OpenShift Container Platform 4.13

リリースノート

新機能のハイライトおよび OpenShift Container Platform リリースの変更内容

Last Updated: 2024-04-20

OpenShift Container Platform 4.13 リリースノート

新機能のハイライトおよび OpenShift Container Platform リリースの変更内容

法律上の通知

概要

以下の OpenShift Container Platform リリースノートでは、新機能および拡張機能のすべて、以前のバージョンからの主な技術上の変更点、主な修正、および一般公開バージョンの既知の問題についてまとめています。

目次

第1章 OPENSHIFT CONTAINER PLATFORM 4.13 リリースノート

Red Hat OpenShift Container Platform では、設定や管理のオーバーヘッドを最小限に抑えながら、セキュアでスケーラブルなリソースに新規および既存のアプリケーションをデプロイするハイブリッドクラウドアプリケーションプラットフォームを開発者や IT 組織に提供します。OpenShift Container Platform は、Java、Javascript、Python、Ruby および PHP など、幅広いプログラミング言語およびフレームワークをサポートしています。

Red Hat Enterprise Linux (RHEL) および Kubernetes にビルドされる OpenShift Container Platform は、最新のエンタープライズレベルのアプリケーションに対してよりセキュアでスケーラブルなマルチテナント対応のオペレーティングシステムを提供するだけでなく、統合アプリケーションランタイムやライブラリーを提供します。OpenShift Container Platform を使用することで、組織はセキュリティー、プライバシー、コンプライアンス、ガバナンスの各種の要件を満たすことができます。

1.1. このリリースについて

OpenShift Container Platform (RHSA-2023:1326) をご利用いただけるようになりました。このリリースでは、CRI-O ランタイムで Kubernetes 1.26 を使用します。以下では、OpenShift Container Platform 4.13 に関連する新機能、変更点および既知の問題について説明します。

OpenShift Container Platform 4.13 クラスターは https://console.redhat.com/openshift で入手できます。OpenShift Container Platform 向けの Red Hat OpenShift Cluster Manager アプリケーションを使用して、OpenShift Container Platform クラスターをオンプレミスまたはクラウド環境のいずれかにデプロイできます。

OpenShift Container Platform 4.13 は Red Hat Enterprise Linux (RHEL) 9.2 をベースにしています。RHEL 9.2 はまだ FIPS 認定のために提出されていません。ただし、特定の期限は確約できませんが、Red Hat は RHEL 9.0 および RHEL 9.2 モジュール、その後は RHEL 9.x のマイナーリリースについても、FIPS 認定を取得することを想定しています。更新は Compliance Activities and Government Standards から入手できる予定です。

OpenShift Container Platform 4.13 は、Red Hat Enterprise Linux (RHEL) 8.6、8.7、8.8 および Red Hat Enterprise Linux CoreOS (RHCOS) 4.13 でサポートされます。

コントロールプレーンには RHCOS マシンを使用する必要があり、コンピュートマシンに RHCOS または RHEL のいずれかを使用できます。

1.2. OPENSHIFT CONTAINER PLATFORM のレイヤー化された依存関係にあるコンポーネントのサポートと互換性

OpenShift Container Platform のレイヤー化された依存関係にあるコンポーネントのサポート範囲は、OpenShift Container Platform のバージョンに関係なく変更されます。アドオンの現在のサポートステータスと互換性を確認するには、リリースノートを参照してください。詳細は、Red Hat OpenShift Container Platform ライフサイクルポリシー を参照してください。

1.3. 新機能および機能拡張

今回のリリースでは、以下のコンポーネントおよび概念に関連する拡張機能が追加されました。

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. RHCOS は RHEL 9.2 を使用するようになりました

RHCOS は、OpenShift Container Platform 4.13 で Red Hat Enterprise Linux (RHEL) 9.2 パッケージを使用するようになりました。これにより、最新の修正、機能、拡張機能、および最新のハードウェアサポートおよびドライバー更新を利用できます。

1.3.1.1.1. OpenShift Container Platform with RHEL 9.2 へのアップグレードに関する考慮事項

このリリースでは、OpenShift Container Platform 4.13 に RHEL 9.2 ベースの RHCOS が導入されており、アップグレードする前に考慮が必要な点がいくつかあります。

- RHEL 8.6 と RHEL 9.2 では一部のコンポーネント設定オプションとサービスが変更されている可能性があります。これは、既存のマシン設定ファイルが無効になっている可能性があることを意味します。
- デフォルトの OpenSSH **/etc/ssh/sshd_config** サーバー設定ファイルをカスタマイズした場合は、この Red Hat ナレッジベースの記事 に従ってファイルを更新する必要があります。
- RHEL 6 ベースのイメージコンテナーは RHCOS コンテナーホストではサポートされていませんが、RHEL 8 ワーカーノードではサポートされています。詳細は、Red Hat コンテナー互換性 マトリクスを参照してください。
- 一部のデバイスドライバーは非推奨になりました。詳細は、RHEL ドキュメント を参照してください。

1.3.1.2. installer-provisioned infrastructure を使用する IBM Power Virtual Server (テクノロジープレビュー)

installer-provisioned infrastructure (IPI) は、OpenShift Container Platform のフルスタックインストールとセットアップを提供します。

詳細は、IBM Power Virtual Server へのインストール準備 を参照してください。

1.3.1.3. IBM Z および IBM(R) LinuxONE での IBM Secure Execution

この機能は、OpenShift Container Platform 4.12 でテクノロジープレビュー機能として導入され、OpenShift Container Platform 4.13 で一般提供が開始されました。IBM Secure Execution は、KVM ゲストのメモリー境界を保護するハードウェア拡張機能です。IBM Secure Execution は、クラスターのワークロードに最高レベルの分離とセキュリティーを提供します。これは、IBM Secure Execution 対応の QCOW2 ブートイメージを使用して有効にすることができます。

IBM Secure Execution を使用するには、ホストマシンのホストキーが必要であり、Ignition 設定ファイルで指定する必要があります。IBM Secure Execution は、LUKS 暗号化を使用してブートボリュームを自動的に暗号化します。

詳細は、IBM Secure Execution を使用した RHCOS のインストール を参照してください。

1.3.1.4. Assisted Installer SaaS は、IBM Power、IBM Z、IBM (R) LinuxONE のプラットフォーム統合サポートを提供します。

console.redhat.com の Assisted Installer SaaS は、Assisted Installer ユーザーインターフェイスまたは REST API のいずれかを使用した、IBM Power、IBM Z、IBM® LinuxONE プラットフォームへの OpenShift Container Platform のインストールをサポートします。統合により、ユーザーは単一のインターフェイスからインフラストラクチャーを管理できます。IBM Power、IBM Z、および IBM® LinuxONE と Assisted Installer SaaS の統合を有効にするには、追加でいくつかのインストール手順を実行します。

詳細は、Assisted Installer を使用したオンプレミスクラスターのインストール を参照してください。

1.3.1.5. RHCOS に lsof を追加

OpenShift Container Platform 4.13 には、RHCOS に **lsof** コマンドが追加されました。

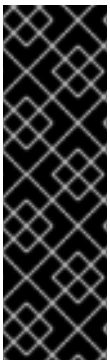
1.3.2. インストールおよび更新

1.3.2.1. VMware vSphere バージョン 8.0 のサポート

OpenShift Container Platform 4.13 は、VMware vSphere バージョン 8.0 をサポートします。VMware vSphere バージョン 7.0 Update 2 にも引き続き OpenShift Container Platform クラスターをインストールできます。

1.3.2.2. VMware vSphere のリージョンとゾーンの有効化

単一の VMware vCenter で実行される複数の vSphere データセンターまたはリージョンに OpenShift Container Platform クラスターをデプロイできます。各データセンターは、複数のクラスターまたはゾーンを実行できます。この設定により、ハードウェアの障害やネットワークの停止によってクラスターに障害が発生するリスクが軽減されます。



重要

VMware vSphere のリージョンおよびゾーン有効化機能は、クラスター内のデフォルトのストレージドライバーとして vSphere Container Storage Interface (CSI) ドライバーを必要とするため、新しくインストールされたクラスターでのみ使用できます。

以前のリリースからアップグレードされたクラスターは、デフォルトでツリー内 vSphere ドライバーを使用します。そのため、この機能を使用するには、クラスターの CSI 自動移行を有効にする必要があります。その後、アップグレードされたクラスターに対して複数のリージョンとゾーンを設定できます。

詳細は、VMware vSphere のリージョンとゾーンの有効化 を参照してください。

1.3.2.3. デフォルトの vSphere install-config.yaml ファイルへの変更

vSphere で OpenShift Container Platform のインストールプログラムを実行すると、デフォルトの **install-config.yaml** ファイルに **vcenters** および **failureDomains** フィールドが含まれるようになり、クラスターに複数のデータセンター、リージョン、およびゾーン情報を指定することを選択できるようになりました。VMware vCenter で実行されている単一のデータセンターで設定される vSphere 環境に OpenShift Container Platform クラスターをインストールする場合は、これらのフィールドを空白のままにできます。

詳細は、VMware vCenter のリージョンとゾーンの設定 を参照してください。

1.3.2.4. 複数の vSphere サブネットをサポートする外部ロードバランサー

OpenShift Container Platform クラスターを、複数のサブネットをサポートする外部ロードバランサーを使用するように設定できます。複数のサブネットを使用する場合は、ロードバランサーターゲットが使用するネットワーク内のすべての IP アドレスを明示的にリストできます。この設定では、ロードバランサーターゲットを再設定せずにネットワーク内でノードを作成および破棄できるため、メンテナンスオーバーヘッドを削減できます。

詳細は、外部ロードバランサーの設定 を参照してください。

1.3.2.5. VMware vSphere にクラスターをインストール前の仮想マシン暗号化をサポート

OpenShift Container Platform 4.13 では、user-provisioned infrastructure を使用して、VMware vSphere にクラスターをインストールする前に仮想マシンを暗号化できます。

詳細は、仮想マシンの暗号化の要件 を参照してください。

1.3.2.6. 3 ノードクラスターのサポート

OpenShift Container Platform 4.13 以降、3 ノードクラスターのデプロイは、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP)、および VMware vSphere でサポートされています。このタイプの OpenShift Container Platform クラスターは、3 つのコントロールプレーンマシンのみから構成され、それがコンピュートマシンとしての役割も果たすため、より小さく、リソース効率の良いクラスターになります。

詳細は、Installing a three-node cluster on AWS、Installing a three-node cluster on Azure、Installing a three-node cluster on GCP、Installing a three-node cluster on vSphere を参照してください。

1.3.2.7. IBM Cloud VPC と既存の VPC リソース

OpenShift Container Platform クラスターを既存の Virtual Private Cloud (VPC) にデプロイする場合、**networkResourceGroupName** パラメーターを使用して、これらの既存のリソースを含むリソースグループの名前を指定できるようになりました。この機能強化により、既存の VPC リソースとサブネットを、インストールプログラムがプロビジョニングするクラスターリソースから分離しておくことができます。その後、**resourceGroupName** パラメーターを使用して、インストーラーによってプロビジョニングされたすべてのクラスターリソースをデプロイするためにインストールプログラムが使用できる既存のリソースグループの名前を指定できます。**resourceGroupName** が定義されていない場合、クラスターの新しいリソースグループが作成されます。

詳細は、Additional IBM Cloud VPC configuration parameters を参照してください。

1.3.2.8. GCP が OpenShift Container Platform クラスターをインストールおよび削除するために最低限必要な権限

OpenShift Container Platform 4.13 では、事前定義されたロールを使用する代わりに、カスタムロールを定義して、Google Cloud Platform (GCP) が OpenShift Container Platform クラスターをインストールおよび削除するために最低限必要なアクセス許可を含めることができるようになりました。これらの権限は、installer-provisioned infrastructure と user-provisioned infrastructure で利用できます。

1.3.2.9. Azure のユーザー定義タグ

OpenShift Container Platform 4.13 では、Azure でタグを設定してリソースをグループ化し、リソースアクセスとコストを管理できます。タグのサポートは、Azure パブリッククラウドで作成されたリソースと、テクノロジープレビュー (TP) としての OpenShift Container Platform 4.13 でのみ使用できます。**install-config.yaml** ファイルで Azure リソースのタグを定義できるのは、OpenShift Container Platform クラスターの作成時のみです。

1.3.2.10. GCP 上の OpenShift Container Platform クラスターを共有 Virtual Private Cloud (VPC) にインストール

OpenShift Container Platform 4.13 では、Google Cloud Platform (GCP) 上の共有 Virtual Private Cloud (VPC) にクラスターをインストールできます。このインストール方法では、VPC を別の GCP プロジェクトと共有するようにクラスターを設定します。共有 VPC を使用すると、組織は複数のプロジェクトから共通 VPC ネットワーク経由でリソースを接続できます。共通 VPC ネットワークでは、内部 IP アドレスを使用することで、組織通信のセキュリティーと効率が向上します。

詳細は、GCP 上のクラスターを共有 VPC にインストール を参照してください。

1.3.2.11. Shielded VM を使用した GCP へのクラスターのインストール

OpenShift Container Platform 4.13 では、クラスターのインストール時に Shielded VM を使用できます。Shielded VM には、セキュアブート、ファームウェアと整合性の監視、ルートキット検出などの追加のセキュリティー機能があります。詳細は、Shielded VM の有効化 および Google の Shielded VM ドキュメントを参照してください。

1.3.2.12. Confidential VM を使用した GCP へのクラスターのインストール

OpenShift Container Platform 4.13 では、クラスターのインストール時に Confidential VM を使用できます。Confidential VM は処理中のデータを暗号化します。詳細は、Google のConfidential Computing ドキュメントを参照してください。Confidential VM と Shielded VM を同時に有効にすることができますが、それらは互いに依存していません。

重要

OpenShift Container Platform 4.13.3 以前のバージョンにおける既知の問題により、Google Cloud Platform (GCP) 上の Confidential 仮想マシンが含まれるクラスターでは、永続ボリュームストレージを使用できません。この問題は OpenShift Container Platform 4.13.4 で解決されています。詳細は、OCPBUGS-11768 を参照してください。

1.3.2.13. AWS 上のクラスターを既存の Virtual Private Cloud (VPC) にインストールするプロセスの改善

OpenShift Container Platform 4.13 では、AWS VPC を使用するクラスターのインストールプロセスが単純化されました。このリリースでは、AWS Local Zones 用に最適化されたマシンプールである **エッジプール** も導入されています。

詳細は、AWS Local Zones を使用したクラスターインストール を参照してください。

1.3.2.14. OpenShift Container Platform 4.12 から 4.13 へのアップグレードには管理者承認が必要

OpenShift Container Platform 4.14 は Kubernetes 1.27 を使用します。これにより、複数の非推奨 API が削除されました。

クラスター管理者は、クラスターを OpenShift Container Platform 4.12 から 4.13 にアップグレードする前に、手動で承認を行う必要があります。削除された API が、クラスター上で実行されている、またはクラスターと対話しているワークロード、ツール、またはその他のコンポーネントによって引き続き使用される OpenShift Container Platform 4.13 にアップグレードした後の問題を防ぐ上で役立ちます。管理者は、削除が予定されている使用中の API に対するクラスターの評価を実施し、影響を受けるコンポーネントを移行して適切な新規 API バージョンを使用する必要があります。これが完了すると、管理者による承認が可能です。

すべての OpenShift Container Platform 4.12 クラスターでは、OpenShift Container Platform 4.13 にアップグレードする前に、この管理者承認が必要になります。

詳細は、OpenShift Container Platform 4.13 への更新の準備 を参照してください。

1.3.2.15. Microsoft Azure が OpenShift Container Platform クラスターをインストールおよび削除するために必要な最小限の権限

OpenShift Container Platform 4.13 では、ビルトインロールを使用する代わりに、カスタムロールを定義して、Microsoft Azure が OpenShift Container Platform クラスターをインストールおよび削除するために最低限必要な権限を含めることができるようになりました。これらの権限は、installer-provisioned infrastructure と user-provisioned infrastructure で利用できます。

1.3.2.16. シングルアーキテクチャーからマルチアーキテクチャーペイロードへの移行

OpenShift Container Platform 4.13 では **oc adm upgrade --to-multi-arch** コマンドが導入され、シングルアーキテクチャーコンピュートマシンを含むクラスターをマルチアーキテクチャーコンピュートマシンを含むクラスターに移行できます。マニフェストにリストされたマルチアーキテクチャーペイロードに更新すると、アーキテクチャーが混在するコンピュートマシンをクラスターに追加できます。

1.3.2.17. vSphere のコントロールプレーン上で実行されるネットワークコンポーネントの設定

vSphere インストール内のコントロールプレーンノード上で仮想 IP (VIP) アドレスを実行する必要がある場合は、コントロールプレーンノード上で排他的に実行されるように **ingressVIP** アドレスを設定する必要があります。デフォルトでは、OpenShift Container Platform は、ワーカーマシン設定プールの任意のノードが **ingressVIP** アドレスをホストすることを許可します。vSphere 環境ではコントロールプレーンノードとは別のサブネットにワーカーノードをデプロイするため、**ingressVIP** アドレスをコントロールプレーンノードで排他的に実行するように設定すると、ワーカーノードを別のサブネットにデプロイすることに起因する問題の発生を防ぐことができます。詳細は、vSphere のコントロールプレーンで実行されるネットワークコンポーネントの設定 を参照してください。

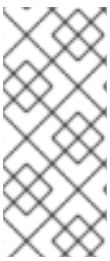
1.3.2.18. 単一ノードを使用した AWS への OpenShift Container Platform クラスターのインストール

OpenShift Container Platform 4.13 では、単一ノードを使用してクラスターを Amazon Web Services (AWS) にインストールできます。単一ノードへのインストールでは、ノードのリソース要件が増加します。詳細は、単一ノードへのクラスターのインストール を参照してください。

1.3.2.19. ユーザーがプロビジョニングしたクラスター内で Bare Metal Operator を使用してベアメタルホストをスケーリング

OpenShift Container Platform 4.13 では、Bare Metal Operator (BMO) およびその他のメタル ^{3} コンポーネントを使用して、既存の user-provisioned infrastructure クラスター内のベアメタルホストをスケーリングできます。ユーザーがプロビジョニングしたクラスターで Bare Metal Operator を使用すると、ホストの管理とスケーリングを単純化および自動化できます。

BMO を使用すると、**BareMetalHost** オブジェクトを設定することでホストを追加または削除できます。**BareMetalHost** オブジェクトインベントリーに既存ホストを **externallyProvisioned** として登録すると、既存ホストを追跡することもできます。



注記

Bare Metal Operator では、プロビジョニングネットワークを使用して、user-provisioned infrastructure クラスターをスケーリングすることはできません。このワークフローはプロビジョニングネットワークをサポートしていないため、仮想メディアネットワークの起動をサポートするベアメタルホストドライバー (**redfish-virtualmedia** や **idrac-virtualmedia** など) のみを使用できます。

ユーザーがプロビジョニングしたクラスターを BMO を使用してスケーリングする方法について、詳しくは ユーザーがプロビジョニングしたクラスターの Bare Metal Operator を使用したスケーリング を参照してください。

1.3.2.20. 64-bit ARM での OpenShift Container Platform

OpenShift Container Platform 4.13 は、64 ビット ARM アーキテクチャーベースの Azure ユーザープロビジョニングインストールでサポートされるようになりました。Agent ベースのインストールプログラムも、64 ビット ARM システムでサポートされるようになりました。インスタンスの可用性やインストールに関するドキュメントの詳細は、各種プラットフォームのサポート対象インストール方法 を参照してください。

1.3.2.21. git-lfs パッケージのサポート

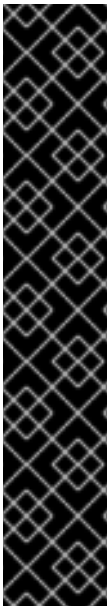
OpenShift Jenkins イメージで **git-lfs** パッケージがサポートされるようになりました。このパッケージでは、OpenShift Jenkins イメージで 200 メガバイト (MB) を超えるアーティファクトを使用できます。

1.3.2.22. oc-mirror プラグインを使用したローカル OCI Operator カタログの追加機能の一般提供を開始

oc-mirror プラグインを使用して、ディスク上のローカル OCI Operator カタログをミラーレジストリーにミラーリングできるようになりました。これは、OpenShift Container Platform 4.12 でテクノロジープレビュー機能として導入され、OpenShift Container Platform 4.13 で一般提供が開始されました。

このリリースでは、ローカル OCI カタログが含まれる場合に次の機能がサポートされます。

- ターゲットミラーレジストリーからのイメージのプルーニング
- 前回ツールを実行してから変更された内容のみをミラーリングする増分ミラーリング
- ターゲットミラーレジストリー内におけるカタログの代替名の namespace 階層



重要

- OpenShift Container Platform 4.12 のテクノロジープレビュー機能である oc-mirror プラグインの OCI ローカルカタログ機能を使用していた場合、完全に切断されたクラスターにミラーリングするための最初の手順として、oc-mirror プラグインの OCI 機能を使用してローカルにカタログをコピーしてから OCI 形式に変換することができなくなりました。
- ローカル OCI カタログをミラーリングする場合、ローカル OCI 形式のカタログとともにミラーリングする OpenShift Container Platform リリースまたは追加のイメージをレジストリーからプルする必要があります。OCI カタログを oc-mirror イメージセットファイルと一緒にディスク上でミラーリングすることはできません。
- **--use-oci-feature** フラグは非推奨になりました。代わりに **--include-local-oci-catalogs** フラグを使用して、ローカル OCI カタログのミラーリングを有効にします。

詳細は、ローカル OCI オペレータカタログの追加 を参照してください。

1.3.2.23. RHOSP 上での障害ドメインを使用するクラスターのデプロイ (テクノロジープレビュー)

RHOSP 上で、複数の障害ドメインにまたがるクラスターをデプロイできるようになりました。大規模なデプロイメントでは、障害ドメインによって回復力とパフォーマンスが向上します。

詳細は、障害ドメインの RHOSP パラメーター を参照してください。

1.3.2.24. RHOSP 上での、ユーザーが管理するロードバランサーを含むクラスターのデプロイ (テクノロジープレビュー)

デフォルトの内部ロードバランサーではなく、ユーザーが管理するロードバランサーを使用して、クラスターを RHOSP にデプロイできるようになりました。

詳細は、ユーザーが管理するロードバランサーを使用した OpenStack 上のクラスターのインストール設定 を参照してください。

1.3.2.25. Nutanix にクラスターをインストールする際のプロジェクトとカテゴリーの使用

OpenShift Container Platform 4.13 では、プロジェクトとカテゴリーを使用して、Nutanix にインストールされたクラスター内のコンピュートプレーン仮想マシンを編成できます。プロジェクトは、権限、ネットワーク、およびその他のパラメーターを管理するためのユーザーロールの論理グループを定義します。カテゴリーを使用すると、共有特性に基づいて仮想マシンのグループにポリシーを適用できます。

詳細は、Nutanix へのクラスターインストール を参照してください。

1.3.2.26. エージェントベースのインストーラーがネットワーク接続チェックを実行

エージェントベースのインストーラーを使用して OpenShift Container Platform 4.13 をインストールする場合、コンソールアプリケーション (テキストユーザーインターフェイスを使用) はインストールプロセスの初期段階でプルチェックを実行して、現在のホストが設定済みのリリースイメージを取得できることを確認します。コンソールアプリケーションは、ユーザーによるネットワーク設定の直接変更を許可することで、問題のトラブルシューティングをサポートします。

詳細は、現在のインストールホストによるリリースイメージのプルを検証 を参照してください。

1.3.3. インストール後の設定

1.3.3.1. マルチアーキテクチャーコンピュートマシンを含む OpenShift Container Platform クラスター

マルチアーキテクチャーコンピュートマシンを含む OpenShift Container Platform 4.13 クラスターの一般提供が開始されました。2 日目の操作として、AWS および Azure インストーラーがプロビジョニングしたインフラストラクチャー上に、異なるアーキテクチャーのコンピュートノードを含むクラスターを作成できるようになりました。ベアメタル上でのユーザープロビジョニングインストールはテクノロジープレビュー機能です。マルチアーキテクチャーコンピュートマシンを使用したクラスター作成の詳細は、OpenShift Container Platform クラスターでのマルチアーキテクチャーコンピュートマシンの設定 を参照してください。

1.3.3.2. vSphere 上のクラスターに複数の障害ドメインを指定する

管理者は、VMware vSphere インスタンスで実行される OpenShift Container Platform クラスターに複数の障害ドメインを指定できます。これは、主要なコントロールプレーンとワークロード要素をデータセンターのさまざまなハードウェアリソースに分散できることを意味します。さらに、ノード間のデータ転送が複数のネットワークにまたがるように、複数のレイヤー 2 ネットワーク設定を使用するようにクラスターを設定できます。

詳細は、VSphere 上のクラスターに複数の障害ドメインの指定 を参照してください。

1.3.4. Web コンソール

1.3.4.1. Developer パースペクティブ

このリリースでは、Web コンソールの **Developer** パースペクティブで次のアクションを実行できるようになりました。

- **Import from Git** フローを使用して、**Serverless Function** を作成します。
- **Add ページ** の **Create Serverless Function** フローを使用して、**Serverless Function** を作成します。
- **Import from Git** ワークフローで、オプションとして **Pipeline-as-code** を選択します。
- ユーザーインターフェイスの次の場所でトラフィックを受信している Pod を確認します。
  - **Topology** ビューのサイドペイン
  - Pod の **Details** ビュー
  - **Pod** リストビュー
- **Web Terminal** をインスタンス化するときに、タイムアウト期間をカスタマイズするか、独自のイメージを指定します。
- 管理者は、すべてのユーザーの **Developer** パースペクティブナビゲーションにデフォルトのリソースが予め固定されるように設定します。

1.3.4.1.1. Pipelines ページを改善

OpenShift Container Platform 4.13 では、**Pipelines** ページのナビゲーションが以下のとおり改善されました。

- **Pipelines** ページに戻っても、前に選択したタブが表示されたままになります。
- **Repository details** ページのデフォルトタブは **PipelinesRuns** になりましたが、**Create Git Repository** フローに従っている場合、デフォルトタブは **Details** になります。

1.3.4.1.2. Helm ページの改善

OpenShift Container Platform 4.13 では、**Helm** ページに次の新機能と更新された機能が追加されました。

- このページで使用される用語は、Helm チャートのインストールとアンインストールではなく、Helm リリースの作成と削除を意味します。
- Helm リリースを非同期的に作成および削除でき、アクションの完了を待たずに Web コンソールで次のタスクを実行できます。
- Helm リリースリストに **Status** 列が追加されました。

1.3.5. OpenShift CLI (oc)

1.3.5.1. 指定された名前空間で must-gather を実行するための新しいフラグが追加されました

OpenShift Container Platform 4.13 では、**--run-namespace** フラグが **oc adm must-gather** コマンドで使用できるようになりました。このフラグを使用して、must-gather ツールを実行する既存の名前空間を指定できます。

詳細は、About the must-gather tool を参照してください。

1.3.5.2. OpenShift CLI (oc) を使用したマニフェストのインポート

OpenShift Container Platform 4.13 では、新しい **oc** コマンドラインインターフェイス (CLI) フラグ **--import-mode** が以下の **oc** コマンドに追加されました。

- **oc import-image**
- **oc tag**

今回の機能強化により、ユーザーは **--import-mode** フラグを **Legacy** または **PreserveOriginal** に設定できます。これにより、**oc import-image** または **oc tag** コマンドの実行時にマニフェストリストの単一のサブマニフェストまたはすべてのマニフェストをインポートするオプションがユーザーに提供されます。

詳細は、Working with manifest lists を参照してください。

1.3.5.3. イメージの os/arch とダイジェストを返す

OpenShift Container Platform 4.13 では、イメージで **oc describe** を実行すると、各マニフェストの os/arch およびダイジェストが返されるようになりました。

1.3.6. IBM Z and IBM(R) LinuxONE

本リリースでは、IBM Z および IBM® LinuxONE は OpenShift Container Platform 4.13 と互換性があります。インストールは、z/VM または Red Hat Enterprise Linux (RHEL) Kernel-based Virtual Machine (KVM) を使用して実行できます。インストール手順については、以下のドキュメントを参照してください。

- z/VM を使用したクラスターの IBM Z および IBM® LinuxONE へのインストール
- ネットワークが制限された環境での z/VM のあるクラスターの IBM Z および IBM® LinuxONE へのインストール
- RHEL KVM を使用したクラスターの IBM Z および IBM® LinuxONE へのインストール
- ネットワークが制限された環境での RHEL KVM のあるクラスターの IBM Z および IBM® LinuxONE へのインストール

重要

コンピュートノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。

IBM Z および IBM(R) LinuxONE の主な機能拡張
OpenShift Container Platform 4.13 の IBM Z および IBM® LinuxONE リリースでは、OpenShift Container Platform のコンポーネントと概念に、改良点と新機能が追加されました。

このリリースでは、IBM Z および IBM® LinuxONE 上で次の機能がサポートされます。

- アシステッドインストーラー
- Cluster Resource Override Operator
- Egress IP
- MetalLB Operator
- Network-Bound Disk Encryption - 外部 Tang サーバー

IBM Secure Execution
OpenShift Container Platform は、IBM Z および IBM® LinuxONE (s390x アーキテクチャー) 上における IBM Secure Execution 用の Red Hat Enterprise Linux CoreOS (RHCOS) ノードの設定をサポートするようになりました。

インストール手順については、以下のドキュメントを参照してください。

- IBM Secure Execution を使用した RHCOS のインストール

1.3.7. IBM Power

このリリースでは、IBM Power は OpenShift Container Platform 4.13 と互換性があります。インストール手順については、以下のドキュメントを参照してください。

- クラスターの IBM Power へのインストール
- ネットワークが制限された環境での IBM Power へのクラスターのインストール

重要

コンピュートノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。

IBM Power の主な機能強化
OpenShift Container Platform 4.13 の IBM Power リリースでは、OpenShift Container Platform のコンポーネントと概念に改良点と新機能が追加されました。

このリリースでは、IBM Power で次の機能がサポートされます。

- アシステッドインストーラー
- Cluster Resource Override Operator
- IBM Power Virtual Server Block CSI Driver Operator (テクノロジープレビュー)
- Egress IP
- IBM Power Virtual Server の installer-provisioned infrastructure の有効化 (テクノロジープレビュー)
- MetalLB Operator
- Network-Bound Disk Encryption - 外部 Tang サーバー

IBM Power、IBM Z、IBM(R) LinuxONE サポートマトリクス

表1.1 OpenShift Container Platform の機能

機能	IBM Power	IBM Z および IBM® LinuxONE
代替の認証プロバイダー	サポート対象	サポート対象
Assisted Installer	サポート対象	サポート対象
ローカルストレージ Operator を使用した自動デバイス検出	サポート対象外	サポート対象
マシンヘルスチェックによる障害のあるマシンの自動修復	サポート対象外	サポート対象外
IBM Cloud 向けクラウドコントローラーマネージャー	サポート対象	サポート対象外
オーバーコミットの制御およびノード上のコンテナーの密度の管理	サポート対象外	サポート対象外
Cron ジョブ	サポート対象	サポート対象
Descheduler	サポート対象	サポート対象
Egress IP	サポート対象	サポート対象
etcd に保存されるデータの暗号化	サポート対象	サポート対象
Helm	サポート対象	サポート対象
Horizontal Pod Autoscaling	サポート対象	サポート対象
IPv6	サポート対象	サポート対象
ユーザー定義プロジェクトのモニタリング	サポート対象	サポート対象
マルチパス化	サポート対象	サポート対象
Network-Bound Disk Encryption - 外部 Tang サーバー	サポート対象	サポート対象
不揮発性メモリーエクスプレスドライブ (NVMe)	サポート対象	サポート対象外
OpenShift CLI (**oc**) プラグイン	サポート対象	サポート対象
Operator API	サポート対象	サポート対象
OpenShift Virtualization	サポート対象外	サポート対象外
IPsec 暗号化を含む OVN-Kubernetes	サポート対象	サポート対象

機能	IBM Power	IBM Z および IBM® LinuxONE
PodDisruptionBudget	サポート対象	サポート対象
Precision Time Protocol (PTP) ハードウェア	サポート対象外	サポート対象外
Red Hat OpenShift Local	サポート対象外	サポート対象外
スケジューラーのプロファイル	サポート対象	サポート対象
SCTP (Stream Control Transmission Protocol)	サポート対象	サポート対象
複数ネットワークインターフェイスのサポート	サポート対象	サポート対象
3 ノードクラスターのサポート	サポート対象	サポート対象
Topology Manager	サポート対象	サポート対象外
SCSI ディスク上の z/VM Emulated FBA デバイス	サポート対象外	サポート対象
4k FCP ブロックデバイス	サポート対象	サポート対象

表1.2 永続ストレージのオプション

機能	IBM Power	IBM Z および IBM® LinuxONE
iSCSI を使用した永続ストレージ	サポート対象 [1]	サポート対象 [1] [2]
ローカルボリュームを使用した永続ストレージ (LSO)	サポート対象 [1]	サポート対象 [1] [2]
hostPath を使用した永続ストレージ	サポート対象 [1]	サポート対象 [1] [2]
ファイバーチャネルを使用した永続ストレージ	サポート対象 [1]	サポート対象 [1] [2]
Raw Block を使用した永続ストレージ	サポート対象 [1]	サポート対象 [1] [2]
EDEV/FBA を使用する永続ストレージ	サポート対象 [1]	サポート対象 [1] [2]

1. 永続共有ストレージは、Red Hat OpenShift Data Foundation またはその他のサポートされているストレージプロトコルを使用してプロビジョニングする必要があります。
2. 共有されていない永続ストレージは、iSCSI、FC、DASD、FCP または EDEV/FBA と共に LSO を使用するなど、ローカルストレージを使用してプロビジョニングする必要があります。

表1.3 Operator

機能	IBM Power	IBM Z および IBM® LinuxONE
Cluster Logging Operator	サポート対象	サポート対象
Cluster Resource Override Operator	サポート対象	サポート対象
Compliance Operator	サポート対象	サポート対象
File Integrity Operator	サポート対象	サポート対象
Local Storage Operator	サポート対象	サポート対象
MetalLB Operator	サポート対象	サポート対象
Network Oberservability Operator	サポート対象	サポート対象外
NFD Operator	サポート対象	サポート対象
NMState Operator	サポート対象	サポート対象
OpenShift Elasticsearch Operator	サポート対象	サポート対象
Vertical Pod Autoscaler Operator	サポート対象	サポート対象

表1.4 Multus CNI プラグイン

機能	IBM Power	IBM Z および IBM® LinuxONE
ブリッジ	サポート対象	サポート対象
host-device	サポート対象	サポート対象
IPAM	サポート対象	サポート対象
IPVLAN	サポート対象	サポート対象

表1.5 CSI ボリューム

機能	IBM Power	IBM Z および IBM® LinuxONE
クローン	サポート対象	サポート対象

機能	IBM Power	IBM Z および IBM® LinuxONE
拡張	サポート対象	サポート対象
スナップショット	サポート対象	サポート対象

1.3.8. Images

1.3.8.1. イメージストリーム上のマニフェストにリストされたイメージのサポート

OpenShift Container Platform 4.13 でじゃ、イメージストリーム上のマニフェストにリストされたイメージのサポートが一般提供されるようになりました。

1.3.9. セキュリティーおよびコンプライアンス

1.3.9.1. AES-GCM 暗号化はサポート対象

OpenShift Container Platform の etcd 暗号化を有効にする場合に、AES-GCM 暗号化タイプがサポートされるようになりました。AES-GCM 暗号化タイプの暗号化キーは毎週ローテーションされます。

詳細は、サポートされている暗号化タイプ を参照してください。

1.3.10. ネットワーク

1.3.10.1. ネットワークメトリクスの強化

1.3.10.1.1. egress_ips_rebalance_total

- メトリック名: **ovnkube_master_egress_ips_rebalance_total**
- **ヘルプメッセージ:The total number of times assigned egress IP(s) needed to be moved to a different node.**

1.3.10.1.2. egress_ips_node_unreachable_total

- メトリック名: **ovnkube_master_egress_ips_node_unreachable_total**
- **ヘルプメッセージ: The total number of times assigned egress IP(s) were unreachable.**

1.3.10.1.3. egress_ips_unassign_latency_seconds

- メトリック名: **ovnkube_master_egress_ips_unassign_latency_seconds**
- **ヘルプメッセージ: The latency of egress IP unassignment from OVN northbound database.**

1.3.10.1.4. interfaces_total

- メトリック名: **ovs_vswitchd_interfaces_total**

- **ヘルプメッセージ**: **The total number of Open vSwitch interface(s) created for pods** および **Open vSwitch interface until its available.**

1.3.10.1.5. interface_up_wait_seconds_total

- メトリック名: **ovs_vswitchd_interface_up_wait_seconds_total**
- **ヘルプメッセージ**: **The total number of seconds that is required to wait for pod.** および **Open vSwitch interface until its available.**

1.3.10.1.6. ovnkube_resource_retry_failures_total

- メトリック名: **ovnkube_resource_retry_failures_total**
- **ヘルプメッセージ**: **The total number of times processing a Kubernetes resource reached the maximum retry limit and was no longer processed.**

1.3.10.2. ネットワークアラートの機能強化

- OVN Kubernetes は、要求を破棄する前に最大 15 回まで要求を再試行します。今回の更新により、この障害が発生した場合、OpenShift Container Platform はクラスター管理者にアラートを出します。各アラートの説明は、コンソールで表示できます。

1.3.10.2.1. NoOvnMasterLeader

- 概要: ovn-kubernetes マスターリーダーはありません。
- コンソールでの説明:

> Networking control plane is degraded. Networking configuration updates applied to the cluster will not be implemented while there is no OVN Kubernetes leader. Existing workloads should continue to have connectivity. OVN-Kubernetes control plane is not functional.

1.3.10.2.2. OVNKubernetesNodeOVSOverflowUserspace

- 概要: OVS vSwitch デーモンは、バッファーオーバーフローが原因でパケットをドロップします。
- コンソールでの説明:

> Netlink messages dropped by OVS vSwitch daemon due to netlink socket buffer overflow. This will result in packet loss.

1.3.10.2.3. OVNKubernetesNodeOVSOverflowKernel

- 概要: OVS カーネルモジュールは、バッファーオーバーフローが原因でパケットをドロップします。
- コンソールでの説明:

> Netlink messages dropped by OVS kernel module due to netlink socket buffer overflow. This will result in packet loss.

1.3.10.3. MetalLB IPAddressPool リソースの IP アドレスを特定の名前空間とサービスに割り当てる

今回の更新により、MetalLB **IPAddressPool** リソースからサービス、名前空間、またはその両方に IP アドレスを割り当てることができます。これは、MetalLB が IP アドレスプールから特定のサービスおよび名前空間に IP アドレスを固定する必要があるマルチテナントのベアメタル環境で役立ちます。多くの IP アドレスプールからサービスと名前空間に IP アドレスを割り当てることができます。次に、これらの IP アドレスプールの優先度を定義して、MetalLB が優先度の高い IP アドレスプールから IP アドレスを割り当てるようにすることができます。

IP アドレスプールからサービスおよび名前空間への IP アドレスの割り当ての詳細は、Configuring MetalLB address pools を参照してください。

1.3.10.4. デュアルポート NIC を備えたノードで OpenShift Container Platform インストールをサポート (テクノロジープレビュー)

この更新により、以下の方法を使用して、OpenShift Container Platform クラスターを 2 つの物理機能 (PF) 上の 2 つの仮想機能 (VF) を持つボンディングインターフェイスにデプロイできるようになります。

- エージェントベースのインストーラー
- installer-provisioned infrastructure のインストール
- user-provisioned infrastructure のインストール

デュアルポート NIC を備えたノードに OpenShift Container Platform をインストールする方法について、詳しくは SR-IOV デバイスの NIC パーティショニング を参照してください。

1.3.10.5. BlueField-2 ネットワークデバイスのデータ処理ユニット (DPU) モードからネットワークインターフェイスコントローラー (NIC) モードへの切り替えのサポートが GA になりました

このリリースでは、BlueField-2 ネットワークデバイスのデータ処理ユニット (DPU) モードからネットワークインターフェイスコントローラー (NIC) モードへの切り替えが一般的に利用可能になりました。

詳細は、Switching BlueField-2 from DPU to NIC を参照してください。

1.3.10.6. ネットワークカードの MT2892 Family [ConnectX-6 Dx] でハードウェアオフロードの一般提供を開始

OpenShift Container Platform 4.13 では、ネットワークカードの MT2892 Family [ConnectX-6 Dx] で OvS ハードウェアオフロードのサポートが追加されました。

詳細は、サポート対象のデバイス を参照してください。

1.3.10.7. OpenShift SDN ネットワークプラグインへの移行

OVN-Kubernetes ネットワークプラグインを使用している場合は、OpenShift SDN ネットワークプラグインに移行できます。

詳細は、OpenShift SDN ネットワークプラグインへの移行を 参照してください。

1.3.10.8. CoreDNS 1.10.1 に更新

OpenShift Container Platform 4.13 は CoreDNS を 1.10.1 に更新します。CoreDNS は、元のクライアントクエリーで指定された DNSSEC DO ビットを使用するようになりました。これにより、クライアントが DNSSEC を要求していない場合、DNS 応答の UDP パケットサイズが削減されます。パケットサイズが小さくなると、TCP 接続の再試行が減るため、DNS 切り捨ての可能性と全体的な DNS 帯域幅の両方が減少します。

1.3.10.9. クラスターネットワークの IP アドレス範囲の拡張

クラスターへのノードの追加をサポートするために、クラスターネットワークを拡張できます。たとえば、クラスターをデプロイし、クラスターネットワーク範囲として **10.128.0.0/19** を指定し、ホスト接頭辞 **23** を指定した場合、16 ノードに制限されます。クラスターの CIDR マスクを **/14** に変更することで、これを 510 ノードに拡張できます。詳細は、クラスターネットワーク範囲の設定 を参照してください。

1.3.10.10. VMware vSphere クラスター上のデュアルスタック IPv4/IPv6

インストーラーがプロビジョンした vSphere クラスターでは、IPv4 をプライマリー IP ファミリーとして、IPv6 をセカンダリーアドレスファミリーとして使用したデュアルスタックネットワークを使用できます。詳細は、ネットワーク設定パラメーター を参照してください。

1.3.10.11. ベアメタルデュアルスタッククラスター上のプライマリー IP アドレスファミリーとしての IPv6

ベアメタルにクラスターをインストールする際に、IPv6 をデュアルスタッククラスター上のプライマリー IP アドレスファミリーとして設定できます。新しいクラスターのインストール時にこの機能を有効にするには、マシンネットワーク、クラスターネットワーク、サービスネットワーク、API VIP、イングレス VIP の IPv4 アドレスファミリーの前に IPv6 アドレスファミリーを指定します。

詳細は以下を参照してください。

- installer-provisioned infrastructure: デュアルスタックネットワーキングを使用したデプロイメント
- user-provisioned infrastructure: ネットワーク設定パラメーター

1.3.10.12. OVN-Kubernetes がセカンダリーネットワークとして使用可能 (テクノロジープレビュー)

このリリースでは、Red Hat OpenShift Networking OVN-Kubernetes ネットワークプラグインで、Pod のセカンダリーネットワークインターフェイスを設定できます。OVN-Kubernetes は、セカンダリーネットワークとしてレイヤー 2 (switched) トポロジーネットワークをサポートします。これはテクノロジープレビュー機能として利用できます。

セカンダリーネットワークとしての OVN-Kubernetes について、詳しくは OVN-Kubernetes 追加ネットワークの設定 を参照してください。

1.3.10.13. OVN-Kubernetes ネットワークプラグインの egress ファイアウォールにノードセレクターを追加

OpenShift Container Platform 4.13 では、**nodeSelector が** OVN-Kubernetes ネットワークプラグインの egress ファイアウォールの宛先仕様に追加されました。この機能を使用すると、ユーザーは 1 つまたは複数のノードにラベルを追加でき、選択したノードの IP アドレスが関連するルールに含まれます。詳細は、EgressFirewall の nodeSelector の例 を参照してください。

1.3.10.14. RHOSP で実行される Kuryr から OVN-Kubernetes へのクラスター移行手順 (テクノロジープレビュー)

RHOSP 上で実行され、Kuryr を使用するクラスターを OVN-Kubernetes に移行できるようになりました。

詳細は、Kuryr ネットワークプラグインから OVN-Kubernetes ネットワークプラグインへの移行 を参照してください。

1.3.10.15. RHOSP 上で実行されるクラスターの egress IP サポートの強化

RHOSP 上で実行され、OVN-Kubernetes を使用するクラスターの場合、予約ポートにフローティング IP アドレスを手動で再割り当てを行う必要がなくなりました。予約ポートが 1 つのノードから削除され、別のノードで再作成された場合、再割り当ては自動的に実行されます。

1.3.10.16. SR-IOV (Single Root I/O Virtualization) でサポートされるハードウェア

OpenShift Container Platform 4.13 はで、以下の SR-IOV デバイスのサポートが追加されました。

- Intel E810-XXVDA4T
- Intel X710 Base T

詳細は、サポート対象のデバイス を参照してください。

1.3.11. ストレージ

1.3.11.1. KMS での再暗号化における顧客管理型キーの使用をサポート

この更新により、AWS のデフォルトの認証情報要求が変更され、Key Management Service (KMS) での再暗号化に顧客が管理するキーを使用できるようになりました。手動モードを使用するように Cloud Credential Operator (CCO) が設定されているクラスターの場合、管理者は **kms:ReEncrypt*** 権限をキーポリシーに追加して、これらの変更を手動で適用する必要があります。他の管理者は、この変更による影響を受けません。(**OCPBUGS-5410**)

1.3.11.2. 論理ボリュームマネージャー(LVM)ストレージのデュアルスタックサポート

OpenShift Container Platform 4.13 では、IPv4 および IPv6 ネットワーク環境のデュアルスタックで LVM ストレージがサポートされます。詳細は、デュアルスタッククラスターネットワークへの変換 を参照してください。

1.3.11.3. GitOps ZTP での LVM ストレージのサポート

OpenShift Container Platform 4.13 では、GitOps ZTP 経由で論理ボリュームマネージャーストレージ (LVM ストレージ) を追加および設定できます。詳細は、PolicyGenTemplate CR を使用した LVM ストレージの設定 と LVM ストレージ を参照してください。

1.3.11.4. 非接続環境での LVM ストレージのサポート

OpenShift Container Platform 4.13 では、非接続環境に LVM ストレージをインストールできます。詳細は、非接続環境での LVM ストレージのインストール を参照してください。

1.3.11.5. ユーザー管理型暗号化の一般提供を開始

ユーザー管理型の暗号化機能を使用すると、インストール中に OpenShift Container Platform ノードのルートボリュームを暗号化するキーを指定でき、すべてのマネージドストレージクラスはこれらのキーを使用してプロビジョニングされたストレージボリュームを暗号化できます。これにより、プラットフォームのデフォルトのアカウントキーではなく、選択したキーを使用してストレージボリュームを暗号化できます。

この機能は、次のストレージタイプをサポートします。

- Amazon Web Services (AWS) Elastic Block Storage (EBS) (詳細は ユーザー管理型の暗号化 を参照)
- Microsoft Azure Disk ストレージ (詳細は ユーザー管理型の暗号化 を参照)
- Google Cloud Platform (GCP) 永続ディスク (PD) ストレージ (詳細は ユーザー管理型の暗号化 を参照)

1.3.11.6. 正常ではないノードシャットダウン後の CSI ボリュームのデタッチ (テクノロジープレビュー)

Container Storage Interface (CSI) ドライバーは、ノードが正常にシャットダウンしない場合はボリュームを自動的にデタッチできるようになりました。ノードが正常にシャットダウンしなかった場合、ノードに out-of-service テイントを手動で追加し、ノードからボリュームを自動的にデタッチできます。これはテクノロジープレビュー機能としてサポートされています。

詳細は、正常ではないノードシャットダウン後の CSK ボリュームのデタッチ を参照してください。

1.3.11.7. VMware vSphere 暗号化サポートの一般提供を開始

vSphere 上で実行されている OpenShift Container Platform 上の仮想マシン (VM) と永続ボリューム (PV) を暗号化できます。

詳細は、vSphere 永続ディスクの暗号化 を参照してください。

1.3.11.8. 複数のデータセンターに対する VMware vSphere CSI トポロジーのサポートの一般提供を開始

OpenShift Container Platform 4.12 では、異なるゾーンおよびリージョンに OpenShift Container Platform for vSphere をデプロイする機能が導入されました。この機能を使用することで、複数のコンピュートクラスターにデプロイできるため、単一障害点を回避するのに役立ちます。OpenShift Container Platform 4.13 では、複数のデータセンターにまたがるデプロイと、インストール中またはインストール後に作成された障害ドメインを使用したトポロジーのセットアップに対するサポートが導入されました。

詳細は、vSphere CSI トポロジー を参照してください。

1.3.11.9. 複数のデフォルトストレージクラスの作成の一般提供を開始

OpenShift Container Platform 4.13 では、複数のデフォルトストレージクラスを作成できます。この機能を使用すると、デフォルトとして定義された 2 番目のストレージクラスを作成できるため、デフォルトのストレージクラスを容易に変更できます。その後は、以前のデフォルトストレージクラスからデフォルトステータスを削除するまで、一時的に 2 つのデフォルトストレージクラスが存在することになります。短期間であればデフォルトストレージクラスが複数存在することも許容されますが、最終的に存在するデフォルトストレージクラスは 1 つにする必要があります。

詳細は、デフォルトストレージクラスの変更 および 複数のデフォルトストレージクラス を参照してください。

1.3.11.10. デフォルトストレージクラスの管理の一般提供を開始

OpenShift Container Platform 4.13 では、**ClusterCSIDriver** オブジェクトに **spec.storageClassState** フィールドが導入されました。これにより、OpenShift Container Platform によって生成されたデフォルトのストレージクラスを管理して、いくつかの目的を達成できます。

- 他の優先ストレージクラスがある場合に、storage operator による最初のデフォルトストレージクラスの作成を阻止します。
- デフォルトのストレージクラスに名前を付け直すか変更します。
- 動的プロビジョニングを無効にして静的プロビジョニングを強制します。

詳細は、デフォルトストレージクラスの管理 を参照してください。

1.3.11.11. 遡及的なデフォルト StorageClass の割り当て (テクノロジープレビュー)

以前は、デフォルトのストレージクラスがない場合、デフォルトのストレージクラスを要求した作成済みの永続ボリューム要求 (PVC) は、手動で削除して再作成しない限り、無期限に保留状態のままでした。OpenShift Container Platform は、これらの PVC にデフォルトストレージクラスを遡って割り当てることができるようになり、保留状態のままにはならなくなりました。この機能を有効にすると、デフォルトストレージクラスが作成されるか、いずれかの既存ストレージクラスがデフォルトとして宣言された後、保留されていたこれらの PVC がデフォルトストレージクラスに割り当てられます。

これはテクノロジープレビュー機能としてサポートされています。

詳細は、デフォルトストレージクラスの欠落 を参照してください。

1.3.11.12. IBM Power Virtual Server Block CSI Driver Operator (テクノロジープレビュー)

OpenShift Container Platform は、IBM Power Virtual Server Block Storage の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。

詳細は、IBM Power Virtual Server Block CSI Driver Operator を参照してください。

1.3.11.13. CSI インライン一時ボリュームの一般提供を開始

Container Storage Interface (CSI) のインライン一時ボリュームは、テクノロジープレビュー機能として OpenShift Container Platform 4.5 に導入されました。これにより、Pod のデプロイ時にインライン一時ボリュームを作成し、Pod の破棄時にインライン一時ボリュームを削除する Pod 仕様を定義できます。現在、この機能は一般提供されています。

この機能は、サポートされている Container Storage Interface (CSI) ドライバーでのみ利用できます。

この機能には、CSI Volume Admission プラグインも含まれており、このプラグインを使用すると、CSI 一時ボリュームをプロビジョニングできる個別の CSI ドライバーの使用を Pod 受け入れ時に制限できるメカニズムを追加できます。管理者またはディストリビューションは、**CSIDriver** オブジェクトに **csi-ephemeral-volume-profile** ラベルを追加できます。その後、ラベルは Admission プラグインによって検査され、強制、警告、および監査を決定するために使用されます。

詳細は、CSI インライン一時ボリューム を参照してください。

1.3.11.14. Microsoft Azure File の自動 CSI 移行の一般利用を開始

OpenShift Container Platform 4.8 以降、インツリーボリュームプラグインの同等の Container Storage Interface (CSI) ドライバーへの自動移行がテクノロジープレビュー機能として利用可能になりました。OpenShift Container Platform 4.10 では、この機能で Azure File のサポートが提供されていました。OpenShift Container Platform 4.13 では、Azure File の自動移行に対するサポートが一般提供されています。Azure File の CSI 移行はデフォルトで有効化され、管理者によるアクションは不要になりました。

この機能は in-tree オブジェクトを自動的に対応する CSI 表現に変換するため、ユーザーに対して完全に透過的である必要があります。変換されたオブジェクトはディスクに保存され、ユーザーデータは移行されません。

in-tree ストレージプラグインを参照するストレージクラスは引き続き機能しますが、デフォルトのストレージクラスを CSI ストレージクラスに切り替えることが推奨されます。

詳細は、CSI の自動移行 を参照してください。

1.3.11.15. VMware vSphere の自動 CSI 移行の一般提供を開始

この機能は in-tree オブジェクトを自動的に対応する CSI 表現に変換するため、ユーザーに対して完全に透過的である必要があります。in-tree ストレージプラグインを参照するストレージクラスは引き続き機能しますが、デフォルトのストレージクラスを CSI ストレージクラスに切り替えることが推奨されます。

OpenShift Container Platform 4.8 以降、インツリーボリュームプラグインの同等の Container Storage Interface (CSI) ドライバーへの自動移行がテクノロジープレビュー機能として利用可能になりました。OpenShift Container Platform 4.10 では、この機能で vSphere のサポートが提供されていました。OpenShift Container Platform 4.13 では、vSphere の自動移行に対するサポートが一般提供されています。

OpenShift Container Platform 4.13 以降の新規インストールの場合、自動移行はデフォルトで有効になっています。OpenShift Container Platform 4.12 以前から 4.13 へのアップグレードでは、ユーザーがオプトインした場合に限り vSphere の自動 CSI 移行が発生します。移行をオプトインする前に、提示された影響を慎重に確認してください。

以下の条件が **すべて** 該当する場合、OpenShift Container Platform 4.12 から 4.13、および 4.13 から 4.14 への更新はブロックされます。

- CSI 移行がまだ有効になっていない
- OpenShift Container Platform が vSphere 7.0u3L+ または 8.0u2+ で実行されていない
- vSphere in-tree （インツリー）永続ボリューム(PV)が存在する。

詳細は、CSI の自動移行 を参照してください。

1.3.11.16. AWS EFS CSI ドライバーのクロスアカウントサポートの一般提供を開始

クロスアカウントのサポートにより、1 つの Amazon Web Services (AWS) アカウントに OpenShift Container Platform クラスターを配置し、AWS Elastic File System (EFS) Container Storage Interface (CSI) ドライバーを使用して別の AWS アカウントにファイルシステムをマウントできます。

詳細は、AWS EFS CSI クロスアカウントのサポート を参照してください。

1.3.11.17. Kubelet ではなく FSGroup を CSI ドライバーに委譲する機能の一般提供を開始

この機能により、ボリュームがマウントされている場合に OpenShift Container Platform は Pod の FSGroup を Container Storage Interface (CSI) ドライバーに提供できます。Microsoft Azure File CSI ドライバーはこの機能に依存します。

1.3.11.18. NFS をサポートする Azure File の一般提供を開始

OpenShift Container Platform 4.13 による、Network File System (NFS) を備えた Azure File Container Storage Interface (CSI) Driver Operator のサポートの一般提供を開始しました。

詳細は、NFS サポート を参照してください。

1.3.12. Operator ライフサイクル

1.3.12.1. OpenShift CLI を使用した Operator バージョンの確認

OpenShift Container Platform 4.13 では、次の OpenShift CLI (**oc**) コマンドを実行することで、システムにインストールできる Operator のバージョンとチャネルを確認できます。

oc description コマンド構文の例

```
$ oc describe packagemanifests <operator_name> -n <catalog_namespace>
```

次のコマンドを実行して、Operator のバージョンとチャネル情報の出力形式を指定できます。

oc get コマンド構文の例

```
$ oc get packagemanifests <operator_name> -n <catalog_namespace> -o <output_format>
```

詳細は、特定の Operator バージョンのインストール を参照してください。

1.3.12.2. マルチテナントクラスター内の Operator

Operator Lifecycle Manager (OLM) のデフォルトの動作は、Operator のインストール時に簡素化することを目的としています。ただし、この動作は、特にマルチテナントクラスターでは柔軟性に欠ける場合があります。

次のトピックに、マルチテナントクラスターでの Operator 管理に関するガイダンスと推奨ソリューションが追加されました。

- マルチテナントクラスター内の Operator
- マルチテナントクラスター用の Operator の複数インスタンスの準備

1.3.12.3. Colocation of Operators in a namespace

Operator Lifecycle Manager (OLM) は、同じ namespace にインストールされている OLM-managed Operator を処理します。つまり、それらの Subscription リソースは、関連する Operator として同じ namespace に配置されます。それらが実際には関連していなくても、いずれかが更新されると、OLM はバージョンや更新ポリシーなどの状態を考慮します。

次のコピックに、Operator のコロケーションに関するガイダンスと、カスタム namespace を使用する代替手順が追加されました。

- Colocation of Operators in a namespace

- Installing global Operators in custom namespaces

1.3.12.4. コピーした CSV が無効化されている場合の Web コンソールの動作を更新

OpenShift Container Platform Web コンソールが更新され、コピーされたクラスターサービスバージョン (CSV) がクラスター上で無効になっている場合の Operator 検出が向上しました。

コピーされた CSV がクラスター管理者によって無効にされている場合、実際にはすべての namespace に CSV がコピーされていなくても、**openshift** namespace からコピーされた CSV を通常ユーザーのすべての namespace に表示するように Web コンソールが変更されます。これにより、通常ユーザーは、namespace でこれらの Operator の詳細を表示したり、グローバルにインストールされた Operator が提供するカスタムリソース (CR) を作成したりできます。

詳細は、コピーした CSV の無効化 を参照してください。

1.3.13. Operator の開発

1.3.13.1. サジェストされた namespace テンプレートをデフォルトノードセレクターを使用して設定

このリリースでは、Operator の作成者は、サジェストされた namespace にデフォルトのノードセレクターを設定できます。ここで、Operator が実行されます。サジェストされた namespace は、**ClusterServiceVersion** (CSV) に含まれる YAML の namespace マニフェストを使用して作成されます。OperatorHub を使用して Operator をクラスターに追加する場合、Web コンソールはインストールプロセス時にクラスター管理者にサジェストされる namespace を自動設定します。

詳細は、サジェストされた namespace をデフォルトノードセレクターを使用して設定 を参照してください。

1.3.13.2. Node Tuning Operator

Node Tuning Operator (NTO) は、**NodeTuning** クラスター機能を使用して有効化/無効化できるようになりました。クラスターのインストール時に無効にした場合は、後で再度有効にできます。詳細は、ノードチューニング機能 を参照してください。

1.3.14. マシン API

1.3.14.1. コントロールプレーンマシンセットの追加プラットフォームサポート

- このリリースでは、コントロールプレーンマシンセットが Google Cloud Platform クラスターでサポートされています。
- このリリースには、Microsoft Azure クラスター上のコントロールプレーンマシンセットのユーザーエクスペリエンスの強化が含まれています。OpenShift Container Platform バージョン 4.13 と共にインストールまたはアップグレードされた Azure クラスターの場合、コントロールプレーンマシンセットのカスタムリソース (CR) を作成する必要はなくなりました。
  - バージョン 4.13 でインストールされたクラスターには、デフォルトでアクティブなコントロールプレーンマシンセットがあります。
  - バージョン 4.13 にアップグレードされたクラスターの場合、非アクティブな CR がクラスターに対して生成され、CR の値がコントロールプレーンマシンに対して正しいことを確認した後にアクティブ化できます。

詳細は、コントロールプレーンマシンセットオペレーターの概要 を参照してください。

1.3.15. Machine Config Operator

1.3.15.1. Red Hat Enterprise Linux CoreOS (RHCOS) イメージ階層化の一般提供を開始

Red Hat Enterprise Linux CoreOS (RHCOS) イメージ階層化の一般提供が開始されました。この機能を使用すると、ベースイメージに追加のイメージを重ねることで、ベース RHCOS イメージ機能を拡張できます。

詳細は、Red Hat Enterprise Linux CoreOS (RHCOS) image layering を参照してください。

1.3.15.2. RHCOS へのサードパーティーおよびカスタムコンテンツの追加のサポート

Red Hat Enterprise Linux CoreOS (RHCOS) イメージの階層化を使用して、Red Hat Enterprise Linux (RHEL) およびサードパーティーパッケージをクラスターノードに追加できるようになりました。

詳細は、Red Hat Enterprise Linux CoreOS (RHCOS) image layering を参照してください。

1.3.15.3. core ユーザーパスワード設定のサポート

RHCOS **core** ユーザーのパスワードを作成できるようになりました。SSH または **oc debug node** コマンドを使用してノードにアクセスできない場合、このパスワードを使用すると、**core** ユーザーを使用して、クラウドプロバイダーのシリアルコンソールまたはベアメタルベースボードコントローラーマネージャー (BMC) を介してノードにアクセスできます。

詳細は、Changing the core user password for node access を参照してください。

1.3.16. ノード

1.3.16.1. タグによるイメージレジストリーリポジトリーのミラーリング

ダイジェスト仕様に加えてイメージタグを使用して、ミラーリングされたレジストリーからイメージをプルできるようになりました。この変更を実現するために、**ImageContentSourcePolicy** (ICSP) オブジェクトは非推奨になりました。**ImageDigestMirrorSet** (IDMS) オブジェクトを使用してダイジェスト仕様を使用してイメージをプルするか、**ImageTagMirrorSet** (ITMS) オブジェクトを使用してイメージタグを使用してイメージをプルできるようになりました。

ICSP オブジェクトの作成に使用した既存の YAML ファイルがある場合は、**oc adm migrate icsp** コマンドを使用して、それらのファイルを IDMS YAML ファイルに変換できます。

これらの新しいオブジェクトの詳細は、Configuring image registry repository mirroring を参照してください。

既存の ICSP YAML ファイルを IDMS YAML ファイルに変換する方法の詳細は、Converting ImageContentSourcePolicy (ICSP) files for image registry repository mirroring 参照してください。

1.3.16.2. crun 一般提供

crun 低レベルコンテナーランタイムは、OpenShift Container Platform 4.13 で一般提供されるようになりました。GA バージョンには新しい機能はありません。

1.3.16.3. Linux コントロールグループバージョン 2 (cgroup v2) の一般提供

Linux Control Group バージョン 2 (cgroup v2) が OpenShift Container Platform 4.13 で一般提供されるようになりました。GA バージョンには新しい機能はありません。

1.3.16.4. Pod Disruption Budget (PDB) の不健全な Pod エビクションポリシー (テクノロジープレビュー)

このリリースでは、テクノロジープレビュー機能として、Pod Disruption Budget (PDB) に対する不健全な Pod エビクションポリシーを指定できます。これは、ノードドレイン中に誤動作しているアプリケーションを排除するのに役立ちます。

このテクノロジープレビュー機能を使用するには、**TechPreviewNoUpgrade** 機能セットを有効にする必要があります。

警告

クラスターで **TechPreviewNoUpgrade** 機能セットを有効にすると、元に戻すことができず、マイナーバージョンの更新が妨げられます。本番クラスターでは、この機能セットを有効にしないでください。

詳細は、不健全な Pod のエビクションポリシーの指定 を参照してください。

1.3.16.5. Metal3 修復のサポート

これまで、Machine Health Checks では自己修復または自己ノード修復プロバイダーの使用が可能でした。このリリースでは、新しい Metal3 修復プロバイダーもベアメタルクラスターでサポートされます。

詳細は、ベアメタルの電源ベースの修復について を参照してください。

1.3.17. モニタリング

本リリースのモニタリングスタックには、以下の新機能および変更された機能が含まれています。

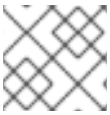
1.3.17.1. モニタリングスタックコンポーネントおよび依存関係の更新

このリリースでは、モニタリングスタックコンポーネントと依存関係が以下のバージョンに更新されます。

- Alertmanager 0.25.0
- kube-state-metrics 2.8.1
- node-exporter 1.5.0
- prom-label-proxy 0.6.0
- Prometheus 2.42.0
- prometheus-operator 0.63.0

- Thanos 0.30.2

1.3.17.2. アラートルールの変更



注記

Red Hat は、記録ルールまたはアラートルールの後方互換性を保証しません。

- **NodeFilesystemAlmostOutOfSpace** アラートは、設計上常にいっぱいになっている特定の **tmpfs** マウントポイントに対して実行されなくなりました。

1.3.17.3. Alertmanager 設定にシークレットを追加する新しいオプション

このリリースでは、コアプラットフォームモニタリングおよびユーザー定義プロジェクトの Alertmanager 設定にシークレットを追加できます。Alertmanager がアラートを送信できるようにレシーバーで認証する必要がある場合は、レシーバーの認証情報を含むシークレットを使用するように Alertmanager を設定できます。

1.3.17.4. node-exporter コレクターを設定するための新しいオプション

このリリースでは、次の Cluster Monitoring Operator (CMO) config map 設定をカスタマイズできます。次の node-exporter コレクターはオプションとなり、有効または無効にできます。

- **buddyinfo** コレクター
- **cpufreq** コレクター
- **netclass** コレクター
- **netdev** コレクター
- **netclass** コレクターの **netlink** バックエンド
- **tcpstat** コレクター

1.3.17.5. ノード関連のダッシュボードをノードのロールごとにフィルタリングする新しいオプション

OpenShift Container Platform Web コンソールで、ノード関連のモニタリングダッシュボードのデータを、ノードのロールに基づきフィルタリングできるようになりました。ワーカーノードなど、特定のロールを持つノードのダッシュボードデータのみを表示したい場合は、この新しいフィルターを使用して、該当するノードロールをすばやく選択できます。

1.3.17.6. メトリクスコレクションプロファイルを有効にする新しいオプション (テクノロジープレビュー)

このリリースでは、デフォルトのプラットフォームモニタリングのためのテクノロジープレビュー機能が導入されており、管理者はメトリクスコレクションプロファイルを設定して、デフォルトの量または最小限の量のメトリクスデータを収集できます。最小プロファイルを有効にすると、アラートなどの基本的なモニタリング機能は引き続き動作しますが、Prometheus が必要とする CPU およびメモリーリソースは減少します。

1.3.18. Network Observability Operator

Network Observability Operator は、OpenShift Container Platform マイナーバージョンのリリースストリームとは独立して更新をリリースします。更新は、現在サポートされているすべての OpenShift Container Platform 4 バージョンでサポートされている単一のローリングストリームを介して使用できます。Network Observability Operator の新機能、機能拡張、バグ修正に関する情報は、Network Observability リリースノート に記載されています。

1.3.19. スケーラビリティーおよびパフォーマンス

1.3.19.1. NUMA Resources Operator を使用した NUMA 対応のスケジューリングが一般提供されました

NUMA Resources Operator を使用した NUMA 対応スケジューリングは、OpenShift Container Platform 4.10 でテクノロジープレビューとして以前に導入され、OpenShift Container Platform 4.13 で一般的に利用可能になりました。

NUMA Resources Operator は、クラスター内で使用可能な NUMA ゾーンの全体像に基づいて、ワークロードのスケジューリングを決定する NUMA 対応のセカンダリースケジューラーをデプロイします。この強化された NUMA 対応のスケジューリングにより、レイテンシーの影響を受けやすいワークロードが単一の NUMA ゾーンで処理され、効率とパフォーマンスが最大化されます。

この更新により、次の機能が追加されます。

- NUMA リソースレポートの API ポーリングの微調整。
- ノードトポロジーエクスポータのノードグループレベルでの設定オプション。

詳細は、Scheduling NUMA-aware workloads を参照してください。

1.3.19.2. 3 ノードクラスターと標準クラスターのワークロードパーティション設定のサポート (テクノロジープレビュー)

今回の更新まで、ワークロードパーティション設定はシングルノードの OpenShift クラスターでのみサポートされていました。この更新により、3 ノードのコンパクトクラスターと標準クラスターのワークロードパーティション設定も可能になりました。ワークロードパーティション設定を使用して、OpenShift Container Platform サービス、クラスター管理ワークロード、およびインフラストラクチャー Pod を分離し、予約された CPU セットで実行できます。

詳細は、ワークロードのパーティション設定 を参照してください。

1.3.19.3. GitOps ZTP を使用した電源状態の設定

OpenShift Container Platform 4.12 では、重要なワークロードと重要でないワークロードの電源状態を設定する機能が導入されました。OpenShift Container Platform 4.13 では、GitOps ZTP を使用して電源状態を設定できます。

この機能の詳細は、PolicyGenTemplates CR を使用した電源状態の設定 を参照してください。

1.3.19.4. TALM および GitOps ZTP を使用したマネージドクラスター更新用のコンテナーイメージの事前キャッシュ

このリリースでは、GitOps ZTP で使用する 2 つの新しい Topology Aware Lifecycle Manager (TALM) 機能が追加されました。

- 新しいチェック機能では、クラスターを更新する前に、マネージドクラスターホスト上に十分な使用可能ディスク領域があることをが確認されます。コンテナーイメージの事前キャッシュ

中に、TALM はホストの使用可能ディスク容量と推定される OpenShift Container Platform イメージのサイズを比較し、ホスト上に十分なディスク容量があることを確認するようになりました。

- **ConfigMap** CR の新しい **excludePrecachePatterns** フィールドが使用可能になり、更新前に TALM がどの事前キャッシュイメージをクラスターホストにダウンロードするかを制御します。

詳細は コンテナーイメージの事前キャッシュフィルターの使用 を参照してください。

1.3.19.5. PTP およびベアメタルイベントの AMQP が HTTP トランスポートに (テクノロジープレビュー)

HTTP は、PTP およびベアメタルイベントインフラストラクチャーのデフォルトトランスポートになりました。AMQ Interconnect は 2024 年 6 月 30 日にライフサイクル終了 (EOL) となります。

詳細は、PTP 高速イベント通知フレームワークについて を参照してください。

1.3.19.6. PTP グランドマスタークロックとして Intel E810 Westport Channel NIC をサポート (テクノロジープレビュー)

PTP Operator を使用して、Intel E810 Westport Channel NIC を PTP グランドマスタークロックとして設定できるようになりました。PTP グランドマスタークロックは、システムクロックとネットワーク時刻の同期に **ts2phc** (タイムスタンプ 2 物理クロック) を使用します。

詳細は、linuxptp サービスをグランドマスタークロックに設定 を参照してください。

1.3.19.7. GitOps ZTP で crn をマネージドクラスターのデフォルトコンテナーランタイムに設定

GitOps ZTP **ztp-site-generate** コンテナーに、crun をデフォルトのコンテナーランタイムに設定する **ContainerRuntimeConfig** CR が追加されました。

GitOps ZTP を使用してインストールするクラスターのパフォーマンスを最適化するには、追加の Day 0 installation manifest CR と併せて、シングルノード OpenShift、3 ノード OpenShift、および標準クラスターのコントロールプレーンとワーカーノードに対して crun を有効にします。

詳細は、crun をデフォルトのコンテナーランタイムに設定 を参照してください。

1.3.19.8. ドキュメントの強化: etcd の概要を追加

OpenShift Container Platform ドキュメントで、etcd のメリットや仕組みを含めた概要を参照できるようになりました。etcd は、Kubernetes のプライマリーデータストアとして、OpenShift Container Platform でのクラスターの設定と管理に対する信頼性の高いアプローチを etcd Operator を介して提供します。詳細は、etcd の概要 を参照してください。

1.3.20. Insights Operator

OpenShift Container Platform 4.13 では、Insights Operator が以下の情報を収集するようになりました。

- **openshift_apps_deploymentconfigs_strategy_total** メトリクス。このメトリックは、デプロイメントの設定からデプロイメントストラテジー情報を収集します。

- マシンに障害が発生する理由を特定するための追加のマシンリソース定義。

- 認証 Operator のパフォーマンスが低下している場合に Insights に通知するためのデフォルトの **ingresscontroller.operator.openshift.io** リソース。

1.3.21. Hosted Control Plane (テクノロジープレビュー)

1.3.21.1. ドキュメントにホストされたコントロールプレーンのセクションを追加

OpenShift Container Platform のドキュメントに、ホストされたコントロールプレーン専用のセクションが追加されました。ここでは、ホストされたクラスターの設定と管理に関連する機能および情報が記載されています。詳細は、ホストされたコントロールプレーン を参照してください。

1.3.21.2. ホストされたコントロールプレーンの更新

OpenShift Container Platform のドキュメントに、ホストされたコントロールプレーンの更新に関する情報が追加されました。ホストされたコントロールプレーンの更新には、ホストされたクラスターとノードプールの更新が含まれます。詳細は、ホストされたコントロールプレーンの更新 を参照してください。

1.3.22. OpenShift Container Platform をシングルノードにインストールするための要件

4.13 は、**x86_64** および **arm64** CPU アーキテクチャーをサポートするようになりました。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.13 では、主に以下のような技術的な変更点が加えられています。

追加のクラウドプロバイダー向けのクラウドコントローラーマネージャー
Kubernetes コミュニティーは、クラウドコントローラーマネージャーを使用することを優先して、基になるクラウドプラットフォームとやり取りするための Kubernetes コントローラーマネージャーの使用を非推奨にすることを計画しています。その結果、新しいクラウドプラットフォームの Kubernetes コントローラーマネージャーサポートを追加する計画はありません。

OpenShift Container Platform のこのリリースで追加された Nutanix 実装は、クラウドコントローラーマネージャーを使用します。さらに、このリリースでは、VMware vSphere のクラウドコントローラーマネージャーを使用する一般提供が導入されました。

クラウドコントローラーマネージャーの詳細は、Kubernetes Cloud Controller Manager のドキュメント を参照してください。

クラウドコントローラーマネージャーおよびクラウドノードマネージャーのデプロイメントおよびライフサイクルを管理するには、Cluster Cloud Controller Manager Operator を使用します。

詳細は、**Platform Operators リファレンス** のCluster Cloud Controller Manager Operator を参照してください。

MCD による一時停止されたプール上の kubelet CA 証明書の同期
これまで、Machine Config Operator (MCO) は、マシン設定の通常更新の一環として、kubelet クライアント認証局 (CA) 証明書 (**/etc/kubernetes/kubelet-ca.crt**) を更新していました。OpenShift Container Platform 4.13 以降、**kubelet-ca.crt** はマシン設定の通常更新の一環として更新されなくなりました。この変更により、証明書が変更されるたびに、Machine Config Daemon (MCD) が自動的に **kubelet-ca.crt** を最新の状態に保ちます。

マシン設定プールが一時停止されている場合、MCD は新しくローテーションされた証明書を該当する

ノードにプッシュできるようになりました。以前のバージョンと同様に、証明書への変更を含むレンダリングされた新しいマシン設定がプールに対して生成されます。プールは、更新が必要であることを示します。この条件は、この製品の将来のリリースで削除される予定です。ただし、証明書は個別に更新されるため、これ以上更新がない場合はプールを一時停止したままにしても安全です。

ノードには常に最新の **kubelet-ca.crt** が必要であるため、**MachineConfigControllerPausedPoolKubeletCA** アラートが削除されました。

SSH キーの場所の変更

OpenShift Container Platform 4.13 では、RHEL 9.2 ベースの RHCOS が導入されています。これまで、SSH キーは RHCOS の **/home/core/.ssh/authorized_keys** にありました。この更新により、RHEL 9.2 ベースの RHCOS では SSH キーが **/home/core/.ssh/authorized_keys.d/ignition** に配置されます。

デフォルトの OpenSSH **/etc/ssh/sshd_config** サーバー設定ファイルをカスタマイズした場合は、この Red Hat ナレッジベースの記事 に従ってファイルを更新する必要があります。

Pod セキュリティーアドミッションの今後の限定的な適用

現在、Pod のセキュリティー違反は警告として表示され、監査ログに記録されますが、Pod が拒否されることはありません。

現在、OpenShift Container Platform の次のマイナーリリースでは、Pod のセキュリティーアドミッションに対するグローバルな制限付きの適用が計画されています。この制限付きの適用が有効になっている場合、Pod セキュリティー違反のある Pod は拒否されます。

この今後の変更に備えて、ワークロードが適用される Pod セキュリティーアドミッションプロファイルと一致していることを確認してください。グローバルまたはネームスペースレベルで定義された強制セキュリティー基準に従って設定されていないワークロードは拒否されます。**restricted-v2** SCC は、制限付き Kubernetes の定義に従ってワークロードを許可します。

Pod のセキュリティー違反が発生している場合は、次のリソースを参照してください。

- Pod のセキュリティー違反の原因となっているワークロードを見つける方法については、Pod のセキュリティー違反の特定 を参照してください。
- Pod セキュリティーアドミッションラベルの同期がいつ実行されるかについては、Pod セキュリティー標準とのセキュリティーコンテキスト制約の同期 を参照してください。Pod セキュリティーアドミッションラベルは、次のような特定の状況では同期されません。
  - ワークロードは、**openshift-** で始まるシステム作成の namespace で実行されています。
  - ワークロードは、Pod コントローラーなしで直接作成された Pod で実行されています。
- 必要に応じて、**pod-security.kubernetes.io/enforce** ラベルを設定して、namespace または Pod にカスタムアドミッションプロファイルを設定できます。

oc-mirror プラグインが OpenShift API エンドポイントからグラフデータコンテナーイメージを取得

oc-mirror OpenShift CLI (**oc**) プラグインは、GitHub からグラフデータリポジトリー全体をダウンロードするのではなく、OpenShift API エンドポイントからグラフデータ tarball をダウンロードするようになりました。このデータを外部ベンダーではなく Red Hat から取得することは、外部コンテンツに対して厳しいセキュリティーとコンプライアンスの制限があるユーザーに適しています。

oc-mirror プラグインがダウンロードするデータから、グラフデータリポジトリー内にあるが OpenShift Update Service には必要ないコンテンツが除外されるようになりました。コンテナーも UBI ではなく UBI Micro をベースイメージとして使用するため、コンテナーイメージは以前よりも大幅に小さくなります。

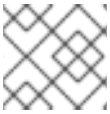
これらの変更は、oc-mirror プラグインのユーザーワークフローには影響しません。

グラフデータコンテナーイメージの Dockerfile を OpenShift API エンドポイントから取得
Dockerfile を使用して OpenShift Update Service のグラフデータコンテナーイメージを作成する場合は、グラフデータの tarball が GitHub ではなく OpenShift API エンドポイントからダウンロードされることに注意してください。

詳細は、OpenShift Update Service グラフデータコンテナーイメージの作成 を参照してください。

vSphere の user-provisioned infrastructure で nodeip-configuration サービスが有効
OpenShift Container Platform 4.13 では、**nodeip-configuration** サービスが vSphere の user-provisioned infrastructure で有効になりました。このサービスは、ノードの起動時に OpenShift Container Platform が Kubernetes API サーバーとの通信に使用するネットワークインターフェイスコントローラー (NIC) を決定します。まれに、アップグレード後にサービスが間違ったノード IP を選択することがあります。このような場合は、**NODEIP_HINT** 機能を使用して元のノード IP を復元できます。ネットワーク問題のトラブルシューティング を参照してください。

Operator SDK 1.28
OpenShift Container Platform 4.13 は Operator SDK 1.28 をサポートします。この最新バージョンのインストール、または最新バージョンへの更新については、Operator SDK CLI のインストール を参照してください。



注記

Operator SDK 1.28 は Kubernetes 1.26 をサポートします。

以前に Operator SDK 1.25 で作成または管理されている Operator プロジェクトがある場合は、Operator SDK 1.28 との互換性を維持するためにプロジェクトを更新してください。

- Go ベースの Operator プロジェクトの更新
- Ansible ベースの Operator プロジェクトの更新
- Helm ベースの Operator プロジェクトの更新
- Hybrid Helm ベースの Operator プロジェクトの更新
- Java ベースの Operator プロジェクトの更新

RHEL 9.2 ベースの RHCOS におけるディスク順序付け動作の変更
OpenShift Container Platform 4.13 では、RHEL 9.2 ベースの RHCOS が導入されています。今回の更新により、シンボリックディスク名が再起動後に変更される可能性があります。その結果、インストール後に設定ファイルを適用する場合、またはサービス作成時に **/dev/sda** などのシンボリック名を使用するディスクを参照するノードをプロビジョニングする場合に、問題が発生する可能性があります。この問題の影響は、設定しているコンポーネントにより異なります。ディスク参照を含め、デバイスには **dev/disk/by-id** など特定の命名スキームを使用することが推奨されます。

この変更により、モニタリングで各ノードのインストールデバイスに関する情報が収集される場合、既存の自動化ワークフローの調整が必要になる可能性があります。

詳細は、RHEL ドキュメント を参照してください。

ホストされたコントロールプレーンのバックアップ、復元、障害復旧に関するドキュメントの移動
OpenShift Container Platform 4.13 のドキュメントでは、ホストされたクラスター上で etcd をバックアップおよび復元する手順と、AWS リージョン内のホストされたクラスターを復元する手順が、

「バックアップと復元」セクションから「ホストされたコントロールプレーン'セクションに移動されました。内容に変更はありません。

1.5. 非推奨および削除された機能

以前のリリースで利用可能であった一部の機能が非推奨になるか、削除されました。

非推奨の機能は依然として OpenShift Container Platform に含まれており、引き続きサポートされますが、本製品の今後のリリースで削除されるため、新規デプロイメントでの使用は推奨されません。OpenShift Container Platform 4.13 で非推奨となり、削除された主な機能の最新のリストについては、以下の表を参照してください。非推奨となり、削除された機能の詳細は、表の後に記載されています。

次の表では、機能は次のステータスでマークされています。

- **一般公開 (GA)**
- **非推奨**
- **廃止**

Operator の非推奨および削除された機能

表1.6 オペレーターは廃止され、トラッカーが削除されました

機能	4.11	4.12	4.13
Operator カタログの SQLite データベース形式	非推奨	非推奨	非推奨

イメージの非推奨および削除された機能

表1.7 イメージは廃止され、トラッカーが削除されました

機能	4.11	4.12	4.13
Cluster Samples Operator の **ImageChangesInProgress** 状態	非推奨	非推奨	非推奨
Cluster Samples Operator の **MigrationInProgress** 状態	非推奨	非推奨	非推奨

インストールの非推奨および削除された機能

表1.8 インストールが非推奨になり、トラッカーが削除されました

機能	4.11	4.12	4.13
vSphere 7.0 Update 1 以前	非推奨	非推奨	削除 [1]
VMware ESXi 7.0 Update 1 以前	非推奨	非推奨	削除 [1]
cluster.local ドメインの CoreDNS ワイルドカードクエリー	一般公開 (GA)	非推奨	削除済み

機能	4.11	4.12	4.13
installer-provisioned infrastructure クラスターにおける **install-config.yaml** ファイル内の **ingressVIP** および **apiVIP** 設定	一般公開 (GA)	非推奨	非推奨

1. OpenShift Container Platform 4.13 の場合、使用するコンポーネントの要件を満たす VMware vSphere バージョン 7.0 Update 2 以降 (VMware vSphere バージョン 8.0 を含む) のインスタンスに OpenShift Container Platform クラスターをインストールする必要があります。

非推奨化および削除されたアプリケーションビルド機能

表1.9 非推奨化および削除された Service Binding Operato のトラッカー

機能	4.11	4.12	4.13
Service Binding Operator	一般公開 (GA)	一般公開 (GA)	非推奨

ストレージの非推奨および削除された機能

表1.10 Storage の廃止と削除されたトラッカー

機能	4.11	4.12	4.13
FlexVolume を使用した永続ストレージ	非推奨	非推奨	非推奨

特殊なハードウェアとドライバーの有効化の非推奨および削除された機能

表1.11 特殊なハードウェアとドライバーの有効化が非推奨になり、トラッカーが削除されました

機能	4.11	4.12	4.13
Special Resource Operator(SRO)	テクノロジープレビュー	廃止	廃止

マルチアーキテクチャーの非推奨および削除された機能

表1.12 マルチアーキテクチャーの非推奨および削除されたトラッカー

機能	4.11	4.12	4.13
IBM Power8 の全モデル (**ppc64le**)	一般公開 (GA)	非推奨	廃止

機能	4.11	4.12	4.13
IBM Power AC922 (**ppc64le**)	一般公開 (GA)	非推奨	廃止
IBM Power IC922 (**ppc64le**)	一般公開 (GA)	非推奨	廃止
IBM Power LC922 (**ppc64le**)	一般公開 (GA)	非推奨	廃止
IBM z13 全モデル (**s390x**)	一般公開 (GA)	非推奨	廃止
IBM® LinuxONE Emperor (**s390x**)	一般公開 (GA)	非推奨	廃止
IBM® LinuxONE Rockhopper (**s390x**)	一般公開 (GA)	非推奨	廃止
AMD64 (x86_64) v1 CPU	一般公開 (GA)	非推奨	廃止

ネットワーキングの非推奨機能と削除された機能

表1.13 ネットワーキングの非推奨化と削除のトラッカー

機能	4.11	4.12	4.13
RHOSP 上の Kuryr	一般公開 (GA)	非推奨	非推奨

Web コンソールの非推奨および削除された機能

表1.14 Web コンソールの非推奨および削除されたトラッカー

機能	4.11	4.12	4.13
マルチクラスターコンソール	テクノロジープレビュー	テクノロジープレビュー	廃止

ノードの非推奨および削除された機能

表1.15 ノードは廃止され、トラッカーが削除されました

機能	4.11	4.12	4.13
ImageContentSourcePolicy (ICSP) オブジェクト	一般公開 (GA)	一般公開 (GA)	非推奨
Kubernetes トポロジーラベル **failure-domain.beta.kubernetes.io/zone**	一般公開 (GA)	一般公開 (GA)	非推奨
Kubernetes トポロジーラベル **Failure-domain.beta.kubernetes.io/region**	一般公開 (GA)	一般公開 (GA)	非推奨

1.5.1. 非推奨の機能

1.5.1.1. Red Hat Virtualization (RHV)の非推奨

OpenShift Container Platform のホストプラットフォームとしての Red Hat Virtualization (RHV) が非推奨に

1.5.1.2. cluster.local ドメインのワイルドカード DNS クエリーを非推奨化

CoreDNS は、**cluster.local** ドメインの下の名前に対するワイルドカード DNS クエリーのサポートを停止します。これらのクエリーは、以前のバージョンと同様に OpenShift Container Platform 4.13 で解決されますが、サポートは将来の OpenShift Container Platform リリースから削除される予定です。

1.5.1.3. RHOSP 上で実行されるクラスターの Kuryr サポート

OpenShift Container Platform 4.12 では、RHOSP 上で実行されるクラスターにおける Kuryr のサポートは非推奨となりました。サポートは、OpenShift Container Platform 4.14 以降に削除されます。

1.5.1.4. ImageContentSourcePolicy オブジェクト

ImageContentSourcePolicy (ICSP) オブジェクトは非推奨になりました。**ImageDigestMirrorSet** (IDMS) オブジェクトを使用してダイジェスト仕様を使用してイメージをプルするか、**ImageTagMirrorSet** (ITMS) オブジェクトを使用してイメージタグを使用してイメージをプルできるようになりました。

これらの新しいオブジェクトの詳細は、Configuring image registry repository mirroring を参照してください。

既存の ICSP YAML ファイルを IDMS YAML ファイルに変換する方法の詳細は、Converting ImageContentSourcePolicy (ICSP) files for image registry repository mirroring 参照してください。

1.5.1.5. Service Binding Operator

Service Binding Operator は非推奨となり、OpenShift Container Platform 4.16 リリースで削除されます。Red Hat は、現行リリースのライフサイクル中はこのコンポーネントの重大なバグ修正とサポートを提供しますが、今後このコンポーネントに対する機能強化は行われません。

1.5.1.6. Toolbox は RHCOS で廃止されました

toolbox スクリプトは非推奨となり、そのサポートは将来の OpenShift Container Platform リリースで削除される予定です。

1.5.1.7. RHEL 9 ドライバーの非推奨化

OpenShift Container Platform 4.13 では、RHEL 9.2 ベースの RHCOS が導入されています。一部のカーネルデバイスドライバーは RHEL 9 で非推奨になりました。詳細は RHEL のドキュメント を参照してください。

1.5.1.8. VMware vSphere 設定パラメーター

OpenShift Container Platform 4.13 では、次の vSphere 設定パラメーターが非推奨になりました。これらのパラメーターは引き続き使用できますが、インストールプログラムはこれらのパラメーターを **install-config.yaml** ファイルに自動的に指定しません。

- **platform.vsphere.vCenter**
- **platform.vsphere.username**
- **platform.vsphere.password**
- **platform.vsphere.datacenter**
- **platform.vsphere.defaultDatastore**
- **platform.vsphere.cluster**
- **platform.vsphere.folder**
- **platform.vsphere.resourcePool**
- **platform.vsphere.apiVIP**
- **platform.vsphere.ingressVIP**
- **platform.vsphere.network**

詳細は、非推奨になった VMware vSphere 設定パラメーター を参照してください。

1.5.1.9. Kubernetes トポロジーラベル

一般的に使用される 2 つの Kubernetes トポロジーラベルが置き換えられます。**Failure-domain.beta.kubernetes.io/zone** ラベルは、**topology.kubernetes.io/zone** に置き換えられます。**Failure-domain.beta.kubernetes.io/region** ラベルは、**topology.kubernetes.io/region** に置き換えられます。置き換え後のラベルは、Kubernetes 1.17 以降および OpenShift Container Platform バージョン 4.4 以降で利用可能です。

現在、非推奨ラベルと置き換え後のラベルの両方がサポートされていますが、非推奨ラベルのサポートは将来のリリースで削除される予定です。削除に備えて、非推奨ラベルを参照するリソース (ボリューム、デプロイメント、その他のワークロードなど) を、置き換え後のラベルを使用するように変更できます。

1.5.2. 削除された機能

1.5.2.1. Kubernetes 1.26 から削除されたベータ版 API

Kubernetes 1.26 では、次の非推奨 API が削除されたため、マニフェストと API クライアントを移行して、適切な API バージョンを使用する必要があります。削除された API の移行について、詳細は Kubernetes documentation を参照してください。

表1.16 Kubernetes 1.26 から削除された API

リソース	削除された API	移行先
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta1**	**flowcontrol.apiserver.k8s.io/v1beta3**
HorizontalPodAutoscaler	**autoscaling/v2beta2**	**autoscaling/v2**
PriorityLevelConfiguration	**flowcontrol.apiserver.k8s.io/v1beta1**	**flowcontrol.apiserver.k8s.io/v1beta3**

1.5.3. 今後の Kubernetes API の削除

OpenShift Container Platform の次のマイナーリリースでは、Kubernetes 1.27 を使用する予定です。現在、Kubernetes 1.27 では非推奨 API の削除が予定されています。

削除予定の Kubernetes API リストについては、アップストリームの Kubernetes ドキュメントで Deprecated API Migration Guide を参照してください。

削除予定である Kubernetes API のクラスターを確認する方法は、Navigating Kubernetes API deprecations and removals を参照してください。

1.5.3.1. ppc64le、s390x、x86_64 v1 CPU アーキテクチャー上の特定のハードウェアモデルを削除

OpenShift Container Platform 4.13 では、以下の非推奨ハードウェアモデルにおける RHCOS 機能のサポートが削除されました。

- IBM Power8 の全モデル (**ppc64le**)
- IBM Power AC922 (**ppc64le**)
- IBM Power IC922 (**ppc64le**)
- IBM Power LC922 (**ppc64le**)
- IBM z13 全モデル (**s390x**)
- IBM® LinuxONE Emperor (**s390x**)
- IBM® LinuxONE Rockhopper (**s390x**)
- AMD64 (**x86_64**) v1 CPU

1.6. バグ修正

ベアメタルハードウェアのプロビジョニング

- これまで、Integrated Lights-Out (iLO) 管理インターフェイスドライバーで設定されたサー

バーに OpenShift Container Platform クラスターノードをデプロイしようとすると、そのノードのプロビジョニングに失敗していました。この失敗は、iLO ドライブに **ilo/use_web_server_for_images** 設定パラメーターがないため、ドライバーがオブジェクトストレージをデフォルトのストレージメカニズムとして使用を試みることで発生していました。この製品にオブジェクトストレージは存在しません。今回の更新により、OpenShift Container Platform 4.13 以降のバージョンでは iLO ドライバーの設定に **ilo/use_web_server_for_images** が追加され、ドライバーは **metal3** Pod で実行される Web サーバーを使用するようになります。(OCPBUGS-5068)

クラウドコンピュート

- Google Cloud Platform クラスターの一部の設定では、内部ロードバランサーは、インストールプログラムによって作成されたインスタンスグループを使用します。以前は、コントロールプレーンマシンを手動で交換すると、新しいコントロールプレーンノードがコントロールプレーンインスタンスグループに割り当てられませんでした。これにより、内部ロードバランサー経由でノードに到達できなくなりました。この問題を解決するには、管理者が Google Cloud コンソールを使用して、コントロールプレーンマシンを正しいインスタンスグループに手動で移動する必要がありました。
このリリースでは、交換用コントロールプレーンノードが正しいインスタンスグループに割り当てられます。(BZ#1970464、OCPCLOUD-1562)

- 以前は、Google Cloud Platform 用に設定されたコンピュートマシンが無効なマシンの調整を試みることができ、それが原因でフェーズが割り当てられないままスタックする可能性がありました。今回のリリースでは、無効な設定を持つマシンは **Failed** 状態になります。(OCPBUGS-4574)

- これまで、コントロールプレーンマシンセットのレプリカが準備完了とみなされるには、リンクされたノードも準備完了になる必要があるにもかかわらず、バッキングマシンが **Running** 状態になると準備完了とみなされていました。このリリースでは、ノードとそのマシンが **Ready** 状態にならなければ、コントロールプレーンマシンセットのレプリカは準備完了とみなされません。(OCPBUGS-8424)

- 以前は、Microsoft Azure クラスター上の高速ネットワーク機能でエラーが発生した場合、**mapi_instance_create_failed** アラートメトリックは開始されませんでした。このリリースでは、欠落していたアラートが追加され、Accelerated Networking が有効になっているクラスターが必要に応じてアラートを生成できるようになりました。(OCPBUGS-5235)

- 以前は、マシンが **Running** 状態になると、それ以降のノードの状態変化はチェックされませんでした。以前の解決策 (OCPBUGS-8424) では、ノードとそのマシンが **Ready** 状態でなければコントロールプレーンマシンセットのレプリカを準備完了とみなさない、という要件が導入されました。その結果、ノードとマシンの準備完了状態をコントロールプレーンマシンセットが逃した場合、レプリカは準備完了になりませんでした。この動作により、Control Plane Machine Set Operator が使用できなくなり、アップグレードがブロックされました。今回のリリースでは、マシンが実行中でノードが準備完了状態ではない場合、準備完了になるまでノードが定期的にチェックされます。この修正により、Control Plane Machine Set Operator が使用できずにアップグレードがブロックされることはなくなりました。(OCPBUGS-10771)

- 以前は、マシンのヘルスチェックが **maxUnhealthy** しきい値を超えてアラートが生成されると、クラスターがマシンのヘルスチェックを正常に調整できるほど健全になってもメトリックはリセットされず、アラートが継続していました。このリリースでは、アラートをいつトリガーするか決定するロジックが改善され、クラスターが健全になるとアラートがクリアされるようになりました。(OCPBUGS-4725)

- 以前の解決策 (OCPBUGS-5546) では、マシン設定オブジェクト内の **MachineConfig.Name** の **clusterName** 割り当てを削除しました。その結果、パラメーターの値は空の文字列となり、IP アドレス名を作成するために **machineName** の値と結合されると、無効な値になっていまし

た。この無効な値が原因で、プロビジョニング中にマシンに障害が発生しました。このリリースでは、有効な IP アドレス名を作成するために、**clusterName** の値がインフラストラクチャーオブジェクトから取得されます。(OCPBUGS-7696)

- Kubernetes 1.26 リリースでは、ノードがルーティングトラフィックを受信しないようにするため、**NotReady** ステータスを持つ健全ではないノードをパブリックロードバランサーから削除するなどの変更が、ノードインフラストラクチャーに導入されました。これらの変更は、Microsoft Azure のクラスター内で実行されているノードに影響を与えました。その結果、ノードは **Ready** ステータスに復帰できず、アウトバウンド接続も確立できませんでした。この更新により、パブリックロードバランサーからノードを切り離さなくても、**NotReady** ステータスでマークされたノードが **kube-proxy** ヘルスプローブで検出されるようになりました。これは、ノードがこれらのフェーズを通してアウトバウンドインターネット接続を維持できることを意味します。(OCPBUGS-7359)

Cloud Credential Operator

- Amazon Simple Storage Service (Amazon S3) は、Amazon S3 バケット設定を更新しました。これにより、Amazon Web Services (AWS) リージョンで作成されたバケットでは、デフォルトで S3 Block Public Access が有効になり、アクセス制御制限 (ACL) が無効になります。この設定では、S3 バケットリソースの使用をプライベートに制限します。OpenShift Container Platform 4.13 では、パブリックでの S3 バケットリソースの使用を可能にするため、デフォルトの S3 バケット設定を考慮して CCO ユーティリティー (**ccoctl**) とインストールプログラムが更新されました。(OCPBUGS-11706、OCPBUGS-11661)

開発者コンソール

- これまで OpenShift Container Platform は、Knative Serving および Eventing に API バージョン **v1alpha1** を使用していましたが、バグのため API バージョン **v1beta1** はサポートされていませんでした。今回の修正により、OpenShift Container Platform は両方の API バージョンをサポートするようになりました。(OCPBUGS-5164)

- 以前は、OpenShift Container Platform コンソールでパイプラインを編集すると、**Pipeline builder** および **YAML view** 設定オプションで正しいデータがレンダリングされませんでした。この問題により、**Pipeline builder** でパイプラインを編集できませんでした。今回の更新により、データが正しく解析され、ビルダーを使用してパイプラインを編集できるようになりました。(OCPBUGS-5016)

- 以前は、トポロジーサイドバーに更新された情報が表示されませんでした。トポロジーサイドバーからリソースを直接更新した場合、サイドバーを再度開いて変更を確認する必要がありました。今回の修正により、更新されたリソースが正しく表示されるようになりました。トポロジーサイドバーで、最新の変更を直接確認できます。(OCPBUGS-4691)

- 以前は、OpenShift Container Platform の **Samples** ページでは、リストされているサンプルのタイプを区別できませんでした。今回の修正により、**Samples** ページに表示されるバッジでサンプルを識別できるようになります。(OCPBUGS-10679)

ドキュメント

以前は、OpenShift Container Platform ドキュメントには、「オンプレミスベアメタルノードを使用してクラスターを拡張する」というタイトルのサブセクションが含まれていました。 これは、正確で最新のドキュメントを維持するために削除されました。

etcd Cluster Operator

- 以前は、Control Plane Machine Set Operator は、クラスターのブートストラップが完了する前にコントロールプレーンマシンを再作成しようとしました。これにより、etcd クラスターのメンバーシップからブートストラップノードが削除され、etcd クォーラムが失われ、クラスター

がオフラインになりました。今回の更新により、Control Plane Machine Set Operator は、etcd Cluster Operator がブートストラップノードを削除した後にのみコントロールプレーンマシンを再作成するようになりました。(OCPBUGS-10960)

ホストされたコントロールプレーン

- 以前は、**HostedControlPlane** オブジェクトは、**HostedCluster** リソースによって設定されたスケジューラープロファイルへの変更を識別しませんでした。さらに、**HostedControlPlane** は変更をスケジューラーに伝達しなかったため、スケジューラーは最新のスケジューラープロファイルの変更を受け取るためにコントロールプレーン Pod を再起動しませんでした。今回の更新により、**HostedControlPlane** はスケジューラープロファイルの変更を認識し、スケジューラーを動的に再起動するようになりました。その結果、スケジューラーはプロファイルの変更を Pod に適用できるようになりました。(OCPBUGS-7091)

- これまで、ホストされたクラスターは OpenID Connect (OIDC) プロバイダー (**oidc**) が使用できないことを考慮せず、そのために **machine** および **machineset** オブジェクトの削除が古くなっていました。今回の更新により、ホストされたクラスターは使用できない **odic** プロバイダーのステータスを検出できるようになりました。そのため、**odic** プロバイダーが使用できないことが原因で、**machine** および **machineset** オブジェクトの削除が古くならなくなりました。(OCPBUGS-10227)

- 以前は、Amazon Web Services (AWS) コンピュートマシンセットの **spec.metadata.annotations** パラメーター値は、コンピューティングマシンからそのノードにコピーされませんでした。そのため、ノードにはコンピュートマシンセットで指定されたアノテーションが欠落していました。このリリースでは、アノテーションがノードに正しく適用されます。(OCPBUGS-4566)

Installer

- 以前は、プライベートクラスターをアンインストールするときに、インストールプログラムが作成した DNS レコードは削除されませんでした。この更新により、インストールプログラムはこれらの DNS レコードを正しく削除するようになりました。(OCPBUGS-7973)

- 以前は、ベアメタル installer-provisioned infrastructure は、ポート 80 を使用して Baseboard Management Controller (BMC) およびデプロイメントエージェントにイメージを提供していました。ポート 80 はインターネット通信用として一般的に選択されるため、セキュリティーリスクが存在する可能性があります。ベアメタル installer-provisioned infrastructure は、ポート 6180 を使用して、デプロイされたクラスター上の **metal3** Pod によって使用されるイメージを提供するようになりました。(OCPBUGS-8511)

- 以前は、踏み台ホストがクラスターノードと同じ VPC ネットワークで実行されている場合、ブートストラップノードとクラスターノードへの SSH アクセスが失敗していました。また、この設定が原因で、一時ブートストラップノードからクラスターノードへの SSH アクセスが失敗していました。これらの問題は、一時ブートストラップノードとクラスターノード間の SSH トラフィックと、同じ VPC ネットワーク上の踏み台ホストからクラスターノードへの SSH トラフィックをサポートするように IBM Cloud セキュリティーグループルールを更新することで修正されました。installer-provisioned infrastructure での障害発生中に、分析用のログとデバッグ情報を正確に収集できるようになりました。(OCPBUGS-8035)

- 以前は、**role** パラメーターが **worker** に設定されているホストの IP アドレスにランデブー IP を設定し、ISO イメージを生成した場合、エージェントベースのインストーラーはクラスターのインストールに失敗していました。この設定に基づいて ISO イメージを生成しようとすると、検証失敗のメッセージが表示されるようになりました。このメッセージを受信したら、**master** ロールを持つホストの IP を使用するように、**agent-config.yaml** ファイルの **rendezvousIP** フィールドを更新する必要があります。(OCPBUGS-2088)

- 以前は、インストールプログラムは、**aws-sdk-go** ライブラリーで定義された新しいリージョ

ン (**ap-south-2**、**ap-southeast-4**、**eu-central-2**、**eu-south-2**、および **me-central-1**) を受け入れませんでした。インストールプログラムを使用してインストール設定ファイルを作成した場合、インストールプログラムはこれらの新しいリージョンをリストしたり、これらのリージョンに対する手動エントリーを受け入れたりしませんでした。今回の更新により、インストールプログラムはこれらのリージョンをサポートし、インストール設定ファイルを作成するときにそれらを指定できるようになりました。(OCPBUGS-10213)

- 以前は、**install-config.yaml** ファイルの **controlPlane.platform.openstack.failureDomain** フィールドに基づいて **Machine.PrimaryNetwork** を設定するコードベースに問題がありました。この問題は、Kuryr で実行される OpenShift Container Platform が、相互間の通信にコントロールプレーンマシンを使用する Red Hat OpenStack Platform (RHOSP) サブネット上のポートを識別する際に影響します。今回の更新により、**failureDomain** Technology Preview コンポーネントで **portTarget** の **control-plane** を設定すると、インストールプログラムによって **Machine.PrimaryNetwork** フィールドにポートの情報が設定され、OpenShift Container Platform クラスターが Kuryr で正常に実行されるようになります。(OCPBUGS-10658)

- 以前は、AWS リソースのタグを解除できないため、**us-gov-west-1** リージョンにデプロイされた AWS クラスターのアンインストールが失敗していました。その結果、プロセスが無限ループに陥り、インストールプログラムがリソースのタグを解除しようとしていました。今回の更新により、再試行が阻止されます。これにより、クラスターのアンインストールは成功します。(BZ#2070744)

- 以前は、Google Cloud Platform (GCP) 上で実行されているプライベート OpenShift Container Platform クラスターは追加のファイアウォールルールを受信して、GCP が内部および外部のロードバランサーに対してヘルスチェックを実行できるようにしていました。プライベートクラスターは内部ロードバランサーのみを使用するため、外部ロードバランサーに対するヘルスチェックの実行は必要はありません。今回の更新により、GCP 上で実行されるプライベートクラスターは、外部ロードバランサーのヘルスチェックに起因する追加のファイアウォールルールを受信しなくなります。(BZ#2110982)

Kubernetes Scheduler

- 以前は、namespace フィルタリングをテストするために **LifeCycleUtilization** プロファイルを除外すると、次のエラーが Descheduler Operator ログに記録されました: **belowE0222 12:43:14.331258 1 target_config_reconciler.go:668] key failed with : only namespace exclusion supported with LowNodeUtilization**。その結果、descheduler クラスター Pod は起動しませんでした。今回の更新により、namespace の除外が **LifeCycleUtilization** プロファイルで機能するようになりました。(OCPBUGS-7876)

管理コンソール

- 以前は、**Create Pod** ボタンのレンダリング時にユーザー権限がチェックされず、必要な権限を持たないユーザーに対してボタンがレンダリングされていました。今回の更新により、**Create Pod** ボタンのレンダリング時にユーザー権限がチェックされ、必要な権限を持つユーザーに対してレンダリングされるようになりました。(BZ#2005232)

- 以前は、**Pod** リソースのアクションメニューに、不要な **PDB add**、**edit**、および **remove** アクションがありました。今回の更新により、アクションは削除されました。(BZ#2110565)

- 以前は、**Details** ページの **PodDisruptionBudget** フィールドに誤ったヘルプメッセージがありました。今回の更新により、より説明的なヘルプメッセージが表示されるようになりました。(BZ#2084452)

- 以前は、メトリクスが無効になっていてナビゲーションメニューに表示されない場合でも、コンソールのルートパスに移動すると、URL が **Overview** ページにリダイレクトされていました。今回の更新では、メトリクスが無効になっている場合、マストヘッドのロゴをクリックす

るか、コンソールのルートパスに移動すると、URL が **project list** ページにリダイレクトされます。(OCPBUGS-3033)

- 以前は、クラスタードロップダウンが常時表示されない位置に配置されていたため、どのクラスターが表示されているかが不明瞭でした。今回の更新により、クラスタードロップダウンがマストヘッドに追加されたため、クラスタードロップダウンが常に表示され、いつでも表示しているクラスターを確認できるようになりました。(OCPBUGS-7089)

- 以前は、クラスターバージョンのステータスが **Failing**、**UpdatingAndFailing**、**Updating** の場合はノードの進行状況バーが表示されるように設定されていたため、クラスターの更新時以外でもノードの進行状況バーが表示されていました。今回の更新により、クラスターバージョンのステータスが **UpdatingAndFailing** または **Updating** の場合にのみノードの進行状況バーが表示されるようになります。(OCPBUGS-6049)

- 以前は、ServiceAccount の **kubeconfig** ファイルをダウンロードすると、エラーが表示され、ServiceAccount トークンに到達できませんでした。このエラーは、自動的に生成されたシークレットが削除されたことが原因で発生していました。今回の更新により、**kubeconfig** のダウンロードアクションが削除され、エラーは発生しなくなります。(OCPBUGS-7308)

- 以前は、Pod のセキュリティー対策が原因でアノテーションが欠落しているため、**Node details** ページの **Terminal** タブにエラーが表示されていました。必要なアノテーションがないと、ノードデバッグ Pod を開始できません。今回の更新では OpenShift Container Platform にこれらのアノテーションが追加されるため、ノードデバッグ Pod の開始が可能になり、エラーなしで **Terminal** タブが読み込まれるようになります。(OCPBUGS-4252)

- 以前は、クラスター管理者が Operator をアンインストールするときに **oc delete csv** コマンドを発行しようとすると、Operator のサブスクリプションがスタック状態になっていました。サブスクリプションに競合が存在したため、管理者は Operator を再インストールできませんでした。今回の更新により、管理者がアンインストールされた Operator を再インストールしようとすると、詳細なエラーメッセージが表示されます。(OCPBUGS-3822)

- 以前は、1 つ以上の既存プラグインが失敗した場合、Web コンソールにはコンソールの更新を促すトースト通知が表示されませんでした。このアクションは、Operator がプラグインをコンソールに追加した後にプラグインを表示するために必要です。今回の更新により、Operator がプラグインを追加すると Web コンソールがそれを確認し、以前に失敗したプラグインかにかかわらず、コンソールにトースト通知を表示します。(OCPBUGS-10249)

- 以前は、終了したコンテナーは、終了したコンテナーごとに **{{label}}** および **{{exitCode}}** コードをレンダリングしていました。今回の更新により、internationalization コードが修正され、読み取り可能な出力メッセージが表示されるようになりました。(OCPBUGS-4206)

- 以前は、リグレッションが導入され、**clusterversion status.availableUpdates** の値が **null** および **Upgradeable=False** の場合に **Cluster Settings** ページでエラーが返されていました。今回の更新により、**status.availableUpdates** の値を **null** 値に設定できるようになりました。(OCPBUGS-6053)

モニタリング

- 以前は、Kubernetes スケジューラーは、複数の再起動操作を受け取ったノードで特定の Pod のスケジューリングをスキップできました。OpenShift Container Platform 4.13 では、30 分以内にスケジューリングできない Pod に対する **KubePodNotScheduled** アラートを組み込むことで、この問題に対処しています。(OCPBUGS-2260)

- 以前は、Thanos Ruler に複数のラベルが定義されている場合、**prometheus-operator** がカスタムリソースを調整するたびに指定された順序でラベルを追加しないため、statefulset が再作成ループに入る可能性がありました。この修正後、**prometheus-operator** は statefulset に追加する前に追加ラベルを並べ替えるようになりました。(OCPBUGS-6055)

- このリリースでは、特定の読み取り専用 **tmpfs** インスタンスに対して **NodeFilesystemAlmostOutOfSpace** が起動されなくなりました。この変更により、設計上いっぱいになっている特定の **tmpfs** マウントポイントに対してアラートが起動される問題が修正されました。(OCPBUGS-6577)

ネットワーク

- これまで、Ingress Operator は、エラーメッセージが表示されるべきときに、**updateIngressClass** 関数ログの成功メッセージを表示していました。今回の更新により、Ingress Operator のログメッセージが正確になりました。(OCPBUGS-6700)

- これまで、Ingress Operator は **ingressClass.spec.parameters.scope** を指定せず、Ingress Class API オブジェクトはデフォルトで **cluster** タイプを指定していました。そのため、Operator の開始時にすべての Ingress クラスで不必要な更新が発生していました。今回の更新により、Ingress Operator は **ingressClass.spec.parameters.scope** で **Cluster** タイプを指定します。(OCPBUGS-6701)

- これまで、Ingress Operator の **ensureNodePortService** ログメッセージに間違ったサービス名が含まれており、誤った情報がログに記録されていました。今回の更新により、Ingress Operator は **ensureNodePortService** に正確なサービスを記録するようになりました。(OCPBUGS-6698)

- これまで、OpenShift Container Platform 4.7.0 および 4.6.20 では、Ingress Operator は OpenShift Container Platform に固有のルーター Pod のアノテーションを使用していました。これは、バグを修正するために liveness プローブの猶予期間を設定する一時的な措置でした。その結果、OpenShift Container Platform は修正を実装するためのパッチを適用する必要がありました。今回の更新により、Ingress Operator は **terminationGracePeriodSeconds** API フィールドを使用し、将来のリリースで以前のパッチを削除できるようになります。(OCPBUGS-4703)

- これまで、CoreDNS は古いツールチェーンを使用してメインバイナリーと古いベースイメージをビルドしていました。今回の更新により、OpenShift Container Platform は 4.13 を使用してツールチェーンとベースイメージをビルドします。(OCPBUGS-6228)

ノード

- これまで、**LifecycleAndUtilization** descheduler プロファイルで有効化される **LowNodeUtilization** ストラテジーは、namespace の除外をサポートしていませんでした。このリリースでは、**LifecycleAndUtilization** descheduler プロファイルが設定されている場合は namespace が適切に除外されます。(OCPBUGS-513)

- これまで、動作のリグレッションにより、Machine Config Operator (MCO) が **kubeletconfig** または **containerruntimeconfig** カスタムリソース (CR) 内に重複した **MachineConfig** オブジェクトを作成していました。重複するオブジェクトの機能が低下し、クラスターのアップグレードに失敗していました。今回の更新により、**kubeletconfig** および **containerruntimeconfig** コントローラーは重複オブジェクトを検出して削除できるようになりました。このアクションにより、機能低下した **MachineConfig** オブジェクトのエラーが削除され、クラスターのアップグレード操作は影響を受けません。(OCPBUGS-7719)

Node Tuning Operator (NTO)

- これまで、Cloud-native Functions (CNF) テストイメージが、CNF が有効になっている OpenShift Container Platform クラスター上でレイテンシーテストを実行するために 使用する **hwlatdetect** ツールには、10 秒の検出期間が設定されていました。この設定を 0.95 秒の検出幅設定と組み合わせると、ツールは割り当てられた検出期間の 9.5% の時間でノードを監視するため、**hwlatdetect** がレイテンシースパイクを見逃す可能性が高まります。今回の更新では検出

期間が 1 秒に設定され、ツールは割り当てられた検出期間の約 95% の時間でノードを監視できるようになりました。監視時間の残りの 5% は、カーネルがシステムタスクを実行できるように未割り当てのままになります。(OCPBUGS-12433)

OpenShift CLI (oc)

- これまで、**oc adm upgrade** コマンドは ClusterVersion の **Failing=True** ステータスを読み取りませんでした。今回の更新により、**oc adm upgrade** には、クラスター状態を要約するときに **Failing=True** 条件の情報が追加されます。これにより、**ClusterOperators** の **Degraded=True** ステータスや、現在のクラスターの動作や将来の更新に影響を与える可能性のある他の問題が可視化されます。(OCPBUGS-3714)

- これまで、**oc-mirror** コマンドは、ミラーリングされたディスクイメージから OCI および FBC Operator のカタログコンテンツをコンソールにビルドしていました。その結果、カタログのすべてのコンテンツがミラーリングされるのではなく、一部のコンテンツがカタログから欠落していました。今回の更新により、ミラーリングされたコンテンツを宛先レジストリーにプッシュする前に、それを反映するカタログイメージがビルドされ、より完全なカタログが作成されるようになります。(OCPBUGS-5805)

- これまで、oc-mirror OpenShift CLI (**oc**) プラグインは、Operator カタログをエントリーとして **ImageContentSourcePolicy** リソースに追加していました。Operator カタログは **CatalogSource** リソース内の宛先レジストリーから直接使用されるため、このリソースにこのエントリーは必要ありません。この問題により、**ImageContentSourcePolicy** リソース内の予期しないエントリーが原因となって、クラスターがリリースイメージ署名リソースを受信する際に影響が出ていました。今回の更新では、oc-mirror プラグインが **ImageContentSourcePolicy** リソースから Operator カタログエントリーを削除するため、クラスターは **CatalogSource** リソース内の Operator カタログから署名リソースを受け取ります。(OCPBUGS-10320)

Operator Lifecycle Manager (OLM)

- Operator のカスタムリソース (CR) のステータスには、Operator が所有するコンポーネントのリストが含まれます。このリストは **group/version/kind** (GVK) の順序で並べられていますが、同じ GVK を持つオブジェクトの順序は変更される可能性があります。Operator が同じ GVK を持つ多くのコンポーネントを所有している場合、コンポーネントの順序が変更されるため、Operator Lifecycle Manager (OLM) が Operator CR のステータスを継続的に更新する可能性があります。このバグ修正により OLM が更新され、Operator のコンポーネント参照順序が確定されるようになりました。その結果、コンポーネントのリストに変化がない場合、OLM は CR を繰り返し更新しようとしなくなりました。(OCPBUGS-2556)

- Operator Lifecycle Manager (OLM) は、Operator の検索とインストールに使用できる一連の **CatalogSource** オブジェクトを管理します。これらのカタログソースはこのアクションのデフォルトソースであり、Red Hat によって管理されます。しかし、OLM システムが認識しない方法で、デフォルトのカタログソースが変更される可能性がありました。デフォルトのカタログソースを操作不能になるような方法で変更すると、OLM 全体で連鎖的な問題が発生し、ユーザーがクラスターで新しい Operator をインストールしたり、既存の Operator をアップグレードしたりできなくなる可能性があります。このバグ修正により、デフォルトのカタログソースを管理する **catalog-operator** ランタイムが更新され、**CatalogSource** 仕様に対する他の変更が認識されるようになります。その結果、デフォルトのカタログソースに変更が加えられると、OLM はその変更を検出し、デフォルトにリセットします。(OCPBUGS-5466)

Red Hat Enterprise Linux CoreOS (RHCOS)

- これまで、Azure には SR-IOV インターフェイスを **NM_UNMANAGED** としてマークする udev ルールが **initramfs** ファイルになかったため、NetworkManager が起動時に SR-IOV インターフェイスを設定していました。今回の更新により、udev ルールが **initramfs** ファイルに追加さ

れ、SR-IOV インターフェイスが NetworkManager によって管理されることはなくなりました。(OCPBUGS-7173)

Security Profiles Operator

- これまで、**net_container** などの別のテンプレートを選択した場合、Security Profiles Operator (SPO) SELinux ポリシーはコンテナーテンプレートから低レベルのポリシー定義を継承しませんでした。このポリシーは、コンテナーテンプレートにのみ存在する低レベルのポリシー定義を必要とするため、機能しません。この問題は、SPO SELinux ポリシーが SELinux ポリシーを SPO カスタム形式から 共通中間言語 (CIL) 形式に変換しようとすると発生しました。今回の更新により、SPO から CIL への変換を必要とする SELinux ポリシーにコンテナーテンプレートが追加されます。さらに、SPO SELinux ポリシーは、サポートされている任意のポリシーテンプレートから低レベルのポリシー定義を継承できるようになりました。(OCPBUGS-12879)

スケーラビリティーおよびパフォーマンス

- これまで、パフォーマンスプロファイルが生成されると、自動的に作成される CRI-O ランタイムファイルが CRI-O ランタイムとして **runc** を使用するように設定されていました。
現在は、パフォーマンスプロファイルの生成時にコンテナーランタイムとして **crun** を設定する機能の一般提供が開始され、作成されたランタイム CRI-O ファイルは **ContainerRuntimeConfig** CR で設定された **defaultRuntime** と一致します。これは **crun** または **runc** のいずれかになります。デフォルトは **runc** です。(OCPBUGS-11813)

ストレージ

- 以前は、**openshift-manila-csi-driver** namespace には、ワークロードのパーティション設定を管理するために必要なラベルが含まれていませんでした。これらのラベルは、選択した CPU セットでの Manila CSI Pod の実行を制限する操作に影響を与えていました。今回の更新により、**openshift-manila-csi-driver** namespace に **workload.openshift.io/allowed** ラベルが追加されました。(OCPBUGS-11341)

Windows コンテナー

- これまで、Windows ノードのアップグレードプロセス中に Microsoft Windows コンテナーのワークロードが完全には空になりませんでした。その結果、アップグレード中のノードにワークロードが残り、サービスが中断されていました。今回の更新により、Windows Machine Config Operator (WMCO) はワークロードをドレインし、ノードのアップグレードが完了するまでノードを遮断します。このアクションにより、Microsoft Windows インスタンスのシームレスなアップグレードが保証されます。(OCPBUGS-5732)

- これまで、Windows Machine Config Operator (WMCO) は **DaemonSet** ワークロードをドレインできませんでした。この問題により、WMCO が削除またはアップグレードしようとした Windows ノードが Windows`DaemonSet` Pod によってブロックされていました。今回の更新により、WMCO にはロールベースのアクセス制御 (RBAC) 権限が追加され、WMCO が **DaemonSet** ワークロードを削除できるようになりました。WMCO は、**containerd** shim で作成されたプロセスを削除することもできるため、WMCO がクラスターからノードを削除すると Windows インスタンス上に **DaemonSet** コンテナーは存在しなくなります。(OCPBUGS-5354)

- これまでは、リポジトリータグがビルドシステムに伝播されなかったため、**containerd** コンテナーランタイムは各 Windows ノードで誤ったバージョンを報告していました。この設定により、**containerd** は Go ビルドバージョンを各 Windows ノードのバージョンとして報告していました。今回の更新により、ビルド時に正しいバージョンがバイナリーに注入され、**containerd** が各 Windows ノードの正しいバージョンを報告するようになります。(OCPBUGS-5378)

1.7. テクノロジープレビューの機能

現在、今回のリリースに含まれる機能にはテクノロジープレビューのものがあります。これらの実験的機能は、実稼働環境での使用を目的としていません。これらの機能に関しては、Red Hat カスタマーポータルの以下のサポート範囲を参照してください。

テクノロジープレビュー機能のサポート範囲

次の表では、機能は次のステータスでマークされています。

- **テクノロジープレビュー**
- **一般公開 (GA)**
- **利用不可**
- **非推奨**

ネットワーキングテクノロジープレビュー機能

表1.17 ネットワーキングテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
境界クロックとして設定される PTP デュアル NIC ハードウェア	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)
Ingress Node Firewall Operator	利用不可	テクノロジープレビュー	テクノロジープレビュー
特定の IP アドレスプールを使用した、ノードのサブセットから MetalLB サービスの BGP モードを使用したアドバタイズ	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
特定の IP アドレスプールを使用した、ノードのサブセットから MetalLB サービスの L2 モードを使用したアドバタイズ	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
SR-IOV ネットワークのマルチネットワークポリシー	利用不可	テクノロジープレビュー	テクノロジープレビュー
セカンダリーネットワークとしての OVN-Kubernetes ネットワークプラグイン	利用不可	利用不可	テクノロジープレビュー
インターフェイス固有の安全な sysctls リストの更新	利用不可	テクノロジープレビュー	テクノロジープレビュー
MT2892 Family [ConnectX-6 Dx] SR-IOV 対応	利用不可	テクノロジープレビュー	一般公開 (GA)

機能	4.11	4.12	4.13
MT2894 Family [ConnectX-6 Lx] SR-IOV 対応	利用不可	テクノロジープレビュー	一般公開 (GA)
MT42822 BlueField-2 in ConnectX-6 NIC mode SR-IOV 対応	利用不可	テクノロジープレビュー	一般公開 (GA)
Silicom STS Family SR-IOV 対応	利用不可	テクノロジープレビュー	一般公開 (GA)
MT2892 Family [ConnectX-6 Dx] OvS Hardware Offload 対応	利用不可	テクノロジープレビュー	一般公開 (GA)
MT2894 Family [ConnectX-6 Lx] OvS Hardware Offload 対応	利用不可	テクノロジープレビュー	一般公開 (GA)
MT42822 BlueField-2 in ConnectX-6 NIC mode OvS Hardware Offload 対応	利用不可	テクノロジープレビュー	一般公開 (GA)
Bluefield-2 の DPU から NIC への切り替え	利用不可	テクノロジープレビュー	一般公開 (GA)
Intel E810-XXVDA4T	利用不可	利用不可	一般公開 (GA)

ストレージテクノロジープレビュー機能

表1.18 ストレージテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
OpenShift ビルドでの共有リソース CSI ドライバーおよびビルド CSI ボリューム	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
CSI ボリューム拡張	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)

機能	4.11	4.12	4.13
CSI Azure File Driver Operator	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
CSI Google Filestore Driver Operator	利用不可	テクノロジープレビュー	テクノロジープレビュー
CSI 自動移行 (Azure ファイル、VMware vSphere)	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)
CSI 自動移行 (Azure Disk、OpenStack Cinder)	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
CSI 自動移行 (AWS EBS、GCP ディスク)	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
CSI インラインの一時ボリューム	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)
CSI 汎用一時ボリューム	利用不可	一般公開 (GA)	一般公開 (GA)
IBM Power Virtual Server Block CSI Driver Operator	利用不可	利用不可	テクノロジープレビュー
Local Storage Operator を使用した自動デバイス検出およびプロビジョニング	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Azure File CSI Operator ドライバーの NFS サポート	利用不可	一般提供	一般提供

インストールテクノロジープレビュー機能

表1.19 インストールテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
kvc を使用したノードへのカーネルモジュールの追加	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

機能	4.11	4.12	4.13
IBM Cloud VPC クラスター (x86_64)	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
選択可能なクラスターインベントリー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
マルチアーキテクチャーコンピュートマシン	利用不可	テクノロジープレビュー	一般公開 (GA)
RHEL の BuildConfigs で共有資格をマウントする	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
エージェントベースの OpenShift Container Platform インストーラー	利用不可	一般公開 (GA)	一般公開 (GA)
AWS Outposts プラットフォーム	利用不可	テクノロジープレビュー	テクノロジープレビュー
SR-IOV デバイスの NIC パーティション設定の有効化	利用不可	利用不可	テクノロジープレビュー
Azure Tagging	利用不可	利用不可	テクノロジープレビュー
GCP Confidential 仮想マシン	利用不可	利用不可	テクノロジープレビュー
installer-provisioned infrastructure を使用した Alibaba Cloud へのクラスターのインストール	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

ノードテクノロジープレビュー機能

表1.20 ノードテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
プリエンプションを実行しない優先順位クラス	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)

機能	4.11	4.12	4.13
Linux コントロールグループバージョン 2 (cgroup v2)	開発者プレビュー	テクノロジープレビュー	一般公開 (GA)
コンテナーランタイムをクロン	利用不可	テクノロジープレビュー	一般公開 (GA)
Cron ジョブのタイムゾーン	利用不可	テクノロジープレビュー	テクノロジープレビュー

マルチアーキテクチャーテクノロジーのプレビュー機能

表1.21 マルチアーキテクチャーテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
arm64 アーキテクチャーでの **kdump**	利用不可	テクノロジープレビュー	テクノロジープレビュー
s390x アーキテクチャーでの **kdump**	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
ppc64le アーキテクチャーでの **kdump**	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
IBM Z および IBM® LinuxONE での IBM Secure Execution	利用不可	テクノロジープレビュー	一般公開 (GA)
installer-provisioned infrastructure を使用する IBM Power Virtual Server	利用不可	利用不可	テクノロジープレビュー

特殊なハードウェアとドライバーの有効化テクノロジープレビュー機能

表1.22 専用のハードウェアとドライバーの有効化テクノロジープレビュートラッカー

機能	4.11	4.12	4.13

機能	4.11	4.12	4.13
ドライバーツールキット	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)
Special Resource Operator(SRO)	テクノロジープレビュー	テクノロジープレビュー	利用不可
ハブアンドスポーククラスターのサポート	利用不可	利用不可	テクノロジープレビュー

Web コンソールのテクノロジープレビュー機能

表1.23 Web コンソールテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
動的プラグイン	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)

スケーラビリティとパフォーマンステクノロジープレビュー機能

表1.24 スケーラビリティとパフォーマンステクノロジープレビュートラッカー

機能	4.11	4.12	4.13
ハイパースレッディング対応の CPU マネージャーポリシー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Node Observability Operator	利用不可	テクノロジープレビュー	テクノロジープレビュー
factory-precaching-cli ツール	利用不可	利用不可	テクノロジープレビュー
ワーカーノードを使用した単一ノードの OpenShift クラスターの拡張	利用不可	テクノロジープレビュー	一般公開 (GA)
Topology Aware Lifecycle Manager (TALM)	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)

機能	4.11	4.12	4.13
マウント namespace のカプセル化	利用不可	利用不可	テクノロジープレビュー
NUMA Resources Operator による NUMA 対応のスケジューリング	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)
PTP およびベアメタルイベントの AMQP を HTTP トランスポートに置き換え	利用不可	利用不可	テクノロジープレビュー
PTP グランドマスタークロックとしての Intel E810 Westport Channel NIC	利用不可	利用不可	テクノロジープレビュー
3 ノードクラスターと標準クラスターのワークロードパーティションの設定	利用不可	利用不可	テクノロジープレビュー

Operator テクノロジープレビュー機能

表1.25 オペレーターテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
ハイブリッド Helm Operator	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Java ベースの Operator	利用不可	テクノロジープレビュー	テクノロジープレビュー
Node Observability Operator	利用不可	利用不可	テクノロジープレビュー
ネットワーク可観測性オペレーター	利用不可	一般公開 (GA)	一般公開 (GA)
プラットフォーム Operator	利用不可	テクノロジープレビュー	テクノロジープレビュー

機能	4.11	4.12	4.13
RukPak	利用不可	利用不可	テクノロジープレビュー
Cert-manager Operator	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)

モニタリングテクノロジープレビュー機能

表1.26 モニタリングテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
ユーザー定義プロジェクトのモニタリングのアラートルーティング	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
プラットフォームモニタリングメトリクスに基づいたアラートルール	利用不可	テクノロジープレビュー	テクノロジープレビュー
メトリクス収集プロファイル	利用不可	利用不可	テクノロジープレビュー

Red Hat OpenStack Platform (RHOSP) テクノロジープレビュー機能

表1.27 RHOSP テクノロジープレビュートラッカー

機能	4.11	4.12	4.13
RHOSP DCN のサポート	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
RHOSP 上のクラスターの外部クラウドプロバイダーのサポート	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)

アーキテクチャーテクノロジープレビューの機能

表1.28 アーキテクチャーテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
ベアメタル上の OpenShift Container Platform のホスト型コントロールプレーン	利用不可	テクノロジープレビュー	テクノロジープレビュー
Amazon Web Services (AWS) 上の OpenShift Container Platform のホスト型コントロールプレーン	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
OpenShift Virtualization 上の OpenShift Container Platform のホスト型コントロールプレーン	利用不可	利用不可	テクノロジープレビュー

マシン管理テクノロジープレビュー機能

表1.29 マシン管理テクノロジープレビュートラッカー

機能	4.11	4.12	4.13
Cluster API によるマシンの管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Alibaba Cloud のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Amazon Web Services のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Google Cloud Platform のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
IBM Cloud 向けクラウドコントローラーマネージャー	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
IBM Cloud Power VS 用クラウドコントローラーマネージャー	利用不可	利用不可	テクノロジープレビュー
Microsoft Azure のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

機能	4.11	4.12	4.13
Nutanix のクラウドコントローラーマネージャー	利用不可	利用不可	一般公開 (GA)
Red Hat OpenStack Platform (RHOSP) のクラウドコントローラーマネージャー	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
VMware vSphere のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)

認証と認可のテクノロジープレビュー機能

表1.30 認証と認可のテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
Pod セキュリティーアドミッションの制限付き適用	利用不可	テクノロジープレビュー	テクノロジープレビュー

Machine Config Operator のテクノロジープレビュー機能

表1.31 Machine Config Operator のテクノロジープレビュートラッカー

機能	4.11	4.12	4.13
Red Hat Enterprise Linux CoreOS (RHCOS) イメージの階層化	利用不可	テクノロジープレビュー	一般公開 (GA)

1.8. 既知の問題

- OpenShift Container Platform 4.1 では、匿名ユーザーは検出エンドポイントにアクセスできました。後のリリースでは、一部の検出エンドポイントは集約された API サーバーに転送されるため、このアクセスを無効にして、セキュリティーの脆弱性の可能性を減らすことができます。ただし、既存のユースケースに支障がで出ないように、認証されていないアクセスはアップグレードされたクラスターで保持されます。
  OpenShift Container Platform 4.1 から 4.13 にアップグレードされたクラスターのクラスター管理者の場合、認証されていないアクセスを無効にするか、またはこれを引き続き許可することができます。認証なしのアクセスが必要な理由が特に無い限り、無効にしてください。認証されていないアクセスを引き続き許可する場合は、それに伴ってリスクが増大することに注意してください。

警告

認証されていないアクセスに依存するアプリケーションがある場合、認証されていないアクセスを取り消すと HTTP **403** エラーが生じる可能性があります。

以下のスクリプトを使用して、検出エンドポイントへの認証されていないアクセスを無効にします。

```
## 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
```

このスクリプトは、認証されていないサブジェクトを以下のクラスターロールバインディングから削除します。

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

(BZ#1821771)

- **oc annotate** コマンドは、等号 (**=**) が含まれる LDAP グループ名では機能しません。これは、コマンドがアノテーション名と値の間に等号を区切り文字として使用するためです。回避策として、**oc patch** または **oc edit** を使用してアノテーションを追加します。(BZ#1917280)

- Git リポジトリーを追加し、GitLab および Bitbucket **pipeline-as-code** リポジトリーで設定すると、無効なリポジトリーリソースが作成されます。その結果、GitLab プロバイダーと Bitbucket プロバイダーの **spec.git_provider.url** Git プロバイダー URL が削除されます。回避策として、Bitbucket に必須の **spec.git_provider.user** フィールドを追加します。さらに、**Git access token** または **Git access token secret**を選択して、Git リポジトリーの追加を続行します。(OCPBUGS-7036)

- 現在、VMware vSphere に OpenShift Container Platform クラスターをインストールする目的でインストールプログラムを macOS で実行する場合、**x509: certificate is not standards compliant** として出力される証明書コンプライアンスの問題が存在します。この問題は、コン

パイラーが新しくサポートされた macOS 証明書規格を認識しないという **golang** コンパイラーの既知の問題に関連しています。この問題に対する回避策はありません。(OSDOCS-5694)

- **ControlPlaneMachineSet** 定義に 3 つを超える障害ドメインを含めると、負荷分散アルゴリズムは既存のコントロールプレーンマシンを優先しません。既存の 3 つの障害ドメインよりもアルファベット順で優先順位が高い 4 番目の障害ドメインを定義に追加すると、4 番目の障害ドメインが既存の障害ドメインよりも優先されます。この動作により、ロールフォワード更新をコントロールプレーンマシンに適用できます。この問題は、使用中の既存障害ドメインの優先順位を、未使用の新規障害ドメインよりも高く設定することで回避できます。このアクションにより、定義に 3 つを超える障害ドメインを追加する過程で、各コントロールプレーンマシンが安定します。(OCPBUGS-11968)

- シングルノード OpenShift インスタンスでは、ノードをドレインして実行中のすべての Pod を削除せずに再起動すると、ワークロードコンテナーのリカバリーで問題が発生する可能性があります。再起動後、すべてのデバイスプラグインの準備が整う前にワークロードが再開され、その結果、リソースが利用できなくなったり、ワークロードが間違った NUMA ノードで実行されたりします。回避策としては、再起動リカバリーの手順中にすべてのデバイスプラグインが再登録された時点でワークロード Pod を再起動します。(OCPBUGS-2180)

- SR-IOV ネットデバイスを使用する Pod を削除するときにエラーが発生する場合があります。このエラーは、ネットワークインターフェイスの名前が変更されると、以前の名前が代替名リストに追加されるという RHEL 9 の変更によって発生します。その結果、SR-IOV 仮想機能 (VF) にアタッチされた Pod が削除されると、VF は元の名前 (例: **ensf0v2**) ではなく、予期しない新しい名前 (例: **dev69**) でプールに戻ります。これは致命的なエラーではありませんが、システムが自動修復する際に Multus および SR-IOV ログにエラーが表示される場合があります。このエラーにより、Pod の削除に追加で数秒かかる場合があります。(OCPBUGS-11281)

- インターフェイス固有の安全な sysct を更新するデーモンセットの YAML 定義における間違った優先クラス名と構文エラーが原因で、**openshift-multus** namespace の **cni-sysctl-allowlist** config map を使用してインターフェイスの安全な sysct リストを変更できません。
回避策: この問題に対処するには、手動で、またはデーモンセットを使用して、ノード上の **/etc/cni/tuning/allowlist.conf** ファイルを変更します。(OCPBUGS-11046)

- OpenShift Container Platform 4.12 で導入された UDP GRO を有効にする新機能を使用すると、すべての veth デバイスが利用可能な CPU ごとに 1 つの RX キューを持つことになります (以前は各 veth に 1 つのキューがありました)。これらのキューは Open Virtual Network によって動的に設定され、レイテンシーチューニングとこのキューの作成の間に同期はありません。レイテンシーチューニングロジックは、veth NIC 作成イベントをモニタリングし、すべてのキューが適切に作成される前に、RPS キュー CPU マスクの設定を開始します。これは、一部の RPS キューマスクが設定されないことを意味します。すべての NIC キューが適切に設定されるわけではないため、タイミングに敏感な CPU を使用して他のコンテナー内のサービスと通信するリアルタイムアプリケーションでは、レイテンシースパイクが発生する可能性があります。カーネルネットワークスタックを使用しないアプリケーションは影響を受けません。(OCPBUGS-4194)

- Cluster Network Operator (CNO) コントローラーが、必要以上に多くのリソースを監視します。その結果、リコンサイラーが過剰にトリガーされ、必要以上に高いレートで API 要求が発生します。毎秒約 1 件の config map アクセス要求が発生します。これにより、CNO と **kube-apiserver** の両方の負荷が増加します。(OCPBUGS-11565)

- OpenShift Container Platform 4.13 の場合、Driver Toolkit (DTK) コンテナーイメージには、ドライバーコンテナーをビルドするために、ソフトウェアスタックの第 2 レイヤーとして **ubi9** イメージが必要です。**ubi8** イメージをソフトウェアスタックの第 2 レイヤーとして使用しようとするとエラーが発生します。(OCPBUGS-11120)

- vSphere プラットフォーム上の一部の OpenShift Container Platform インストールで CSI ドライバーを使用する場合、vSphere CSI ドライバーの起動中に vCenter からノードに関する情報

を取得できず、ドライバーは再試行しないため、vSphere CSI ドライバーが正しく起動しないことがあります。
回避策: SSH を使用して vsphere-syncer プロセスの現在のリーダーであるノードに接続し、vsphere-syncer コンテナーを (crictl を使用して) 再起動すると、この問題が軽減されてドライバーが正常に起動します。(OCPBUGS-13385)

- OpenShift Container Platform 4.13 の場合、OpenShift 4.13 に付属する Red Hat Enterprise Linux CoreOS (RHCOS) イメージからはベアメタルワーカーを起動できないため、ベアメタルワーカーを使用して Red Hat OpenStack Platform (RHOSP) 16.2 上にバージョン 4.13 をインストールすると失敗します。RHCOS イメージにバイトオーダーマーカーがないことが、根本的な問題となっています。この問題の修正は次の 16.2 ビルドで計画されています。(OCPBUGS-13395)

- RHEL 9.2 の既知の問題により、Confidential VM を含む GCP クラスターでは永続ボリュームを使用できません。(OCPBUGS-7582)

- **openvswitch2.15** がインストールされている OpenShift Container Platform 4.12 クラスターで実行されている Red Hat Enterprise Linux (RHEL) ワーカーは、OpenShift Container Platform 4.13 にアップグレードすると失敗します。**upgrade.yml** Playbook は次のエラーメッセージで失敗します: **package openvswitch2.17-2.17.0-88.el8fdp.x86_64 conflicts with openvswitch2.15 provided by openvswitch2.15-2.15.0-136.el8fdp.x86_64**。
この問題を回避するには、OpenShift Container Platform 4.13 に更新する前に、手動で **openvswitch2.15** パッケージを削除し、**openvswitch2.17** パッケージをインストールします。次に、**upgrade.yml** Playbook を実行して RHEL ワーカーを更新し、更新プロセスを完了します。(OCPBUGS-11677)

- ストレージをワークロードに接続するときに、ディスク検出が遅延します。(OCPBUGS-11149)

- OpenShift Container Platform 4.12 から 4.13 に更新すると、Mellanox NIC は SR-IOV ネットワークノードポリシーの名前を変更します (例: **ens7f0** から **ens7f0np0** に変更)。この名前の変更は、RHEL 9 カーネルへの更新により発生します。その結果、インターフェイスが見つからないため仮想機能 (VF) を作成できません。SR-IOV ネットワークノードポリシーでは、この名前変更を考慮する必要があります。たとえば、ポリシーで **ens7f0** が参照されている場合は、更新する前に **ens7f0np0** をポリシーに追加します。
この問題を回避するには、OpenShift Container Platform 4.13 に更新する前に、**SriovNetworkNodePolicy** カスタムリソース (CR) を手動で編集して **ens7f0np0** を追加する必要があります。(OCPBUGS-13186) 次のコードは、互換性を確保するために両方の名前が **SriovNetworkNodePolicy** に追加されたポリシー更新の例を示しています。

```
# ...
deviceType: netdevice
nicSelector:
  deviceID: “101d”
  pfNames:
    - ens7f0
    - ens7f0np0
  vendor: ‘15b3’
nodeSelector:
  feature.node.kubernetes.io/sriov-capable: ‘true’
numVfs: 4
# ...
```

- Pod の削除時に SR-IOV 仮想機能 (VF)の MAC アドレスをリセットすると、Intel E810 NIC で失敗する可能性があります。その結果、SR-IOV VF を持つ Pod の作成には、Intel E810 NIC カードで最大 2 分かかる場合があります。(OCPBUGS-5892)

- クラスターのアップグレードに使用するサブスクリプションポリシーで無効なサブスクリプションチャネルを指定すると、Topology Aware Lifecycle Manager (TALM) は、TALM がポリシーを適用した直後にアップグレードが成功したことを示します。これは、**Subscription** リソースが **AtlatestKnown** 状態のままであるためです。(OCPBUGS-9239)

- システムクラッシュの発生後、**kdump** は、Intel E810 NIC と ice ドライバーがインストールされている HPE Edgeline e920t および HPE ProLiant DL110 Gen10 サーバー上で **vmcore** クラッシュダンプファイルを生成できません。(RHELPLAN-138236)

- GitOps ZTP では、**SiteConfig** CR を使用して複数のノードを含むマネージドクラスターをプロビジョニングする場合、1 つ以上のノードに **SiteConfig** CR で設定された **diskPartition** リソースがあると、ディスクパーティションが失敗します。(OCPBUGS-9272)

- PTP 境界クロック (T-BC) が設定され、DU アプリケーションがデプロイされたクラスターでは、最大 40 秒間、vDU ホスト上の T-BC のフォロワーインターフェイスからメッセージが断続的に送信されません。ログ内のエラーレートは異なる場合があります。以下はエラーログの例です。

  出力例

  ```
  2023-01-15T19:26:33.017221334+00:00 stdout F phc2sys[359186.957]: [ptp4l.0.config]
  nothing to synchronize
  ```

  (RHELPLAN-145492)

- GitOps ZTP を使用してシングルノード OpenShift クラスターをインストールし、HTTP トランスポートを使用して PTP およびベアメタルイベントを設定すると、**linuxptp-daemon** デーモン Pod のデプロイが断続的に失敗します。必要な **PersistentVolumeClaim** (**PVC**) リソースは作成されますが、Pod にマウントされません。次のボリュームマウントエラーが報告されます。

  出力例

  ```
  mount: /var/lib/kubelet/plugins/kubernetes.io/local-volume/mounts/local-pv-bc42d358:
  mount(2) system call failed: Structure needs cleaning.
  ```

  この問題を回避するには、**cloud-event-proxy-store-storage-class-http-events PVC** CR を削除し、PTP Operator を再デプロイします。(OCPBUGS-12358)

- **SiteConfig** CR でセキュアブートが有効になっているシングルノード OpenShift マネージドクラスターの GitOps Zero Touch Provisioning (ZTP) プロビジョニング中にホストのプロビジョニングを実行すると、**BareMetalHost** CR に対して複数の **ProvisioningError** エラーが報告されます。このエラーは、セキュアブート設定が Baseboard Management Controller (BMC) に正常に適用されているが、**BareMetalHost** CR の適用後にホストの電源が入っていないことを示します。この問題を回避するには、以下の手順を実行します。

  1. ホストを再起動します。これにより、GitOps ZTP パイプラインは確実にセキュアブート設定を適用します。

  2. 同じ設定でクラスターの GitOps ZTP プロビジョニングを再起動します。

  (OCPBUGS-8434)

- デュアルスタック GitOps ZTP ハブクラスターをインストールした後に、デュアルスタック仮想 IP アドレス (VIP) を有効にし、**Provisioning** CR で **virtualMediaViaExternalNetwork** フラグを有効にすると、**IRONIC_EXTERNAL_URL_V6** 環境変数に IPv4 アドレスが誤って割り当て

られます。(OCPBUGS-4248)

- ZT サーバーの **BiosRegistry** 言語が、**en** ではなく **en-US** に設定されています。これにより、マネージドクラスターホストの GitOps ZTP プロビジョニング中に問題が発生します。ZT サーバー用に生成された **FirmwareSchema** CR の **allowable_values**、**attribute_type**、**read_only** フィールドが入力されていません。(OCPBUGS-4388)

- OpenShift Container Platform バージョン 4.13.0 では、エージェントベースのインストーラーでクラスターをインストールしようとするとエラーが発生します。ディスクの読み取り段階の後にエラーが返され、クラスターのインストールがスタックします。このエラーは HPEsplunk Gen10 サーバーで検出されます。(OCPBUGS-13138)

- RFC2544 のパフォーマンステストは、ネットワークを通過するパケットの **Max delay** 値が最小しきい値を超えることを示しています。このリグレッションは、Telco RAN DU プロファイルを実行している OpenShift Container Platform 4.13 クラスターで発生します。(OCPBUGS-13224)

- OpenShift Container Platform 4.13 がインストールされたシングルノード OpenShift クラスターで実行されたパフォーマンステストでは、**oslat** の最大レイテンシーが 20 マイクロ秒を超えています。(RHELPLAN-155443)

- OpenShift Container Platform 4.13 がインストールされたシングルノード OpenShift クラスターで実行されたパフォーマンステストでは、**cyclictest** の最大レイテンシーが 20 マイクロ秒を超えています。(RHELPLAN-155460)

- DPDK の CPU ロードバランシングの無効化 で説明されている低遅延チューニングに関連付けられた **cpu-load-balancing.crio.io: "disable"** アノテーションは、ワークロードパーティショニングが設定されていないシステムでは機能しません。具体的には、ワークロードのパーティション設定 で説明されているように、インフラストラクチャーが **cpuPartitioningMode** を **AllNodes** 値に設定していないクラスターに影響します。
  該当するクラスターの達成可能なレイテンシーに影響を与え、低レイテンシーワークロードの適切な動作を妨げる可能性があります。(OCPBUGS-13163)

- Nutanix プラットフォーム上の OpenShift Container Platform 4.12 クラスターでは、Nutanix Cloud Control Manager (CCM) に必要な設定がない場合は、**Upgradeable=False** 状態が発生する可能性があります。この状態を解決するには、How to create the ConfigMaps and Secrets needed to upgrade to OpenShift 4.13 when using Nutanix as a Platform を参照してください。

- 現在、非常に多くのファイルを含む永続ボリューム (PV) を使用すると、Pod が起動しないか、起動に過度に時間がかかる場合があります。詳細は、ナレッジベースアーティクル を参照してください。(BZ1987112)

- コントロールプレーンノードにスケジュールされている Azure File NFS ボリュームを含む Pod を作成すると、マウントが拒否されます。(OCPBUGS-18581)
  この問題を回避するには、コントロールプレーンノードがスケジュール可能で、Pod がワーカーノードで実行できる場合は、**nodeSelector** または Affinity を使用してワーカーノードで Pod をスケジュールします。

- vSphere でのエージェントベースのインストールは、ノードテイントの削除に失敗したために失敗します。これにより、インストールが保留状態のままになります。シングルノードの OpenShift クラスターは影響を受けません。この問題を回避するには、次のコマンドを実行してノードテイントを手動で削除します。

```
$ oc adm taint nodes <node_name>
node.cloudprovider.kubernetes.io/uninitialized:NoSchedule-
```

(OCPBUGS-20049)

- 静的 IP アドレス指定と Tang 暗号化を使用して OpenShift Container Platform クラスターをインストールする場合、ノードはネットワーク設定なしで起動します。この状況により、ノードは Tang サーバーにアクセスできなくなり、インストールが失敗します。この状況に対処するには、各ノードのネットワーク設定を **ip** インストーラー引数として設定する必要があります。

  1. インストーラーでプロビジョニングされるインフラストラクチャーの場合、インストール前に次の手順を実行して、各ノードの **IP** インストーラー引数としてネットワーク設定を指定します。

     a. マニフェストを作成します。

     b. 各ノードについて、アノテーションを使用して **BareMetalHost** カスタムリソースを変更し、ネットワーク設定を含めます。以下に例を示します。

```
$ cd ~/clusterconfigs/openshift
$ vim openshift-worker-0.yaml
```

```
apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  annotations:
    bmac.agent-install.openshift.io/installer-args: '["--append-karg", "ip=<static_ip>::
<gateway>:<netmask>:<hostname_1>:<interface>:none", "--save-partindex", "1", "-
n"]' 1 2 3 4 5
    inspect.metal3.io: disabled
    bmac.agent-install.openshift.io/hostname: <fqdn> 6
    bmac.agent-install.openshift.io/role: <role> 7

  generation: 1
  name: openshift-worker-0
  namespace: mynamespace
spec:
  automatedCleaningMode: disabled
  bmc:
    address: idrac-virtualmedia://<bmc_ip>/redfish/v1/Systems/System.Embedded.1
8
    credentialsName: bmc-secret-openshift-worker-0
    disableCertificateVerification: true
  bootMACAddress: 94:6D:AE:AB:EE:E8
  bootMode: "UEFI"
  rootDeviceHints:
    deviceName: /dev/sda
```

ip 設定については、次のように置き換えます。

1. **<static_ip>** は、ノードの静的 IP アドレスに置き換えます (例: **192.168.1.100**)
2. **<gateway>** は、ネットワークのゲートウェイの IP アドレスに置き換えます (例: **192.168.1.1**)
3. **<netmask>** は、ネットワークマスクに置き換えます (例: **255.255.255.0**)
4. **<hostname_1>** は、ノードのホスト名に置き換えます (例: **node1.example.com**)

5 **<interface>** は、ネットワークインターフェイスの名前に置き換えます (例: **eth0**)

6 **<fqdn>** は、ノードの完全修飾ドメイン名に置き換えます。

7 **<role>** は、ノードのロールを反映する **worker** または **master** に置き換えます。

8 **<bmc_ip>** は、必要に応じて BMC IP アドレス、BMC のプロトコルとパスに置き換えます。

c. ファイルを **clusterconfigs/openshift** ディレクトリーに保存します。

d. クラスターを作成します。

2. Assisted Installer を使用してインストールする場合は、インストール前に API を使用して各ノードのインストーラー引数を変更し、ネットワーク設定を **IP** インストーラー引数として追加します。以下に例を示します。

```
$ curl https://api.openshift.com/api/assisted-install/v2/infra-
envs/${infra_env_id}/hosts/${host_id}/installer-args \
-X PATCH \
-H "Authorization: Bearer ${API_TOKEN}" \
-H "Content-Type: application/json" \
-d '
   {
    "args": [
     "--append-karg",
     "ip=<static_ip>::<gateway>:<netmask>:<hostname_1>:<interface>:none", 1 2
3 4 5
     "--save-partindex",
     "1",
     "-n"
    ]
   }
 ' | jq
```

以前のネットワーク設定の場合は、次のように置き換えます。

1 **<static_ip>** は、ノードの静的 IP アドレスに置き換えます (例: **192.168.1.100**)

2 **<gateway>** は、ネットワークのゲートウェイの IP アドレスに置き換えます (例: **192.168.1.1**)

3 **<netmask>** は、ネットワークマスクに置き換えます (例: **255.255.255.0**)

4 **<hostname_1>** は、ノードのホスト名に置き換えます (例: **node1.example.com**)

5 **<interface>** は、ネットワークインターフェイスの名前に置き換えます (例: **eth0**)

詳細とサポートについては、Red Hat Support チームにお問い合わせください。

(OCPBUGS-23119)

1.9. 非同期エラータの更新

OpenShift Container Platform 4.13 のセキュリティー、バグ修正、拡張機能の更新は、Red Hat Network 経由で非同期エラータとして発表されます。OpenShift Container Platform 4.13 のすべてのエラータは Red Hat カスタマーポータルから入手できます。非同期エラータについては、OpenShift Container Platform ライフサイクル を参照してください。

Red Hat カスタマーポータルのユーザーは、Red Hat Subscription Management (RHSM) のアカウント設定でエラータの通知を有効にできます。エラータ通知を有効にすると、登録されたシステムに関連するエラータが新たに発表されるたびに、メールで通知が送信されます。

注記

OpenShift Container Platform のエラータ通知メールを生成させるには、Red Hat カスタマーポータルのユーザーアカウントでシステムが登録されており、OpenShift Container Platform エンタイトルメントを使用している必要があります。

以下のセクションは、これからも継続して更新され、今後の OpenShift Container Platform 4.13 バージョンの非同期リリースで発表されるエラータの拡張機能およびバグ修正に関する情報を追加していきます。たとえば、OpenShift Container Platform 4.13.z などのバージョン付けされた非同期リリースについてはサブセクションで説明します。さらに、エラータの本文がアドバイザリーで指定されたスペースに収まらないリリースの詳細は、その後のサブセクションで説明します。

重要

OpenShift Container Platform のいずれのバージョンについても、クラスターの更新 に関する指示には必ず目を通してください。

1.9.1. RHSA-2023:1326 - OpenShift Container Platform 4.13.0 イメージリリース、バグ修正およびセキュリティー更新アドバイザリー

発行日: 2023-05-17

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.0 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:1326 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:1325 アドバイザリーによって提供されます。更新プログラムに含まれるセキュリティー更新プログラムのリストは、RHSA-2023:6143 アドバイザリーに記載されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.0 --pullspecs
```

1.9.2. RHSA-2023:3304 - OpenShift Container Platform 4.13.1 のバグ修正とセキュリティー更新

発行日: 2023-05-30

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.1 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:3304 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:3303 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.1 --pullspecs
```

1.9.2.1. バグ修正

- 以前は、支援付きインストールで一時的なエラーが発生することがありました。このエラーが発生すると、インストールは復元できませんでした。この更新により、一時的なエラーが正しく再試行されるようになりました。(OCPBUGS-13138)
- 以前は、ネストされたパスが予想される最大 path-components を超えると、一部のレジストリーで oc-mirror OpenShift CLI (**oc**) プラグインが **401 unauthorized** エラーで失敗していました。この更新により、**--max-nested-paths** フラグのデフォルトの整数は 0 (制限なし) に設定されます。その結果、生成された **ImageContentSourcePolicy** には、デフォルトで使用される namespace レベルではなく、リポジトリーレベルまでのソースおよびミラー参照が含まれます。(OCPBUGS-13591)

1.9.2.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.3. RHSA-2023:3367 - OpenShift Container Platform 4.13.2 のバグ修正とセキュリティー更新

発行日 2023 年 6 月 7 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.2 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:3367 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:3366 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.2 --pullspecs
```

1.9.3.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.4. RHSA-2023:3537 - OpenShift Container Platform 4.13.3 のバグ修正とセキュリティー更新

発行日: 2023 年 6 月 13 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.3 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:3537 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、 RHSA-2023:3536 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

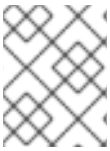
以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.3 --pullspecs
```

1.9.4.1. 機能

1.9.4.1.1. ZTP による iPXE ネットワークブートのサポート

GitOps Zero Touch Provisioning (ZTP) は、スポーククラスターのデプロイメントの一環として、Bare Metal Operator (BMO) を使用して、ターゲットホスト上で Red Hat Enterprise Linux CoreOS (RHCOS) を起動します。今回の更新では、GitOps ZTP は、これらの RHCOS インストール用の Preboot ExecutionEnvironment (iPXE) ネットワークブートのオプションを追加して、BMO の機能を活用します。



注記

iPXE ネットワークブートを使用するには、Red Hat Advanced Cluster Management (RHACM) 2.8 以降を使用する必要があります。

詳細は、SiteConfig および GitOps ZTP を使用したマネージドクラスターのデプロイ を参照してください。

1.9.4.2. バグ修正

- 以前のシングルノード OpenShift では、ノードの再起動時に競合状態が発生し、デバイスに異常が発生しているか、割り当て不可の状態であっても、ノード上のデバイスを要求しているアプリケーション Pod が許可される可能性がありました。これにより、アプリケーションがデバイスにアクセスしようとするとランタイムに失敗していました。この更新により、Pod によって要求されたリソースは、デバイスプラグインが kubelet に自己登録されており、割り当てられるノード上に正常なデバイスが存在する場合にのみ割り当てられます。
  これらの条件が満たされない場合、Pod は **UnexpectedAdmissionError** エラーで許可に失敗する可能性があり、これは予想される動作です。アプリケーション Pod がデプロイメントの一部である場合、障害が発生すると、後続の Pod がスピンアップされ、最終的にデバイスが割り当て可能な状態になると正常に実行されます。(OCPBUGS-14438)

- 以前は、クライアント TLS (mTLS) が Ingress コントローラー上に設定されており、クライアント CA バンドルの認証局 (CA) をダウンロードするには 1MB を超える証明書失効リスト (CRL) が必要でした。そのため、CRL **ConfigMap** オブジェクトサイズの制限により更新は実行されませんでした。CRL が欠落しているため、有効なクライアント証明書を使用した接続が、エラー **unknown ca** で拒否される可能性がありました。今回の更新により、各 Ingress コントローラーの CRL **ConfigMap** はなくなりました。代わりに、各ルーター Pod は CRL を直接ダウンロードし、有効なクライアント証明書を使用した接続が拒否されなくなりました。(OCPBUGS-13967)

- 以前は、クライアント TLS (mTLS) が Ingress コントローラー上で設定されていたため、配布元の認証局 (CA) と発行元の CA が一致せず、間違った証明書失効リスト (CRL) がダウンロードされていました。その結果、正しい CRL の代わりに間違った CRL がダウンロードされ、有効なクライアント証明書を使用した接続が **unknown ca** のエラーメッセージで拒否されていました。今回の更新により、ダウンロードした CRL はそれらを配布元の CA によって追跡されるようになりました。これにより、有効なクライアント証明書が拒否されなくなります。(OCPBUGS-13964)

1.9.4.3. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.5. RHSA-2023:3614 - OpenShift Container Platform 4.13.4 のバグ修正とセキュリティー更新

発行日: 2023 年 6 月 23 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.4 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:3614 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:3612 アドバイザリーによって提供されます。更新プログラムに含まれるセキュリティー更新プログラムのリストは、RHSA-2023:6143 アドバイザリーに記載されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.4 --pullspecs
```

1.9.5.1. バグ修正

- 以前は、Google Cloud Platform (GCP) 上の Confidential 仮想マシンが含まれるクラスターでは、永続ボリュームストレージを使用できませんでした。この問題は、OpenShift Container Platform 4.13.3 以前のバージョンで継続しています。OpenShift Container Platform 4.13.4 以降では、GCP 上の Confidential 仮想マシンが含まれるクラスターで、永続ボリュームストレージを使用できるようになりました。(OCPBUGS-11768)

- 以前は、Vault と Vault Enterprise に欠陥があり、AWS IAM ID とロールを検証するために Vault が依存する値が、認証を省略したり、認証を回避したりすることができました。(BZ#2167337)

- 以前は、GitOps ZTP では、**SiteConfig** CR を使用して複数のノードを含むマネージドクラスターをプロビジョニングすると、1 つ以上のノードに **SiteConfig** CR で設定された **diskPartition** リソースがある場合、ディスクパーティションが失敗していました。(OCPBUGS-13161)

- 以前のバージョンでは、すべてのクラスターがすでに準拠していると、誤解を招くバックアップ条件が **ClusterGroupUpgrade** (**CGU**) CR で報告されていました。(OCPBUGS-13700)

- 以前は、複数のクラスターのスケーリングアップグレード中に、クラスターのアップグレード **CGU** CR が **BackupTimeout** エラーでアップグレードに失敗することがありました。(OCPBUGS-7422)

1.9.5.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.6. RHSA-2023:4091 - OpenShift Container Platform 4.13.5 のバグ修正とセキュリティー更新

発行日 2023-07-20

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.5 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:4091 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:4093 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.5 --pullspecs
```

1.9.6.1. バグ修正

- これまで、ゲートウェイ API 機能は、ゲートウェイドメインの末尾にドットが付いた DNS レコードを提供していませんでした。そのため、DNS レコードのステータスが GCP プラットフォームで利用できなくなりました。今回の更新により、ゲートウェイ API ゲートウェイの DNS レコードが適切にプロビジョニングされ、ゲートウェイサービスの DNS コントローラーがドメイン内にドットがない場合に末尾のドットを追加するようになったため、ゲートウェイ API 機能が GCP で動作するようになりました。(OCPBUGS-15434)

- 以前のバージョンは、**Developer** コンソールの **Pipelines** ページを使用してリポジトリーを追加し、コードリポジトリー URL として GitLab または Bitbucket Pipelines を **Git リポジトリー URL** として入力した場合、作成された **Repository** リソースは無効でした。これは、**git_provider.url** 仕様にスキーマがないことが原因で発生していましたが、現在は修正されています。(OCPBUGS-15410)

- 今回のリリースでは、**git_provider.user** 仕様がコード **Repository** オブジェクトとしてパイプラインに追加されました。この仕様では、Git プロバイダーが Bitbucket の場合、ユーザー名を指定する必要があります。(OCPBUGS-15410)

- 本リリースでは、**Pipelines → Create → Add Git Repository** ページの **Secret** フィールドが必須になりました。**Show configuration options** をクリックし、リポジトリーの Git アクセストークンまたは Git アクセストークンシークレットを設定する必要があります。(OCPBUGS-15410)

- 以前は、**Developer** コンソールで **Helm** に移動し、**リポジトリー** タブをクリックし、Helm チャートリポジトリーの kebab メニューから **Edit HelmChartRepository** を選択して Helm チャートリポジトリーを編集しようとすると、**404: Page Not Found** エラーを示す **エラー** ページが表示されました。これは、コンポーネントパスが最新ではないことが原因でした。この問題は修正されています。(OCPBUGS-15130)

1.9.6.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.7. RHSA-2023:4226 - OpenShift Container Platform 4.13.6 のバグ修正とセキュリティー更新

発行日: 2023-07-27

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.6 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:4226 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:4229 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.6 --pullspecs
```

1.9.7.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.8. RHSA-2023:4456: OpenShift Container Platform 4.13.8 のバグ修正とセキュリティー更新

発行日: 2023 年 8 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.8 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:4456 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:4459 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.8 --pullspecs
```

1.9.8.1. バグ修正

- 以前は、Red Hat OpenStack Platform (RHOSP) の実際のロードバランサーのアドレスは表示されませんでした。この更新により、実際のロードバランサーアドレスが追加され、RHOSP ロードバランサーオブジェクトのアノテーションに表示されるようになりました。(OCPBUGS-15973)

1.9.8.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.9. RHSA-2023:4603 - OpenShift Container Platform 4.13.9 のバグ修正とセキュリティー更新

発行日: 2023 年 8 月 16 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.9 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:4603 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:4606 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.9 --pullspecs
```

1.9.9.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.10. RHSA-2023:4731 - OpenShift Container Platform 4.13.10 のバグ修正とセキュリティー更新

発行日: 2023-08-30

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.10 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:4731 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:4734 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.10 --pullspecs
```

1.9.10.1. バグ修正

- 以前は、Mint モードを使用し、そのルートシークレットが削除されたクラスターでは、4.13.8 から 4.13.9 へのアップグレード中に問題が発生していました。これは、4.13.9 にバックポートされた Ingress Operator の認証情報要求の変更が原因でした。今回の更新により、バージョン 4.13.9 以降への更新でこれらのクラスターに問題は発生しなくなりました。(OCPBUGS-17733)

1.9.10.2. 既知の問題

- OpenShift Container Platform 4.12 に UDP Generic Receive Offload (GRO) を有効にする新機能を追加すると、すべての仮想イーサネットペア (veth) デバイスで利用可能な CPU ごとに 1 つの RX キューを持つことになります。以前は、veth ごとに 1 つのキューがありました。これらのキューは Open Virtual Network によって動的に設定され、レイテンシーチューニングとこのキュー作成は同期されません。
  レイテンシーチューニングロジックは、veth NIC 作成イベントをモニタリングし、すべてのキューが適切に作成される前に、Receive Packet Steering (RPS) キュー CPU マスクの設定を開始します。これは、一部の RPS キューマスクが設定されないことを意味します。すべての NIC キューが適切に設定されるわけではないため、タイミングに制限のある CPU を使用して他のコンテナー内のサービスと通信するリアルタイムアプリケーションでは、レイテンシースパイクが発生する可能性があります。カーネルネットワークスタックを使用しないアプリケーションは影響を受けません。(OCPBUGS-17794)

1.9.10.3. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.11. RHBA-2023:4905 - OpenShift Container Platform 4.13.11 のバグ修正

発行日: 2023-09-05

OpenShift Container Platform リリース 4.13.11 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:4905 アドバイザリーに記載されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.11 --pullspecs
```

1.9.11.1. バグ修正

- 以前のバージョンでは、一部の Pod が **終了** 状態のままになると、OpenShift Container Platform で問題が確認されました。これにより、許可リストコントローラーの調整ループに影響があり、これにより、不要な再試行が発生し、複数の Pod の作成が発生していました。今回の更新により、許可リストコントローラーは、現在のデーモンセットに属する Pod のみを検査します。その結果、1 つ以上の Pod の準備ができていない場合に再試行が発生しなくなりました。(**OCPBUGS-16019**)

1.9.11.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.12. RHBA-2023:5011 - OpenShift Container Platform 4.13.12 のバグ修正

発行日: 2023-09-12

OpenShift Container Platform リリース 4.13.12 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:5011 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:5014 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.12 --pullspecs
```

1.9.12.1. 機能

1.9.12.1.1. NUMA 対応スケジューリング用 SR-IOV ネットワークトポロジーの除外

このリリースでは、SR-IOV ネットワークの Non-Uniform Memory Access (NUMA) ノードの Topology Manager に対するアドバタイズを除外できるようになりました。SR-IOV ネットワークの NUMA ノードをアドバタイズしないため、NUMA 対応の Pod スケジューリング中に、より柔軟に SR-IOV ネットワークをデプロイできます。

たとえば、シナリオによっては、単一 NUMA ノード上の Pod の CPU およびメモリーリソースを最大化することが優先されます。Topology Manager に Pod の SR-IOV ネットワークリソースの NUMA ノードに関するヒントを提供しないことで、Topology Manager は SR-IOV ネットワークリソースと

Pod の CPU およびメモリーリソースを異なる NUMA ノードにデプロイできます。以前の OpenShift Container Platform リリースでは、Topology Manager はすべてのリソースを同じ NUMA ノードに配置しようとしていました。

NUMA 対応の Pod スケジューリングにおける柔軟な SR-IOV ネットワークデプロイメントについて、詳しくは NUMA 対応スケジューリング用 SR-IOV ネットワークトポロジーの除外 を参照してください。

1.9.12.1.2. Google Cloud Provider クラスター用のカスタム Red Hat Enterprise Linux CoreOS (RHCOS) イメージの使用

デフォルトで、インストールプログラムは、コントロールプレーンおよびコンピュートマシンの開始に使用される Red Hat Enterprise Linux CoreOS (RHCOS)イメージをダウンロードしてインストールします。今回の機能拡張により、インストール設定ファイル (install-config.yaml) を変更してカスタム RHCOS イメージを指定することにより、デフォルトの動作をオーバーライドできるようになりました。クラスターをデプロイする前に、次のインストールパラメーターを変更できます。

- **controlPlane.platform.gcp.osImage.project**
- **controlPlane.platform.gcp.osImage.name**
- **compute.platform.gcp.osImage.project**
- **compute.platform.gcp.osImage.name**
- **platform.gcp.defaultMachinePlatform.osImage.project**
- **platform.gcp.defaultMachinePlatform.osImage.name**

これらのパラメーターの詳細は、追加の Google Cloud Platform 設定パラメーター を参照してください。

1.9.12.1.3. Network API の Service オブジェクトにおける allocateLoadBalancerNodePorts のサポート

Service オブジェクト下の Network API の **ServiceSpec** コンポーネントは、ユーザーがサービスで作成する属性を記述します。OpenShift Container Platform 4.13 では、**ServiceSpec** コンポーネント内の **allocateLoadBalancerNodePorts** 属性がサポートされるようになりました。**allocateLoadBalancerNodePorts** 属性は、 **NodePorts** が **LoadBalancer** 型のサービスに自動的に割り当てられるかどうかを定義します。

1.9.12.2. バグ修正

- 以前は、バックエンドが 1 つしかない場合、OpenShift Container Platform ルーターは重みが 0 のルートにトラフィックを送信していました。今回の更新により、ルーターは重みが 0 の単一バックエンドを持つルートにトラフィックを送信しなくなりました。(OCPBUGS-17107)

1.9.12.3. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.13. RHSA-2023:5155 - OpenShift Container Platform 4.13.13 のバグ修正とセキュリティー更新

発行日: 2023-09-20

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.13 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:5155 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:5158 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.13 --pullspecs
```

1.9.13.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.14. RHBA-2023:5382 - OpenShift Container Platform 4.13.14 のバグ修正

発行日: 2023-10-05

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.14 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:5382 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:5388 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.14 --pullspecs
```

1.9.14.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.15. RHBA-2023:5467 - OpenShift Container Platform 4.13.15 のバグ修正

発行日: 2023-10-10

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.15 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:5467 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:5470 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.15 --pullspecs
```

1.9.15.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.16. RHSA-2023:5672 - OpenShift Container Platform 4.13.17 のバグ修正とセキュリティー更新

発行日: 2023-10-17

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.17 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:5672 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:5675 アドバイザリーによって提供されます。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.17 --pullspecs
```

1.9.16.1. バグ修正

- 以前は、ユーザーがポート番号なしで **EndpointSlice** ポートを作成した場合、CoreDNS が予期せず終了していました。この更新により、CoreDNS が予期せず終了することを防ぐための検証が CoreDNS に追加されました。(**OCPBUGS-19985**)

1.9.16.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.17. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.18 --pullspecs
```

1.9.17.1. バグ修正

- **etcdctl** バイナリーは、ローカルマシンに無期限にキャッシュされ、更新ができなくなりました。バイナリーは、**cluster-backup.sh** スクリプトが呼び出されるたびにプルされるようになりました。(**OCPBUGS-20488**)

1.9.17.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.18. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2023-10-31

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.19 --pullspecs
```

1.9.18.1. 機能

1.9.18.1.1. apiserver.config.openshift.io が Insights Operator によって追跡されるようになりました

Insights Operator の実行後、**APIServer.config.openshift.io** の監査プロファイルに関する情報とともに、パス **config/apiserver.json** のアーカイブで新しいファイルが利用できるようになります。

監査プロファイルにアクセスすると、どの監査ポリシーが共通であること、最も一般的に使用されるプロファイル、業界間のどのような違い、どのようなカスタマイズが適用されるかを理解するのに役立ちます。

1.9.18.2. バグ修正

- 以前は、Cluster Version Operator (CVO) が **SecurityContextConstraints** リソースを期待どおりに調整しませんでした。CVO は、SCC リソースの **Volumes** フィールドをリリースイメージで定義された状態に適切に調整するようになりました。システム SCC リソースへのユーザーの変更は許容されます。
  今後の OpenShift Container Platform バージョンでは、システム SCC リソースのユーザー変更の許容を停止するため、CVO はユーザー変更の SCC を検出するとマイナーバージョン更新ゲートを適用するようになりました。ユーザーは、OpenShift Container Platform の将来のマイナーバージョンに更新する前に、変更されていないシステムの SCC リソースにワークロードを準拠させる必要があります。詳細は、**4.14 にアップグレードする前に Resolving "Detected modified SecurityContextConstraints" 更新ゲートを** 参照してください。(**OCPBUGS-19472**)

1.9.18.3. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.19. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。本リリース用の RPM パッケージはありません。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.21 --pullspecs
```

1.9.19.1. バグ修正

- 以前のバージョンでは、egress IP は Azure プライベートクラスターの egress ノードに適用できませんでした。このパッチにより、アウトバウンド接続にアウトバウンドルールを使用する Azure セットアップの egress IP が有効になります。このようなセットアップでは、Azure が持つアーキテクチャー上の制約により、egress IP として機能するセカンダリー IP はアウトバウンド接続ができません。このリリースでは、一致する Pod にはインターネットへの送信接続がなくなりますが、インフラストラクチャーネットワーク内の外部サーバーに到達できるようになりました。(OCPBUGS-22299)

1.9.19.2. 既知の問題

- **ClusterGroupUpdate** CR の開始時に、選択したすべてのクラスターが準拠している場合、TALM はポリシーの修正をスキップします。同じ **ClusterGroupUpdate** CR 内のカタログソースポリシーとサブスクリプションポリシーが変更された Operator の更新は完了しません。サブスクリプションポリシーは、カタログソースの変更が適用されるまで準拠の状態が続くためスキップされます。
  回避策として、common-subscription ポリシーの 1 つの CR に簡単な変更を追加します（例：**metadata.annotations.upgrade: "1"**）。これにより、**ClusterGroupUpdate** CR の開始前にポリシーが非準拠になります。(OCPBUGS-2812)

1.9.19.3. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.20. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2023 年 11 月 15 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.22 --pullspecs
```

1.9.20.1. バグ修正

- 以前は、copy コマンドに **-p** フラグオプションがありませんでした。このコマンドは **-p** フラグをサポートし、コマンドがタイムスタンプを保持するようになりました。(OCPBUGS-29246)

- 以前のバージョンでは、**Burstable** コンテナーは、パフォーマンスプロファイルで設定されたノードに予約された CPU でのみ実行できました。これにより、Red Hat Enterprise Linux (RHEL) 9 が CPU アフィニティーと **cpuset** コンポーネントの動作を変更し、**cpuset** が変更されたときに CPU アフィニティーがリセットされませんでした。今回のリリースより、新たに実行中のコンテナーの **cpuset** コンポーネントと対話するコンポーネントはすべて、CPU アフィニティーがリセットされます。これは、**Burstable** コンテナーが、現在ピニングされた **Guaranteed** コンテナーに割り当てられていないすべての CPU にアクセスできることを意味します。(OCPBUGS-20365)

1.9.20.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.21. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2023 年 11 月 21 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2024:1563 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.23 --pullspecs
```

1.9.21.1. 機能

1.9.21.1.1. Web ブラウザーを使用した CLI へのログイン

このリリースでは、新しい **oc** コマンドラインインターフェイス(CLI)フラグ、**--web** が **oc login** コマンドで使用できるようになりました。

この機能拡張により、Web ブラウザーを使用してログインできるようになり、コマンドラインにアクセストークンを挿入する必要がなくなります。

詳細は、Web ブラウザーを使用した OpenShift CLI へのログイン を参照してください。

1.9.21.2. バグ修正

- 以前は、すべての Redfish 仮想メディアデバイスを使用してハードウェアをプロビジョニングすることができないため、Ironic は Cisco UCS ハードウェアを新しい baremetalhost としてプロビジョニングできませんでした。このリリースでは、Ironic がハードウェアをプロビジョニングするために使用できるすべてのデバイスを調べるため、Redfish Virtual Media を使用して Cisco UCS ハードウェアをプロビジョニングできるようになりました。(OCPBUGS-19078)

- 以前は、IP が割り当てられて未割り当ての LB サービスがあるときに、metallb のコントローラーが再起動していました。これにより、metallb のコントローラーがすでに割り当てられている IP を別の LB サービスに移動し、ワークロードが壊れていました。このリリースでは、metallb のコントローラーは、IP が割り当てられているサービスを処理します。(OCPBUGS-23160)

1.9.21.3. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.22. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2023 年 11 月 29 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2024:1563 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.24 --pullspecs
```

1.9.22.1. バグ修正

- 以前は、CSI ストレージを持つノードでクラスターオートスケーラーを使用すると、**CrashBackoff** ループが発生する可能性がありました。このリリースでは、エラー処理を改善するために依存関係が更新され、**CrashBackoff** ループが発生しなくなりました。(OCPBUGS-29246)

1.9.22.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.23. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2023-12-06

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2024:1563 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.25 --pullspecs
```

-

1.9.23.1. バグ修正

- 以前は、Image Registry Operator は、5 分ごとにアクセスキーを取得する一環として、ストレージアカウントリストエンドポイントへの API 呼び出しを行っていました。多くの OpenShift Container Platform (OCP) クラスターを含むプロジェクトでは、これにより API 制限に達し、新規クラスターの作成を試みると 429 エラーが発生する可能性があります。このリリースでは、呼び出し間隔が 5 分から 20 分に延長されました。(OCPBUGS-22126)

1.9.23.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.24. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.26 --pullspecs
```

1.9.24.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.25. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

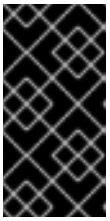
このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.27 --pullspecs
```

1.9.25.1. バグ修正

- 以前は、クラスター内に **ImageContentSourcePolicy** (ICSP)オブジェクトがある場合、**ImageDigestMirrorSet** (IDMS)および **ImageTagMirrorSet** (ITMS)オブジェクトは使用できませんでした。そのため、IDMS または ITMS オブジェクトを使用するには、クラスター内の ICSP オブジェクトを削除する必要があり、クラスターの再起動が必要でした。このリリースでは、ICSP、IDMS、および ITMS オブジェクトが同じクラスター内で同時に機能するようになりました。これで、クラスターのインストール後に 3 種類のオブジェクトのいずれかまたはすべてを使用して、リポジトリーミラーリングを設定できるようになります。詳細は、 Image Registry リポジトリーのミラーリングについて を参照してください。(RHIBMCS-185)



重要

ICSP オブジェクトを使用してリポジトリーミラーリングを設定することは、非推奨の機能です。非推奨の機能は依然として OpenShift Container Platform に含まれており、引き続きサポートされますが、本製品の今後のリリースで削除されるため、新規デプロイメントでの使用は推奨されません。

1.9.25.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.26. RHBA-2023:3977 - OpenShift Container Platform 4.12.24 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

OpenShift Container Platform リリース 4.13.12 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:1451 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.28 --pullspecs
```

1.9.26.1. バグ修正

- 以前は、異なる DNS 接尾辞が原因で、**ccoctl** は China で AWS セキュリティートークンサービス(STS)リソースを作成できませんでした。このリリースでは、**ccoctl** を使用して China リージョンに STS リソースを作成でき、クラスターを正常にインストールできるようになりました。(OCPBUGS-25369)

1.9.26.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.27. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 1 月 17 日

OpenShift Container Platform リリース 4.13.12 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2024:1563 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.29 --pullspecs
```

1.9.27.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.28. RHBA-2023:3977 - OpenShift Container Platform 4.12.24 のバグ修正とセキュリティー更新

発行日: 2024 年 1 月 24 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:1451 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2024:1563 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.30 --pullspecs
```

1.9.28.1. バグ修正

- 以前は、ミラーリングリリースに EUS チャネルを使用すると、**oc-mirror** コマンドを使用したミラーリングに失敗していました。この問題は、**oc-mirror** が EUS チャネルが偶数番号のリリースのみであることを認識しなかったために発生しました。このリリースでは、**oc-mirror** コマンドのユーザーは、ミラーリングリリースに EUS チャネルを使用できるようになりました。(OCPBUGS-26595)

1.9.28.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.29. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.31 --pullspecs
```

1.9.29.1. バグ修正

- 以前は、Whereabouts CNI プラグインによって作成されたプールから IP アドレスが割り当てられた Pod が、ノードの強制再起動後に **ContainerCreating** 状態でスタックしていました。このリリースでは、ノードの強制再起動後の IP 割り当てに関連する Whereabouts CNI プラグインの問題が解決されました。(OCPBUGS-27367)

- 以前は、デフォルトでは、**container_t** SELinux コンテキストは **dri_device_t** オブジェクトにアクセスできませんでした。これにより、DRI デバイスへのアクセスが提供されます。新しいコンテナーポリシー **container-selinux** により、Pod がデバイスプラグインを使用して **dri_device_t** オブジェクトにアクセスできるようになりました。(OCPBUGS-27416)

1.9.29.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.30. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

2024 年 2 月 7 日発行

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.32 --pullspecs
```

1.9.30.1. 機能

この z-stream リリースには次の機能が含まれています。

1.9.30.1.1. whereabouts cron スケジュールの設定の有効化

- Whereabouts 調整スケジュールは 1 日に 1 回実行されるようにハードコードされており、再設定できませんでした。このリリースでは、**ConfigMap** オブジェクトにより、Whereabouts cron スケジュールの設定が有効になりました。詳細は、Whereabouts IP リコンサイラーのスケジュールの設定 を参照してください。

1.9.30.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.31. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.33 --pullspecs
```

1.9.31.1. バグ修正

- 以前は、OpenShift Container Platform を更新すると、DNS クエリーが失敗することがありました。これは、CoreDNS 1.10.1 を使用する非 EDNS クエリーに対してアップストリームが 512 バイトを超えるペイロードを返すためです。このリリースでは、準拠していないアップストリームを持つクラスターは、オーバーフローエラー時に TCP で再試行でき、アップグレード時に機能が中断されるのを防ぐことができます。(OCPBUGS-28205)

- 以前は、Amazon Elastic File System (EFS) Container Storage Interface (CSI) ドライバーコンテナーに適用される CPU の制限により、EFS ボリュームへの I/O 操作のパフォーマンス低下の問題が発生していました。EFS CSI ドライバーの CPU 制限が削除され、パフォーマンスの低下の問題は存在しなくなりました。(OCPBUGS-28979)

1.9.31.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.32. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.34 --pullspecs
```

1.9.32.1. バグ修正

- 以前は、最新のチャネルとデフォルトのチャネルを選択的にミラーリングし、新しいリリースによって新しいチャネルが導入されると、現在のデフォルトチャネルが無効になりました。これにより、新しいデフォルトチャネルの自動割り当てが失敗していました。このリリースでは、**currentDefault** チャネルをオーバーライドする **ImageSetConfig** カスタムリソース(CR)の **defaultChannel** フィールドを定義できるようになりました。(OCPBUGS-28899)

1.9.32.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.33. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 2 月 28 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2024:1563 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.35 --pullspecs
```

1.9.33.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.34. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 3 月 6 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.36 --pullspecs
```

1.9.34.1. バグ修正

- 以前は、**udev** イベントと物理デバイスに関連付けられた作成キューの間の競合状態により、一部のキューがゼロにリセットされる必要がある場合に、間違った Receive Packet Steering

(RPS) マスクで設定されていました。これにより、物理デバイスのキューに RPS マスクが設定され、Receive Side Scaling (RSS) の代わりに RPS が使用されることになり、パフォーマンスに影響を与える可能性がありました。この修正により、イベントはデバイスの作成時ではなくキューの作成ごとにトリガーされるように変更されました。これにより、欠落するキューがないことが保証されます。すべての物理デバイスのキューが、空の正しい RPS マスクを使用してセットアップされるようになりました。(OCPBUGS-24353)

1.9.34.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.35. RHBA-2023:5467 - OpenShift Container Platform 4.13.15 のバグ修正

発行日: 2024-03-13

OpenShift Container Platform リリース 4.13.12 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:1451 アドバイザリーに記載されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.37 --pullspecs
```

1.9.35.1. バグ修正

- 以前は、**ovn-ipsec-containerized** および **ovn-ipsec-host** デーモンには、**チェック先** の代わりに **openssl** パラメーター： **-checkedn** の誤字のエラーが含まれていました。このエラーにより、**ovn-ipsec** Pod が再起動するたびに証明書のローテーションが行われました。このリリースでは、パラメーター名が修正され、Internet Protocol Security (IPsec)が使用する証明書が期待どおりに自動的にローテーションされるようになりました。(OCPBUGS-30150)

- 以前のバージョンでは、Machine Config Operator (MCO)の **nodeStatusUpdateFrequency** メカニズムのデフォルト値が **0** 秒から **10** 秒に変更されました。これにより、メカニズムによってノードステータスレポートが増加し、**nodeStatusReportFrequency** パラメーターによって決定され、この影響を受けるコントロールプレーンの CPU リソースが発生しました。このリリースでは、**nodeStatusReportFrequency** のデフォルト値が **5** 分に設定され、CPU リソースの問題は発生しなくなりました。(OCPBUGS-30285)

1.9.35.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.36. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2024:1563 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.38 --pullspecs
```

1.9.36.1. バグ修正

- 以前のバージョンでは、アベイラビリティーゾーンサポートのない Microsoft Azure リージョンで実行されるマシンセットは、Spot インスタンスの **AvailabilitySets** オブジェクトを常に作成していました。この操作により、インスタンスは可用性セットをサポートしていないため、Spot インスタンスが失敗しました。マシンセットは、zonal に設定されたリージョンで動作する Spot インスタンスの **AvailabilitySets** オブジェクトを作成しなくなりました。(OCPBUGS-29906)

- 以前は、アプリケーションセレクターの名前が間違っていたため、**manila-csi-driver-controller-metrics** サービスには空のエンドポイントがありました。このリリースでは、アプリケーションセレクター名が **openstack-manila-csi** に変更され、問題は修正されました。(OCPBUGS-26224)

1.9.36.2. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.37. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1559 アドバイザリーに記載されています。この更新用の RPM パッケージはありません。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.39 --pullspecs
```

1.9.37.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.38. RHBA-2024:1761 - OpenShift Container Platform 4.13.40 バグ修正の更新

発行日：2024-04-18

OpenShift Container Platform リリース 4.13.40 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHBA-2024:1761 アドバイザリーにまとめられています。更新に含まれる RPM パッケージは、RHSA-2024:1763 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.13.40 --pullspecs
```

1.9.38.1. 更新

既存の OpenShift Container Platform 4.13 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。