs d'entrée avec des valeurs de paramètres **reloadInterval** qui n'étaient pas prises en charge auparavant. (OCPBUGS-236)

- Auparavant, le Cluster DNS Operator utilisait les bibliothèques GO Kubernetes qui étaient basées sur Kubernetes 1.24 alors qu'OpenShift Container Platform 4.12 est basée sur Kubernetes 1.25. Avec cette mise à jour, l'API GO Kubernetes est v1.25.2, ce qui aligne le Cluster DNS Operator avec OpenShift Container Platform 4.12 qui utilise les API Kubernetes 1.25. (lien : OCPBUGS-1558)

- Auparavant, la configuration de **disableNetworkDiagnostics** à **true** ne persistait pas lorsque le pod **network-operator** était recréé. Avec cette mise à jour, la propriété de configuration **disableNetworkDiagnostics** de network`operator.openshift.io/cluster` ne se réinitialise plus à sa valeur par défaut après le redémarrage de l'opérateur réseau. (OCPBUGS-392)

- Auparavant, **ovn-kubernetes** ne configurait pas l'adresse MAC correcte des interfaces liées dans **br-ex** bridge. Par conséquent, un nœud qui utilise le bonding pour l'interface Kubernetes primaire ne parvient pas à rejoindre le cluster. Avec cette mise à jour, **ovn-kubernetes** configure l'adresse MAC correcte des interfaces liées dans le pont **br-ex**, et les nœuds qui utilisent le bonding pour l'interface Kubernetes primaire rejoignent le cluster avec succès. (BZ2096413)

- Auparavant, lorsque l'opérateur d'entrée était configuré pour activer l'utilisation de mTLS, l'opérateur ne vérifiait pas si les CRL devaient être mises à jour jusqu'à ce qu'un autre événement l'oblige à procéder à une réconciliation. Par conséquent, les LCR utilisées pour mTLS pouvaient devenir obsolètes. Avec cette mise à jour, l'opérateur d'entrée procède désormais automatiquement à la réconciliation lorsqu'une CRL expire, et les CRL seront mises à jour à l'heure spécifiée par leur champ **nextUpdate**. (BZ#2117524)

Nœud

- Auparavant, un message d'erreur concernant les liens symboliques était imprimé sous forme de données brutes au lieu d'être formaté comme une erreur, ce qui le rendait difficile à comprendre. Cette correction formate le message d'erreur correctement, afin qu'il soit facilement compréhensible. (BZ#1977660)

- Auparavant, les seuils d'éviction difficiles des kubelets étaient différents des valeurs par défaut de Kubernetes lorsqu'un profil de performance était appliqué à un nœud. Avec cette version, les valeurs par défaut ont été mises à jour pour correspondre aux valeurs par défaut de Kubernetes. (OCPBUGS-4362).

OpenShift CLI (oc)

- La version 4.12 d'OpenShift Container Platform corrige un problème lié à l'ouverture d'une session de débogage sur un nœud cible lorsque l'espace de noms cible n'a pas le niveau de sécurité approprié. Cela provoquait l'affichage d'un message d'erreur sur la sécurité du pod dans la CLI de **oc**. Si l'espace de noms existant ne contient pas les niveaux de sécurité appropriés, OpenShift Container Platform crée désormais un espace de noms temporaire lorsque vous entrez dans le mode de débogage **oc** sur un nœud cible. (OCPBUGS-852)

- Auparavant, sur l'architecture macOS arm64, le binaire **oc** devait être signé manuellement. Par conséquent, le binaire **oc** ne fonctionnait pas comme prévu. Cette mise à jour implémente un binaire auto-signé pour imiter **oc**. Par conséquent, le binaire **oc** fonctionne correctement sur les architectures macOS arm64. (BZ#2059125)

- Auparavant, **must-gather** essayait de collecter des ressources qui n'étaient pas présentes sur le serveur. Par conséquent, **must-gather** affichait des messages d'erreur. Désormais, avant de collecter des ressources, **must-gather** vérifie si la ressource existe. Par conséquent, **must-gather** n'affiche plus d'erreur lorsqu'il ne parvient pas à collecter des ressources inexistantes sur le serveur. (BZ#2095708)

- La version 4.12 d'OpenShift Container Platform met à jour la bibliothèque **oc-mirror**, afin qu'elle prenne en charge les images de plates-formes multi-archives. Cela signifie que vous pouvez choisir parmi une plus grande sélection d'architectures, telles que **arm64**, lors de la mise en miroir d'une charge utile de plate-forme. (OCPBUGS-617)

Gestionnaire du cycle de vie des opérateurs (OLM)

- Avant la version 4.12 d'OpenShift Container Platform, le contrôleur **package-server-manager** n'annulait pas les modifications apportées à une version de service de cluster (CSV) **package-server**, en raison d'un problème avec la fonction **on-cluster**. Ces changements persistants peuvent avoir un impact sur la façon dont un opérateur démarre dans un cluster. Pour OpenShift Container Platform 4.12, le contrôleur **package-server-manager** reconstruit toujours une CSV **package-server** à son état d'origine, de sorte qu'aucune modification de la CSV ne persiste après une opération de mise à niveau du cluster. La fonction **on-cluster** ne contrôle plus l'état d'un CSV **package-server**. (OCPBUGS-867)

- Auparavant, Operator Lifecycle Manager (OLM) tentait de mettre à jour les espaces de noms pour appliquer un label, même si le label était présent dans l'espace de noms. Par conséquent, les demandes de mise à jour augmentaient la charge de travail des services API et etcd. Avec cette mise à jour, OLM compare les étiquettes existantes avec les étiquettes attendues sur un espace de noms avant d'émettre une mise à jour. Par conséquent, OLM ne tente plus d'effectuer des demandes de mise à jour inutiles sur les espaces de noms. (BZ#2105045)

- Auparavant, Operator Lifecycle Manager (OLM) empêchait les mises à niveau mineures de clusters qui ne devraient pas être bloquées en raison d'une erreur de calcul du champ **spec.DesiredVersion** des ressources personnalisées **ClusterVersion**. Avec cette mise à jour, OLM n'empêche plus les mises à niveau de clusters qui devraient être prises en charge. (BZ#2097557)

- Auparavant, le conciliateur mettait à jour l'annotation d'une ressource sans faire de copie de la ressource. Cela provoquait une erreur qui mettait fin au processus de rapprochement. Avec cette mise à jour, le processus de rapprochement ne s'arrête plus à cause de cette erreur. (BZ#2105045)

- Le **package-server-manifest** (PSM) est un contrôleur qui s'assure que la bonne **package-server** Cluster Service Version (CSV) est installée sur un cluster. Auparavant, les modifications apportées à la CSV **package-server** n'étaient pas annulées en raison d'une erreur logique dans la fonction de réconciliation dans laquelle un objet sur le cluster pouvait influencer l'objet attendu. Les utilisateurs pouvaient modifier le fichier CSV **package-server** sans que les modifications soient annulées. En outre, les mises à niveau des clusters ne mettaient pas à jour le YAML pour le CSV **package-server**. Avec cette mise à jour, la version attendue du CSV est désormais toujours construite à partir de zéro, ce qui supprime la possibilité pour un objet sur le cluster d'influencer les valeurs attendues. Par conséquent, le PSM annule désormais toute tentative de modification du CSV **package-server**, et les mises à niveau de clusters déploient désormais le CSV attendu **package-server**. (OCPBUGS-858)

- Auparavant, OLM mettait à niveau un opérateur en fonction de son statut CRD. Un CRD répertorie les références des composants dans un ordre défini par l'identifiant groupe/version/genre (GVK). Les opérateurs qui partagent les mêmes composants peuvent amener le GVK à modifier les listes de composants d'un opérateur, ce qui peut nécessiter davantage de ressources système pour mettre à jour en permanence l'état d'un CRD. Avec

cette mise à jour, le gestionnaire du cycle de vie des opérateurs (OLM) met désormais à niveau un opérateur en fonction des références des composants de l'opérateur. Une modification de l'état de la définition des ressources personnalisées (CRD) d'un opérateur n'a pas d'incidence sur le processus de mise à niveau de l'opérateur OLM.(OCPBUGS-3795)

SDK de l'opérateur

- Avec cette mise à jour, vous pouvez maintenant définir le contexte de sécurité pour le pod de registre en incluant le champ de configuration **securityContext** dans la spécification du pod. Le contexte de sécurité s'appliquera alors à tous les conteneurs du pod. Le champ **securityContext** définit également les privilèges du module. (BZ#2091864)

Opérateur d'intégrité des fichiers

- Auparavant, l'opérateur d'intégrité des fichiers déployait des modèles en utilisant l'espace de noms **openshift-file-integrity** dans les autorisations de l'opérateur. Lorsque l'opérateur tentait de créer des objets dans l'espace de noms, il échouait en raison de problèmes d'autorisation. Avec cette version, les ressources de déploiement utilisées par OLM sont mises à jour pour utiliser l'espace de noms correct, ce qui résout les problèmes d'autorisation et permet aux utilisateurs d'installer et d'utiliser l'opérateur dans des espaces de noms autres que ceux par défaut. (BZ#2104897)

- Auparavant, les dépendances sous-jacentes de l'opérateur d'intégrité des fichiers modifiaient la manière dont les alertes et les notifications étaient gérées, et l'opérateur n'envoyait donc pas de métriques. Avec cette version, l'opérateur s'assure que le point de terminaison des mesures est correct et accessible au démarrage. (BZ#2115821)

- Auparavant, les alertes émises par l'opérateur d'intégrité des fichiers ne définissaient pas d'espace de noms. Il était donc difficile de comprendre d'où venait l'alerte ou quel était le composant responsable de son émission. Avec cette version, l'opérateur inclut l'espace de noms dans lequel il a été installé dans l'alerte, ce qui permet de déterminer plus facilement le composant qui a besoin d'attention. (BZ#2101393)

- Auparavant, l'opérateur d'intégrité des fichiers ne gérait pas correctement la modification des alertes lors d'une mise à niveau. Par conséquent, les alertes n'incluaient pas l'espace de noms dans lequel l'opérateur était installé. Avec cette version, l'opérateur inclut l'espace de noms dans lequel il a été installé dans l'alerte, ce qui permet de déterminer plus facilement le composant qui nécessite une attention particulière. (BZ#2112394)

- Auparavant, la propriété du compte de service pour l'opérateur d'intégrité des fichiers régressait en raison des mises à jour OLM sous-jacentes, et les mises à jour de 0.1.24 à 0.1.29 étaient interrompues. Avec cette mise à jour, l'opérateur passe par défaut à la version 0.1.30. (BZ#2109153)

- Auparavant, le démon File Integrity Operator utilisait le paramètre **ClusterRoles** au lieu du paramètre **Roles** pour une modification récente des autorisations. Par conséquent, OLM ne pouvait pas mettre à jour l'opérateur. Avec cette version, le démon Opérateur utilise à nouveau le paramètre **Roles** et les mises à jour des anciennes versions vers la version 0.1.29 sont réussies. (BZ#2108475)

Opérateur de conformité

- Auparavant, l'opérateur de conformité utilisait une ancienne version de l'Operator SDK, qui est une dépendance pour la construction des opérateurs. Cela provoquait des alertes sur les fonctionnalités Kubernetes obsolètes utilisées par le SDK de l'opérateur. Avec cette version, l'Opérateur de Conformité est mis à jour à la version 0.1.55, qui inclut une version mise à jour du SDK de l'Opérateur. (BZ#2098581)

- Auparavant, l'application de la remédiation automatique pour les règles **rhcos4-high-master-sysctl-kernel-yama-ptrace-scope** et **rhcos4-sysctl-kernel-core-pattern** entraînait des échecs ultérieurs de ces règles dans les résultats de l'analyse, même si elles avaient été remédiées. Ce problème est corrigé dans cette version. (BZ#2094382)

- Auparavant, l'opérateur de conformité codait en dur les notifications dans l'espace de noms par défaut. Par conséquent, les notifications de l'opérateur n'apparaissaient pas si l'opérateur était installé dans un autre espace de noms. Ce problème est corrigé dans cette version. (BZ#2060726)

- Auparavant, l'opérateur de conformité ne parvenait pas à récupérer les ressources de l'API lorsqu'il analysait les configurations des machines sans les spécifications d'Ignition. Cela provoquait le blocage de la boucle de vérification **api-check-pods**. Avec cette version, l'Opérateur de Conformité est mis à jour pour gérer de manière élégante les pools de configuration de machines sans spécifications Ignition. (BZ#2117268)

- Auparavant, l'opérateur de conformité maintenait les configurations de machines dans un état bloqué parce qu'il ne pouvait pas déterminer la relation entre les configurations de machines et les configurations de kubelets. Cela était dû à des hypothèses incorrectes sur les noms des configurations de machines. Avec cette version, l'opérateur de conformité est capable de déterminer si une configuration kubelet est un sous-ensemble d'une configuration machine. (BZ#2102511)

Serveur API OpenShift

- Auparavant, l'ajout d'un membre pouvait entraîner la suppression des membres précédents d'un groupe. En conséquence, l'utilisateur perdait ses privilèges de groupe. Avec cette version, les dépendances ont été supprimées et les utilisateurs ne perdent plus leurs privilèges de groupe. (OCPBUGS-533)

Red Hat Enterprise Linux CoreOS (RHCOS)

- Auparavant, la mise à jour vers Podman 4.0 empêchait les utilisateurs d'utiliser des images personnalisées avec des conteneurs Toolbox sur RHCOS. Ce correctif met à jour le code de la bibliothèque Toolbox pour prendre en compte le nouveau comportement de Podman, de sorte que les utilisateurs peuvent maintenant utiliser des images personnalisées avec Toolbox sur RHCOS comme prévu. (BZ#2048789)

- Auparavant, la commande **podman exec** ne fonctionnait pas bien avec les conteneurs imbriqués. Les utilisateurs rencontraient ce problème lorsqu'ils accédaient à un nœud à l'aide de la commande **oc debug**, puis exécutaient un conteneur à l'aide de la commande **toolbox**. De ce fait, les utilisateurs ne pouvaient pas réutiliser les boîtes à outils sur RHCOS. Ce correctif met à jour le code de la bibliothèque de boîtes à outils pour tenir compte de ce comportement, de sorte que les utilisateurs peuvent désormais réutiliser les boîtes à outils sur RHCOS. (BZ#1915537)

- Avec cette mise à jour, l'exécution de la commande **toolbox** vérifie désormais les mises à jour de l'image par défaut avant de lancer le conteneur. Cela améliore la sécurité et fournit aux utilisateurs les dernières corrections de bogues. (BZ#2049591)

- Auparavant, la mise à jour vers Podman 4.0 empêchait les utilisateurs d'exécuter la commande **toolbox** sur RHCOS. Ce correctif met à jour le code de la bibliothèque de la boîte à outils pour tenir compte du nouveau comportement de Podman, de sorte que les utilisateurs peuvent désormais exécuter **toolbox** sur RHCOS comme prévu. (BZ#2093040)

- Auparavant, les modules de politique SELinux personnalisés n'étaient pas correctement pris en charge par **rpm-ostree**, de sorte qu'ils n'étaient pas mis à jour en même temps que le reste du

système lors de la mise à jour. Cela se traduisait par des défaillances dans des composants non liés. En attendant que les améliorations de l'espace utilisateur SELinux soient intégrées dans une future version d'OpenShift Container Platform, cette mise à jour fournit une solution de contournement à RHCOS qui reconstruira et rechargera la politique SELinux pendant le démarrage, si nécessaire. (OCPBUGS-595)

Évolutivité et performance

- Le profil accordé a été modifié pour attribuer la même priorité que **ksoftirqd** et **rcuc** aux nouveaux kthreads par CPU (**ktimers**) ajoutés dans un récent patch du noyau Red Hat Enterprise Linux (RHEL). Pour plus d'informations, voir OCPBUGS-3475, BZ#2117780 et BZ#2122220.

- Auparavant, les redémarrages du service **tuned** provoquaient une réinitialisation incorrecte de la configuration de **irqbalance**, ce qui conduisait à une opération IRQ servie à nouveau sur les CPU isolés, violant ainsi les garanties d'isolation. Avec cette correction, la configuration du service **irqbalance** est correctement préservée à travers les redémarrages du service **tuned** (explicites ou causés par des bogues), préservant ainsi les garanties d'isolation du CPU en ce qui concerne le service d'IRQ. (OCPBUGS-585)

- Auparavant, lorsque le démon tuned était redémarré dans le désordre dans le cadre du cluster Node Tuning Operator, l'affinité CPU des gestionnaires d'interruption était réinitialisée et le tuning était compromis. Avec cette correction, le plugin **irqbalance** dans tuned est désactivé, et OpenShift Container Platform s'appuie maintenant sur la logique et l'interaction entre **CRI-O** et **irqbalance**.(BZ#2105123)

- Auparavant, un script d'accroche à faible latence s'exécutant pour chaque nouveau périphérique **veth** prenait trop de temps lorsque le nœud était en charge. Les retards accumulés lors des événements de démarrage de pods provoquaient un temps de déploiement lent pour **kube-apiserver** et dépassaient parfois le délai de déploiement de 5 minutes. Avec cette correction, le temps de démarrage des conteneurs devrait être plus court et se situer dans le seuil des 5 minutes. (BZ#2109965).

- Auparavant, le thread de contrôle **oslat** était colocalisé avec l'un des threads de test, ce qui provoquait des pics de latence dans les mesures. Avec cette correction, le programme d'exécution **oslat** réserve désormais une unité centrale pour le thread de contrôle, ce qui signifie que le test utilise une unité centrale de moins pour l'exécution des threads occupés. (BZ#2051443)

- Les outils de mesure de la latence, également connus sous les noms de **oslat**, **cyclictest** et **hwlatdetect**, s'exécutent désormais sur des unités centrales complètement isolées, sans le processus d'aide fonctionnant en arrière-plan qui pourrait provoquer des pics de latence, ce qui permet d'obtenir des mesures de latence plus précises. (OCPBUGS-2618)

- Auparavant, bien que la référence **PolicyGenTemplate** pour **group-du-sno-ranGen.yaml** comprenne deux entrées **StorageClass**, la politique générée n'en comprenait qu'une seule. Avec cette mise à jour, la politique générée inclut désormais les deux politiques. (BZ#2049306).

Stockage

- Auparavant, les vérifications des volumes éphémères génériques échouaient. Avec cette mise à jour, les vérifications des volumes extensibles incluent désormais les volumes éphémères génériques. (BZ#2082773)

- Auparavant, si plus d'un secret était présent pour vSphere, l'opérateur vSphere CSI choisissait un secret de manière aléatoire et provoquait parfois le redémarrage de l'opérateur. Avec cette

mise à jour, un avertissement apparaît lorsqu'il y a plus d'un secret sur l'opérateur vCenter CSI. (BZ#2108473)

- Auparavant, OpenShift Container Platform détachait un volume lorsqu'un pilote d'interface de stockage de conteneurs (CSI) n'était pas en mesure de démonter le volume d'un nœud. Détacher un volume sans le démonter n'est pas autorisé par les spécifications CSI et les pilotes pourraient entrer dans un état **undocumented**. Avec cette mise à jour, les pilotes CSI sont détachés avant le démontage uniquement sur les nœuds malsains, ce qui permet d'éviter l'état **undocumented**. (BZ#2049306)

- Auparavant, il manquait des annotations sur la VolumeSnapshotClass de l'opérateur du pilote Manila CSI. Par conséquent, le snapshotter Manila CSI ne pouvait pas localiser les secrets et ne pouvait pas créer d'instantanés avec la VolumeSnapshotClass par défaut. Cette mise à jour corrige le problème afin que les noms de secrets et les espaces de noms soient inclus dans la classe VolumeSnapshotClass par défaut. Par conséquent, les utilisateurs peuvent désormais créer des instantanés dans le Manila CSI Driver Operator à l'aide de la classe VolumeSnapshotClass par défaut. (BZ#2057637)

- Les utilisateurs peuvent désormais choisir d'utiliser la fonction expérimentale VHD sur Azure File. Pour ce faire, ils doivent spécifier le paramètre **fstype** dans une classe de stockage et l'activer avec **--enable-vhd=true**. Si **fstype** est utilisé et que la fonctionnalité n'est pas définie sur **true**, les volumes ne seront pas provisionnés.
  Pour ne pas utiliser la fonction VHD, supprimez le paramètre **fstype** de votre classe de stockage. (BZ#2080449)

- Auparavant, si plus d'un secret était présent pour vSphere, l'opérateur vSphere CSI choisissait un secret de manière aléatoire et provoquait parfois le redémarrage de l'opérateur. Avec cette mise à jour, un avertissement apparaît lorsqu'il y a plus d'un secret sur l'opérateur vCenter CSI. (BZ#2108473)

Console web (perspective développeur)

- Auparavant, les utilisateurs ne pouvaient pas désélectionner un secret Git dans les formulaires d'ajout et d'édition. Par conséquent, les ressources devaient être recréées. Ce correctif résout le problème en ajoutant l'option de choisir **No Secret** dans la liste des options de sélection des secrets. Ainsi, les utilisateurs peuvent facilement sélectionner, désélectionner ou détacher les secrets attachés. (BZ#2089221)

- Dans OpenShift Container Platform 4.9, lorsqu'il y a peu ou pas de données dans le site **Developer Perspective**, la plupart des diagrammes ou graphiques de surveillance (consommation de CPU, utilisation de la mémoire et bande passante) affichent une plage de -1 à 1. Cependant, aucune de ces valeurs ne peut jamais descendre en dessous de zéro. Ce problème sera résolu dans une prochaine version. (BZ#1904106)

- Avant cette mise à jour, les utilisateurs ne pouvaient pas faire taire les alertes dans la perspective **Developer** de la console web d'OpenShift Container Platform lorsqu'un service Alertmanager défini par l'utilisateur était déployé, car la console web transmettait la demande au service Alertmanager de la plateforme dans l'espace de noms **openshift-monitoring**. Avec cette mise à jour, lorsque vous visualisez la perspective **Developer** dans la console web et que vous essayez de faire taire une alerte, la demande est transmise au service Alertmanager correct. (OCPBUGS-1789)

- Auparavant, il y avait un problème connu dans le formulaire **Add Helm Chart Repositories** pour étendre le catalogue des développeurs d'un projet. Les guides **Quick Start** indiquent que vous pouvez ajouter le CR **ProjectHelmChartRepository** dans l'espace de noms requis, mais ils ne

mentionnent pas que pour ce faire, vous avez besoin de l'autorisation du kubeadmin. Ce problème a été résolu avec **Quickstart** qui mentionne les étapes correctes pour créer **ProjectHelmChartRepository** CR. (BZ#2057306)

1.7. CARACTÉRISTIQUES DE L'APERÇU TECHNOLOGIQUE

Certaines fonctionnalités de cette version sont actuellement en avant-première technologique. Ces fonctionnalités expérimentales ne sont pas destinées à une utilisation en production. Notez l'étendue de l'assistance suivante sur le portail client de Red Hat pour ces fonctionnalités :

Aperçu de la technologie Fonctionnalités Support Champ d'application

Dans les tableaux suivants, les caractéristiques sont marquées par les statuts suivants :

- *Technology Preview*
- *General Availability*
- *Not Available*
- *Deprecated*

Caractéristiques de l'aperçu de la technologie de mise en réseau

Tableau 1.14. Technologie de mise en réseau - Aperçu du tracker

Fonctionnalité	4.10	4.11	4.12
PTP - matériel NIC unique configuré comme horloge frontière	Avant-première technologique	Disponibilité générale	Disponibilité générale
Matériel PTP double NIC configuré en tant qu'horloge frontière	Non disponible	Avant-première technologique	Avant-première technologique
Événements PTP avec horloge périphérique	Avant-première technologique	Disponibilité générale	Disponibilité générale
Liaison au niveau du pod pour les réseaux secondaires	Disponibilité générale	Disponibilité générale	Disponibilité générale
Opérateur DNS externe	Avant-première technologique	Disponibilité générale	Disponibilité générale

Fonctionnalité	4.10	4.11	4.12
Opérateur d'équilibreur de charge AWS	Non disponible	Avant-première technologique	Avant-première technologique
Opérateur du pare-feu du nœud d'entrée	Non disponible	Non disponible	Avant-première technologique
Annoncer en mode BGP le service MetalLB à partir d'un sous-ensemble de nœuds, en utilisant un pool spécifique d'adresses IP	Non disponible	Avant-première technologique	Disponibilité générale
Annoncer en mode L2 le service MetalLB à partir d'un sous-ensemble de nœuds, à l'aide d'un groupe spécifique d'adresses IP	Non disponible	Avant-première technologique	Avant-première technologique
Politiques multi-réseaux pour les réseaux SR-IOV	Non disponible	Non disponible	Avant-première technologique
Mise à jour de la liste des sysctls sûrs spécifiques à l'interface	Non disponible	Non disponible	Avant-première technologique
Famille MT2892 [ConnectX-6 Dx] Prise en charge SR-IOV	Non disponible	Non disponible	Avant-première technologique
Famille MT2894 [ConnectX-6 Lx] Prise en charge SR-IOV	Non disponible	Non disponible	Avant-première technologique
MT42822 BlueField-2 en mode ConnectX-6 NIC support SR-IOV	Non disponible	Non disponible	Avant-première technologique
Support SR-IOV de la famille Silicom STS	Non disponible	Non disponible	Avant-première technologique

Fonctionnalité	4.10	4.11	4.12
Famille MT2892 [ConnectX-6 Dx] Prise en charge du déchargement matériel OvS	Non disponible	Non disponible	Avant-première technologique
Famille MT2894 [ConnectX-6 Lx] Prise en charge du déchargement matériel OvS	Non disponible	Non disponible	Avant-première technologique
MT42822 BlueField-2 en mode ConnectX-6 NIC support OvS Hardware Offload	Non disponible	Non disponible	Avant-première technologique
Passage de Bluefield-2 de DPU à NIC	Non disponible	Non disponible	Avant-première technologique

Caractéristiques de l'aperçu de la technologie de stockage

Tableau 1.15. Suivi de l'aperçu de la technologie du stockage

Fonctionnalité	4.10	4.11	4.12
Pilote CSI des ressources partagées et volumes CSI de construction dans les constructions OpenShift	Avant-première technologique	Avant-première technologique	Avant-première technologique
Expansion du volume de l'ISC	Avant-première technologique	Disponibilité générale	Disponibilité générale
CSI Azure File Driver Operator	Avant-première technologique	Disponibilité générale	Disponibilité générale
CSI Google Filestore Driver Operator	Non disponible	Non disponible	Avant-première technologique

Fonctionnalité	4.10	4.11	4.12
Migration automatique CSI (Azure file, VMware vSphere)	Avant-première technologique	Avant-première technologique	Avant-première technologique
Migration automatique CSI (Azure Disk, OpenStack Cinder)	Avant-première technologique	Disponibilité générale	Disponibilité générale
Migration automatique CSI (AWS EBS, disque GCP)	Avant-première technologique	Avant-première technologique	Disponibilité générale
Volumes éphémères en ligne CSI	Avant-première technologique	Avant-première technologique	Avant-première technologique
Volumes éphémères génériques CSI	Non disponible	Disponibilité générale	Disponibilité générale
Ressource partagée Pilote CSI	Avant-première technologique	Avant-première technologique	Avant-première technologique
CSI Google Filestore Driver Operator	Non disponible	Non disponible	Avant-première technologique
Découverte automatique des appareils et approvisionnement avec le Local Storage Operator	Avant-première technologique	Avant-première technologique	Avant-première technologique

Caractéristiques de l'aperçu de la technologie d'installation

Tableau 1.16. Installation Technology Preview tracker

Fonctionnalité	4.10	4.11	4.12

Fonctionnalité	4.10	4.11	4.12
Ajouter des modules de noyau aux nœuds avec kvc	Avant-première technologique	Avant-première technologique	Avant-première technologique
Clusters IBM Cloud VPC	Avant-première technologique	Avant-première technologique	Disponibilité générale
Inventaire des grappes sélectionnable	Avant-première technologique	Avant-première technologique	Avant-première technologique
Machines de calcul à architecture multiple	Non disponible	Avant-première technologique	Avant-première technologique
Mise en miroir déconnectée avec le plugin CLI oc-mirror	Avant-première technologique	Disponibilité générale	Disponibilité générale
Monter des droits partagés dans BuildConfigs dans RHEL	Avant-première technologique	Avant-première technologique	Avant-première technologique
Installateur de la plateforme de conteneurs OpenShift basé sur un agent	Non disponible	Non disponible	Disponibilité générale
Plate-forme AWS Outposts	Non disponible	Non disponible	Avant-première technologique

Caractéristiques de l'aperçu technologique de Node

Tableau 1.17. Suivi de l'aperçu technologique des nœuds

Fonctionnalité	4.10	4.11	4.12
Classes de priorité non prioritaires	Avant-première technologique	Avant-première technologique	Avant-première technologique

Fonctionnalité	4.10	4.11	4.12
Opérateur du bilan de santé du nœud	Avant-première technologique	Disponibilité générale	Disponibilité générale
Groupe de contrôle Linux version 2 (cgroup v2)	Non disponible	Non disponible	Avant-première technologique
exécution d'un conteneur crun	Non disponible	Non disponible	Avant-première technologique

Caractéristiques de l'aperçu de la technologie multi-architecture

Tableau 1.18. Suivi de l'aperçu de la technologie multi-architecture

Fonctionnalité	4.10	4.11	4.12
kdump sur **x86_64** architecture	Avant-première technologique	Disponibilité générale	Disponibilité générale
kdump sur **arm64** architecture	Non disponible	Avant-première technologique	Avant-première technologique
kdump sur **s390x** architecture	Avant-première technologique	Avant-première technologique	Avant-première technologique
kdump sur **ppc64le** architecture	Avant-première technologique	Avant-première technologique	Avant-première technologique
IBM Secure Execution sur IBM zSystems et LinuxONE	Non disponible	Non disponible	Avant-première technologique

Fonctionnalités de l'aperçu de la technologie sans serveur

Tableau 1.19. Suivi de l'aperçu de la technologie sans serveur (Serverless Technology Preview)

Fonctionnalité	4.10	4.11	4.12
Fonctions sans serveur	Avant-première technologique	Avant-première technologique	Avant-première technologique

Matériel spécialisé et activation des pilotes Fonctionnalités de l'aperçu technologique

Tableau 1.20. Activation de matériel spécialisé et de pilotes Suivi de l'aperçu technologique

Fonctionnalité	4.10	4.11	4.12
Driver Toolkit	Avant-première technologique	Avant-première technologique	Disponibilité générale
Opérateur spécial de ressources (OSR)	Avant-première technologique	Avant-première technologique	Non disponible
Prise en charge des grappes en étoile (Hub and spoke)	Non disponible	Non disponible	Avant-première technologique

Fonctionnalités de l'aperçu technologique de la console Web

Tableau 1.21. Suivi de l'aperçu technologique de la console Web

Fonctionnalité	4.10	4.11	4.12
Plugins dynamiques	Avant-première technologique	Avant-première technologique	Disponibilité générale

Évolutivité et performances Caractéristiques de l'aperçu technologique

Tableau 1.22. Évolutivité et performances Suivi de l'aperçu technologique

Fonctionnalité	4.10	4.11	4.12

Fonctionnalité	4.10	4.11	4.12
Politique de gestion de l'unité centrale tenant compte de l'hyperthreading	Avant-première technologique	Avant-première technologique	Avant-première technologique
Opérateur d'observabilité du nœud	Non disponible	Avant-première technologique	Avant-première technologique
outil factory-precaching-cli	Non disponible	Non disponible	Avant-première technologique
Ajouter des nœuds de travail à des clusters OpenShift à nœud unique avec GitOps ZTP	Non disponible	Non disponible	Avant-première technologique
Gestionnaire du cycle de vie tenant compte de la topologie (TALM)	Avant-première technologique	Avant-première technologique	Disponibilité générale
Encapsulation de l'espace de noms de montage	Non disponible	Non disponible	Avant-première technologique

Caractéristiques de l'aperçu technologique de l'opérateur

Tableau 1.23. Technologie de l'opérateur Aperçu du tracker

Fonctionnalité	4.10	4.11	4.12
Opérateur de barre hybride	Avant-première technologique	Avant-première technologique	Avant-première technologique
Opérateur basé sur Java	Non disponible	Avant-première technologique	Avant-première technologique

Fonctionnalité	4.10	4.11	4.12
Opérateur d'observabilité du nœud	Non disponible	Non disponible	Avant-première technologique
Opérateur de l'observabilité du réseau	Non disponible	Non disponible	Disponibilité générale
Opérateurs de plateforme	Non disponible	Non disponible	Avant-première technologique
RukPak	Non disponible	Non disponible	Avant-première technologique
Opérateur Cert-manager	Avant-première technologique	Avant-première technologique	Avant-première technologique

Caractéristiques de l'aperçu de la technologie de surveillance

Tableau 1.24. Technologie de surveillance Traceur de prévisualisation

Fonctionnalité	4.10	4.11	4.12
Routage des alertes pour le suivi de projets définis par l'utilisateur	Avant-première technologique	Disponibilité générale	Disponibilité générale
Règles d'alerte basées sur les mesures de surveillance de la plate-forme	Non disponible	Avant-première technologique	Avant-première technologique

Fonctionnalités de l'aperçu technologique de Red Hat OpenStack Platform (RHOSP)

Tableau 1.25. Suivi de l'aperçu technologique de la RHOSP

Fonctionnalité	4.10	4.11	4.12

Fonctionnalité	4.10	4.11	4.12
Prise en charge de RHOSP DCN	Avant-première technologique	Avant-première technologique	Avant-première technologique
Prise en charge des fournisseurs de nuages externes pour les clusters sur RHOSP	Avant-première technologique	Avant-première technologique	Disponibilité générale
Déchargement matériel OVS pour les clusters sur RHOSP	Avant-première technologique	Disponibilité générale	Disponibilité générale

Caractéristiques de l'aperçu technologique de l'architecture

Tableau 1.26. Architecture Technology Preview tracker (en anglais)

Fonctionnalité	4.10	4.11	4.12
Plans de contrôle hébergés pour OpenShift Container Platform sur métal nu	Non disponible	Non disponible	Avant-première technologique
Plans de contrôle hébergés pour OpenShift Container Platform sur Amazon Web Services (AWS)	Non disponible	Avant-première technologique	Avant-première technologique

Gestion des machines Caractéristiques de l'aperçu technologique

Tableau 1.27. Gestion des machines Technologie Suivi de l'aperçu

Fonctionnalité	4.10	4.11	4.12
Gérer les machines avec l'API Cluster	Non disponible	Avant-première technologique	Avant-première technologique
Fuseaux horaires des tâches Cron	Non disponible	Non disponible	Avant-première technologique

Fonctionnalité	4.10	4.11	4.12
Gestionnaire de contrôleur de nuage pour Alibaba Cloud	Avant-première technologique	Avant-première technologique	Avant-première technologique
Gestionnaire de contrôleur de nuage pour Amazon Web Services	Avant-première technologique	Avant-première technologique	Avant-première technologique
Gestionnaire de contrôleur cloud pour Google Cloud Platform	Avant-première technologique	Avant-première technologique	Avant-première technologique
Gestionnaire de contrôleur cloud pour Microsoft Azure	Avant-première technologique	Avant-première technologique	Avant-première technologique
Gestionnaire de contrôleur cloud pour Red Hat OpenStack Platform (RHOSP)	Avant-première technologique	Avant-première technologique	Disponibilité générale
Gestionnaire de contrôleur de nuage pour VMware vSphere	Avant-première technologique	Avant-première technologique	Avant-première technologique
Opérateur de mise à l'échelle automatique des métriques personnalisées	Non disponible	Avant-première technologique	Avant-première technologique

Authentification et autorisation Caractéristiques de l'aperçu technologique

Tableau 1.28. Authentification et autorisation Technologie Preview tracker

Fonctionnalité	4.10	4.11	4.12
Pod sécurité admission application restreinte	Non disponible	Non disponible	Avant-première technologique

1.8. PROBLÈMES CONNUS

- Dans OpenShift Container Platform 4.1, les utilisateurs anonymes pouvaient accéder aux terminaux de découverte. Les versions ultérieures ont révoqué cet accès afin de réduire la surface d'attaque possible pour les exploits de sécurité, car certains points de terminaison de découverte sont transmis à des serveurs d'API agrégés. Cependant, l'accès non authentifié est préservé dans les clusters mis à jour afin que les cas d'utilisation existants ne soient pas interrompus.
  Si vous êtes un administrateur de cluster pour un cluster qui a été mis à niveau de OpenShift Container Platform 4.1 à 4.12, vous pouvez soit révoquer, soit continuer à autoriser l'accès non authentifié. À moins qu'il n'y ait un besoin spécifique pour l'accès non authentifié, vous devriez le révoquer. Si vous continuez à autoriser l'accès non authentifié, soyez conscient des risques accrus.

  AVERTISSEMENT

  Si vous avez des applications qui dépendent d'un accès non authentifié, elles peuvent recevoir des erreurs HTTP **403** si vous révoquez l'accès non authentifié.

  Utilisez le script suivant pour révoquer l'accès non authentifié aux terminaux de découverte :

  ```
  ## Snippet to remove unauthenticated group from all the cluster role bindings
  $ for clusterrolebinding in cluster-status-binding discovery system:basic-user
  system:discovery system:openshift:discovery ;
  do
  ### Find the index of unauthenticated group in list of subjects
  index=$(oc get clusterrolebinding ${clusterrolebinding} -o json | jq 'select(.subjects!=null) |
  .subjects | map(.name=="system:unauthenticated") | index(true)');
  ### Remove the element at index from subjects array
  oc patch clusterrolebinding ${clusterrolebinding} --type=json --patch "[{'op': 'remove','path':
  '/subjects/$index'}]";
  done
  ```

  Ce script supprime les sujets non authentifiés des liaisons de rôles de cluster suivantes :

  - **cluster-status-binding**
  - **discovery**
  - **system:basic-user**
  - **system:discovery**
  - **system:openshift:discovery**

  (BZ#1821771)

- Par intermittence, un cluster IBM Cloud VPC peut échouer à s'installer parce que certaines machines de travail ne démarrent pas. Au contraire, ces machines de travail restent dans la phase **Provisioned**.

Il existe une solution de contournement pour ce problème. À partir de l'hôte où vous avez effectué l'installation initiale, supprimez les machines qui ont échoué et exécutez à nouveau le programme d'installation.

1. Vérifiez que l'état de l'équilibreur de charge d'application interne (ALB) pour le serveur API maître est **active**.

   a. Identifiez l'ID d'infrastructure du cluster en exécutant la commande suivante :

   ```
   $ oc get infrastructure/cluster -ojson | jq -r '.status.infrastructureName'
   ```

   b. Connectez-vous au compte IBM Cloud de votre cluster et ciblez la région correcte pour votre cluster.

   c. Vérifiez que l'état de l'ALB interne est **active** en exécutant la commande suivante :

   ```
   $ ibmcloud is lb <cluster_ID>-kubernetes-api-private  --output json | jq -r
   '.provisioning_status'
   ```

2. Identifiez les machines qui sont dans la phase **Provisioned** en exécutant la commande suivante :

   ```
   $ oc get machine -n openshift-machine-api
   ```

   Exemple de sortie

   ```
   NAME                                PHASE        TYPE       REGION    ZONE       AGE
   example-public-1-x4gpn-master-0     Running      bx2-4x16   us-east   us-east-1  23h
   example-public-1-x4gpn-master-1     Running      bx2-4x16   us-east   us-east-2  23h
   example-public-1-x4gpn-master-2     Running      bx2-4x16   us-east   us-east-3  23h
   example-public-1-x4gpn-worker-1-xqzzm  Running      bx2-4x16   us-east   us-east-1
   22h
   example-public-1-x4gpn-worker-2-vg9w6  Provisioned  bx2-4x16   us-east   us-east-2
   22h
   example-public-1-x4gpn-worker-3-2f7zd  Provisioned  bx2-4x16   us-east   us-east-3
   22h
   ```

3. Supprimez chaque machine défaillante en exécutant la commande suivante :

   ```
   $ oc delete machine <name_of_machine> -n openshift-machine-api
   ```

4. Attendez que les machines des travailleurs supprimés soient remplacées, ce qui peut prendre jusqu'à 10 minutes.

5. Vérifiez que les nouvelles machines de travail sont dans la phase **Running** en exécutant la commande suivante :

   ```
   $ oc get machine -n openshift-machine-api
   ```

   Exemple de sortie

   ```
   NAME                                PHASE    TYPE       REGION    ZONE       AGE
   example-public-1-x4gpn-master-0     Running  bx2-4x16   us-east   us-east-1  23h
   ```

```
example-public-1-x4gpn-master-1        Running   bx2-4x16   us-east   us-east-2   23h
example-public-1-x4gpn-master-2        Running   bx2-4x16   us-east   us-east-3   23h
example-public-1-x4gpn-worker-1-xqzzm  Running   bx2-4x16   us-east   us-east-1   23h
example-public-1-x4gpn-worker-2-mnlsz  Running   bx2-4x16   us-east   us-east-2
8m2s
example-public-1-x4gpn-worker-3-7nz4q  Running   bx2-4x16   us-east   us-east-3
7m24s
```

6. Terminez l'installation en exécutant la commande suivante. Une nouvelle exécution du programme d'installation permet de s'assurer que le site **kubeconfig** de la grappe est correctement initialisé :

```
$ ./openshift-install wait-for install-complete
```

(OCPBUGS#1327)

- La commande **oc annotate** ne fonctionne pas pour les noms de groupes LDAP qui contiennent un signe égal (**=**), car la commande utilise le signe égal comme délimiteur entre le nom et la valeur de l'annotation. Pour contourner le problème, utilisez **oc patch** ou **oc edit** pour ajouter l'annotation. (BZ#1917280)

- En raison de l'inclusion d'anciennes images dans certains index d'images, l'exécution de **oc adm catalog mirror** et **oc image mirror** peut entraîner l'erreur suivante : **error: unable to retrieve source image**. En guise de solution temporaire, vous pouvez utiliser l'option **--skip-missing** pour contourner l'erreur et continuer à télécharger l'index d'images. Pour plus d'informations, voir Échec de la mise en miroir de l'opérateur du service Mesh.

- Lorsque vous utilisez la fonctionnalité d'adresse IP egress dans OpenShift Container Platform on RHOSP, vous pouvez attribuer une adresse IP flottante à un port de réservation afin de disposer d'une adresse SNAT prévisible pour le trafic egress. L'association d'adresses IP flottantes doit être créée par le même utilisateur que celui qui a installé le cluster OpenShift Container Platform. Sinon, toute opération de suppression ou de déplacement de l'adresse IP de sortie est bloquée indéfiniment en raison de l'insuffisance des privilèges. Lorsque ce problème se produit, un utilisateur disposant de privilèges suffisants doit désactiver manuellement l'association d'adresses IP flottantes pour résoudre le problème. (OCPBUGS-4902)

- Il y a un problème connu avec l'installation de Nutanix où l'installation échoue si vous utilisez des certificats 4096-bit avec Prism Central 2022.x. Au lieu de cela, utilisez des certificats 2048-bit. (KCS)

- La suppression du profil de détection de transfert bidirectionnel (BFD) et de l'adresse **bfdProfile** ajoutée à la ressource homologue du protocole de passerelle frontalière (BGP) ne désactive pas le BFD. Au lieu de cela, le pair BGP commence à utiliser le profil BFD par défaut. Pour désactiver le BFD à partir d'une ressource homologue BGP, supprimez la configuration de l'homologue BGP et recréez-la sans profil BFD. (BZ#2050824)

- En raison d'un problème non résolu au niveau de l'API des métadonnées, vous ne pouvez pas installer des clusters qui utilisent des workers bare-metal sur RHOSP 16.1. Les clusters sur RHOSP 16.2 ne sont pas concernés par ce problème. (BZ#2033953)

- L'attribut **loadBalancerSourceRanges** n'est pas supporté, et est donc ignoré, dans les services de type load-balancer dans les clusters qui tournent sous RHOSP et utilisent le fournisseur OVN Octavia. Il n'y a pas de solution à ce problème. (OCPBUGS-2789)

- Après une mise à jour de la source du catalogue, OLM met du temps à mettre à jour l'état de

l'abonnement. Cela peut signifier que l'état de la politique d'abonnement peut continuer à s'afficher comme conforme lorsque le gestionnaire du cycle de vie Topology Aware (TALM) décide si une remédiation est nécessaire. En conséquence, l'opérateur spécifié dans la politique d'abonnement n'est pas mis à niveau. Comme solution de contournement, incluez un champ **status** dans la section **spec** de la politique de source de catalogue comme suit :

```
metadata:
  name: redhat-operators-disconnected
spec:
  displayName: disconnected-redhat-operators
  image: registry.example.com:5000/disconnected-redhat-operators/disconnected-redhat-operator-index:v4.11
status:
  connectionState:
    lastObservedState: READY
```

Cela réduit le délai nécessaire à OLM pour extraire la nouvelle image d'index et préparer le pod, réduisant ainsi le délai entre l'achèvement de la remédiation de la politique de source du catalogue et la mise à jour de l'état de l'abonnement. Si le problème persiste et que la mise à jour de l'état de la politique d'abonnement est toujours en retard, vous pouvez appliquer une autre CR **ClusterGroupUpdate** avec la même politique d'abonnement, ou une CR **ClusterGroupUpdate** identique avec un nom différent. (OCPBUGS-2813)

- TALM ne procède pas à la remédiation d'une politique si tous les clusters sélectionnés sont conformes lorsque le CR **ClusterGroupUpdate** est démarré. La mise à jour des opérateurs avec une politique de source de catalogue modifiée et une politique d'abonnement dans la même CR **ClusterGroupUpdate** ne se termine pas. La politique d'abonnement est ignorée car elle est toujours conforme jusqu'à ce que la modification de la source du catalogue soit appliquée. Pour contourner le problème, ajoutez la modification suivante à un CR de la politique **common-subscription**, par exemple :

```
metadata.annotations.upgrade: "1"
```

La politique n'est donc pas conforme avant le début de la CR **ClusterGroupUpdate**. (OCPBUGS-2812)

- Sur une instance OpenShift à nœud unique, le redémarrage sans vidanger le nœud pour supprimer tous les pods en cours d'exécution peut entraîner des problèmes avec la récupération des conteneurs de charge de travail. Après le redémarrage, la charge de travail redémarre avant que tous les plugins de périphérique soient prêts, ce qui entraîne l'indisponibilité des ressources ou l'exécution de la charge de travail sur le mauvais nœud NUMA. La solution consiste à redémarrer les modules de charge de travail lorsque tous les plugins de périphériques se sont réenregistrés au cours de la procédure de reprise après redémarrage. (OCPBUGS-2180)

- La valeur par défaut de **dataset_comparison** est actuellement **ieee1588**. Le dataset_comparison recommandé est **G.8275.x**. Il est prévu de le corriger dans une prochaine version d'OpenShift Container Platform. À court terme, vous pouvez mettre à jour manuellement la configuration de ptp pour inclure la version recommandée **dataset_comparison**. (OCPBUGS-2336)

- La valeur par défaut de **step_threshold** est 0.0. La valeur recommandée pour **step_threshold** est 2.0. Il est prévu que cela soit corrigé dans une future version d'OpenShift Container Platform. À court terme, vous pouvez mettre à jour manuellement la configuration de ptp pour inclure la version recommandée **step_threshold**. (OCPBUGS-3005)

- Le CR **BMCEventSubscription** ne parvient pas à créer un abonnement Redfish pour un cluster

spoke dans un environnement multi-cluster déployé par ACM, où le service metal3 ne fonctionne que sur un cluster hub. La solution consiste à créer l'abonnement en appelant directement l'API Redfish, par exemple en exécutant la commande suivante :

```
curl -X POST -i --insecure -u "<BMC_username>:<BMC_password>"
https://<BMC_IP>/redfish/v1/EventService/Subscriptions \
    -H 'Content-Type: application/json' \
    --data-raw '{
    "Protocol": "Redfish",
    "Context": "any string is valid",
    "Destination": "https://hw-event-proxy-openshift-bare-metal-
events.apps.example.com/webhook",
    "EventTypes": ["Alert"]
    }'
```

Vous devriez recevoir une réponse **201 Created** et un en-tête avec **Location: /redfish/v1/EventService/Subscriptions/<sub_id>** qui indique que l'abonnement aux événements Redfish a été créé avec succès. (OCPBUGSM-43707)

- Lors de l'utilisation du pipeline ZTP GitOps pour installer un cluster OpenShift à un seul nœud dans un environnement déconnecté, il devrait y avoir deux **CatalogSource** CRs appliqués dans le cluster. L'un des CR **CatalogSource** est supprimé à la suite de plusieurs redémarrages de nœuds. Comme solution de contournement, vous pouvez changer les noms par défaut, tels que **certified-operators** et **redhat-operators**, des sources de catalogue. (OCPBUGSM-46245)

- Si un canal d'abonnement non valide est spécifié dans la politique d'abonnement utilisée pour effectuer une mise à niveau de cluster, le Topology Aware Lifecycle Manager indique une mise à niveau réussie juste après l'application de la politique, car l'état **Subscription** reste **AtLatestKnown**. (OCPBUGSM-43618)

- La définition de partition de disque **SiteConfig** échoue lorsqu'elle est appliquée à plusieurs nœuds d'un cluster. Lorsqu'un CR **SiteConfig** est utilisé pour provisionner un cluster compact, la création d'une configuration **diskPartition** valide sur plusieurs nœuds échoue avec une erreur du plugin Kustomize. (OCPBUGSM-44403)

- Si le démarrage sécurisé est actuellement désactivé et que vous essayez de l'activer à l'aide de ZTP, l'installation du cluster ne démarre pas. Lorsque le démarrage sécurisé est activé via ZTP, les options de démarrage sont configurées avant que le CD virtuel ne soit attaché. Par conséquent, lors du premier démarrage à partir du disque dur existant, le démarrage sécurisé est activé. L'installation du cluster est bloquée car le système ne démarre jamais à partir du CD. (OCPBUGSM-45085)

- En utilisant Red Hat Advanced Cluster Management (RHACM), les déploiements de cluster de rayons sur les serveurs Dell PowerEdge R640 sont bloqués lorsque le média virtuel ne déconnecte pas l'ISO dans la console iDRAC après avoir écrit l'image sur le disque. Comme solution de contournement, déconnectez l'ISO manuellement via l'onglet Média virtuel dans la console iDRAC. (OCPBUGSM-45884)

- Les applications à faible latence qui s'appuient sur des minuteries à haute résolution pour réveiller leurs threads peuvent présenter des latences de réveil plus élevées que prévu. Bien que la latence de réveil attendue soit inférieure à 20us, des latences supérieures peuvent occasionnellement être observées lors de l'exécution de l'outil cyclictest pendant de longues durées (24 heures ou plus). Les tests ont montré que les latences de réveil sont inférieures à 20us pour plus de 99,999999% des échantillons. (RHELPLAN-138733)

- Une carte d'interface réseau Chapman Beach d'Intel doit être installée dans un emplacement

PCIe bifurqué pour que les deux ports soient visibles. Il existe également une limitation dans l'outil devlink actuel de RHEL 8.6 qui empêche la configuration de 2 ports dans l'emplacement PCIe bifurqué. (RHELPLAN-142458)

- La désactivation d'un SR-IOV VF lorsqu'un port tombe en panne peut entraîner un délai de 3 à 4 secondes avec les cartes d'interface réseau d'Intel. (RHELPLAN-126931)
- Lors de l'utilisation de cartes réseau Intel, le trafic IPV6 s'arrête lorsqu'une adresse IPV6 est attribuée à un VF SR-IOV. (RHELPLAN-137741)
- Lors de l'utilisation du délestage de bandes VLAN, le drapeau de délestage (**ol_flag**) n'est pas toujours défini correctement avec le pilote iavf. (RHELPLAN-141240)
- Un blocage peut se produire si une allocation échoue lors d'un changement de configuration du pilote de glace. (RHELPLAN-130855)
- Les VF SR-IOV envoient des paquets GARP avec la mauvaise adresse MAC lorsqu'ils utilisent des cartes réseau Intel. (RHELPLAN-140971)
- Lorsque vous utilisez la méthode ZTP de GitOps pour gérer les clusters et que vous supprimez un cluster dont l'installation n'est pas terminée, le nettoyage de l'espace de noms du cluster sur le cluster hub peut être suspendu indéfiniment. Pour terminer la suppression de l'espace de noms, supprimez le finalisateur **baremetalhost.metal3.io** de deux CR dans l'espace de noms du cluster :

  1. Retirer le finalisateur du secret pointé par le CR **.spec.bmc.credentialsName** de BareMetalHost.

  2. Retirer le finalisateur de **BareMetalHost** CR. Lorsque ces finaliseurs sont supprimés, la terminaison de l'espace de noms s'effectue en quelques secondes. (OCPBUGS-3029)

- L'ajout d'une nouvelle fonctionnalité dans l'OCP 4.12 qui active UDP GRO fait également que tous les appareils veth ont une file d'attente RX par CPU disponible (auparavant, chaque veth avait une file d'attente). Ces files d'attente sont configurées dynamiquement par OVN et il n'y a pas de synchronisation entre le réglage de la latence et la création de cette file d'attente. La logique de réglage de la latence surveille les événements de création des cartes réseau des veth et commence à configurer les masques de CPU des files d'attente RPS avant que toutes les files d'attente ne soient correctement créées. Cela signifie que certains masques de file d'attente RPS ne sont pas configurés. Étant donné que toutes les files d'attente des cartes réseau ne sont pas configurées correctement, il est possible que des pics de latence se produisent dans une application en temps réel qui utilise des processeurs sensibles au temps pour communiquer avec des services dans d'autres conteneurs. Les applications qui n'utilisent pas la pile réseau du noyau ne sont pas affectées. (OCPBUGS-4194)
- Problèmes connus de l'opérateur de plate-forme et du RukPak :
  - La suppression d'un opérateur de plate-forme entraîne la suppression en cascade des ressources sous-jacentes. Cette logique de suppression en cascade ne peut supprimer que les ressources définies dans le format de regroupement de l'opérateur basé sur le gestionnaire du cycle de vie de l'opérateur (OLM). Dans le cas où un opérateur de plateforme crée des ressources qui sont définies en dehors de ce format de bundle, l'opérateur de plateforme est responsable de la gestion de cette interaction de nettoyage. Ce comportement peut être observé lors de l'installation de l'opérateur cert-manager en tant qu'opérateur de plate-forme, puis lors de sa suppression. Le comportement attendu est qu'un espace de noms créé par l'opérateur cert-manager est laissé derrière lui.

  - Le gestionnaire de la plate-forme Operators ne dispose d'aucune logique permettant de

comparer l'état actuel et l'état souhaité de la ressource **BundleDeployment** gérée par le cluster. Cela permet à un utilisateur disposant d'un contrôle d'accès basé sur les rôles (RBAC) suffisant de modifier manuellement cette ressource sous-jacente **BundleDeployment** et peut conduire à des situations dans lesquelles les utilisateurs peuvent escalader leurs autorisations jusqu'au rôle **cluster-admin**. Par défaut, vous devez limiter l'accès à cette ressource à un petit nombre d'utilisateurs qui en ont explicitement besoin. Le seul client pris en charge pour la ressource **BundleDeployment** dans le cadre de cette version d'aperçu technologique est le composant de gestion des opérateurs de la plate-forme.

  - Le composant Marketplace d'OLM est une fonctionnalité optionnelle qui peut être désactivée. Cela a des conséquences pour la version Technology Preview, car les opérateurs de plate-forme ne proviennent actuellement que de la source de catalogue **redhat-operators** gérée par le composant Marketplace. En guise de solution de contournement, un administrateur de cluster peut créer cette source de catalogue manuellement.

  - Les implémentations du provisionneur RukPak n'ont pas la capacité d'inspecter la santé ou l'état des ressources qu'elles gèrent. Cela a des conséquences sur la remontée de l'état de la ressource **BundleDeployment** générée vers la ressource **PlatformOperator** qui la possède. Si un bundle **registry v1** contient des manifestes qui peuvent être appliqués avec succès au cluster, mais qui échoueront au moment de l'exécution, comme un objet **Deployment** référençant une image inexistante, le résultat est un état réussi reflété dans les ressources individuelles **PlatformOperator** et **BundleDeployment**.

  - Les administrateurs de clusters qui configurent les ressources **PlatformOperator** avant la création du cluster ne peuvent pas facilement déterminer le nom du paquet souhaité sans s'appuyer sur un cluster existant ou sur des exemples documentés. Il n'existe actuellement aucune logique de validation garantissant qu'une ressource **PlatformOperator** configurée individuellement pourra être déployée avec succès dans le cluster.

- Lors de l'utilisation de la fonctionnalité OCI Technology Preview avec le plugin CLI oc-mirror, le catalogue miroir intègre tous les bundles Operator, au lieu de ne filtrer que ceux spécifiés dans le fichier de configuration de l'ensemble d'images. (OCPBUGS-5085)

- Il y a actuellement un problème connu lorsque vous exécutez l'installateur OpenShift Container Platform basé sur l'agent pour générer une image ISO à partir d'un répertoire où la version précédente a été utilisée pour la génération d'image ISO. Un message d'erreur s'affiche avec la version qui ne correspond pas. Pour contourner le problème, créez et utilisez un nouveau répertoire. (OCPBUGS#5159)

- Les capacités définies dans le fichier **install-config.yaml** ne sont pas appliquées dans l'installation d'OpenShift Container Platform basée sur un agent. Actuellement, il n'y a pas de solution de contournement. (OCPBUGS#5129)

- Les équilibreurs de charge entièrement remplis sur RHOSP qui sont créés avec le pilote OVN peuvent contenir des pools qui sont bloqués dans un statut de création en attente. Ce problème peut affecter les clusters déployés sur RHOSP. Pour résoudre ce problème, mettez à jour vos paquets RHOSP. (BZ#2042976)

- Les mises à jour en masse des membres de l'équilibreur de charge sur RHOSP peuvent renvoyer un code 500 en réponse aux requêtes **PUT**. Ce problème peut affecter les clusters déployés sur RHOSP. Pour résoudre ce problème, mettez à jour vos paquets RHOSP. (BZ#2100135)

- Les clusters qui utilisent des fournisseurs de cloud externes peuvent ne pas récupérer les informations d'identification mises à jour après la rotation. Les plateformes suivantes sont concernées :

- Nuage d'Alibaba
- IBM Cloud VPC
- IBM Power
- Virtualisation OpenShift
- RHOSP

En guise de solution, redémarrez les pods **openshift-cloud-controller-manager** en exécutant la commande suivante :

```
$ oc delete pods --all -n openshift-cloud-controller-manager
```

(OCPBUGS-5036)

- Il y a un problème connu lorsque **cloud-provider-openstack** essaie de créer des moniteurs de santé sur les équilibreurs de charge OVN en utilisant l'API pour créer des équilibreurs de charge entièrement peuplés. Ces moniteurs de santé sont bloqués dans le statut **PENDING_CREATE**. Après leur suppression, les équilibreurs de charge associés sont bloqués dans un statut **PENDING_UPDATE**. Il n'y a pas de solution. (BZ#2143732)

- En raison d'un problème connu, pour utiliser des réseaux IPv6 avec état avec des clusters fonctionnant sous RHOSP, vous devez inclure **ip=dhcp,dhcpv6** dans les arguments du noyau des nœuds de travail. (OCPBUGS-2104)

- Il n'est pas possible de créer un macvlan sur la fonction physique (PF) lorsqu'une fonction virtuelle (VF) existe déjà. Ce problème concerne le NIC Intel E810. (BZ#2120585)

- Il y a actuellement un problème connu lors de la configuration manuelle d'adresses et de routes IPv6 sur un cluster OpenShift Container Platform IPv4. Lors de la conversion vers un cluster dual-stack, les pods nouvellement créés restent dans le statut **ContainerCreating**. Actuellement, il n'y a pas de solution de contournement. Ce problème devrait être résolu dans une prochaine version d'OpenShift Container Platform. (OCPBUGS-4411)

- Lorsqu'un cluster OVN installé sur IBM Public Cloud compte plus de 60 nœuds de travail, la création simultanée d'au moins 2000 services et objets de route peut faire en sorte que les pods créés en même temps restent dans l'état **ContainerCreating**. Si ce problème se produit, la saisie de la commande **oc describe pod <podname>** affiche les événements avec l'avertissement suivant : **FailedCreatePodSandBox…failed to configure pod interface: timed out waiting for OVS port binding (ovn-installed)**. Il n'existe actuellement aucune solution à ce problème. (OCPBUGS-3470)

- Lorsqu'une machine de plan de contrôle est remplacée sur un cluster qui utilise le fournisseur de réseau OVN-Kubernetes, les pods liés à OVN-Kubernetes peuvent ne pas démarrer sur la machine de remplacement. Dans ce cas, l'absence de réseau sur la nouvelle machine empêche etcd de remplacer l'ancienne machine. En conséquence, le cluster est bloqué dans cet état et peut se dégrader. Ce comportement peut se produire lorsque le plan de contrôle est remplacé manuellement ou par le jeu de machines du plan de contrôle.
  Il n'existe actuellement aucune solution pour résoudre ce problème. Pour éviter ce problème, désactivez le jeu de machines du plan de contrôle et ne remplacez pas manuellement les machines du plan de contrôle si votre cluster utilise le fournisseur de réseau OVN-Kubernetes. (OCPBUGS-5306)

- Si un cluster déployé via ZTP a des politiques qui ne sont pas conformes et qu'aucun objet

ClusterGroupUpdates n'est présent, vous devez redémarrer les pods TALM. Le redémarrage de TALM crée l'objet **ClusterGroupUpdates** approprié, ce qui renforce la conformité de la politique. (OCPBUGS-4065)

- Actuellement, un problème de conformité de certificat, spécifiquement sorti comme **x509: certificate is not standards compliant**, existe lorsque vous exécutez le programme d'installation sur macOS dans le but d'installer un cluster OpenShift Container Platform sur VMware vSphere. Ce problème est lié à un problème connu avec le compilateur **golang** dans la mesure où le compilateur ne reconnaît pas les normes de certificat macOS nouvellement prises en charge. Il n'existe pas de solution à ce problème. (OSDOCS-5694)

1.9. MISES À JOUR ASYNCHRONES DE L'ERRATA

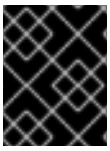
Les mises à jour de sécurité, les corrections de bogues et les améliorations pour OpenShift Container Platform 4.12 sont publiées en tant qu'errata asynchrone via le Red Hat Network. Tous les errata d'OpenShift Container Platform 4.12 sont disponibles sur le portail client de Red Hat . Consultez le cycle de vie d'OpenShift Container Platform pour plus d'informations sur les errata asynchrones.

Les utilisateurs du portail client de Red Hat peuvent activer les notifications d'errata dans les paramètres du compte pour la gestion des abonnements Red Hat (RHSM). Lorsque les notifications d'errata sont activées, les utilisateurs sont notifiés par courriel lorsque de nouveaux errata concernant leurs systèmes enregistrés sont publiés.

NOTE

Les comptes utilisateurs du portail client Red Hat doivent avoir des systèmes enregistrés et consommer des droits OpenShift Container Platform pour que les courriels de notification d'errata d'OpenShift Container Platform soient générés.

Cette section continuera d'être mise à jour au fil du temps pour fournir des notes sur les améliorations et les corrections de bugs pour les futures versions d'errata asynchrones d'OpenShift Container Platform 4.12. Les versions asynchrones versionnées, par exemple sous la forme OpenShift Container Platform 4.12.z, seront détaillées dans des sous-sections. En outre, les versions pour lesquelles le texte d'errata ne peut pas tenir dans l'espace fourni par l'avis seront détaillées dans les sous-sections suivantes.



IMPORTANT

Pour toute version d'OpenShift Container Platform, consultez toujours les instructions relatives à la mise à jour correcte de votre cluster.

1.9.1. RHSA-2022:7399 - Avis de mise à jour de sécurité, de correction de bogues et de publication de l'image d'OpenShift Container Platform 4.12.0

Publié : 2023-01-17

La version 4.12.0 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHSA-2022:7399. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHSA-2022:7398.

L'espace disponible n'a pas permis de documenter toutes les images de conteneurs de cette version dans l'avis. Voir l'article suivant pour des notes sur les images de conteneurs de cette version :

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.0 --pullspecs
```

1.9.1.1. Caractéristiques

1.9.1.1.1. Disponibilité générale de la liaison au niveau du pod pour les réseaux secondaires

Avec cette mise à jour, **Using pod-level bonding** est désormais disponible de manière générale.

1.9.2. RHSA-2023:0449 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.1

Publié : 2022-01-30

La version 4.12.1 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHSA-2023:0449. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:0448.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.1 --pullspecs
```

1.9.2.1. Bug fixes

- Auparavant, en raison d'une vérification erronée dans le fournisseur de cloud OpenStack, les équilibreurs de charge étaient alimentés avec des adresses IP externes lorsque tous les équilibreurs de charge Octavia étaient créés. Cela augmentait le temps de traitement des load balancers. Avec cette mise à jour, les équilibreurs de charge sont toujours créés de manière séquentielle et les adresses IP externes sont renseignées une par une. (**OCPBUGS-5403**)

- Auparavant, le site **cluster-image-registry-operator** utilisait par défaut la réclamation de volume persistant (PVC) lorsqu'il ne parvenait pas à atteindre Swift. Avec cette mise à jour, l'échec de la connexion à l'API Red Hat OpenStack Platform (RHOSP) ou d'autres défaillances incidentes amènent le site **cluster-image-registry-operator** à réessayer la sonde. Au cours de la nouvelle tentative, le défaut de PVC ne se produit que si le catalogue RHOSP est correctement trouvé et qu'il ne contient pas de stockage d'objets ; ou alternativement, si le catalogue RHOSP est présent et que l'utilisateur actuel n'a pas l'autorisation de lister les conteneurs. (**OCPBUGS-5154**)

1.9.2.2. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.3. RHSA-2023:0569 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.2

Délivré : 2023-02-07

La version 4.12.2 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHSA-2023:0569. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:0568.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.2 --pullspecs
```

1.9.3.1. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.4. RHSA-2023:0728 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.3

Publié : 2023-02-16

La version 4.12.3 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHSA-2023:0728. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHSA-2023:0727.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.3 --pullspecs
```

1.9.4.1. Bug fixes

- Auparavant, lorsqu'une machine de plan de contrôle était remplacée sur un cluster qui utilisait le fournisseur de réseau OVN-Kubernetes, les pods liés à OVN-Kubernetes ne démarraient parfois pas sur la machine de remplacement, et empêchaient etcd de l'autoriser à remplacer l'ancienne machine. Avec cette mise à jour, les pods liés à OVN-Kubernetes démarrent sur la machine de remplacement comme prévu.(**OCPBUGS-6494**)

1.9.4.2. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.5. RHSA-2023:0769 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.4

Issued: 2023-02-20

La version 4.12.4 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHSA-2023:0769. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:0768.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.4 --pullspecs
```

1.9.5.1. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.6. RHSA-2023:0890 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.5

Publié : 2023-02-28

La version 4.12.5 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHSA-2023:0890. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:0889.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.5 --pullspecs
```

1.9.6.1. Bug fixes

- Auparavant, dans la liste des dépôts, vous ne pouviez voir le **PipelineRuns** que lorsque le statut était **Succeeded** ou **Failed** mais pas lorsque le statut était **Running**. Avec cette correction, lorsque le **PipelineRuns** est déclenché, vous pouvez le voir dans la liste des dépôts avec le statut **Running**. (OCPBUGS-6816)

- Auparavant, lors de la création d'un **Secret**, le modèle **Start Pipeline** créait une valeur JSON invalide, ce qui rendait le secret inutilisable et faisait échouer le **PipelineRun**. Avec cette correction, le modèle **Start Pipeline** crée une valeur JSON valide pour **Secret**. Vous pouvez désormais créer des secrets valides tout en démarrant un pipeline. (OCPBUGS-6671)

- Auparavant, lorsqu'une ressource **BindableKinds** n'avait pas de statut, la console web se bloquait, récupérant et affichant les mêmes données en boucle. Avec cette correction, vous pouvez définir le tableau d'état de la ressource **BindableKinds** sur **[]**, en vous attendant à ce qu'il existe sans champ d'état. Par conséquent, le navigateur web ou l'application ne se bloque pas. (OCPBUGS-4072)

- Auparavant, les webhooks associés **<kn-service-name>-github-webhook-secret** n'étaient pas supprimés lors de la suppression d'un service Knative (**kn**) d'OpenShift Container Platform. Avec cette correction, tous les secrets de webhook associés sont supprimés. Maintenant, vous pouvez créer un service Knative (**kn**) avec le même nom que celui qui a été supprimé. (OCPBUGS-7437)

1.9.6.2. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.7. RHSA-2023:1034 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.6

Délivré : 2023-03-07

La version 4.12.6 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHBA-2023:1034. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHSA-2023:1033.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.6 --pullspecs
```

1.9.7.1. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.8. RHBA-2023:1163 - Mise à jour des corrections de bogues de OpenShift Container Platform 4.12.7

Délivré : 2023-03-13

La version 4.12.7 d'OpenShift Container Platform est maintenant disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHBA-2023:1163. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:1162.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.7 --pullspecs
```

1.9.8.1. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.9. RHBA-2023:1269 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.8

Issued: 2023-03-21

La version 4.12.8 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHBA-2023:1269. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHSA-2023:1268.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.8 --pullspecs
```

1.9.9.1. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.10. RHSA-2023:1409 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.9

Publié : 2023-03-27

La version 4.12.9 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHSA-2023:1409. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHSA-2023:1408.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.9 --pullspecs
```

1.9.10.1. Bug fixes

- Auparavant, la validation n'empêchait pas les utilisateurs d'installer un cluster GCP dans un VPC partagé s'ils n'activaient pas la porte de la fonctionnalité Technology Preview. Par conséquent, vous pouviez installer un cluster dans un VPC partagé sans activer la porte de la fonctionnalité d'aperçu technologique. Cette version a ajouté une validation de la porte de fonctionnalité à la version 4.12, de sorte que vous devez activer **featureSet: TechPreviewNoUpgrade** pour installer un cluster GCP dans un VPC partagé. (**OCPBUGS-7469**)

- Auparavant, la configuration de la migration MTU était parfois nettoyée avant la fin de la migration, ce qui entraînait l'échec de la migration. Cette version garantit que la migration MTU est préservée lorsque la migration est en cours afin que la migration puisse se terminer avec succès. (**OCPBUGS-7445**)

1.9.10.2. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.11. RHBA-2023:1508 - Mise à jour des corrections de bogues de OpenShift Container Platform 4.12.10

Délivré : 2023-04-03

La version 4.12.10 d'OpenShift Container Platform est maintenant disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHBA-2023:1508. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:1507.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.10 --pullspecs
```

1.9.11.1. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.12. RHSA-2023:1645 - Mise à jour de sécurité et correction de bogues pour OpenShift Container Platform 4.12.11

Publié : 2023-04-11

La version 4.12.11 d'OpenShift Container Platform, qui inclut des mises à jour de sécurité, est désormais disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHBA-2023:1645. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:1644.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.11 --pullspecs
```

1.9.12.1. Caractéristiques

1.9.12.1.1. Nouvelle option pour le plugin oc-mirror : --max-nested-paths

Avec cette mise à jour, vous pouvez maintenant utiliser le drapeau **--max-nested-paths** pour le plugin oc-mirror afin de spécifier le nombre maximum de chemins imbriqués pour les registres de destination qui limitent les chemins imbriqués. La valeur par défaut est **2**.

1.9.12.1.2. Nouveau drapeau pour le plugin oc-mirror : --skip-pruning

Avec cette mise à jour, vous pouvez désormais utiliser le drapeau **--skip-pruning** pour le plugin oc-mirror afin de désactiver l'élagage automatique des images du registre du miroir cible.

1.9.12.2. Bug fixes

- Auparavant, la commande **openshift-install agent create cluster-manifests** nécessitait une liste non vide de **imageContentSources** dans le fichier **install-config.yaml**. Si aucune source de contenu d'image n'était fournie, la commande générait l'erreur **failed to write asset (Mirror Registries Config) to disk: failed to write file: open .: is a directory**. Avec cette mise à jour, la commande fonctionne, que la section **imageContentSources** du fichier **install-config.yaml** contienne ou non quelque chose. (OCPBUGS-8384)

- Auparavant, le fournisseur OpenStack Machine API devait être redémarré pour que les nouveaux identifiants cloud soient utilisés en cas de rotation du fichier OpenStack **clouds.yaml**. Par conséquent, la capacité d'un MachineSet à s'échelonner jusqu'à zéro était affectée. Avec cette mise à jour, les identifiants cloud ne sont plus mis en cache et le fournisseur d'API OpenStack Machine lit le secret correspondant à la demande. (OCPBUGS-10603)

1.9.12.3. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.13. RHBA-2023:1734 - Correction d'un bug sur OpenShift Container Platform 4.12.12

Publié : 2023-04-13

La version 4.12.12 d'OpenShift Container Platform est maintenant disponible. La liste des corrections de bogues incluses dans cette mise à jour est documentée dans l'avis RHBA-2023:1734. Il n'y a pas de paquets RPM pour cette mise à jour.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.12 --pullspecs
```

1.9.13.1. Mise à jour

Tous les utilisateurs d'OpenShift Container Platform 4.12 sont informés que le seul défaut corrigé dans cette version est limité au temps d'installation ; par conséquent, il n'est pas nécessaire de mettre à jour les clusters précédemment installés vers cette version.

1.9.14. RHBA-2023:1750 - Mise à jour des corrections de bogues de OpenShift Container Platform 4.12.13

Publié : 2023-04-19

La version 4.12.13 d'OpenShift Container Platform est maintenant disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHBA-2023:1750. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:1749.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.13 --pullspecs
```

1.9.14.1. Caractéristiques

1.9.14.1.1. L'admission à la sécurité des pods est soumise à des restrictions (Avant-première technologique)

Avec cette version, l'admission à la sécurité des pods restreinte à *enforcement* est disponible en tant que fonctionnalité d'aperçu technologique en activant l'ensemble de fonctionnalités **TechPreviewNoUpgrade**. Si vous activez le jeu de fonctionnalités **TechPreviewNoUpgrade**, les pods sont rejetés s'ils ne respectent pas les normes de sécurité des pods, au lieu d'afficher uniquement un avertissement.

NOTE

L'application restreinte de l'admission à la sécurité des pods n'est activée que si vous activez l'ensemble de fonctionnalités **TechPreviewNoUpgrade** après l'installation de votre cluster OpenShift Container Platform. Elle n'est pas activée si vous activez l'ensemble de fonctionnalités **TechPreviewNoUpgrade** pendant l'installation du cluster.

Pour plus d'informations, voir Comprendre les portes de fonctionnalités .

1.9.14.2. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.

1.9.15. RHBA-2023:1858 - Mise à jour des corrections de bogues de OpenShift Container Platform 4.12.14

Publié : 2023-04-24

La version 4.12.14 d'OpenShift Container Platform est maintenant disponible. La liste des corrections de bogues incluses dans la mise à jour est documentée dans l'avis RHBA-2023:1858. Les paquets RPM inclus dans la mise à jour sont fournis par l'avis RHBA-2023:1857.

Vous pouvez visualiser les images de conteneurs de cette version en exécutant la commande suivante :

```
$ oc adm release info 4.12.14 --pullspecs
```

1.9.15.1. Caractéristiques

1.9.15.1.1. Le fournisseur de cloud OpenStack est mis à jour à la version 1.25

Avec cette version, le fournisseur de cloud Red Hat OpenStack Platform (RHOSP) est mis à jour vers la version 1.25.5. La mise à jour inclut l'ajout d'une annotation pour les adresses IP réelles des équilibreurs de charge et la source globale pour **math/rand** packages are seeded in **main.go**.

1.9.15.2. Mise à jour

Pour mettre à jour un cluster OpenShift Container Platform 4.12 existant vers cette dernière version, voir Mise à jour d'un cluster à l'aide du CLI pour les instructions.