OpenShift Container Platform 4.16

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: 2024-07-04

OpenShift Container Platform 4.16 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、新機能および機能拡張のすべて、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 4.16 リリースノート 3
1.1. このリリースについて 3
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 4
1.3. 新機能および機能拡張 4
1.4. 主な技術上の変更点 31
1.5. 非推奨および削除された機能 33
1.6. バグ修正 39
1.7. テクノロジープレビュー機能のステータス 66
1.8. 既知の問題 76
1.9. 非同期エラータの更新 78

第1章 OPENSHIFT CONTAINER PLATFORM 4.16 リリースノート

Red Hat OpenShift Container Platform は、開発者と IT 組織に対して、最小限の設定と管理により、新規および既存のアプリケーションの両方を安全でスケーラブルなリソースにデプロイするための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-2024:0041) が利用可能になりました。このリリースでは、CRI-O ランタイムで Kubernetes 1.29 を使用します。以下では、OpenShift Container Platform 4.16 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 4.16 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 4.16 は、Red Hat Enterprise Linux (RHEL) 8.8-8.10、および Red Hat Enterprise Linux CoreOS (RHCOS) 9.4 でサポートされています。

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。RHEL マシンは OpenShift Container Platform 4.16 では非推奨となり、今後のリリースでは削除される予定です。

OpenShift Container Platform 4.14 以降、偶数リリースの Extended Update Support (EUS) フェーズでは、**x86_64**、64 ビット ARM (**aarch64**)、IBM Power® (**ppc64le**)、IBM Z® (**s390x**) アーキテクチャーを含むすべてのサポート対象アーキテクチャーで、利用可能なライフサイクルの合計が 24 カ月に延長されます。これに加えて、Red Hat は、**Additional EUS Term 2** と呼ばれる 12 カ月間の追加の EUS アドオンも提供しており、これにより利用可能なライフサイクルが 24 カ月から 36 カ月に延長されます。Additional EUS Term 2 は、OpenShift Container Platform のすべてのアーキテクチャーバリアントで利用できます。

すべてのバージョンのサポートの詳細は、Red Hat OpenShift Container Platform のライフサイクルポリシー を参照してください。

4.16 リリース以降、Red Hat では 3 つの新しいライフサイクル分類 (Platform Aligned、Platform Agnostic、Rolling Stream) を導入し、同梱される Cluster Operator の管理を簡素化しています。これらのライフサイクル分類により、クラスター管理者にはさらなる簡素化と透明性が提供され、各 Operator のライフサイクルポリシーを理解し、予測可能なサポート範囲でクラスターのメンテナンスおよびアップグレード計画を形成できるようになります。詳細は、OpenShift Operator のライフサイクル を参照してください。

OpenShift Container Platform は FIPS 用に設計されています。FIPS モードでブートされた Red Hat Enterprise Linux (RHEL) または Red Hat Enterprise Linux CoreOS (RHCOS) を実行する場合、OpenShift Container Platform コアコンポーネントは、**x86_64**、**ppc64le**、および **s390x** アーキテクチャーのみで、FIPS 140-2/140-3 検証のために NIST に提出された RHEL 暗号化ライブラリーを使用します。

NIST 検証プログラムの詳細は、暗号化モジュール検証プログラム を参照してください。検証のために提出された RHEL 暗号化ライブラリーの個別バージョンの最新の NIST ステータスについては、政府の標準規格 を参照してください。

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 が RHEL 9.4 を使用するように

RHCOS は、OpenShift Container Platform 4.16 で Red Hat Enterprise Linux (RHEL) 9.4 パッケージを使用するようになりました。これらのパッケージにより、OpenShift Container Platform インスタンスが最新の修正、機能、機能拡張、ハードウェアサポート、およびドライバーの更新を確実に受け取ることができます。この変更から除外される OpenShift Container Platform 4.14 は、ライフサイクル全体にわたって RHEL 9.2 Extended Update Support (EUS) パッケージを引き続き使用する EUS リリースです。

1.3.1.2. iSCSI ブートボリュームのサポート

このリリースにより、RHCOS を Small Computer Systems Interface (iSCSI) ブートデバイスにインストールできるようになりました。iSCSI のマルチパスもサポートされています。詳細は、iSCSI ブートデバイスに RHCOS を手動でインストールする および iBFT を使用して iSCSI ブートデバイスに RHCOS をインストールする を参照してください。

1.3.1.3. Intel® Virtual RAID on CPU (VROC) を使用した RAID ストレージのサポート

このリリースでは、RHCOS を Intel® VROC RAID デバイスにインストールできるようになりました。Intel® VROC デバイスへの RAID の設定の詳細は、Intel® Virtual RAID on CPU (VROC) データボリュームの設定 を参照してください。

1.3.2. インストールおよび更新

1.3.2.1. AWS インストールで Terraform に代わって Cluster API を使用

OpenShift Container Platform 4.16 では、インストールプログラムは Terraform の代わりに Cluster API を使用して、Amazon Web Services へのインストール中にクラスターインフラストラクチャーをプロビジョニングします。この変更の結果、いくつかの追加の権限が必要になります。詳細は、IAM ユーザーに必要な AWS 権限 を参照してください。

さらに、コントロールプレーンおよびコンピュートマシンへの SSH アクセスはマシンネットワークに公開されなくなり、コントロールプレーンとコンピュートマシンに関連付けられたセキュリティーグループに制限されます。

警告

Cluster API 実装を使用した Amazon Web Services (AWS) のクラスターをシークレットまたはトップシークレットリージョンにインストールすることは、OpenShift Container Platform 4.16 のリリース時点ではテストされていません。このドキュメントは、シークレットリージョンへのインストールがテストされたときに更新されます。Network Load Balancer のシークレットまたはトップシークレットリージョンのセキュリティーグループのサポートには既知の問題があり、インストールが失敗します。詳細は、OCPBUGS-33311 を参照してください。

1.3.2.2. VMware vSphere インストールで Terraform に代わって Cluster API を使用

OpenShift Container Platform 4.16 では、インストールプログラムは、VMware vSphere へのインストール中にクラスターインフラストラクチャーをプロビジョニングするために、Terraform ではなく Cluster API を使用します。

1.3.2.3. Nutanix インストールで Terraform に代わって Cluster API を使用

OpenShift Container Platform 4.16 では、インストールプログラムは、Nutanix へのインストール中にクラスターインフラストラクチャーをプロビジョニングするために、Terraform ではなく Cluster API を使用します。

1.3.2.4. Google Cloud Platform (GCP) インストールで Terraform に代わって Cluster API を使用 (テクノロジープレビュー)

OpenShift Container Platform 4.16 では、インストールプログラムは、GCP へのインストール中にクラスターインフラストラクチャーをプロビジョニングするために、Terraform ではなく Cluster API を使用します。この機能は、OpenShift Container Platform 4.16 でテクノロジープレビューとして利用できます。テクノロジープレビュー機能を有効にするには、インストール前に **install-config.yaml** ファイルで **featureSet: TechPreviewNoUpgrade** パラメーターを設定します。別の方法として、インストールする前に以下のスタンザを **install-config.yaml** ファイルに追加して、他のテクノロジープレビュー機能なしで Cluster API インストールを有効にすることもできます。

```
featureSet: CustomNoUpgrade
featureGates:
- ClusterAPIInstall=true
```

詳細は、オプションの設定パラメーター を参照してください。

1.3.2.5. Ingress 機能

Ingress 機能は設定可能なクラスター機能となり、Red Hat HyperShift ではオプションになりました。これは設定不可能であり、スタンドアロンの OpenShift Container Platform では常に有効になっています。

警告

Ingress 機能を無効にしないでください。OpenShift Container Platform クラスターは、Ingress 機能が無効になっていると実行されません。

1.3.2.6. Assisted Installer (テクノロジープレビュー) を使用した Alibaba Cloud へのインストール

このリリースにより、OpenShift Container Platform インストールプログラムは、Alibaba Cloud プラットフォームでの installer-provisioned installation をサポートしなくなりました。現在テクノロジープレビュー機能である Assisted Installer を使用して、Alibaba Cloud にクラスターをインストールできます。詳細は、Alibaba Cloud へのインストール を参照してください。

1.3.2.7. オプションのクラウドコントローラーマネージャークラスター機能

OpenShift Container Platform 4.16 では、インストール中にクラウドコントローラーマネージャー機能を無効にできます。詳細は、クラウドコントローラーマネージャーの機能 を参照してください。

1.3.2.8. OpenShift Container Platform 4.16 における FIPS インストール要件

この更新により、FIPS 対応クラスターをインストールする場合、FIPS モードで動作するように設定された RHEL 9 コンピューターからインストールプログラムを実行し、インストールプログラムの FIPS 対応バージョンを使用する必要があります。詳細は、FIPS 暗号のサポート を参照してください。

1.3.2.9. VMware vSphere のオプションの追加タグ

OpenShift Container Platform 4.16 では、VMware vSphere クラスターによってプロビジョニングされた仮想マシン (VM) に最大 10 個のタグを追加できます。これらのタグは、クラスターが廃止された際にインストールプログラムが関連する仮想マシンを識別して削除するために使用するクラスター固有の一意のタグに加え、使用されます。

クラスターの作成時に、**install-config.yaml** ファイルで VMware vSphere 仮想マシンのタグを定義できます。詳細は、インストーラーでプロビジョニングされる VMware vSphere クラスターの **install-config.yaml** ファイルのサンプル を参照してください。

マシンセットを使用して、既存のクラスター上のコンピュートまたはコントロールプレーンマシンのタグを定義できます。詳細は、コンピュート または コントロールプレーン のマシンセットの「マシンセットを使用してマシンにタグを追加する」を参照してください。

1.3.2.10. OpenShift Container Platform 4.15 から 4.16 に更新する際に必要な管理者の承認

OpenShift Container Platform 4.16 は、いくつかの 非推奨の API が削除された Kubernetes 1.29 を使用します。

クラスター管理者は、クラスターを OpenShift Container Platform 4.15 から 4.16 に更新する前に、手動で承認を行う必要があります。これは、OpenShift Container Platform 4.16 に更新した後、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、削除された API が引き続き使用されているという問題を防ぐのに役立ちます。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 4.15 クラスターは、OpenShift Container Platform 4.16 に更新する前に、この管理者の承認が必要です。

詳細は、OpenShift Container Platform 4.16 への更新の準備 を参照してください。

1.3.2.11. コンソールに表示されないように kubeadmin パスワードを保護する

このリリースにより、クラスターの作成時に **--skip-password-print** フラグを使用することで、インストール後に **kubeadmin** パスワードがコンソールに表示されないようにすることができます。パスワードは、**auth** ディレクトリーで引き続きアクセス可能です。

1.3.2.12. OpenShift ベースの Appliance Builder (テクノロジープレビュー)

このリリースにより、OpenShift ベースの Appliance Builder 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。Appliance Builder を使用すると、自己完結型の OpenShift Container Platform クラスターのインストールが可能になります。つまり、インターネット接続や外部レジストリーに依存しません。これは、Agent-based Installer を含むディスクイメージをビルドするコンテナーベースのユーティリティーであり、これを使用して複数の OpenShift Container Platform クラスターをインストールできます。

詳細は、OpenShift ベースの Appliance Builder ユーザーガイド を参照してください。

1.3.2.13. AWS へのインストールでの Bring your own IPv4 (BYOIP) 機能の有効化

このリリースにより、**publicIpv4Pool** フィールドを使用して Elastic IP アドレス (EIP) を割り当てることで、Amazon Web Services (AWS) にインストールするときに、bring your own public IPv4 addresses (BYOIP) 機能を有効化できるようになりました。BYOIP を有効にするために 必要な権限 があることを確認する必要があります。詳細は、オプションの AWS 設定パラメーター を参照してください。

1.3.2.14. ダンマーム (サウジアラビア) とヨハネスブルグ (南アフリカ) のリージョンに GCP をデプロイする

OpenShift Container Platform 4.16 は、サウジアラビアのダンマーム (**me-central2**) リージョンと南アフリカのヨハネスブルグ (**africa-south1**) リージョンの Google Cloud Platform (GCP) にデプロイできます。詳細は、サポートされている GCP リージョン を参照してください。

1.3.2.15. Google Cloud Platform (GCP) 上の NVIDIA H100 インスタンスタイプへのインストール

このリリースにより、GCP にクラスターをインストールするときに、GPU 対応の NVIDIA H100 マシンにコンピュートノードをデプロイできます。詳細は、GCP のテスト済みインスタンスタイプ と、アクセラレーター最適化マシンファミリー に関する Google のドキュメント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. Multiarch Tuning Operator (テクノロジープレビュー) を使用したマルチアーキテクチャークラスター上のワークロードの管理

このリリースにより、Multiarch Tuning Operator を使用して、マルチアーキテクチャークラスター上のワークロードを管理できます。この Operator は、マルチアーキテクチャークラスター、およびマルチ

アーキテクチャーコンピュート設定に移行しているシングルアーキテクチャークラスター内の運用エクスペリエンスを強化します。これは、アーキテクチャーを考慮したワークロードスケジューリングをサポートするために、**ClusterPodPlacementConfig** カスタムリソース (CR) を実装します。

詳細は、Multiarch Tuning Operator を使用したマルチアーキテクチャークラスターでのワークロードの管理 を参照してください。

重要

Multiarch Tuning Operator はテクノロジープレビュー機能のみです。ネットワークシナリオが制限されたクラスターはサポートされません。

1.3.3.2. 64 ビット ARM コントロールプレーンマシンを備えたクラスターに 64 ビット x86 コンピュートマシンを追加するためのサポート

この機能は、64 ビット ARM コントロールプレーンマシンを備えたマルチアーキテクチャークラスターに 64 ビット x86 コンピュートマシンを追加するためのサポートを提供します。このリリースにより、64 ビット ARM コントロールプレーンマシンを使用し、すでに 64 ビット ARM コンピュートマシンが含まれているクラスターに、64 ビット x86 コンピュートマシンを追加できます。

1.3.3.3. 複数のペイロードを持つ Agent-based Installer クラスターのインストールのサポート

この機能は、**multi** ペイロードを持つ Agent-based Installer クラスターのインストールをサポートします。**multi** ペイロードを持つ Agent-based Installer クラスターをインストールした後、異なるアーキテクチャーのコンピュートマシンをクラスターに追加できます。

1.3.4. Web コンソール

1.3.4.1. フランス語とスペイン語の言語サポート

このリリースにより、Web コンソールでフランス語とスペイン語がサポートされるようになりました。Web コンソールの言語は、**User Preferences** ページの **Language** リストから更新できます。

1.3.4.2. Patternfly 4 は 4.16 で非推奨に

このリリースにより、Web コンソールで Patternfly 4 と React Router 5 が非推奨になりました。すべてのプラグインはできるだけ早く Patternfly 5 および React Router 6 に移行する必要があります。

1.3.4.3. 管理者パースペクティブ

このリリースでは、Web コンソールの **管理者** パースペクティブに次の更新が導入されています。

- Google Cloud Platform (GCP) トークン認可、**Auth Token GCP**、および **Configurable TLS ciphers** フィルターが OperatorHub の **インフラストラクチャー機能** フィルターに追加されました。
- **system:admin** ユーザーの偽装に関する情報が記載された新しいクイックスタート (**Impersonating the system:admin user**) が利用可能です。
- Pod の最後の終了状態を **コンテナーリスト** ページと **コンテナーの詳細** ページで表示できるようになりました。
- 適切な **RoleBinding** を検索しなくても、**Groups** および **Group details** ページから **Impersonate Group** アクションを利用できるようになりました。

1.3.4.3.1. OpenShift Container Platform Web コンソールでのノード CSR 処理

このリリースにより、OpenShift Container Platform Web コンソールはノード証明書署名要求 (CSR) をサポートします。

1.3.4.3.2. クロスストレージクラスのクローンと復元

このリリースにより、クローンまたは復元操作を完了するときに、同じプロバイダーからストレージクラスを選択できるようになりました。この柔軟性により、レプリカ数が異なるストレージクラス間でのシームレスな移行が可能になります。たとえば、レプリカが 3 つのストレージクラスからレプリカが 2/1 のストレージクラスに移動します。

1.3.4.4. Developer パースペクティブ

このリリースでは、Web コンソールの **開発者** パースペクティブに次の更新が導入されています。

- 検索時に、**Search** ページの **Resources** リストに新しいセクションが追加され、最近検索した項目が検索された順序で表示されるようになりました。
- このリリースにより、**はじめに** のセクションを折りたたんだり展開したりできるようになりました。

1.3.4.4.1. コンソール Telemetry

このリリースにより、クラスター Telemetry も有効になっている場合に匿名ユーザー分析が有効になりました。これはほとんどのクラスターのデフォルトであり、Web コンソールの使用方法に関するメトリクスを Red Hat に提供します。クラスター管理者は、各クラスターでこれを更新し、フロントエンド Telemetry をオプトイン、オプトアウト、または無効にすることができます。

1.3.5. OpenShift CLI (oc)

1.3.5.1. oc-mirror プラグイン v2 (テクノロジープレビュー)

OpenShift Container Platform の oc-mirror プラグイン v2 には、Operator イメージやその他の OpenShift Container Platform コンテンツのミラーリングプロセスを改善する新しい機能が含まれています。

以下は、oc-mirror プラグイン v2 の主な機能拡張と機能です。

- **IDMS および ITMS オブジェクトの自動生成**:
  oc-mirror プラグイン v2 は、実行ごとに **ImageDigestMirrorSet** (IDMS) および **ImageTagMirrorSet** (ITMS) オブジェクトの包括的なリストを自動的に生成します。これらのオブジェクトは、oc-mirror プラグイン v1 で使用される **ImageContentSourcePolicy** (ICSP) を置き換わるものです。この機能拡張により、Operator イメージを手動でマージおよびクリーンアップする必要がなくなり、必要なイメージがすべて含まれるようになります。
- **CatalogSource オブジェクト**:
  CatalogSource オブジェクトの作成では、プラグインが、関連するすべてのカタログインデックスの CatalogSource オブジェクトを生成するようになり、切断されたクラスターへの oc-mirror の出力アーティファクトの適用が強化されました。
- **検証の改善**:
  oc-mirror プラグイン v2 は、イメージが以前にミラーリングされたかどうかに関係なく、イメージセット設定で指定された完全なイメージセットがレジストリーにミラーリングされていることを確認します。これにより、ミラーリングは包括的かつ信頼性の高いものとなります。

- **キャッシュシステム**:
  新しいキャッシュシステムはメタデータに置き換わり、新しいイメージのみをアーカイブに組み込むことでアーカイブサイズを最小限に抑えます。これによりストレージが最適化され、パフォーマンスが向上します。

- **日付による選択ミラーリング**:
  ユーザーはミラーリングの日付に基づいてミラーリングアーカイブを生成できるようになり、新しいイメージを選択的に含めることができるようになりました。

- **強化されたイメージ削除コントロール**:
  自動プルーニングに代わって **Delete** 機能が導入され、ユーザーはイメージの削除を今まで以上に制御できるようになります。

- **registries.conf のサポート**:
  oc-mirror プラグイン v2 は、同じキャッシュを使用して複数のエンクレーブへのミラーリングを容易にする **registries.conf** ファイルをサポートしています。これにより、ミラーリングされたイメージを管理する際の柔軟性と効率性が向上します。

- **Operator バージョンのフィルタリング**:
  ユーザーはバンドル名で Operator バージョンをフィルタリングできるため、ミラーリングプロセスに含まれるバージョンをより正確に制御できます。

oc-mirror v1 と v2 の違い

oc-mirror プラグイン v2 には数多くの機能拡張が加えられていますが、oc-mirror プラグイン v1 の一部の機能は oc-mirror プラグイン v2 にはまだ含まれていません。

- Helm チャート: Helm チャートは oc-mirror プラグイン v2 には存在しません。

- **ImageSetConfig v1alpha2**: API バージョン **v1alpha2** は利用できません。ユーザーは **v2alpha1** に更新する必要があります。

- ストレージメタデータ (**storageConfig**): ストレージメタデータは、oc-mirror プラグイン v2 **ImageSetConfiguration** では使用されません。

- 自動プルーニング: oc-mirror プラグイン v2 の新しい **Delete** 機能に置き換えられました。

- リリース署名: リリース署名は、oc-mirror プラグイン v2 では生成されません。

- 一部のコマンド: **init**、**list**、**describe** コマンドは、oc-mirror プラグイン v2 では使用できません。

oc-mirror プラグイン v2 の使用

oc-mirror プラグイン v2 を使用するには、oc-mirror コマンドラインに **--v2** フラグを追加します。

oc-mirror OpenShift CLI (**oc**) プラグインは、必要なすべての OpenShift Container Platform コンテンツとその他のイメージをミラーレジストリーにミラーリングするために使用され、切断されたクラスターのメンテナンスを簡素化します。

1.3.5.2. oc adm upgrade status コマンドの導入 (テクノロジープレビュー)

以前は、**oc adm upgrade** コマンドがクラスター更新のステータスに関して提供する情報は、限定されていました。このリリースでは、**oc adm upgrade status** コマンドが追加されました。このコマンドは、**oc adm upgrade** コマンドからステータス情報を分離し、コントロールプレーンのステータスやワーカーノードの更新など、クラスターの更新に関する特定の情報を提供します。

1.3.5.3. リソースの短縮名が重複している場合の警告

このリリースにより、短縮名を使用してリソースをクエリーする場合、クラスター内に同じ短縮名を持つカスタムリソース定義 (CRD) が複数存在すると、OpenShift CLI (**oc**) から警告が返されます。

警告例

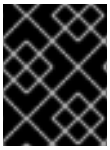
```
Warning: short name "ex" could also match lower priority resource examples.test.com
```

1.3.5.4. リソースを削除するときに確認を要求する新しいフラグ (テクノロジープレビュー)

このリリースにより、**oc delete** コマンドに新しい **--interactive** フラグが導入されました。**--interactive** フラグが **true** に設定されている場合、ユーザーが削除を確認した場合にのみリソースが削除されます。このフラグはテクノロジープレビュー機能として利用できます。

1.3.6. IBM Z と IBM LinuxONE

このリリースにより、IBM Z® および IBM® LinuxONE は OpenShift Container Platform 4.16 と互換性を持つようになりました。z/VM、LPAR、または Red Hat Enterprise Linux (RHEL) カーネルベースの仮想マシン (KVM) を使用して、インストールを実行できます。インストール手順については、IBM Z および IBM LinuxONE へのインストールの準備 を参照してください。



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 LinuxONE の主な機能拡張
OpenShift Container Platform 4.16 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。

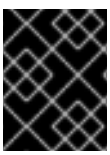
このリリースでは、IBM Z® および IBM® LinuxONE 上で次の機能がサポートされます。

- RHEL KVM の Agent-based Installer ISO ブート
- Ingress Node Firewall Operator
- LPAR 内のマルチアーキテクチャーコンピュートマシン
- z/VM および LPAR のセキュアブート

1.3.7. IBM Power

IBM Power® は OpenShift Container Platform 4.16 と互換性を持つようになりました。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。

- 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 の主な機能拡張

OpenShift Container Platform 4.16 の IBM Power® リリースでは、OpenShift Container Platform コンポーネント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。

- CPU マネージャー
- Ingress Node Firewall Operator

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

OpenShift Container Platform 4.14 以降、Extended Update Support (EUS) は IBM Power® および IBM Z® プラットフォームに拡張されています。詳細は、OpenShift EUS の概要 を参照してください。

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
Agent-based Installer	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
FIPS 暗号	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
Hosted Control Plane (テクノロジープレビュー)	サポート対象	サポート対象

機能	IBM Power®	IBM Z® および IBM® LinuxONE
IBM Secure Execution	サポート対象外	サポート対象
IBM Power® Virtual Server の installer-provisioned infrastructure の有効化	サポート対象	サポート対象外
単一ノードへのインストール	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
マルチアーキテクチャーコンピュートノード	サポート対象	サポート対象
マルチアーキテクチャーコントロールプレーン	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
Non-volatile Memory Express drives (NVMe)	サポート対象	サポート対象外
Power10 用の nx-gzip (ハードウェアアクセラレーション)	サポート対象	サポート対象外
oc-mirror プラグイン	サポート対象	サポート対象
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
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
セキュアブート	サポート対象外	サポート対象
SCTP (Stream Control Transmission Protocol)	サポート対象	サポート対象

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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
IBM Power® 上のさまざまな SMT レベルをサポートする **openshift-install** ユーティリティー (ハードウェアアクセラレーション)	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. 永続的な非共有ストレージは、iSCSI、FC などのローカルストレージを使用するか、DASD、FCP、または EDEV/FBA での LSO 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
cert-manager Operator for Red Hat OpenShift	サポート対象	サポート対象
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
Cost Management Metrics 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
HyperShift Operator	テクノロジープレビュー	テクノロジープレビュー
IBM Power® Virtual Server Block CSI Driver Operator	サポート対象	サポート対象外
Ingress Node Firewall 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 Observability Operator	サポート対象	サポート対象
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
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. 認証および認可

1.3.8.1. 既存のクラスターで Microsoft Entra Workload ID を有効にする

このリリースにより、Microsoft Entra Workload ID を有効にして、既存の Microsoft Azure OpenShift Container Platform クラスターで短期認証情報を使用できるようになりました。この機能は、OpenShift Container Platform バージョン 4.14 および 4.15 でもサポートされるようになりました。詳細は、トークンベースの認証の有効化 を参照してください。

1.3.9. ネットワーク

1.3.9.1. OpenShift SDN ネットワークプラグインが今後のメジャーアップグレードをブロックする

OpenShift Container Platform がサポートされる唯一のネットワークプラグインとして OVN-Kubernetes に移行する一環として、OpenShift Container Platform 4.16 以降では、クラスターが OpenShift SDN ネットワークプラグインを使用する場合、OVN-Kubernetes に移行せずに OpenShift Container Platform の今後のメジャーバージョンにアップグレードすることはできません。OVN-Kubernetes への移行の詳細は、OpenShift SDN ネットワークプラグインからの移行 を参照してください。

アップグレードを試みると、Cluster Network Operator は以下のステータスを報告します。

```
- lastTransitionTime: "2024-04-11T05:54:37Z"
  message: Cluster is configured with OpenShiftSDN, which is not supported in the
    next version. Please follow the documented steps to migrate from OpenShiftSDN
    to OVN-Kubernetes in order to be able to upgrade. https://docs.openshift.com/container-
platform/4.16/networking/ovn_kubernetes_network_provider/migrate-from-openshift-sdn.html
  reason: OpenShiftSDNConfigured
  status: "False"
  type: Upgradeable
```

1.3.9.2. PTP グランドマスタークロックとしてのデュアル NIC Intel E810 Westport Channel (一般提供)

デュアル Intel E810 Westport Channel ネットワークインターフェイスコントローラー (NIC) のグランドマスタークロック (T-GM) として **linuxptp** サービスを設定する機能が、OpenShift Container Platform で一般提供されました。ホストシステムクロックは、Global Navigation Satellite Systems (GNSS) タイ

ムソースに接続された NIC から同期されます。2 つ目の NIC は、GNSS に接続されている NIC によって提供される 1PPS タイミングの出力に同期されます。詳細は、linuxptp サービスをデュアル E810 Westport Channel NIC のグランドマスタークロックとして設定する を参照してください。

1.3.9.3. 高可用性システムクロックを備えたデュアル NIC Intel E810 PTP 境界クロック (一般提供)

linuxptp サービス **ptp4l** および **phc2sys** を、デュアル PTP 境界クロック (T-BC) の高可用性 (HA) システムクロックとして設定できます。

詳細は、デュアル NIC Intel E810 PTP 境界クロック用の高可用性システムクロックとして linuxptp を設定する を参照してください。

1.3.9.4. ネットワーク接続を確認するための Pod 配置の設定

クラスターコンポーネント間のネットワーク接続を定期的にテストするために、Cluster Network Operator (CNO) は **network-check-source** デプロイメントと **network-check-target** デーモンセットを作成します。OpenShift Container Platform 4.16 では、ノードセレクターを設定してノードを設定し、ソース Pod とターゲット Pod を実行してネットワーク接続を確認できます。詳細は、エンドポイントへの接続の確認 を参照してください。

1.3.9.5. 1 つのネットワークセキュリティーグループ (NSG) ルールに複数の CIDR ブロックを定義する

このリリースにより、Microsoft Azure でホストされている OpenShift Container Platform クラスターの NSG で IP アドレスと範囲がより効率的に処理されるようになりました。その結果、**allowedSourceRanges** フィールドを使用する Microsoft Azure クラスター内のすべての Ingress コントローラーの Classless Inter-Domain Routings (CIDRs) の最大制限が、約 1000 から 4000 CIDR に増加しました。

1.3.9.6. OpenShift SDN から Nutanix 上の OVN-Kubernetes への移行

このリリースにより、OpenShift SDN ネットワークプラグインから OVN-Kubernetes への移行が Nutanix プラットフォームでサポートされるようになりました。詳細は、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。

1.3.9.7. CoreDNS と Egress ファイアウォール間のインテグレーションの改善 (テクノロジープレビュー)

このリリースにより、OVN-Kubernetes は新しい **DNSNameResolver** カスタムリソースを使用して、Egress ファイアウォールルール内の DNS レコードを追跡します。これはテクノロジープレビューとして利用できます。このカスタムリソースは、ワイルドカード DNS 名と通常の DNS 名の両方の使用をサポートし、変更に関連付けられた IP アドレスに関係なく DNS 名にアクセスできるようにします。

詳細は、DNS 解決の改善とワイルドカードドメイン名の解決 を参照してください。

1.3.9.8. SR-IOV ネットワークポリシーの更新中の並列ノードドレイン

このリリースにより、ネットワークポリシーの更新中にノードを並行してドレインするように SR-IOV Network Operator を設定できるようになります。ノードを並列にドレインするオプションにより、SR-IOV ネットワーク設定の展開が高速化されます。**SriovNetworkPoolConfig** カスタムリソースを使用して、並列ノードドレインを設定し、Operator が並列ドレインできるプール内のノードの最大数を定義できます。

詳細は、SR-IOV ネットワークポリシーの更新中に並列ノードドレインを設定する を参照してください。

1.3.9.9. SR-IOV Network Operator は SriovOperatorConfig CR を自動的に作成しなくなる

OpenShift Container Platform 4.16 以降、SR-IOV Network Operator は **SriovOperatorConfig** カスタムリソース (CR) を自動的に作成しなくなりました。SR-IOV Network Operator の設定 で説明されている手順を使用して、**SriovOperatorConfig** CR を作成します。

1.3.9.10. 二重タグ付きパケット (QinQ) のサポート

このリリースにより、**QinQ support** とも呼ばれる 802.1Q-in-802.1Q が導入されました。QinQ は 2 番目の VLAN タグを導入します。ここで、サービスプロバイダーは外部タグを自社用に指定して柔軟性を提供し、内部タグは顧客の VLAN 専用のままになります。パケット内に 2 つの VLAN タグが存在する場合、外側の VLAN タグは 802.1Q または 802.1ad のいずれかになります。内部 VLAN タグは常に 802.1Q である必要があります。

詳細は、SR-IOV 対応ワークロードに対する QinQ サポートの設定 を参照してください。

1.3.9.11. オンプレミスインフラストラクチャー用のユーザー管理ロードバランサーの設定

このリリースにより、ベアメタル、VMware vSphere、Red Hat OpenStack Platform (RHOSP)、Nutanix などのオンプレミスインフラストラクチャー上で OpenShift Container Platform クラスターを設定し、デフォルトのロードバランサーの代わりにユーザー管理のロードバランサーを使用できるようになりました。この設定では、クラスターの **install-config.yaml** ファイルで **loadBalancer.type: UserManaged** を指定する必要があります。

ベアメタルインフラストラクチャーにおけるこの機能の詳細は、**OpenShift インストール環境のセットアップ** の ユーザー管理ロードバランサーのサービス を参照してください。

1.3.9.12. iptables の検出と警告

このリリースにより、クラスター内に **iptables** ルールを使用する Pod がある場合、将来的な非推奨を警告する以下のイベントメッセージが表示されます。

> This pod appears to have created one or more iptables rules. IPTables is deprecated and will no longer be available in RHEL 10 and later. You should consider migrating to another API such as nftables or eBPF.

詳細は、nftables の使用 を参照してください。サードパーティーのソフトウェアを実行している場合は、ベンダーに問い合わせて、**nftables** ベースのバージョンがすぐに利用可能になるか確認してください。

1.3.9.13. OpenShift Container Platform サービスの Ingress ネットワークフロー

このリリースでは、OpenShift Container Platform サービスの Ingress ネットワークフローを表示できます。この情報を使用して、ネットワークの Ingress トラフィックを管理し、ネットワークセキュリティーを向上させることができます。

詳細は、OpenShift Container Platform ネットワークフローマトリックス を参照してください。

1.3.9.14. 既存のデュアルスタックネットワークへのパッチ適用

このリリースにより、クラスターインフラストラクチャーにパッチを適用することで、既存のデュアルスタック設定のクラスターに API および Ingress サービス用の IPv6 仮想 IP (VIP) を追加できます。

クラスターを OpenShift Container Platform 4.16 にすでにアップグレードしていて、シングルスタッククラスターネットワークをデュアルスタッククラスターネットワークに変換する必要がある場合は、YAML 設定パッチファイルでクラスターに対して以下を指定する必要があります。

- 最初の **machineNetwork** 設定上の API および Ingress サービス用の IPv4 ネットワーク。
- 2 つ目の **machineNetwork** 設定上の API および Ingress サービス用の IPv6 ネットワーク。

詳細は、**IPv4/IPv6 デュアルスタックネットワークへの変換** の 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。

1.3.9.15. MetalLB と FRR-K8s のインテグレーション (テクノロジープレビュー)

このリリースにより、Kubernetes に準拠した方法で **FRR** API のサブセットを公開する Kubernetes ベースの **DaemonSet** である **FRR-K8s** が導入されました。クラスター管理者は、**FRRConfiguration** カスタムリソース (CR) を使用して、MetalLB Operator がバックエンドとして **FRR-K8s** デーモンセットを使用するように設定できます。これを利用して、ルートの受信などの FRR サービスを操作できます。

詳細は、MetalLB と FRR-K8s のインテグレーションの設定 を参照してください。

1.3.9.16. 外部マネージド証明書を使用したルートの作成（テクノロジープレビュー）

このリリースでは、OpenShift Container Platform ルートを、ルート API の **.spec.tls.externalCertificate** フィールドを利用してサードパーティーの証明書管理ソリューションで設定できます。これにより、シークレットを介して外部で管理される TLS 証明書を参照し、証明書の手動管理をなくしてプロセスを合理化できます。外部で管理される証明書を使用すると、エラーを減らし、よりスムーズな証明書の更新プロセスを確保し、OpenShift ルーターによる更新された証明書への迅速な提供を可能にします。詳細は、外部管理証明書を使用したルートの作成 を 参照してください。

1.3.9.17. AdminNetworkPolicy が一般公開される

この機能では、**AdminNetworkPolicy** (ANP) と **BaselineAdminNetworkPolicy** (BANP) という 2 つの新しい API が提供されます。namespace が作成される前に、クラスター管理者は ANP と BANP を使用して、クラスター全体にクラスタースコープのネットワークポリシーと保護を適用できます。ANP はクラスタースコープであるため、各 namespace でネットワークポリシーを複製することなく、ネットワークのセキュリティーを大規模に管理できるソリューションを管理者に提供します。

詳細は、**IPv4/IPv6 デュアルスタックネットワークへの変換** の 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。

1.3.9.18. OVN-Kubernetes ネットワークプラグインへのライブマイグレーション

以前は、OpenShift SDN から OVN-Kubernetes に移行する場合、利用できるオプションは **オフライン** 移行方式のみでした。このプロセスにはダウンタイムが含まれており、その間はクラスターにアクセスできませんでした。

このリリースでは、**ライブ** マイグレーション方式が導入されています。ライブマイグレーション方式は、OpenShift SDN ネットワークプラグインとそのネットワーク設定、接続、および関連リソースを、サービスを中断することなく OVN-Kubernetes ネットワークプラグインに移行するプロセスです。これは、OpenShift Container Platform、Red Hat OpenShift Dedicated、Red Hat OpenShift Service on

AWS、および Microsoft Azure Red Hat OpenShift のデプロイメントタイプで利用できます。HyperShift デプロイメントタイプでは使用できません。この移行方式は、継続的なサービス可用性を必要とするデプロイメントタイプにとって有用で、以下のような利点があります。

- 継続的なサービスの可用性
- ダウンタイムの最小化
- 自動ノード再起動
- OpenShift SDN 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シームレスな移行

OVN-Kubernetes への移行は、一方向のプロセスとなるよう意図されています。

詳細は、OVN-Kubernetes ネットワークプラグインへのライブマイグレーションの概要 を参照してください。

1.3.9.19. Whereabouts を使用したマルチテナントネットワークの IP 設定の重複

以前は、同じ CIDR 範囲を 2 回設定できず、Whereabouts CNI プラグインがこれらの範囲から IP アドレスを個別に割り当てることができませんでした。この制限により、異なるグループが重複している CIDR 範囲を選択する必要があるマルチテナント環境で問題が発生しました。

このリリースでは、Whereabouts CNI プラグインが、**network_name** パラメーターを含めることで重複する IP アドレス範囲をサポートします。管理者は、**network_name** パラメーターを使用して、個別の **NetworkAttachmentDefinitions** 内で同じ CIDR 範囲を複数回設定できます。これにより、各範囲に独立した IP アドレスの割り当てが可能になります。

この機能には、強化された namespace の処理、**IPPool** カスタムリソース (CR) の適切な namespace への保存、および Multus によって許可された場合の namespace 間のサポートも含まれています。これらの改善により、マルチテナント環境での柔軟性と管理機能が向上します。

この機能の詳細は、Whereabouts を使用した動的 IP アドレス割り当ての設定 を参照してください。

1.3.9.20. OVN-Kubernetes ネットワークプラグインの内部 IP アドレス範囲の変更のサポート

OVN-Kubernetes ネットワークプラグインを使用する場合は、transit、join、および masquerade サブネットを設定できます。transit サブネットと join サブネットは、クラスターのインストール中またはインストール後に設定できます。masquerade サブネットは、インストール時に設定する必要があります。インストール後は変更できません。サブネットのデフォルトは以下のとおりです。

- transit サブネット: **100.88.0.0/16** および **fd97::/64**
- join サブネット: **100.64.0.0/16** および **fd98::/64**
- masquerade サブネット: **169.254.169.0/29** および **fd69::/125**

これらの設定フィールドの詳細は、Cluster Network Operator 設定オブジェクト を参照してください。既存のクラスターでの transit サブネットと join サブネットの設定に関する詳細は、OVN-Kubernetes 内部 IP アドレスサブネットの設定を参照してください。

1.3.9.21. IPsec Telemetry

Telemetry および Insights Operator は IPsec 接続の Telemetry を収集します。詳細は、Telemetry によって収集されるデータの表示 を参照してください。

1.3.10. ストレージ

1.3.10.1. HashiCorp Vault が Secrets Store CSI Driver Operator で利用可能に (テクノロジープレビュー)

Secrets Store CSI Driver Operator を使用して、HashiCorp Vault から OpenShift Container Platform の Container Storage Interface (CSI) ボリュームにシークレットをマウントできるようになりました。Secrets Store CSI Driver Operator は、テクノロジープレビュー機能として利用できます。

利用可能なシークレットストアプロバイダーの完全なリストについては、シークレットストアプロバイダー を参照してください。

Secrets Store CSI Driver Operator を使用して HashiCorp Vault からシークレットをマウントする方法の詳細は、HashiCorp Vault からのシークレットのマウント を参照してください。

1.3.10.2. Microsoft Azure File でボリュームのクローン作成がサポートされる (テクノロジープレビュー)

OpenShift Container Platform 4.16 では、テクノロジープレビュー機能として、Microsoft Azure File Container Storage Interface (CSI) Driver Operator のボリュームのクローン作成機能が導入されています。ボリュームのクローン作成により、既存の永続ボリューム (PV) が複製され、OpenShift Container Platform におけるデータ損失を防ぎます。標準ボリュームを使用する場合と同じように、ボリュームクローンを使用することもできます。

詳細は、Azure File CSI Driver Operator および CSI ボリュームのクローン作成 を参照してください。

1.3.10.3. Node Expansion Secret が一般提供へ

Node Expansion Secret 機能を使用すると、ボリュームへのアクセスにノード拡張操作を実行するためのシークレット (たとえば、Storage Area Network (SAN) ファブリックにアクセスするための認証情報) が必要な場合でも、クラスターはマウントされたボリュームのストレージを拡張できます。OpenShift Container Platform 4.16 では、これは一般提供機能としてサポートされています。

1.3.10.4. vSphere CSI のスナップショットの最大数の変更が一般提供へ

VMware vSphere Container Storage Interface (CSI) のスナップショットのデフォルトの最大数は、ボリュームあたり 3 です。OpenShift Container Platform 4.16 では、スナップショットの最大数をボリュームあたり最大 32 に変更できるようになりました。また、vSAN および仮想ボリュームデータストアのスナップショットの最大数を細かく制御することもできます。OpenShift Container Platform 4.16 では、これは一般提供機能としてサポートされています。

詳細は、vSphere のスナップショットの最大数の変更 を参照してください。

1.3.10.5. 永続ボリュームの最終フェーズ遷移時間パラメーター (テクノロジープレビュー)

OpenShift Container Platform 4.16 では、永続ボリューム (PV) が別のフェーズ (**pv.Status.Phase**) に移行するたびに更新されるタイムスタンプを持つ新しいパラメーター **LastPhaseTransitionTime** が導入されました。この機能はテクノロジープレビューのステータスでリリースされています。

1.3.10.6. CIFS/SMB CSI Driver Operator を使用した永続ストレージ (テクノロジープレビュー)

OpenShift Container Platform は、Common Internet File System (CIFS) ダイアレクト/Server Message Block (SMB) プロトコル用の 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。このドライバーを管理する CIFS/SMB CSI Driver Operator は、テクノロジープレビューのステータスです。

詳細は、CIFS/SMB CSI Driver Operator を参照してください。

1.3.10.7. SELinux コンテキストマウントを備えた RWOP が一般提供へ

OpenShift Container Platform 4.14 では、永続ボリューム (PV) と永続ボリューム要求 (PVC) 用のテクニカルプレビューステータスの新しいアクセスモードである ReadWriteOncePod (RWOP) が導入されました。既存の ReadWriteOnce アクセスモードでは、PV または PVC をシングルノード上の複数の Pod で使用できますが、RWOP はシングルノード上の単一 Pod でのみ使用できます。ドライバーにより有効化されている場合、RWOP は **PodSpec** またはコンテナーに設定されている SELinux コンテキストマウントを使用します。これにより、ドライバーは正しい SELinux ラベルを使用してボリュームを直接マウントできます。これにより、ボリュームを再帰的に再ラベルする必要がなくなり、Pod の起動が大幅に高速化されます。

OpenShift Container Platform 4.16 では、この機能が一般提供されています。

詳細は、アクセスモード を参照してください。

1.3.10.8. vSphere CSI Driver 3.1 で CSI トポロジー要件が更新される

マルチゾーンクラスターでの VMware vSphere Container Storage Interface (CSI) ボリュームのプロビジョニングと使用をサポートするには、デプロイメントが CSI ドライバーによって課される特定の要件に一致している必要があります。これらの要件は 3.1.0 以降に変更されており、OpenShift Container Platform 4.16 は古いタグ付け方法と新しいタグ付け方法の両方を受け入れますが、VMware vSphere は古いタグ付け方法を無効な設定と見なすため、新しいタグ付け方法を使用する必要があります。問題を防ぐために、古いタグ付け方法は使用しないでください。

詳細は、vSphere CSI トポロジーの要件 を参照してください。

1.3.10.9. シックプロビジョニングされたストレージ設定のサポート

この機能は、シックプロビジョニングされたストレージの設定をサポートします。**LVMCluster** カスタムリソース (CR) で **deviceClasses.thinPoolConfig** フィールドを除外すると、論理ボリュームはシックプロビジョニングされます。シックプロビジョニングされたストレージを使用する場合、次の制限があります。

- ボリュームのクローン作成ではコピーオンライトはサポートされません。
- **VolumeSnapshotClass** はサポートされていません。したがって、CSI スナップショットはサポートされていません。
- オーバープロビジョニングはサポートされていません。その結果、PersistentVolumeClaims (PVC) のプロビジョニングされた容量がボリュームグループからすぐに削減されます。
- シンメトリクスはサポートされていません。シックプロビジョニングされたデバイスは、ボリュームグループメトリクスのみをサポートします。

LVMCluster CR の設定に関する詳細は、LVMCluster カスタムリソースについて を参照してください。

1.3.10.10. LVMCluster カスタムリソースでデバイスセレクターが設定されていない場合の新しい警告メッセージのサポート

この更新により、**LVMCluster** カスタムリソース (CR) で **deviceSelector** フィールドを設定していない場合に、新しい警告メッセージが表示されるようになります。

LVMCluster CR は、**deviceSelector** フィールドが設定されているかを示す新しいフィールド **deviceDiscoveryPolicy** をサポートします。**deviceSelector** フィールドを設定しない場合、LVM Storage は **deviceDiscoveryPolicy** フィールドを **RuntimeDynamic** に自動的に設定します。それ以外の場合、**deviceDiscoveryPolicy** フィールドは **Preconfigured** に設定されます。

LMVCluster CR から **deviceSelector** フィールドを除外することは推奨されません。**deviceSelector** フィールドを設定しない場合の制限の詳細は、ボリュームグループへのデバイスの追加について を参照してください。

1.3.10.11. ボリュームグループへの暗号化デバイスの追加をサポート

この機能は、暗号化されたデバイスをボリュームグループに追加するためのサポートを提供します。OpenShift Container Platform のインストール中に、クラスターノードでディスク暗号化を有効にすることができます。デバイスを暗号化した後、**LVMCluster** カスタムリソースの **deviceSelector** フィールドで LUKS 暗号化デバイスへのパスを指定できます。ディスク暗号化の詳細は、ディスク暗号化について および ディスク暗号化とミラーリングの設定 を参照してください。

ボリュームグループへのデバイスの追加に関する詳細は、ボリュームグループへのデバイスの追加について を参照してください。

1.3.11. Operator ライフサイクル

1.3.11.1. Operator API の名前が ClusterExtension (テクノロジープレビュー) に変更される

Operator Lifecycle Manager (OLM) 1.0 の以前のテクノロジープレビューフェーズでは、Operator Controller コンポーネントによって **operator.operators.operatorframework.io** として提供される新しい **Operator** API が導入されました。OpenShift Container Platform 4.16 では、この API の名前は **ClusterExtension** に変更され、OLM 1.0 のこのテクノロジープレビューフェーズでは **clusterextension.olm.operatorframework.io** として提供されます。

この API は、ユーザー向け API を単一のオブジェクトに統合することで、**registry+v1** バンドル形式を介した Operator を含むインストール済みエクステンションの管理を効率化します。**ClusterExtension** へ名前を変更することで、以下に対応します。

- クラスターの機能を拡張する簡素化された機能をより正確に反映する
- より柔軟なパッケージ形式をより良く表現する
- **Cluster** の接頭辞が **ClusterExtension** オブジェクトがクラススコープであることを明確に示す。これは、Operator が namespace スコープまたはクラススコープのいずれかになる可能性がある従来の OLM からの変更です。

詳細は、Operator Controller を参照してください。

重要

現在、OLM 1.0 は次の基準を満たす拡張機能のインストールをサポートしています。

- 拡張機能では **AllNamespaces** インストールモードを使用する必要があります。
- 拡張機能では Webhook を使用しないでください。

Webhook を使用するクラスター拡張機能、または単一または指定された namespace のセットを対象とするクラスター拡張機能はインストールできません。

1.3.11.2. Operator Lifecycle Manager (OLM) 1.0 (テクノロジープレビュー) のクラスターエクステンションのステータス条件メッセージと非推奨通知が改善される

このリリースにより、OLM 1.0 はインストールされたクラスターエクステンションに対して、次のステータス条件メッセージを表示します。

- 特定のバンドル名
- インストール済みバージョン
- 健全性レポートの改善
- パッケージ、チャネル、バンドルの非推奨通知

1.3.11.3. OLM 1.0 でのレガシー OLM アップグレードエッジのサポート (テクノロジープレビュー)

インストールされたクラスター拡張機能のアップグレードエッジを決定する場合、Operator Lifecycle Manager (OLM) 1.0 は、OpenShift Container Platform 4.16 以降、従来の OLM セマンティックをサポートします。このサポートは、**replaces**、**skips**、**skipRange** ディレクティブなど、従来の OLM の動作に従いますが、いくつかの違いがあります。

従来の OLM セマンティックをサポートすることで、OLM 1.0 はカタログからのアップグレードグラフを正確に認識するようになりました。

注記

セマンティックバージョン (semver) のアップグレード制約のサポートは OpenShift Container Platform 4.15 で導入されましたが、このテクノロジープレビューフェーズでは従来の OLM セマンティクスを優先するため 4.16 では無効になっています。

詳細は、アップグレード制約セマンティクス を参照してください。

1.3.12. ビルド

認証されていないユーザーが system:webhook ロールバインディングから削除される
このリリースにより、認証されていないユーザーは **system:webhook** ロールバインディングにアクセスできなくなります。OpenShift Container Platform 4.16 より前では、認証されていないユーザーが **system:webhook** ロールバインディングにアクセスできました。認証されていないユーザーのアクセスを変更することで、セキュリティーの層が追加されます。ユーザーは必要な場合にのみ、これを有効にする必要があります。この変更は新しいクラスターに対するものであり、以前のクラスターには影響しません。

認証されていないユーザーに特定の namespace の **system:webhook** ロールバインディングを許可する

ことが推奨されるユースケースがあります。**system:webhook** クラスターロールを使用すると、ユーザーは GitHub、GitLab、Bitbucket などの OpenShift Container Platform 認証メカニズムを使用しない外部システムからビルドをトリガーできます。クラスター管理者は、このユースケースを容易にするために、認証されていないユーザーに **system:webhook** ロールバインディングへのアクセスを許可できます。

重要

認証されていないアクセスを変更するときは、常に組織のセキュリティー標準に準拠していることを確認してください。

認証されていないユーザーに、特定の namespace の **system:webhook** ロールバインディングへのアクセスを許可するには、認証されていないユーザーを system:webhook ロールバインディングに追加する を参照してください。

1.3.13. Machine Config Operator

1.3.13.1. 未使用のレンダリングされたマシン設定のガベージコレクション

このリリースにより、未使用のレンダリングされたマシン設定をガベージコレクションできるようになりました。**oc adm prune renderedmachineconfigs** コマンドを使用すると、未使用のレンダリングされたマシン設定を表示し、削除するものを決定してから、不要になったレンダリングされたマシン設定を一括削除できます。マシン設定が多すぎると、マシン設定の操作が混乱する可能性があり、ディスク容量やパフォーマンスの問題の原因にもなります。詳細は、未使用のレンダリングされたマシン設定の管理 を参照してください。

1.3.13.2. ノード中断ポリシー (テクノロジープレビュー)

デフォルトでは、**MachineConfig** オブジェクトのパラメーターに特定の変更を加えると、Machine Config Operator (MCO) は、そのマシン設定に関連付けられているノードをドレインして再起動します。ただし、ワークロードの中断をほとんどまたはまったく必要としない Ignition 設定オブジェクトの一連の変更を定義するノード中断ポリシーを MCO namespace に作成できます。詳細は、ノード中断ポリシーを使用してマシン設定の変更による中断を最小限に抑える を参照してください。

1.3.13.3. クラスター上の RHCOS イメージのレイヤー化 (テクノロジープレビュー)

Red Hat Enterprise Linux CoreOS (RHCOS) イメージのレイヤー化により、テクノロジープレビュー機能として、カスタムレイヤー化イメージをクラスター内に直接自動的にビルドできるようになりました。以前は、クラスターの外部でカスタムレイヤーイメージをビルドし、そのイメージをクラスターにプルする必要がありました。イメージレイヤー機能を使用して、ベースイメージに追加のイメージをレイヤー化することで、ベース RHCOS イメージの機能を拡張できます。詳細は、RHCOS イメージのレイヤー化 を参照してください。

1.3.13.4. ブートイメージの更新 (テクノロジープレビュー)

デフォルトでは、MCO は Red Hat Enterprise Linux CoreOS (RHCOS) ノードを起動するために使用するブートイメージを削除しません。その結果、クラスター内のブートイメージはクラスターとともに更新されません。クラスターを更新するたびにブートイメージも更新するようにクラスターを設定できるようになりました。詳細は、ブートイメージの更新 を参照してください。

1.3.14. マシン管理

1.3.14.1. クラスターオートスケーラーのエクスパンダーの設定

このリリースにより、クラスターオートスケーラーは **LeastWaste**、**Priority**、および **Random** エクスパンダーを使用できるようになりました。これらのエクスパンダーを設定して、クラスターをスケーリングするときにマシンセットの選択に影響を与えることができます。詳細は、クラスターオートスケーラーの設定 を参照してください。

1.3.14.2. VMware vSphere の Cluster API を使用したマシンの管理 (テクノロジープレビュー)

このリリースにより、VMware vSphere クラスターのテクノロジープレビューとして、OpenShift Container Platform に統合されたアップストリーム Cluster API を使用してマシンを管理する機能が導入されました。この機能は、Machine API を使用してマシンを管理するための追加または代替の機能になります。詳細は、Cluster API について を参照してください。

1.3.14.3. コントロールプレーンマシンセットの vSphere 障害ドメインの定義

このリリースでは、コントロールプレーンマシンセットの vSphere 障害ドメインを定義する、以前はテクノロジープレビューだった機能が一般提供されました。詳細は、VMware vSphere のコントロールプレーン設定オプション を参照してください。

1.3.15. ノード

1.3.15.1. Vertical Pod Autoscaler Operator Pod の移動

Vertical Pod Autoscaler Operator (VPA) は、レコメンダー、アップデーター、アドミッションコントローラーの 3 つのコンポーネントで設定されます。Operator と各コンポーネントには、コントロールプレーンノードの VPA namespace に独自の Pod があります。VPA Operator とコンポーネント Pod をインフラストラクチャーノードまたはワーカーノードに移動できます。詳細は、Vertical Pod Autoscaler Operator コンポーネントの移動 を参照してください。

1.3.15.2. must-gather によって収集された追加情報

このリリースにより、**oc adm must-gather** コマンドによって以下の追加情報が収集されます。

- OpenShift CLI (**oc**) バイナリーバージョン
- must-gather ログ

これらの追加は、特定のバージョンの **oc** の使用から生じる可能性のある問題を特定するのに役立ちます。**oc adm must-gather** コマンドは、使用されたイメージと、must-gather ログに収集できなかったデータがあるかどうかもリスト表示します。

詳細は、must-gather ツールについて を参照してください。

1.3.15.3. BareMetalHost リソースの編集

OpenShift Container Platform 4.16 以降では、ベアメタルノードの **BareMetalHost** リソースでベースボード管理コントローラー (BMC) アドレスを編集できます。ノードは **Provisioned**、**ExternallyProvisioned**、**Registering**、または **Available** 状態である必要があります。**BareMetalHost** リソースの BMC アドレスを編集しても、ノードのプロビジョニングは解除されません。詳細は、BareMetalHost リソースの編集 を参照してください。

1.3.15.4. ブータブルでない ISO のアタッチ

OpenShift Container Platform 4.16 以降では、**DataImage** リソースを使用して、プロビジョニングされたノードに汎用のブータブルでない ISO 仮想メディアイメージをアタッチできます。リソースを適用す

ると、次回の再起動時にオペレーティングシステムから ISO イメージにアクセスできるようになります。この機能をサポートするために、ノードが Redfish またはそれから派生したドライバーを使用している。ノードが **Provisioned** または **ExternallyProvisioned** 状態である。詳細は、ブータブルでない ISO をベアメタルノードにアタッチする を参照してください。

1.3.16. モニタリング

このリリースのクラスター内モニタリングスタックには、以下の新機能および修正された機能が含まれます。

1.3.16.1. 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

このリリースには、クラスター内モニタリングスタックコンポーネントと依存関係に関する以下のバージョン更新が含まれています。

- kube-state-metrics が 2.12.0 へ
- Metrics Server が 0.7.1 へ
- node-exporter が 1.8.0 へ
- Prometheus が 2.52.0 へ
- Prometheus Operator が 0.73.2 へ
- Thanos が 0.35.0 へ

1.3.16.2. 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。

- Cluster Monitoring Operator 設定が非推奨のフィールドを使用する際に監視するための **ClusterMonitoringOperatorDeprecatedConfig** アラートを追加しました。
- Prometheus Operator がオブジェクトステータスの更新に失敗した際に監視するための **PrometheusOperatorStatusUpdateErrors** アラートを追加しました。

1.3.16.3. Metrics API の一般提供 (GA) にアクセスするための Metrics Server コンポーネント (テクノロジープレビュー)

Metrics Server コンポーネントが一般提供され、非推奨の Prometheus Adapter の代わりに自動的にインストールされるようになりました。Metrics Server はリソースメトリクスを収集し、他のツールや API が使用できるように **metrics.k8s.io** Metrics API サービスで公開します。これにより、コアプラットフォーム Prometheus スタックがこの機能の処理から解放されます。詳細は、Cluster Monitoring Operator の config map API 参照のMetricsServerConfig を参照してください。

1.3.16.4. Alertmanager API への読み取り専用アクセスを許可する新しいモニタリングロール

このリリースでは、**openshift-monitoring** プロジェクトの Alertmanager API への読み取り専用アクセスを許可する新しい **monitoring-alertmanager-view** ロールが導入されました。

1.3.16.5. VPA メトリクスが kube-state-metrics エージェントで利用可能に

Vertical Pod Autoscaler (VPA) メトリクスが、**kube-state-metrics** エージェントを通じて利用可能になりました。VPA メトリクスは、非推奨後にネイティブサポートアップストリームから削除された前と同様の説明形式に従います。

1.3.16.6. コンポーネントを監視するためのプロキシーサービスの変更

このリリースでは、Prometheus、Alertmanager、Thanos Ruler の前のプロキシーサービスが OAuth から **kube-rbac-proxy** に更新されました。この変更は、適切なロールとクラスターロールを持たずにこれらの API エンドポイントにアクセスするサービスアカウントとユーザーに影響する可能性があります。

1.3.16.7. Prometheus が重複サンプルを処理する方法の変更

このリリースでは、Prometheus がターゲットをスクレイピングするときに、同じ値であっても重複したサンプルがサイレントに無視されなくなりました。最初のサンプルが受け入れられ、**prometheus_target_scrapes_sample_duplicate_timestamp_total** カウンターが増加し、これにより、**PrometheusDuplicateTimestamps** アラートがトリガーされる可能性があります。

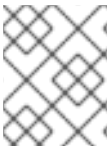
1.3.17. Network Observability Operator

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 を参照してください。

1.3.18. スケーラビリティーおよびパフォーマンス

1.3.18.1. ワークロードパーティショニングの強化

このリリースにより、CPU 制限と CPU リクエストの両方を含むワークロードアノテーションを使用してデプロイされたプラットフォーム Pod では、CPU 制限が正確に計算され、特定の Pod の CPU クォータとして適用されます。以前のリリースでは、ワークロードパーティショニングされた Pod に CPU 制限とリクエストの両方が設定されていた場合、それらは Webhook によって無視されていました。Pod はワークロードパーティショニングのメリットを享受できず、特定のコアにロックダウンされませんでした。この更新により、リクエストと制限が Webhook によって正しく解釈されるようになりました。



注記

CPU 制限の値がアノテーション内のリクエストの値と異なる場合、CPU 制限はリクエストと同じものと見なされることが想定されています。

詳細は、ワークロードのパーティショニング を参照してください。

1.3.18.2. Linux Control Groups バージョン 2 がパフォーマンスプロファイル機能でサポートされるようになる

OpenShift Container Platform 4.16 以降では、パフォーマンスプロファイルが存在する場合でも、すべての新しいデプロイメントで、Control Groups バージョン 2 (cgroup v2) (cgroup2 または cgroupsv2 とも呼ばれる) がデフォルトで有効になっています。

OpenShift Container Platform 4.14 以降、cgroups v2 がデフォルトになりましたが、パフォーマンスプロファイル機能では cgroups v1 を使用する必要がありました。この問題は解決されています。

cgroup v1 は、最初のインストール日が OpenShift Container Platform 4.16 より前のパフォーマンスプロファイルを持つアップグレードされたクラスターで引き続き使用されます。**node.config** オブジェクトの **cgroupMode** フィールドを **v1** に変更することで、cgroup v1 を現在のバージョンで引き続き使用できます。

詳細は、ノードでの Linux cgroup バージョンの設定 を参照してください。

1.3.18.3. etcd データベースのサイズを増やすためのサポート (テクノロジープレビュー)

このリリースにより、etcd のディスククォータを増やすことができます。これはテクノロジープレビューの機能です。詳細は、etcd のデータベースサイズの増加 を参照してください。

1.3.18.4. 予約コア周波数のチューニング

このリリースでは、Node Tuning Operator は、予約済みおよび分離されたコア CPU の **PerformanceProfile** で CPU 周波数の設定をサポートします。これは、特定の周波数を定義するために使用できるオプションの機能です。次に、Node Tuning Operator は Intel ハードウェアの **intel_pstate** CPUFreq ドライバーを有効にして、これらの周波数を設定します。FlexRAN のようなアプリケーションの周波数については、Intel の推奨事項に従う必要があります。このようなアプリケーションでは、デフォルトの CPU 周波数をデフォルトの実行周波数よりも低い値に設定する必要があります。

1.3.18.5. Node Tuning Operator intel_pstate ドライバーのデフォルト設定

以前は、RAN DU プロファイルの場合、**PerformanceProfile** で **realTime** ワークロードヒントを **true** に設定すると、常に **intel_pstate** が無効になりました。このリリースでは、Node Tuning Operator は **TuneD** を使用して基盤となる Intel ハードウェアを検出し、プロセッサーの世代に基づいて **intel_pstate** カーネルパラメーターを適切に設定します。これにより、**intel_pstate** が **realTime** および **highPowerConsumption** ワークロードヒントから切り離されます。**intel_pstate** は、基盤となるプロセッサーの世代のみに依存するようになりました。

IceLake 以前のプロセッサーの場合、**intel_pstate** はデフォルトで非アクティブ化されていますが、IceLake 以降の世代のプロセッサーの場合は、**intel_pstate** は **active** に設定されています。

1.3.19. エッジコンピューティング

1.3.19.1. RHACM PolicyGenerator リソースを使用して GitOps ZTP クラスターポリシーを管理する (テクノロジープレビュー)

PolicyGenerator リソースと Red Hat Advanced Cluster Management (RHACM) を使用して、GitOps ZTP でマネージドクラスターのポリシーをデプロイできるようになりました。**PolicyGenerator** API は Open Cluster Management 標準の一部であり、**PolicyGenTemplate** API では不可能なリソースへパッチを適用する一般的な方法を提供します。**PolicyGenTemplate** リソースを使用してポリシーを管理およびデプロイすることは、今後の OpenShift Container Platform リリースでは非推奨になります。

詳細は、PolicyGenerator リソースを使用したマネージドクラスターポリシーの設定 を参照してください。

注記

PolicyGenerator API は現在、アイテムのリストを含むカスタム Kubernetes リソースとのパッチのマージをサポートしていません。たとえば、**PtpConfig** CR の場合などです。

1.3.19.2. TALM ポリシーの修正

このリリースにより、Topology Aware Lifecycle Manager (TALM) は Red Hat Advanced Cluster Management (RHACM) 機能を使用して、マネージドクラスターの **inform** ポリシーを修復します。この機能拡張により、ポリシーの修復中に Operator が **inform** ポリシーの **enforce** コピーを作成する必要がなくなります。この機能拡張により、コピーされたポリシーによるハブクラスターのワークロードも軽減され、マネージドクラスターのポリシーの修復に必要な全体的な時間も短縮されます。

詳細は、マネージドクラスターのポリシーの更新 を参照してください。

1.3.19.3. GitOps ZTP の高速プロビジョニング (テクノロジープレビュー)

このリリースにより、シングルノード OpenShift の GitOps ZTP の高速プロビジョニングを使用することで、クラスターのインストールにかかる時間を短縮できます。高速 ZTP は、ポリシーから派生した Day 2 マニフェストを早い段階で適用することで、インストールを高速化します。

GitOps ZTP の高速プロビジョニングの利点は、デプロイメントの規模に応じて増大します。完全なアクセラレーションは、クラスターの数が多いほど、より大きなメリットをもたらします。クラスターの数が少ない場合、インストール時間の短縮はそれほど大きくありません。

詳細は、GitOps ZTP の高速プロビジョニング を参照してください。

1.3.19.4. Lifecycle Agent を使用したシングルノード OpenShift クラスターのイメージベースアップグレード

このリリースでは、Lifecycle Agent を使用して、シングルノード OpenShift クラスターの OpenShift Container Platform <4.y> から <4.y+2>、および <4.yz> から <4.y.z+n> へのイメージベースアップグレードをオーケストレーションできます。Lifecycle Agent は、参加するクラスターの設定に一致する Open Container Initiative (OCI) イメージを生成します。OCI イメージに加えて、イメージベースアップグレードでは、**ostree** ライブラリーと OADP Operator を使用して、元のプラットフォームバージョンとターゲットプラットフォームバージョン間の移行時にアップグレードとサービスの停止時間を短縮します。

詳細は、シングルノード OpenShift クラスターのイメージベースのアップグレードについて を参照してください。

1.3.19.5. GitOps ZTP と RHACM を使用してマネージドクラスターに IPsec 暗号化をデプロイする (テクノロジープレビュー)

GitOps ZTP と Red Hat Advanced Cluster Management (RHACM) を使用してデプロイするマネージドシングルノード OpenShift クラスターで IPsec 暗号化を有効化できるようになりました。マネージドクラスターの外部にある Pod と IPsec エンドポイント間の外部トラフィックを暗号化できます。OVN-Kubernetes クラスターネットワーク上のノード間のすべての Pod 間ネットワークトラフィックが、Transport モードの IPsec で暗号化されます。

詳細は、GitOps ZTP および SiteConfig リソースを使用したシングルノード OpenShift クラスターの IPsec 暗号化の設定 を参照してください。

1.3.20. セキュリティー

新しい署名者認証局 (CA) である **openshift-etcd** が、証明書の署名用として利用できるようになりました。この CA は、既存の CA とのトラストバンドルに含まれています。2 つの CA シークレット (**etcd-signer** および **etcd-metric-signer**) もローテーションに使用できます。このリリース以降、すべての証

明書は実証済みのライブラリーに移行します。この変更により、**cluster-etcd-operator** によって管理されていなかったすべての証明書の自動ローテーションが可能になります。すべてのノードベースの証明書は現在の更新プロセスを続行します。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.16 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。

HAProxy バージョン 2.8
OpenShift Container Platform 4.16 は HAProxy 2.8 を使用します。

SHA-1 証明書が HAProxy での使用でサポートされなくなる
SHA-1 証明書は HAProxy での使用がサポートされなくなりました。OpenShift Container Platform 4.16 で SHA-1 証明書を使用する既存のルートと新しいルートの両方が拒否され、機能しなくなります。安全なルートの作成の詳細は、セキュリティー保護されたルート を参照してください。

etcd チューニングパラメーター
このリリースにより、etcd チューニングパラメーターを、次のようにパフォーマンスを最適化し、レイテンシーを短縮する値に設定できるようになりました。

- **""** (デフォルト)
- **Standard (標準)**
- **Slower**

認証されていないユーザーが一部のクラスターロールから削除される
このリリースにより、認証されていないユーザーは、特定の機能セットに必要な特定のクラスターロールにアクセスできなくなります。OpenShift Container Platform 4.16 より前では、認証されていないユーザーが特定のクラスターロールにアクセスできました。認証されていないユーザーに対するこのアクセスを変更すると、セキュリティーの層が追加されるため、必要な場合にのみ有効にする必要があります。この変更は新しいクラスターに対するものであり、以前のクラスターには影響しません。

認証されていないユーザーに対して、特定のクラスターロールのアクセス権の付与を推奨するユースケースがあります。認証されていないユーザーに、特定の機能に必要な特定のクラスターロールへのアクセスを付与するには、認証されていないグループをクラスターロールに追加する を参照してください。

重要

認証されていないアクセスを変更するときは、常に組織のセキュリティー標準に準拠していることを確認してください。

RHCOS dasd イメージアーティファクトは、IBM Z(R) および IBM(R) LinuxONE (s390x) ではサポートされなくなりました。
このリリースにより、**s390x** アーキテクチャーの **dasd** イメージアーティファクトが OpenShift Container Platform イメージビルドパイプラインから削除されます。同一の、同じ機能を備えた **metal4k** イメージアーティファクトを引き続き使用できます。

ExternalTrafficPolicy=Local サービスに設定された EgressIP のサポート
以前は、EgressIP が選択された Pod が、**externalTrafficPolicy** が **Local** に設定されたサービスのバックエンドとしても機能することはサポートされていませんでした。この設定を試みると、Pod に到達するサービス Ingress トラフィックが、EgressIP をホストする Egress ノードに誤って再ルーティングさ

れました。これは、着信サービストラフィック接続への応答の処理方法に影響し、**externalTrafficPolicy** が **Local** に設定されている場合に接続が切断され、サービスが利用できなくなったため、サービスが機能しなくなりました。

OpenShift Container Platform 4.16 では、OVN-Kubernetes は、選択された同じ Pod セットで、**ExternalTrafficPolicy=Local** サービスと EgressIP 設定を同時に使用できるようになりました。OVN-Kubernetes は、EgressIP Pod から発信されたトラフィックのみを Egress ノードに再ルーティングし、EgressIP Pod からの Ingress サービストラフィックへの応答を、Pod が配置されている同じノード経由でルーティングするようになりました。

従来のサービスアカウント API トークンシークレットは、サービスアカウントごとに生成されなくなりました。
OpenShift Container Platform 4.16 より前では、統合された OpenShift イメージレジストリーが有効になっているときに、クラスター内のすべてのサービスアカウントに対してレガシーサービスアカウント API トークンシークレットが生成されました。OpenShift Container Platform 4.16 以降では、統合された OpenShift イメージレジストリーが有効になっている場合、各サービスアカウントに対して従来のサービスアカウント API トークンシークレットが生成されなくなります。

さらに、統合された OpenShift イメージレジストリーが有効になっている場合、すべてのサービスアカウントに対して生成されるイメージプルシークレットは、従来のサービスアカウント API トークンを使用しなくなります。代わりに、イメージプルシークレットは、期限が切れる前に自動的に更新されるバインドされたサービスアカウントトークンを使用するようになりました。

詳細は、自動的に生成されたイメージプルシークレット を参照してください。

クラスターで使用されている従来のサービスアカウント API トークンシークレットを検出する方法、または不要な場合にそれらを削除する方法については、Red Hat ナレッジベースのアーティクル記事 Long-lived service account API tokens in OpenShift Container Platform を参照してください。

外部クラウド認証プロバイダーのサポート
このリリースでは、Amazon Web Services (AWS)、Google Cloud Platform (GCP)、および Microsoft Azure クラスター上のプライベートレジストリーへの認証機能が、ツリー内プロバイダーから OpenShift Container Platform に同梱されるバイナリーに移動されました。この変更は、Kubernetes 1.29 で導入されたデフォルトの外部クラウド認証プロバイダーの動作をサポートします。

Build クラスター機能が無効な場合、builder サービスアカウントが作成されなくなる
このリリースにより、**Build** クラスター機能を無効にすると、**builder** サービスアカウントとそれに対応するシークレットは作成されなくなります。

詳細は、ビルド機能 を参照してください。

デフォルトの OLM 1.0 アップグレード制約が従来の OLM セマンティクスに変更される (テクノロジープレビュー)
OpenShift Container Platform 4.16 では、Operator Lifecycle Manager (OLM) 1.0 のデフォルトのアップグレード制約がセマンティックバージョン管理 (semver) から従来の OLM セマンティクスに変更されます。

詳細は、OLM 1.0 でのレガシー OLM アップグレードエッジのサポート (テクノロジープレビュー) を参照してください。

OLM 1.0 からの RukPak Bundle API の削除 (テクノロジープレビュー)
OpenShift Container Platform 4.16 では、Operator Lifecycle Manager (OLM) 1.0 によって、RukPak コンポーネントによって提供されていた **Bundle** API が削除されます。RukPak **BundleDeployment** API はそのまま残っており、従来の Operator Lifecycle Manager (OLM) バンドル形式で編成された Kubernetes YAML マニフェストを展開するための **registry+v1** バンドルをサポートしています。

詳細は、Rukpak (テクノロジープレビュー) を参照してください。

dal12 リージョンの追加
このリリースにより、**dal12** リージョンが IBM Power® VS インストーラーに追加されました。

IBM Power (R) Virtual Server に追加されたリージョン
このリリースにより、新しい IBM Power® Virtual Server (VS) リージョン **osa21**、**syd04**、**lon06**、および **sao01** にデプロイする機能が導入されました。

IBM Power (R) Virtual Server クラスター API が 0.8.0 に更新されました
このリリースでは、IBM Power® VS CAPI がバージョン 0.8.0 に更新されました。

ServiceInstanceNameToGUID の追加デバッグステートメント
このリリースでは、**ServiceInstanceNameToGUID** 関数にデバッグステートメントが追加されました。

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 4.16 内で非推奨化および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**
- **削除済み**

Operator のライフサイクルと開発の非推奨および削除された機能

表1.6 Operator のライフサイクルと開発の非推奨および削除されたトラッカー

機能	4.14	4.15	4.16
Operator SDK	一般公開 (GA)	一般公開 (GA)	非推奨
Ansible ベースの Operator プロジェクト用のスキャフォールディングツール	一般公開 (GA)	一般公開 (GA)	非推奨
Helm ベースの Operator プロジェクト用のスキャフォールディングツール	一般公開 (GA)	一般公開 (GA)	非推奨
Go ベースの Operator プロジェクト用のスキャフォールディングツール	一般公開 (GA)	一般公開 (GA)	非推奨

機能	4.14	4.15	4.16
ハイブリッド Helm ベースの Operator プロジェクト用のスキャフォールディングツール	テクノロジープレビュー	テクノロジープレビュー	非推奨
Java ベースの Operator プロジェクト用のスキャフォールディングツール	テクノロジープレビュー	テクノロジープレビュー	非推奨
Platform Operator	テクノロジープレビュー	テクノロジープレビュー	削除済み
プレーンバンドル	テクノロジープレビュー	テクノロジープレビュー	削除済み
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 クラスターサンプル Operator が廃止され、トラッカーが削除される

機能	4.14	4.15	4.16
Cluster Samples Operator	一般公開 (GA)	一般公開 (GA)	非推奨

非推奨および削除された機能の監視

表1.8 非推奨および削除されたトラッカーのモニタリング

機能	4.14	4.15	4.16
コアプラットフォームモニタリング用の専用サービスモニターを有効にする **dedicatedServiceMonitors** 設定	一般公開 (GA)	非推奨	削除済み
Prometheus からリソースメトリクスを照会し、メトリクス API で公開する **prometheus-adapter** コンポーネント	一般公開 (GA)	非推奨	削除済み

インストールの非推奨および削除された機能

表1.9 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	4.14	4.15	4.16
OpenShift SDN ネットワークプラグイン	非推奨	削除済み [1]	削除済み

機能	4.14	4.15	4.16
oc adm release extract の **--cloud** パラメーター	非推奨	非推奨	非推奨
cluster.local ドメインの CoreDNS ワイルドカードクエリー	非推奨	非推奨	非推奨
RHOSP の **compute.platform.openstack.rootVolume.type**	非推奨	非推奨	非推奨
RHOSP の **controlPlane.platform.openstack.rootVolume.type**	非推奨	非推奨	非推奨
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	非推奨	非推奨	非推奨
パッケージベースの RHEL コンピュートマシン	一般公開 (GA)	一般公開 (GA)	非推奨
Amazon Web Services (AWS) の **platform.aws.preserveBootstrapIgnition** パラメーター	一般公開 (GA)	一般公開 (GA)	非推奨
Amazon Web Services (AWS)、VMware vSphere、Nutanix 向け Terraform インフラストラクチャープロバイダー	一般公開 (GA)	一般公開 (GA)	削除済み
Google Cloud Platform (GCP) 向け Terraform インフラストラクチャープロバイダー	一般公開 (GA)	一般公開 (GA)	テクノロジープレビューとして削除可能
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	削除済み

1. OpenShift SDN ネットワークプラグインは、バージョン 4.15 のインストールプログラムではサポートされなくなりましたが、OpenShift SDN プラグインを使用するクラスターをバージョン 4.14 からバージョン 4.15 にアップグレードできます。

非推奨および削除されたクラスターの更新

表1.10 非推奨および削除されたトラッカーの更新

機能	4.14	4.15	4.16

ストレージの非推奨および削除された機能

表1.11 Storage の廃止と削除されたトラッカー

機能	4.14	4.15	4.16
FlexVolume を使用した永続ストレージ	非推奨	非推奨	非推奨
AliCloud Disk CSI Driver Operator	一般公開 (GA)	一般公開 (GA)	削除済み

ネットワーキングの非推奨機能と削除された機能

表1.12 ネットワーキングの非推奨化と削除のトラッカー

機能	4.14	4.15	4.16
RHOSP 上の Kuryr	非推奨	削除済み	削除済み
OpenShift SDN ネットワークプラグイン	非推奨	非推奨	非推奨
iptables	非推奨	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1.13 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	4.14	4.15	4.16
Patternfly 4	一般公開 (GA)	非推奨	非推奨
React Router 5	一般公開 (GA)	非推奨	非推奨

ノードの非推奨および削除された機能

表1.14 ノードは廃止され、トラッカーが削除されました

機能	4.14	4.15	4.16
ImageContentSourcePolicy (ICSP) オブジェクト	非推奨	非推奨	非推奨
Kubernetes トポロジーラベル **failure-domain.beta.kubernetes.io/zone**	非推奨	非推奨	非推奨
Kubernetes トポロジーラベル **Failure-domain.beta.kubernetes.io/region**	非推奨	非推奨	非推奨
cgroup v1	一般公開 (GA)	一般公開 (GA)	非推奨

ワークロードの非推奨および削除された機能

表1.15 ワークロードの非推奨および削除されたトラッカー

機能	4.14	4.15	4.16
DeploymentConfig オブジェクト	非推奨	非推奨	非推奨

ベアメタルモニタリングの非推奨および削除された機能

表1.16 Bare Metal Event Relay Operator トラッカー

機能	4.14	4.15	4.16
Bare Metal Event Relay Operator	テクノロジープレビュー	非推奨	非推奨

1.5.1. 非推奨の機能

1.5.1.1. Linux Control Groups バージョン 1 が廃止される

Red Hat Enterprise Linux (RHEL) 9 では、デフォルトモードは cgroup v2 です。Red Hat Enterprise Linux (RHEL) 10 がリリースされると、systemd は cgroup v1 モードでの起動をサポートしなくなり、cgroup v2 モードのみが利用可能になります。そのため、cgroup v1 は OpenShift Container Platform 4.16 以降では非推奨となっています。cgroup v1 は、今後の OpenShift Container Platform リリースで削除される予定です。

1.5.1.2. Cluster Samples Operator

Cluster Samples Operator は、OpenShift Container Platform 4.16 リリースで非推奨になりました。Cluster Samples Operator は、S2I 以外のサンプル (イメージストリームとテンプレート) の管理とサポートの提供を停止します。Cluster Samples Operator には、新しいテンプレート、サンプル、または Source-to-Image 以外 (S2I 以外) のイメージストリームは追加されません。ただし今後のリリースで Cluster Samples Operator が削除されるまで、既存の S2I ビルダーイメージストリームとテンプレートは引き続き更新されます。

1.5.1.3. パッケージベースの RHEL コンピュートマシン

このリリースにより、パッケージベースの RHEL ワーカーノードのインストールは非推奨になりました。今後のリリースでは、RHEL ワーカーノードは削除され、サポートされなくなります。

RHCOS イメージの階層化により、この機能が置き換えられ、ワーカーノードのベースオペレーティングシステムへの追加パッケージのインストールがサポートされます。

イメージのレイヤー化の詳細は、RHCOS イメージのレイヤー化 を参照してください。

1.5.1.4. Operator SDK CLI ツールおよび関連するテストおよびスキャフォールディングツールが非推奨に

Operator プロジェクトの関連スキャフォールディングおよびテストツールなど、Red Hat がサポートするバージョンの Operator SDK CLI ツールは非推奨となり、OpenShift Container Platform の今後の

リリースで削除される予定です。Red Hat は、現在のリリースライフサイクル中にこの機能のバグ修正とサポートを提供しますが、この機能は今後、機能拡張の提供はなく、OpenShift Container Platform リリースから削除されます。

新しい Operator プロジェクトを作成する場合、Red Hat がサポートするバージョンの Operator SDK は推奨されません。既存の Operator プロジェクトを使用する Operator 作成者は、OpenShift Container Platform 4.16 でリリースされるバージョンの Operator SDK CLI ツールを使用してプロジェクトを維持し、OpenShift Container Platform の新しいバージョンを対象とする Operator リリースを作成できます。

Operator プロジェクトの次の関連ベースイメージは **非推奨** ではありません。これらのベースイメージのランタイム機能と設定 API は、バグ修正と CVE への対応のために引き続きサポートされます。

- Ansible ベースの Operator プロジェクトのベースイメージ
- Helm ベースの Operator プロジェクトのベースイメージ

サポートされていない、コミュニティーによって管理されているバージョンの Operator SDK については、Operator SDK (Operator Framework) を参照してください。

1.5.1.5. Amazon Web Services (AWS) の preserveBootstrapIgnition パラメーターが非推奨に

install-config.yaml ファイル内の Amazon Web Services の **preserveBootstrapIgnition** パラメーターが非推奨になりました。代わりに **bestEffortDeleteIgnition** パラメーターを使用できます。

1.5.2. 削除された機能

1.5.2.1. ディスクパーティション設定方法が非推奨に

SiteConfig カスタムリソース (CR) の **nodes.diskPartition** セクションは、OpenShift Container Platform 4.16 リリースで非推奨になりました。この設定は、あらゆるユースケースに対してより柔軟にディスクパーティションを作成できる **ignitionConfigOverride** 方法に置き換えられました。

詳細は、SiteConfig を使用したディスクパーティションの設定 を参照してください。

1.5.2.2. Platform Operator とプレーンバンドルが削除される (テクノロジープレビュー)

OpenShift Container Platform 4.16 では、Operator Lifecycle Manager (OLM) 1.0 (テクノロジープレビュー) のプロトタイプであった Platform Operator (テクノロジープレビュー) とプレーンバンドル (テクノロジープレビュー) が削除されます。

1.5.2.3. BMC アドレス指定用 Dell iDRAC ドライバーの削除

OpenShift Container Platform 4.16 は、Dell iDRAC の BMC アドレス指定 に記載されているように、Dell サーバーでのベースボード管理コントローラー (BMC) アドレス指定をサポートします。具体的には、**idrac-virtualmedia**、**redfish**、**ipmi** をサポートします。以前のバージョンでは、**idrac** は含まれていましたが、文書化もサポートもされていませんでした。OpenShift Container Platform 4.16 では、**idrac** は削除されました。

1.5.2.4. コアプラットフォームモニタリングの専用サービスモニター

このリリースにより、コアプラットフォームモニタリングの専用のサービスモニター機能が削除されました。**openshift-monitoring** namespace の **cluster-monitoring-config** config map オブジェクトでこの機能を有効にすることはできなくなりました。この機能に代わり、アラートと時間集計が正確となる

ように Prometheus 機能が改善されました。この改善された機能はデフォルトでアクティブになり、専用のサービスモニター機能は廃止されます。

1.5.2.5. コアプラットフォームモニタリング用の Prometheus Adapter

このリリースにより、コアプラットフォームモニタリング用の Prometheus Adapter コンポーネントが削除されました。これは、新しい Metrics Server コンポーネントに置き換えられました。

1.5.2.6. MetalLB AddressPool カスタムリソース定義 (CRD) が削除される

MetalLB **AddressPool** カスタムリソース定義 (CRD) は、いくつかのバージョンで非推奨になりました。ただし、このリリースでは、CRD は完全に削除されています。MetalLB アドレスプールを設定するためにサポートされている唯一の方法は、**IPAddressPools** CRD を使用することです。

1.5.2.7. Service Binding Operator のドキュメントが削除される

このリリースでは、Service Binding Operator (SBO) がサポートされなくなったため、SBO のドキュメントが削除されました。

1.5.2.8. AliCloud CSI Driver Operator がサポート対象外に

OpenShift Container Platform 4.16 では、AliCloud Container Storage Interface (CSI) Driver Operator はサポート対象外になりました。

1.5.2.9. Kubernetes 1.29 からベータ API が削除される

Kubernetes 1.29 では、以下の非推奨 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1.17 Kubernetes 1.29 から削除された API

リソース	削除された API	移行先	大きな変更
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta2**	**flowcontrol.apiserver.k8s.io/v1** または **flowcontrol.apiserver.k8s.io/v1beta3**	いいえ
PriorityLevelConfiguration	**flowcontrol.apiserver.k8s.io/v1beta2**	**flowcontrol.apiserver.k8s.io/v1** または **flowcontrol.apiserver.k8s.io/v1beta3**	はい

1.6. バグ修正

API サーバーと認証

- 以前は、**ephemeral** ボリュームと **csi** ボリュームは、アップグレードされたクラスターの Security Context Constraints (SCC) に適切に追加されませんでした。このリリースにより、アップグレードされたクラスター上の SCC が適切に更新され、**ephemeral** ボリュームと **csi** ボリュームが含まれるようになりました。(OCPBUGS-33522)

- 以前は、**ImageRegistry** 機能が有効になっているクラスターの OAuth クライアントでは **ServiceAccounts** リソースを使用できませんでした。このリリースにより、この問題は修正されました。(OCPBUGS-30319)

- 以前は、空のセキュリティーコンテキストを持つ Pod を作成し、すべての Security Context Constraints (SCC) にアクセスできる場合、Pod は **anyuid** SCC を受け取りました。**ovn-controller** コンポーネントが Pod にラベルを追加した後、Pod は SCC 選択のために再度承認され、ここで Pod は **privileged** などのエスカレートされた SCC を受け取りました。このリリースにより、この問題は解決され、Pod は SCC 選択に再承認されなくなりました。(OCPBUGS-11933)

- 以前は、**hostmount-anyuid** Security Context Constraints (SCC) にはクラスターロールが組み込まれていませんでした。これは、SCC の名前がクラスターロールで誤って **hostmount** と命名されていたためです。このリリースにより、クラスターロール内の SCC 名が **hostmount-anyuid** に適切に更新され、**hostmount-anyuid** SCC が機能するクラスターロールを持つようになりました。(OCPBUGS-33184)

- 以前は、OpenShift Container Platform 4.7 より前に作成されたクラスターには、**SecretTypeTLS** タイプのシークレットがいくつかありました。OpenShift Container Platform 4.16 にアップグレードすると、これらのシークレットは削除され、**kubernetes.io/tls** タイプで再作成されます。この削除により競合状態が発生し、シークレットの内容が失われる可能性があります。このリリースにより、シークレットタイプの変更が自動的に行われるようになり、OpenShift Container Platform 4.7 より前に作成されたクラスターは、これらのシークレットの内容を失うリスクなしに 4.16 にアップグレードできるようになりました。(OCPBUGS-31384)

- 以前は、一部の Kubernetes API サーバーイベントに正しいタイムスタンプがありませんでした。このリリースにより、Kubernetes API サーバーイベントに正しいタイムスタンプが設定されるようになりました。(OCPBUGS-27074)

- 以前は、Kubernetes API Server Operator は、Prometheus ルールが OpenShift Container Platform 4.13 で削除済みにもかかわらず、確実に削除しようとしてこのルールの削除を試みていました。その結果、数分ごとに監査ログに削除失敗のメッセージが表示されていました。このリリースにより、Kubernetes API Server Operator はこの存在しないルールを削除しようとしなくなり、監査ログに削除失敗メッセージが表示されなくなりました。(OCPBUGS-25894)

ベアメタルハードウェアのプロビジョニング

- 以前は、Redfish の新しいバージョンでは、Manager リソースを使用して、RedFish Virtual Media API の Uniform Resource Identifier (URI) を廃止していました。このため、仮想メディア用の新しい Redfish URI を使用するハードウェアはプロビジョニングされなくなりました。このリリースにより、Ironic API は、RedFish Virtual Media API にデプロイする正しい Redfish URI を識別するため、非推奨となった URI または新しい URI のいずれかに依存するハードウェアをプロビジョニングできます。(OCPBUGS-30171)

- 以前は、Bare Metal Operator (BMO) は、Operator Pod の受信トラフィックと送信トラフィックを制御するためのリーダーロックを使用していませんでした。OpenShift **Deployment** オブジェクトに新しい Operator Pod が含まれると、新しい Pod が **ClusterOperator** ステータスなどのシステムリソースと競合し、これにより発信される Operator Pod がすべて終了しました。この問題は、ベアメタルノードを含まないクラスターにも影響を及ぼしました。このリリースにより、BMO に新しい Pod トラフィックを管理するためのリーダーロックが含まれ、この修正により競合する Pod の問題が解決されます。(OCPBUGS-25766)

- 以前は、インストールの開始前に **BareMetalHost** オブジェクトを削除しようとすると、metal3 Operator は **PreprovImage** イメージの作成を試行しました。このイメージを作成するプロセスが原因で、特定のプロセスに **BareMetalHost** オブジェクトが引き続き存在していました。この

リリースにより、この状況に対する例外が追加され、実行中のプロセスに影響を与えずに **BareMetalHost** オブジェクトが削除されるようになりました。(OCPBUGS-33048)

- 以前は、Hewlett Packard Enterprise (HPE) Lights Out (iLO) 5 のコンテキストにおける Redfish 仮想メディアでは、異なるハードウェアモデルにおける他の無関係な問題を回避するために、ベアメタルマシンの圧縮が強制的に無効にされていました。このため、各 iLO 5 ベアメタルマシンから **FirmwareSchema** リソースが失われていました。Redfish Baseboard Management Controller (BMC) エンドポイントからメッセージレジストリーを取得するために圧縮する必要があります。このリリースでは、**FirmwareSchema** リソースを必要とする各 iLO 5 ベアメタルマシンで圧縮が強制的に無効にされなくなりました。(OCPBUGS-31104)

- 以前は、**inspector.ipxe** 設定ファイルで **IRONIC_IP** 変数が使用されていましたが、括弧があるため IPv6 アドレスを考慮していませんでした。その結果、ユーザーが誤った **boot_mac_address** を指定すると、iPXE は **inspector.ipxe** 設定ファイルにフォールバックしました。この設定ファイルには括弧が含まれていなかったため、不正な形式の IPv6 ホストヘッダーが提供されました。このリリースにより、**inspector.ipxe** 設定ファイルが更新され、IPv6 アドレスを考慮した **IRONIC_URL_HOST** 変数を使用するようになり、問題は解決されました。(OCPBUGS-22699)

- 以前は、Ironic Python Agent は、ディスクを消去するときに、すべてのサーバーディスクのセクターサイズが 512 バイトであると想定していました。このため、ディスクの消去に失敗しました。このリリースにより、Ironic Python Agent はディスクセクターサイズをチェックし、ディスクワイプが成功するようにディスクワイプ用の個別の値を設定します。(OCPBUGS-31549)

ビルド

- 以前は、以前のバージョンから 4.16 に更新されたクラスターでは、認証されていない Webhook によってビルドがトリガーされることが引き続き許可されていました。このリリースにより、新しいクラスターではビルド Webhook の認証が必要になります。クラスター管理者が namespace またはクラスター内で認証されていない Webhook を許可しない限り、ビルドが認証されていない Webhook によってトリガーされることはありません。(OCPBUGS-33378)

- 以前は、開発者またはクラスター管理者がプロキシー情報に小文字の環境変数名を使用した場合、これらの環境変数はビルド出力コンテナーイメージに引き継がれていました。ランタイム時にプロキシー設定がアクティブになっていたため、設定を解除する必要がありました。このリリースにより、***_PROXY** 環境変数の小文字バージョンが、ビルドされたコンテナーイメージにリークされることが阻止されます。現在、**buildDefaults** はビルド中にのみ保持され、ビルドプロセス用に作成された設定は、レジストリーにイメージをプッシュする前にのみ削除されます。(OCPBUGS-34825)

クラウドコンピュート

- 以前は、Cloud Controller Manager (CCM) Operator は、きめ細かい権限ではなく、Google Cloud Platform (GCP) で事前定義されたロールを使用していました。このリリースにより、CCM Operator が更新され、GCP クラスターに対してきめ細かい権限を使用できるようになりました。(OCPBUGS-26479)

- 以前は、インストールプログラムは、VMware vSphere 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) の **spec.template.spec.providerSpec.value** セクションの **network.devices**、**template**、および **workspace** フィールドに値を入力していました。これらのフィールドは vSphere 障害ドメインで設定する必要があり、インストールプログラムでこれらのフィールドを設定すると、意図しない動作が発生していました。これらのフィールドを更新してもコントロールプレーンマシンの更新はトリガーされず、コントロールプレーンマシンセットが削除されるとこれらのフィールドはクリアされていました。
  このリリースにより、インストールプログラムが更新され、障害ドメイン設定に含まれる値が入力されなくなりました。これらの値が障害ドメイン設定で定義されていない場合 (たとえば、

以前のバージョンから OpenShift Container Platform 4.16 に更新されたクラスターの場合)、インストールプログラムによって定義された値が使用されます。(OCPBUGS-32947)

- 以前は、再起動中のマシンに関連付けられたノードが一時的に **Ready=Unknown** のステータスになると、Control Plane Machine Set Operator で **UnavailableReplicas** 条件がトリガーされていました。この状態により、Operator は **Available=False** 状態になり、この状態は管理者の即時介入を必要とする機能しないコンポーネントを示しているため、アラートがトリガーされます。このアラートは、再起動中の短時間かつ予期される使用不可状態に対してトリガーされることはありません。このリリースにより、不要なアラートがトリガーされないように、ノードの未準備に対する猶予期間が追加されました。(OCPBUGS-34970)

- 以前は、API サーバーへの接続の一時的な障害など、マシンの作成中にブートストラップデータの取得に一時的な障害が発生すると、マシンがターミナル障害状態になりました。このリリースにより、マシンの作成中にブートストラップデータの取得に失敗した場合、最終的に成功するまで無期限に再試行されます。(OCPBUGS-34158)

- 以前は、ポートリストが渡されなかったため、エラー状態のサーバーを削除するときに、Machine API Operator がパニックを起こしていました。このリリースにより、**ERROR** 状態にスタックしているマシンを削除しても、コントローラーはクラッシュしなくなりました。(OCPBUGS-34155)

- 以前は、クラスターオートスケーラーのオプションの内部関数が実装されていない場合、ログエントリーが繰り返し発生していました。この問題は本リリースで解決されています。(OCPBUGS-33932)

- 以前は、VMware vSphere クラスターへのインストール中にパスのないテンプレートを使用してコントロールプレーンマシンセットが作成されると、Control Plane Machine Set Operator は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) の変更または削除を拒否していました。このリリースにより、Operator はコントロールプレーンのマシンセット定義で vSphere のテンプレート名を許可します。(OCPBUGS-32295)

- 以前は、インフラストラクチャーリソースが設定されていなかったため、VMware vSphere クラスターを更新しようとすると、Control Plane Machine Set Operator がクラッシュしていました。このリリースにより、Operator はこのシナリオを処理して、クラスターの更新を続行できるようになります。(OCPBUGS-31808)

- 以前は、ユーザーがテイントを含むコンピュートマシンセットを作成した際に、**Value** フィールドを指定しないことを選択できました。このフィールドを指定しないと、クラスターオートスケーラーがクラッシュしました。このリリースにより、クラスターオートスケーラーが更新され、空の **Value** フィールドを処理できるようになりました。(OCPBUGS-31421)

- 以前は、IPv6 サービスは RHOSP クラウドプロバイダーで誤って内部としてマークされていたため、OpenShift Container Platform サービス間で IPv6 ロードバランサーを共有できませんでした。このリリースにより、IPv6 サービスは内部としてマークされず、ステートフル IPv6 アドレスを使用するサービス間で IPv6 ロードバランサーを共有できるようになりました。この修正により、ロードバランサーはサービスの **loadBalancerIP** プロパティーで定義されているステートフル IPv6 アドレスを使用できるようになります。(OCPBUGS-29605)

- 以前は、コントロールプレーンマシンが unready とマークされ、コントロールプレーンマシンセットの修正によって変更が開始されると、unready のマシンは途中で削除されていました。この時期尚早なアクションにより、複数のインデックスが同時に置き換えられていました。このリリースにより、インデックス内にマシンが 1 台しか存在しない場合、コントロールプレーンマシンセットによってマシンが削除されなくなりました。この変更により、変更が時期尚早にロールアウトされることが阻止され、一度に複数のインデックスが置き換えられることが阻止されます。(OCPBUGS-29249)

- 以前は、Azure API への接続が最大 16 分間ハングすることがありました。このリリースにより、API 呼び出しのハングを防ぐためにタイムアウトが導入されました。(OCPBUGS-29012)

- 以前は、Machine API IBM Cloud コントローラーは、**klogr** パッケージからの完全なロギングオプションを統合していませんでした。その結果、Kubernetes バージョン 1.29 以降ではコントローラーがクラッシュしました。このリリースにより、不足しているオプションが含まれるようになり、問題が解決しました。(OCPBUGS-28965)

- 以前は、Cluster API IBM Power Virtual Server コントローラー Pod は、サポートされていない IBM Cloud プラットフォームで起動していました。このため、コントローラー Pod が作成フェーズで停止していました。このリリースにより、クラスターは IBM Power Virtual Server と IBM Cloud の違いを検出するようになりました。これでクラスターは、サポートされているプラットフォームでのみ起動します。(OCPBUGS-28539)

- 以前は、解析エラーのため、マシンオートスケーラーはコンピュートマシンセット仕様に直接設定されたテイントを考慮できませんでした。これにより、コンピュートマシンセットのテイントに依存してゼロからスケーリングする場合に、望ましくないスケーリング動作が発生する可能性がありました。このリリースにより、この問題は解決され、マシンオートスケーラーは正しくスケールアップし、ワークロードのスケジュールを妨げるテイントを識別できるようになりました。(OCPBUGS-27509)

- 以前は、アベイラビリティーゾーンをサポートしていない Microsoft Azure リージョンで実行されたマシンセットは、常にスポットインスタンスの **AvailabilitySets** オブジェクトを作成していました。この操作が原因で、インスタンスが可用性セットをサポートしていなかったことから、スポットインスタンスは失敗していました。このリリースにより、マシンセットは、ゾーン設定されていないリージョンで動作するスポットインスタンスの **AvailabilitySets** オブジェクトを作成しなくなりました。(OCPBUGS-25940)

- 以前は、OpenShift Container Platform 4.14 で kubelet からイメージ認証情報を提供するコードが削除されたため、プルシークレットを指定しないと Amazon Elastic Container Registry (ECR) からイメージをプルする操作が失敗していました。このリリースには、kubelet の ECR 認証情報を提供する別の認証情報プロバイダーが含まれています。(OCPBUGS-25662)

- 以前は、Azure ロードバランサーのデフォルトの仮想マシンタイプが **Standard** から **VMSS** に変更されましたが、サービスタイプのロードバランサーコードでは、標準の VM をロードバランサーにアタッチできませんでした。このリリースにより、OpenShift Container Platform デプロイメントとの互換性を維持するために、デフォルトの仮想マシンタイプが元に戻されます。(OCPBUGS-25483)

- 以前は、OpenShift Container Platform では、OpenStack Cloud Controller Manager によって作成された RHOSP ロードバランサーリソースの名前にクラスター名が含まれていませんでした。この動作により、単一の RHOSP プロジェクトで実行されている複数のクラスターで **LoadBalancer** サービスの名前が同じ場合に問題が発生していました。このリリースにより、クラスター名が Octavia リソースの名前に含まれるようになりました。以前のクラスターバージョンからアップグレードすると、ロードバランサーの名前が変更されます。新しい名前は、**kube_service_kubernetes_<namespace>_<service-name>** ではなく、**kube_service_<cluster-name>_<namespace>_<service-name>** のパターンに従います。(OCPBUGS-13680)

- 以前は、大量のサービスオブジェクトを同時に作成または削除すると、各サービスを順番に処理するサービスコントローラーの機能が低下していました。これにより、サービスコントローラーの短いタイムアウトの問題が発生し、オブジェクトのバックログの問題も発生しました。このリリースでは、サービスコントローラーは最大 10 個のサービスオブジェクトを同時に処理できるようになり、バックログとタイムアウトの問題が軽減されました。(OCPBUGS-13106)

- 以前は、ノードの名前を取得するロジックでは、AWS メタデータサービスから返されるホスト名に複数の値が存在する可能性を考慮していませんでした。VPC Dynamic Host Configuration

Protocol (DHCP) オプションに複数のドメインが設定されている場合、このホスト名は複数の値を返す可能性があります。複数の値間のスペースによりロジックがクラッシュしました。このリリースにより、最初に返されたホスト名のみをノード名として使用するようにロジックが更新されました。(OCPBUGS-10498)

- 以前は、Machine API Operator は、Microsoft Azure クラスターで不要な **virtualMachines/extensions** 権限を要求していました。このリリースにより、不要な認証情報の要求が削除されました。(OCPBUGS-29956)

Cloud Credential Operator

- 以前は、Cloud Credential Operator (CCO) には、Microsoft Azure 上にプライベートクラスターを作成するために必要ないくつかの権限がありませんでした。これらの権限が不足していたため、Microsoft Entra Workload ID を使用して Azure プライベートクラスターをインストールできませんでした。このリリースには不足している権限が含まれ、これにより、Workload ID を使用して Azure プライベートクラスターをインストールできます。(OCPBUGS-25193)

- 以前は、バグにより、Cloud Credential Operator (CCO) がメトリクスで誤ったモードを報告していました。クラスターはデフォルトモードでしたが、メトリクスでは認証情報削除モードであると報告されました。この更新では、キャッシュされたクライアントの代わりにライブクライアントが使用されるため、ルート認証情報を取得できるようになり、CCO はメトリクスで誤ったモードを報告しなくなりました。(OCPBUGS-26488)

- 以前は、Microsoft Entra Workload ID を使用する OpenShift Container Platform クラスター上の Cloud Credential Operator 認証情報モードメトリクスは、手動モードを使用して報告されていました。このリリースにより、Workload ID を使用するクラスターが更新され、Pod アイデンティティーで手動モードを使用していることが報告されるようになりました。(OCPBUGS-27446)

- 以前は、ベアメタルクラスターで Amazon Web Services (AWS) ルートシークレットを作成すると、Cloud Credential Operator (CCO) Pod がクラッシュしていました。この問題は本リリースで解決されています。(OCPBUGS-28535)

- 以前は、ミントモードで Cloud Credential Operator (CCO) を使用する Google Cloud Platform (GCP) クラスターからルート認証情報を削除すると、約 1 時間後に CCO の機能が低下していました。機能低下状態では、CCO はクラスター上のコンポーネント認証情報のシークレットを管理できません。この問題は本リリースで解決されています。(OCPBUGS-28787)

- 以前は、Cloud Credential Operator (CCO) は、Amazon Web Services (AWS) へのインストール中に、存在しない **s3:HeadBucket** 権限をチェックしていました。CCO がこの権限を見つけられなかった場合、提供された認証情報は mint モードには不十分であると判断されました。このリリースにより、CCO は存在しない権限をチェックしなくなりました。(OCPBUGS-31678)

Cluster Version Operator

- このリリースでは、**ClusterOperatorDown** および **ClusterOperatorDegraded** アラートが拡張されて ClusterVersion 条件がカバーされ、**Available=False** (**ClusterOperatorDown**) および **Failing=True** (**ClusterOperatorDegraded**) のアラートが送信されます。以前のリリースでは、これらのアラートは **ClusterOperator** の条件のみを対象としていました。(OCPBUGS-9133)

- 以前は、OpenShift Container Platform 4.15.0、4.14.0、4.13.17、および 4.12.43 で導入された Cluster Version Operator (CVO) の変更により、リスク評価が失敗し、CVO が新しい更新推奨事項を取得できなくなっていました。リスク評価が失敗したとき、バグが原因で CVO は更新推奨サービスを見落としていました。このリリースにより、更新リスクが正常に評価されているかどうかに関係なく、CVO は更新推奨サービスのポーリングを継続し、問題が解決されました。(OCPBUGS-25708)

開発者コンソール

- 以前は、サーバーレス作成フォームでサーバーレス関数が作成されても、**BuilldConfig** は作成されませんでした。この更新により、Pipelines Operator がインストールされていない場合、特定のリソースに対してパイプラインリソースが作成されず、またはサーバーレス関数の作成中にパイプラインが追加されないため、期待どおりに **BuildConfig** が作成されるようになります。(OCPBUGS-34143)

- 以前は、Pipelines Operator をインストールした後、Pipeline テンプレートがクラスターで使用できるようになるまでに時間がかかりましたが、ユーザーは引き続きデプロイメントを作成できました。この更新により、選択したリソースにパイプラインテンプレートが存在しない場合は、**Import from Git** ページの **Create** ボタンが無効になります。(OCPBUGS-34142)

- 以前は、**トポロジー** ページでノードの最大数は **100** に設定されていました。"Loading is taking longer than expected." という警告が継続的に表示されました。この更新により、ノードの制限が **300** に増加されました。(OCPBUGS-32307)

- この更新により、**ServiceBinding** の作成時およびコンポーネントのバインド時、または現在の namespace で **ServiceBinding** が見つかった場合に、**ServiceBinding list**、**ServiceBinding details**、**Add**、および **Topology** ページに、OpenShift Container Platform 4.15 で Service Binding が非推奨になったことを通知するアラートメッセージが追加されました。(OCPBUGS-32222)

- 以前は、チャート名が異なる場合、Helm Plugin のインデックスビューには Helm CLI と同じ数のチャートが表示されませんでした。このリリースでは、Helm カタログは **charts.openshift.io/name** と **charts.openshift.io/provider** を検索するようになり、すべてのバージョンが 1 つのカタログタイトルにグループ化されるようになりました。(OCPBUGS-32059)

- 以前は、**TaskRun details** ページの **TaskRun** 名の近くに **TaskRun** のステータスが表示されませんでした。この更新により、**TaskRun** ステータスはページ見出しの **TaskRun** の名前の横に表示されるようになりました。(OCPBUGS-31745)

- 以前は、リソースフィールドがペイロードに追加され、リソースが非推奨になると、パイプラインにパラメーターを追加するとエラーが発生しました。この更新により、リソースフィールドがペイロードから削除され、パイプラインにパラメーターを追加できるようになりました。(OCPBUGS-31082)

- このリリースでは、OpenShift Pipelines プラグインが更新され、カスタムリソース定義 (CRD) **ClusterTriggerBinding**、**TriggerTemplate**、および **EventListener** の最新の Pipeline Trigger API バージョンがサポートされるようになりました。(OCPBUGS-30958)

- 以前は、**CustomTasks** は認識されなかったか、**Pending** 状態のままでした。この更新により、パイプライン **Lis** ページと **Lis** ページから、**CustomTasks** を簡単に識別できるようになりました。(OCPBUGS-29513)

- 以前は、**Image** タグを含むビルド出力イメージがあった場合、**Output Image** リンクは正しい **ImageStream** ページにリダイレクトされませんでした。この更新により、リンクにタグを追加せずに **ImageStream** ページの URL を生成することでこの問題は修正されました。(OCPBUGS-29355)

- 以前は、指定されたリソースの API バージョンが最近更新されたため、**BuildRun** ログは **BuildRun** の **Logs** タブに表示されませんでした。この更新により、**TaskRuns** のログが、Builds Operator の v1alpha1 バージョンと v1beta1 バージョンの両方の **BuildRun** ページの **Logs** タブに再度追加されました。(OCPBUGS-27473)

- 以前は、スケール限度値を設定するアノテーションは、**autoscaling.knative.dev/maxScale** と

autoscaling.knative.dev/minScale に設定されていました。この更新により、スケール限度値を設定するアノテーションが **autoscaling.knative.dev/min-scale** と **autoscaling.knative.dev/max-scale** に更新され、特定の時点でアプリケーションに提供できるレプリカの最小数と最大数が決定されます。アプリケーションのスケーリング限度を設定して、コールドスタートを防止したり、コンピューティングコストを制御したりできます。(OCPBUGS-27469)

- 以前は、Tekton Results API からの **PipelineRuns** の **Log** タブのロードが完了しませんでした。このリリースにより、Kubernetes API または Tekton Results API からロードされた PipelineRuns に対して、このタブが完全にロードされるようになりました。(OCPBUGS-25612)

- 以前は、Kubernetes API または Tekton Results API からロードされた **PipelineRun** を区別するためのインジケーターは表示されませんでした。この更新により、Kubernetes API または Tekton Results API からロードされた **PipelineRuns** 間を区別するために、**PipelineRun list** ページと **details** ページに小さなアーカイブアイコンが表示されるようになりました。(OCPBUGS-25396)

- 以前は、**PipelineRun list** ページで、すべての TaskRuns が取得され、**pipelineRun** 名に基づいて分けられていました。この更新により、**Failed** および **Cancelled** の PipelineRun に対してのみ、TaskRuns が取得されるようになりました。**Failed** および **Cancelled** PipelineRuns に関連付けられた PipelineRuns と TaskRuns を取得するためのキャッシュメカニズムも追加されました。(OCPBUGS-23480)

- 以前は、**Topology** ビューの仮想マシンノードとその他の非仮想マシンノードの間にビジュアルコネクターが存在しませんでした。この更新により、ビジュアルコネクターが仮想マシンノードと非仮想マシンノードの間に配置されます。(OCPBUGS-13114)

etcd Cluster Operator

- 以前は、etcd ロールアウトを確認するためにブートストラップ中に使用されていた **wait-for-ceo** コマンドは、一部の障害モードでエラーを報告しませんでした。このリリースにより、エラーが発生した場合に **cmd** が終了した場合に、それらのエラーメッセージが **bootkube** スクリプトに表示されるようになりました。(OCPBUGS-33495)

- 以前は、etcd Cluster Operator が Pod の健全性チェック中にパニック状態になり、**etcd** クラスターへのリクエストが失敗していました。このリリースにより問題が修正され、このようなパニック状況は発生しなくなりました。(OCPBUGS-27959)

- 以前は、etcd Cluster Operator は実行されていないコントローラーをデッドロックとして誤って識別し、これにより不要な Pod の再起動が発生していました。このリリースにより、この問題が修正され、Operator は Pod を再起動せずに、実行されていないコントローラーを健全ではない etcd メンバーとしてマークするようになりました。(OCPBUGS-30873)

Hosted Control Plane

- 以前は、Multus Container Network Interface (CNI) では、ホストされたクラスターで **Other** ネットワークタイプを使用すると、証明書署名要求 (CSR) が承認される必要がありました。適切なロールベースのアクセス制御 (RBAC) ルールは、ネットワークタイプが **Other** で、Calico に設定された場合にのみ設定されました。その結果、ネットワークタイプが **Other** で Cilium に設定されている場合、CSR は承認されませんでした。この更新により、すべての有効なネットワークタイプに対して正しい RBAC ルールが設定され、**Other** ネットワークタイプを使用するときに RBAC が適切に設定されるようになりました。(OCPBUGS-26977)

- 以前は、Amazon Web Services (AWS) ポリシーの問題により、Cluster API プロバイダー AWS が必要なドメイン情報を取得できませんでした。その結果、カスタムドメインを使用した AWS のホストされたクラスターのインストールに失敗しました。この更新により、ポリシーの問題

は解決されます。(OCPBUGS-29391)

- 以前は、非接続環境では、HyperShift Operator はレジストリーのオーバーライドを無視していました。その結果、ノードプールへの変更は無視され、ノードプールでエラーが発生しました。今回の更新により、メタデータのインスペクターは HyperShift Operator の調整中に期待どおりに動作し、オーバーライドイメージが適切に入力されるようになりました。(OCPBUGS-34773)

- 以前は、HyperShift Operator が **RegistryOverrides** メカニズムを使用して内部レジストリーからイメージを検査していませんでした。このリリースにより、HyperShift Operator の調整中にメタデータインスペクターが期待どおりに機能し、**OverrideImages** が適切に入力されます。(OCPBUGS-32220)

- 以前は、Red Hat OpenShift Cluster Manager コンテナーには正しい Transport Layer Security (TLS) 証明書がありませんでした。その結果、切断されたデプロイメントではイメージストリームを使用できませんでした。この更新により、TLS 証明書がプロジェクトボリュームとして追加されました。(OCPBUGS-34390)

- 以前は、KAS Pod の **azure-kms-provider-active** コンテナーは、Dockerfile でシェル形式のエントリーポイントステートメントを使用していました。その結果、コンテナーは失敗しました。この問題を解決するには、エントリーポイントステートメントに **exec** 形式を使用します。(OCPBUGS-33940)

- 以前は、**konnectivity-agent** デーモンセットは **ClusterIP** DNS ポリシーを使用していました。その結果、CoreDNS がダウンすると、データプレーン上の **konnectivity-agent** Pod がプロキシーサーバー URL を解決できず、コントロールプレーンの **konnectivity-server** が失敗することがありました。この更新により、**konnectivity-agent** デーモンセットが **dnsPolicy: Default** を使用するように変更されました。**konnectivity-agent** は、ホストシステムの DNS サービスを使用してプロキシーサーバーアドレスを検索するため、CoreDNS に依存しなくなりました。(OCPBUGS-31444)

- 以前は、リソースが見つからないため、再作成の試行が失敗していました。その結果、Hosted Cluster Config Operator ログに多数の **409** 応答コードが記録されました。この更新により、Hosted Cluster Config Operator が既存のリソースを再作成しないように、特定のリソースがキャッシュに追加されました。(OCPBUGS-23228)

- 以前は、ホストされたクラスターでは Pod セキュリティー違反アラートが表示されませんでした。この更新により、アラートがホストされたクラスターに追加されます。(OCPBUGS-31263)

- 以前は、非接続環境のホストされたクラスターの **recycler-pod** テンプレートは、**quay.io/openshift/origin-tools:latest** を指していました。その結果、リサイクラー Pod は起動に失敗しました。この更新により、リサイクラー Pod イメージは OpenShift Container Platform ペイロード参照を指すようになりました。(OCPBUGS-31398)

- この更新により、切断されたデプロイメントでは、HyperShift Operator は管理クラスターから新しい **ImageContentSourcePolicy** (ICSP) または **ImageDigestMirrorSet** (IDMS) を受信し、すべての調整ループでそれらを HyperShift Operator と Control Plane Operator に追加します。ICSP または IDMS を変更すると、**control-plane-operator** Pod が再起動されます。(OCPBUGS-29110)

- この更新により、**ControllerAvailabilityPolicy** 設定は、設定後にイミュータブルになります。**SingleReplica** と **HighAvailability** 間の変更はサポートされていません。(OCPBUGS-27282)

- この更新により、**machine-config-operator** カスタムリソース定義 (CRD) の名前が変更され、Hosted Control Plane でリソースが適切に省略されるようになりました。(OCPBUGS-34575)

- この更新により、Hosted Control Plane の **kube-apiserver**、**openshift-apiserver**、および **oauth-apiserver** Pod に保存される監査ログファイルのサイズが削減されます。(OCPBUGS-31106)

- 以前は、HyperShift Operator が **RegistryOverrides** メカニズムを使用して内部レジストリーからイメージを検査していませんでした。このリリースでは、Hypershift Operator の調整中にメタデータインスペクターが期待どおりに機能し、**OverrideImages** が適切に入力されます。(OCPBUGS-29494)

Image Registry

- 以前は、イメージストリームタグをインポートした後、**ImageContentSourcePolicy** (ICSP) カスタムリソース (CR) は **ImageDigestMirrorSet** (IDMS) または **ImageTagMirrorSet** (ITMS) CR と共存できませんでした。OpenShift Container Platform は、他の CR タイプではなく ICSP を選択しました。このリリースにより、これらのカスタムリソースが共存できるため、イメージストリームタグをインポートした後、OpenShift Container Platform は必要な CR を選択できるようになりました。(OCPBUGS-30279)

- 以前は、**oc tag** コマンドは新しいタグを作成するときにタグ名を検証しませんでした。無効な名前のタグからイメージが作成されると、**podman pull** コマンドが失敗していました。このリリースにより、検証手順で新しいタグに無効な名前がないかチェックし、無効な名前を持つ既存のタグを削除できるようになったため、この問題は発生しなくなりました。(OCPBUGS-25703)

- 以前は、Image Registry Operator は独自の IBM Power® Virtual Server リージョンのリストを維持していたため、新しいリージョンはリストに追加されませんでした。このリリースでは、Operator は新しいリージョンをサポートできるように、リージョンへのアクセスに外部ライブラリーに依存します。(OCPBUGS-26767)

- 以前は、イメージレジストリーの Microsoft Azure パスフィックスジョブが機能するには、**AZURE_CLIENT_ID** および **TENANT_CLIENT_ID** パラメーターの存在が必要とされましたが、これは誤りでした。これにより、有効な設定でエラーメッセージが出力されていました。このリリースにより、これらのパラメーターが必要かどうかを検証するために Identity and Access Management (IAM) サービスアカウントキーにチェック項目が追加され、クラスターのアップグレード操作が失敗しなくなりました。(OCPBUGS-32328)

- 以前は、イメージレジストリーは Amazon Web Services (AWS) リージョン **ca-west-1** をサポートしていませんでした。このリリースでは、イメージレジストリーをこのリージョンにデプロイできるようになりました。(OCPBUGS-29233)

- 以前は、Image Registry Operator 設定で **virtualHostedStyle** パラメーターが **regionEndpoint** に設定されていた場合、イメージレジストリーは仮想ホストスタイル設定を無視していました。このリリースでは、問題が解決され、ダウンストリームのみのバージョンである仮想ホストスタイルの代わりに、新しいアップストリームディストリビューション設定である強制パススタイルが使用されるようになりました。(OCPBUGS-34166)

- 以前は、サービスエンドポイントのオーバーライドが有効になっている IBM Power® Virtual Server 上で OpenShift Container Platform クラスターを実行すると、Cloud Credential Operator (CCO) Operator はオーバーライドするサービスエンドポイントを無視していました。このリリースにより、CCO Operator はオーバーライドするサービスエンドポイントを無視しなくなりました。(OCPBUGS-32491)

- 以前は、Image Registry Operator はエンドポイントサービスのクラスターレベルのオーバーライドを無視していたため、IBM Cloud® の非接続環境でのクラスターの設定が困難でした。この問題は、installer-provisioned infrastructure でのみ存在していました。このリリースにより、Image Registry Operator はこれらのクラスターレベルのオーバーライドを無視しなくなりました。(OCPBUGS-26064)

インストーラー

- 以前は、Google Cloud Platform (GCP) に無効な設定の 3 ノードクラスターをインストールすると、パニックエラーが発生して失敗しましたが、失敗の理由は報告されませんでした。このリリースでは、インストールプログラムはインストール設定を検証し、3 ノードクラスターを GCP に正常にインストールします。(OCPBUGS-35103)

- 以前は、プルシークレットのパスワードにコロンが含まれている場合、Assisted Installer によるインストールは失敗していました。このリリースにより、パスワードにコロンを含むプルシークレットによって、Assisted Installer が失敗することはなくなりました。(OCPBUGS-34400)

- 以前は、Agent-based のクラスターにノードを追加するプロセスを監視するために使用される **monitor-add-nodes** コマンドは、権限エラーのために実行に失敗しました。このリリースにより、コマンドは権限がある正しいディレクトリーで動作します。(OCPBUGS-34388)

- 以前は、長いクラスター名はユーザーに警告することなくトリミングされていました。このリリースにより、インストールプログラムは長いクラスター名をトリミングするときにユーザーに警告します。(OCPBUGS-33840)

- 以前は、クラスターをインストールするときに、**install-config.yaml** で無効にされていても、Ingress 機能は必須であるため有効になっていました。このリリースにより、**install-config.yaml** で Ingress 機能が無効になっていると、インストールプログラムは失敗します。(OCPBUGS-33794)

- 以前は、OpenShift Container Platform は、Amazon Web Services (AWS) リージョンの **ca-west-1** にインストールされたクラスターのクォータチェックを実行していませんでした。このリリースにより、このリージョンでクォータが適切に適用されます。(OCPBUGS-33649)

- 以前は、インストールプログラムが OpenShift Container Platform API が利用できないことを検出できない場合がありました。Microsoft Azure インストールのブートストラップノードのディスクサイズを増やすことで、追加のエラーが解決されました。このリリースでは、インストールプログラムは API が利用できないかどうかを正しく検出します。(OCPBUGS-33610)

- 以前は、Microsoft Azure クラスターのコントロールプレーンノードは、**Read-only** キャッシュを使用していました。このリリースにより、Microsoft Azure コントロールプレーンノードは **ReadWrite** キャッシュを使用します。(OCPBUGS-33470)

- 以前は、プロキシーが設定された Agent-based のクラスターをインストールするときに、プロキシー設定にパーセント記号 (**%**) で始まる文字列が含まれているとインストールが失敗していました。このリリースにより、インストールプログラムがこの設定テキストを正しく検証します。(OCPBUGS-33024)

- 以前は、インストールプログラムがバケットを 2 回作成しようとしたため、GCP へのインストールが失敗する可能性がありました。このリリースにより、インストールプログラムはバケットを 2 回作成しようとしなくなりました。(OCPBUGS-32133)

- 以前は、まれにタイミングの問題により、インストール中にすべてのコントロールプレーンノードが Agent-based のクラスターに追加されない場合がありました。このリリースにより、インストール中にすべてのコントロールプレーンノードが正常に再起動され、クラスターに追加されます。(OCPBUGS-32105)

- 以前は、非接続環境で Agent-based のインストールプログラムを使用すると、認証局 (CA) トラストバンドルに不要な証明書が追加されていました。このリリースにより、CA バンドル **ConfigMap** には、ユーザーが明示的に指定した CA のみが含まれます。(OCPBUGS-32042)

- 以前は、Amazon Web Services (AWS) にクラスターをインストールするときに、存在しない

s3:HeadBucket 権限をインストールプログラムが要求していました。このリリースにより、インストールプログラムは代わりに **s3:ListBucket** 権限を正しく要求するようになりました。(OCPBUGS-31813)

- 以前は、SSH 接続の問題によりインストールプログラムがブートストラップからログを収集できなかった場合、仮想マシン (VM) シリアルコンソールログが収集されていても提供されませんでした。このリリースにより、ブートストラップマシンへの SSH 接続が失敗した場合でも、インストールプログラムは仮想マシンシリアルコンソールログを提供します。(OCPBUGS-30774)

- 以前は、静的 IP アドレスを使用して VMware vSphere にクラスターをインストールすると、他のテクノロジープレビュー機能との競合により、クラスターによって静的 IP アドレスのないコントロールプレーンマシンが作成される可能性がありました。このリリースにより、Control Plane Machine Set Operator は、コントロールプレーンマシンの静的 IP 割り当てを正しく管理します。(OCPBUGS-29114)

- 以前は、ユーザー提供の DNS を使用して GCP にクラスターをインストールすると、インストールプログラムは GCP DNS ネットワーク内で DNS を引き続き検証しようとしていました。このリリースにより、インストールプログラムはユーザー提供の DNS に対してこの検証を実行しません。(OCPBUGS-29068)

- 以前は、非プライベート IBM Cloud® クラスターと同じドメイン名を使用している IBM Cloud® 上のプライベートクラスターを削除する場合、一部のリソースが削除されませんでした。このリリースにより、クラスターが削除されると、すべてのプライベートクラスターリソースが削除されます。(OCPBUGS-28870)

- 以前は、設定文字列にパーセント記号 (**%**) を使用した文字列を含むプロキシーを使用してクラスターをインストールすると、クラスターのインストールが失敗していました。このリリースにより、インストールプログラムは "%" を含むプロキシー設定文字列を正しく検証します。(OCPBUGS-27965)

- 以前は、**OpenShiftSDN** ネットワークプラグインは、削除されていたにもかかわらず、引き続きインストールプログラムで使用できました。このリリースにより、インストールプログラムは、このネットワークプラグインを使用したクラスターのインストールを適切に阻止します。(OCPBUGS-27813)

- 以前は、Amazon Web Services (AWS) Wavelengths または Local Zones のクラスターを、Wavelengths または Local Zones のいずれか (両方ではない) をサポートするリージョンにインストールすると、インストールが失敗しました。このリリースにより、Wavelength または Local Zones のいずれかをサポートするリージョンへのインストールが成功します。(OCPBUGS-27737)

- 以前は、既存のクラスターと同じクラスター名とベースドメインを使用するクラスターのインストールを試行し、DNS レコードセットの競合のためにインストールが失敗した場合、2 番目のクラスターを削除すると、元のクラスターの DNS レコードセットも削除されていました。このリリースにより、保存されたメタデータにはクラスタードメインではなくプライベートゾーン名が含まれるため、削除されたクラスターからは正しい DNS レコードのみが削除されます。(OCPBUGS-27156)

- 以前は、Agent-based のインストールのインストール設定ファイルで設定されたプラットフォーム固有のパスワードが、**agent-gather** コマンドの出力に存在する可能性がありました。このリリースにより、**agent-gather** の出力からパスワードが編集されます。(OCPBUGS-26434)

- 以前は、バージョン 4.15 または 4.16 でインストールされた OpenShift Container Platform クラスターでは、バージョン 4.14 のデフォルトのアップグレードチャネルが表示されていました。このリリースにより、インストール後にクラスターに正しいアップグレードチャネルが設定さ

れます。(OCPBUGS-26048)

- 以前は、VMware vSphere クラスターを削除するときに、一部の **TagCategory** オブジェクトの削除に失敗しました。このリリースにより、クラスターが削除されると、クラスター関連のすべてのオブジェクトが正しく削除されます。(OCPBUGS-25841)

- 以前は、**baremetal** プラットフォームタイプを指定しても、**install-config.yaml** で **baremetal** 機能を無効にすると、役立つエラーが表示されずに長いタイムアウト後にインストールが失敗していました。このリリースにより、インストールプログラムは説明を伴うエラーを提供し、**baremetal** 機能が無効になっている場合はベアメタルインストールを試行しません。(OCPBUGS-25835)

- 以前は、VMware vSphere がノードを正しく初期化できないため、Assisted Installer を使用して VMware vSphere にインストールすると失敗する可能性がありました。このリリースにより、VMware vSphere 上の Assisted Installer インストールは、すべてのノードが初期化された状態で正常に完了します。(OCPBUGS-25718)

- 以前は、**install-config.yaml** ファイルで指定されたアーキテクチャーと一致しない仮想マシンタイプを選択した場合、インストールは失敗していました。このリリースにより、インストールを開始する前に検証チェックによってアーキテクチャーが一致していることが確認されます。(OCPBUGS-25600)

- 以前は、コントロールプレーンのレプリカに無効な数 (2 など) が指定された場合、Agent-based のインストールが失敗する可能性がありました。このリリースにより、インストールプログラムによって、Agent-based のインストールに対して 1 つまたは 3 つのコントロールプレーンレプリカを指定することが必須となりました。(OCPBUGS-25462)

- 以前は、コントロールプレーンマシンセットのテクノロジープレビュー機能を使用して VMware vSphere にクラスターをインストールすると、結果として得られるコントロールプレーンマシンセットの設定に重複した障害ドメインがありました。このリリースにより、インストールプログラムは正しい障害ドメインを持つコントロールプレーンマシンセットを作成します。(OCPBUGS-25453)

- 以前は、installer-provisioned installation の前に必要な **iam:TagInstanceProfile** 権限が検証されなかったため、Identity and Access Management (IAM) 権限が不足しているとインストールが失敗していました。このリリースにより、インストールを開始する前に検証チェックによって権限が含まれていることが確認されます。(OCPBUGS-25440)

- 以前は、インストールプログラムでは、Cloud Credential が必須であるにもかかわらず、Cloud Credential 情報機能が無効になっているベアメタル以外のプラットフォームにユーザーがクラスターをインストールすることを阻止しませんでした。このリリースにより、インストールプログラムによってエラーが生成され、Cloud Credential 情報が無効になっている状態でのインストールが阻止されます (ベアメタルプラットフォームを除く)。(OCPBUGS-24956)

- 以前は、インスタンスタイプでサポートされているアーキテクチャーとは異なるアーキテクチャーを設定すると、一部のリソースが作成された後にインストールが途中で失敗していました。このリリースにより、検証チェックにより、インスタンスタイプが指定されたアーキテクチャーと互換性があるかどうかが検証されます。アーキテクチャーに互換性がない場合、インストールが開始される前にプロセスが失敗します。(OCPBUGS-24575)

- 以前は、インストールプログラムは、Cloud Controller Manager が無効になっているクラウドプロバイダーにユーザーがクラスターをインストールすることを阻止しなかったため、有用なエラーメッセージを表示せずに失敗していました。このリリースにより、クラウドプラットフォームへのインストールには Cloud Controller Manager 機能が必要であることを示すエラーが、インストールプログラムによって生成されます。(OCPBUGS-24415)

- 以前は、IBM Cloud® API からの予期しない結果が原因で、インストールプログラムが IBM

Cloud® にインストールされたクラスターを削除できないことがありました。このリリースでは、IBM Cloud® にインストールされたクラスターをインストールプログラムによって確実に削除できるようになりました。(OCPBUGS-20085)

- 以前は、インストールプログラムでは、FIPS 対応のクラスターを FIPS 対応の Red Hat Enterprise Linux (RHEL) ホストからインストールするという要件が強制されませんでした。このリリースにより、インストールプログラムによって FIPS 要件が強制されます。(OCPBUGS-15845)

- 以前は、**install-config.yaml** ファイルに設定されたプロキシー情報は、ブートストラッププロセスに適用されませんでした。このリリースにより、プロキシー情報がブートストラップ Ignition データに適用され、その後ブートストラップマシンに適用されます。(OCPBUGS-12890)

- 以前は、IBM Power® Virtual Server プラットフォームに Dynamic Host Configuration Protocol (DHCP) ネットワーク名がない場合、DHCP リソースは削除されませんでした。このリリースでは、**ERROR** 状態の DHCP リソースがチェックによって検索され、削除されるため、この問題は発生しなくなります。(OCPBUGS-35224)

- 以前は、Cluster API を使用して installer-provisioned infrastructure 上に IBM Power® Virtual Server クラスターを作成すると、ロードバランサーがビジー状態になり、停止していました。このリリースにより、**PollUntilContextCancel** ループで 'AddIPToLoadBalancerPool' コマンドを使用して、ロードバランサーを再起動できます。(OCPBUGS-35088)

- 以前は、FIPS 対応ノードを備えたベアメタルプラットフォーム上の installer-provisioned installation により、インストールに失敗していました。このリリースにより、この問題は解決されました。(OCPBUGS-34985)

- 以前は、IBM Power® Virtual Server 上で installer-provisioned installation のインストール設定を作成するときに、管理者が OpenShift CLI (**oc**) でコマンドを入力しなかった場合、survey が停止していました。**install-config** survey でデフォルトのリージョンが設定されていなかったため、survey は停止しました。このリリースにより、この問題は解決されました。(OCPBUGS-34728)

- 以前は、SATA ハードウェアを使用するソリッドステートドライブ (SSD) は取り外し可能として識別されていました。OpenShift Container Platform の Assisted Installer は、適切なディスクが見つからず、インストールが停止したと報告していました。このリリースでは、リムーバブルディスクがインストール対象になります。(OCPBUGS-34652)

- 以前は、ノード間で IPv6 接続を確立できたにもかかわらず、デュアルスタックネットワークを使用した Agent-based のインストールは、IPv6 接続チェックの失敗により失敗していました。このリリースでは、この問題は解決されました。(OCPBUGS-31631)

- 以前は、プログラミングエラーにより、コントロールプレーンにポリシーがセットされたコンピュートサーバーグループをスクリプトが作成していました。その結果、コンピュートグループでは **install-config.yaml** ファイルの **serverGroupPolicy** プロパティーが無視されました。この修正により、コンピュートマシンプールの **install-config.yaml** ファイルで設定されたサーバーグループポリシーが、スクリプトフローのインストール時に適用されます。(OCPBUGS-31050)

- 以前は、**openshift-baremetal-install** バイナリーを使用する Agent-based のインストールを設定するときに、Agent-based Installer は誤って libvirt ネットワークインターフェイスの検証を試行していました。これにより、次のエラーが発生する可能性があります。

  ```
  Platform.BareMetal.externalBridge: Invalid value: "baremetal": could not find interface
  "baremetal"
  ```

この更新により、Agent-based のインストール方法では libvirt が必要ないため、この誤った検証が無効になり、問題が解決されました。(OCPBUGS-30941)

- 以前は、Open vSwitch ベースの Software Defined Networking (SDN) または Open Virtual Network (OVN) 以外のデュアルスタックネットワークでネットワークタイプを使用すると、検証エラーが発生しました。このリリースにより、この問題は解決されました。(OCPBUGS-30232)

- 以前は、RHOSP 上の user-provisioned infrastructure インストールの **nodePort** サービスの IPv6 ポート範囲が閉じられていたため、特定のノードポートを介したトラフィックがブロックされていました。このリリースにより、**security-group.yaml** Playbook に適切なセキュリティーグループルールが追加され、問題が解決されました。(OCPBUGS-30154)

- 以前は、**openshift-install agent create cluster-manifests** コマンドを使用して生成されたマニフェストは、タイプデータが含まれていなかったため、OpenShift Container Platform クラスターに直接適用されませんでした。このリリースにより、マニフェストにタイプデータが追加されました。管理者はマニフェストを適用して、Agent-based インストールと同じ設定を使用する Zero Touch Provisioning (ZTP) インストールを開始できるようになりました。(OCPBUGS-29968)

- 以前は、**aarch64** エージェント ISO の生成中に、**aarch64** アーキテクチャーに必要なファイルの名前が誤って変更されていました。このリリースにより、指定されたファイルの名前は変更されません。(OCPBUGS-28827)

- 以前は、VMware vSphere にクラスターをインストールするときに、ESXi ホストがメンテナンスモードになっていると、インストールプログラムがホストからバージョン情報を取得できないため、インストールが失敗していました。このリリースにより、インストールプログラムはメンテナンスモードの ESXi ホストからバージョン情報を取得しようとしないため、インストールを続行できます。(OCPBUGS-27848)

- 以前は、IBM Cloud® Terraform プラグインは、クラスターのインストール中に非プライベートサービスエンドポイントの使用を誤って阻止していました。このリリースにより、IBM Cloud® Terraform プラグインはインストール時に非プライベートサービスエンドポイントをサポートします。(OCPBUGS-24473)

- 以前は、VMware vSphere にクラスターをインストールするには、データストアへのフルパスを指定する必要がありました。このリリースにより、インストールプログラムはデータストアのフルパスと相対パスを受け入れるようになりました。(OCPBUGS-22410)

- 以前は、Agent-based インストールプログラムを使用して OpenShift Container Platform クラスターをインストールすると、インストール前の多数のマニフェストによって Ignition ストレージがいっぱいになり、インストールが失敗する可能性がありました。このリリースにより、Ignition ストレージが拡張され、より多くのインストールマニフェストを保存できるようになりました。(OCPBUGS-14478)

- 以前は、**coreos-installer iso kargs show <iso>** コマンドをエージェント ISO ファイルで使用すると、指定された ISO に埋め込まれたカーネル引数が出力に正しく表示されませんでした。このリリースにより、コマンド出力に情報が正しく表示されるようになりました。(OCPBUGS-14257)

- 以前は、Agent-based インストールでは、**ImageContentSource** オブジェクトは非推奨でしたが、**ImageDigestSources** の代わりに作成されていました。このリリースにより、Agent-based のインストールプログラムによって **ImageDigestSource** オブジェクトが作成されます。(OCPBUGS-11665)

- 以前は、Power VS の破棄機能に問題があり、期待どおりにすべてのリソースが削除されませんでした。このリリースでは、この問題は解決されました。(OCPBUGS-29425)

Insights Operator

- Insights Operator は、**openshift-monitoring** の外部で以下のカスタムリソースのインスタンスを収集するようになりました。
  - 種類: **Prometheus** グループ: **monitoring.coreos.com**
  - 種類: **AlertManager** グループ: **monitoring.coreos.com**
    (OCPBUGS-35086)

Kubernetes コントローラーマネージャー

- 以前は、フォアグラウンド削除カスケードストラテジーを使用して **ClusterResourceQuota** リソースを削除しても、完全に削除されませんでした。このリリースにより、フォアグラウンドカスケードストラテジーを使用する場合、**ClusterResourceQuota** リソースが適切に削除されるようになりました。(OCPBUGS-22301)

Machine Config Operator

- 以前は、**MachineConfigNode** オブジェクトは適切な所有者で作成されていませんでした。その結果、**MachineConfigNode** オブジェクトをガベージコレクションすることができず、以前に生成されたが役に立たなくなったオブジェクトが削除されませんでした。このリリースにより、**MachineConfigNode** オブジェクトの作成時に適切な所有者が設定され、廃止されたオブジェクトがガベージコレクションで使用できるようになりました。(OCPBUGS-30090)

- 以前は、**nodeStatusUpdateFrequency** パラメーターのデフォルト値が **0s** から **10s** に変更されました。この変更により、値が **nodeStatusReportFrequency** 値にリンクされていたため、**nodeStatusReportFrequency** が大幅に増加しました。その結果、コントロールプレーン Operator と API サーバーの CPU 使用率が高まりました。この修正により、**nodeStatusReportFrequency** の値が手動で **5m** に設定され、CPU 使用率の増加を阻止します。(OCPBUGS-29713)

- 以前は、環境変数の入力ミスにより、スクリプトは **node.env** ファイルが存在するかどうかを検出できませんでした。このため、再起動のたびに **node.env** ファイルが上書きされ、kubelet ホスト名が修正されませんでした。この修正により、入力ミスが修正されました。その結果、**node.env** への編集は再起動後も保持されるようになりました。(OCPBUGS-27261)

- 以前は、**kube-apiserver** サーバーの認証局 (CA) 証明書がローテーションされたときに、Machine Config Operator (MCO) が適切に反応せず、ディスク上の kubelet kubeconfig を更新しませんでした。これは、ノード上の kubelet と一部の Pod が最終的に API サーバーと通信できなくなり、ノードが **NotReady** 状態になったことを意味しました。このリリースにより、MCO は変更に適切に反応し、ディスク上の kubeconfig を更新して、ローテーション時に APIServer との認証済み通信を継続できるようにし、kubelet/MCDaemon Pod も再起動します。認証局の有効期間は 10 年であるため、このローテーションはめったに発生せず、通常は中断されません。(OCPBUGS-25821)

- 以前は、新しいノードが、クラスターに追加されたり、クラスターから削除された場合、**MachineConfigNode** (MCN) オブジェクトは反応しませんでした。その結果、関係のない MCN オブジェクトが存在しました。このリリースにより、ノードが追加または削除されたときに、Machine Config Operator が MCN オブジェクトを適切に削除および追加します。(OCPBUGS-24416)

- 以前は、**nodeip-configuration** サービスはシリアルコンソールにログを送信しなかったため、ネットワークが利用できず、ノードにアクセスできない場合に問題をデバッグすることが困難でした。このリリースにより、**nodeip-configuration** サービスは、ノードへのネットワークアクセスがない場合でも、デバッグを容易にするために出力をシリアルコンソールに記録します。(OCPBUGS-19628)

- 以前は、**MachineConfigPool** で **OnClusterBuild** 機能が有効になっていて、**configmap** が無効な **imageBuilderType** で更新された場合、machine-config ClusterOperator は degraded になりませんでした。このリリースにより、Machine Config Operator (MCO) **ClusterOperator** ステータスは、同期するたびに **OnClusterBuild** 入力を検証し、入力が無効な場合は **ClusterOperator** が degraded になるようにします。(OCPBUGS-18955)

- 以前は、**machine config not found** エラーが報告されたときに、問題をトラブルシューティングして修正するための情報が不十分でした。このリリースにより、Machine Config Operator にアラートとメトリクスが追加されました。その結果、**machine config not found** エラーをトラブルシューティングして修正するための詳細な情報が得られます。(OCPBUGS-17788)

- 以前は、ノードにホスト名を設定するために使用されていた Afterburn サービスは、メタデータサービスが利用可能になるのを待機している間にタイムアウトし、OVN-Kubernetes を使用してデプロイするときに問題が発生していました。現在、Afterburn サービスはメタデータサービスが利用可能になるまでより長い時間待機するようになり、タイムアウトの問題が解決されました。(OCPBUGS-11936)

- 以前は、ノードが **MachineConfigPool** から削除された場合、Machine Config Operator (MCO) はエラーやノードの削除を報告しませんでした。MCO は、ノードがプール内にない場合のノードの管理をサポートしておらず、ノードが削除された後にノード管理が停止したことを示すものはありませんでした。このリリースにより、ノードがすべてのプールから削除されると、MCO によってエラーがログに記録されるようになりました。(OCPBUGS-5452)

管理コンソール

- 以前は、**Completed** ステータスの Pod に対して **Debug container** リンクは表示されませんでした。このリリースにより、リンクは期待どおりに表示されます。(OCPBUGS-34711)

- 以前は、PatternFly 5 の問題により、Web コンソールのテキストボックスのサイズを変更できませんでした。このリリースにより、テキストボックスのサイズが再び変更可能になりました。(OCPBUGS-34393)

- 以前は、Web コンソールではフランス語とスペイン語は利用できませんでした。このリリースにより、フランス語とスペイン語の翻訳が利用可能になりました。(OCPBUGS-33965)

- 以前は、マストヘッドロゴは **max-height** の 60 ピクセルに制限されていませんでした。その結果、高さが 60 ピクセルを超えるロゴがネイティブサイズで表示され、これが原因でマストヘッドのサイズも大きくなりすぎていました。このリリースにより、マストヘッドロゴの高さの最大値が 60px に制限されました。(OCPBUGS-33523)

- 以前は、**HealthCheck** コントローラーに return ステートメントが欠落していたため、特定の状況下でパニックが発生していました。このリリースにより、**HealthCheck** コントローラーに適切な return ステートメントが追加されたため、パニックが発生しなくなりました。(OCPBUGS-33505)

- 以前は、誤ったフィールドが API サーバーに送信されていましたが、通知されていませんでした。警告を表示する Admission Webhook の実装により、同じアクションで警告通知が返されます。この問題を解決するための修正が提供されました。(OCPBUGS-33222)

- 以前は、タイムスタンプが存在しない場合、**StatusItem** のメッセージテキストがアイコンと垂直方向でずれる可能性がありました。このリリースにより、メッセージテキストが正しく配置されるようになりました。(OCPBUGS-33219)

- 以前は、作成者フィールドは自動入力され、必須ではありませんでした。API の更新により、OpenShift Container Platform 4.15 以降ではフィールドが空になりました。このリリースにより、正しい検証のためにフィールドが必須としてマークされています。(OCPBUGS-31931)

- 以前は、Web コンソールの YAML エディターには **Create** ボタンがなく、サンプルは Web コンソールに表示されませんでした。このリリースにより、**Create** ボタンとサンプルが表示されるようになりました。(OCPBUGS-31703)

- 以前は、外部 OpenID Connect (OIDC) 機能のブリッジサーバーフラグを変更すると、ローカル開発でブリッジサーバーが起動しなくなりました。このリリースにより、フラグの使用法が更新され、ブリッジサーバーが起動します。(OCPBUGS-31695)

- 以前は、VMware vSphere 接続を編集するときに、実際に値が変更されていなくてもフォームが送信されることがありました。その結果、不要なノードの再起動が発生しました。このリリースにより、コンソールがフォームの変更を検出するようになり、値が変更されていない場合は送信を許可しなくなりました。(OCPBUGS-31613)

- 以前は、**from the console** フォームメソッドが使用された場合、**NetworkAttachmentDefinition** は常にデフォルトの namespace に作成されていました。選択された名前も考慮されず、選択された名前とランダムな接尾辞を持つ **NetworkAttachmentDefinition** オブジェクトが作成されます。このリリースにより、**NetworkAttachmentDefinition** オブジェクトが現在のプロジェクトに作成されます。(OCPBUGS-31558)

- 以前は、**AlertmanagerRecieversNotConfigured** アラートの **Configure** ボタンをクリックしても、**Configuration** ページが表示されませんでした。このリリースにより、**AlertmanagerRecieversNotConfigured** アラートのリンクが修正され、**Configuration** ページに移動できるようになりました。(OCPBUGS-30805)

- 以前は、**ListPageFilters** を使用するプラグインは、2 つのフィルター (ラベルと名前) のみを使用していました。このリリースにより、プラグインが複数のテキストベースの検索フィルターを設定できるようにするパラメーターが追加されました。(OCPBUGS-30077)

- 以前は、クイックスタート項目をクリックしても応答がありませんでした。このリリースでは、クイックスタートの選択をクリックすると、クイックスタートウィンドウが表示されます。(OCPBUGS-29992)

- 以前は、最初の試行で認証検出に失敗すると、OpenShift Container Platform Web コンソールが予期せず終了していました。このリリースにより、認証の初期化が更新され、失敗するまで最大 5 分間再試行されるようになりました。(OCPBUGS-29479)

- 以前は、CLI で Image Manifest Vulnerability (IMV) が作成された後、**Image Manifest Vulnerability** ページにエラーメッセージが表示されるという問題がありました。このリリースにより、エラーメッセージは表示されなくなりました。(OCPBUGS-28967)

- 以前は、アクションフックの一部としてフック内のモーダルダイアログを使用すると、コンソールフレームワークがレンダリングサイクルの一部として null オブジェクトを渡したため、エラーが発生していました。このリリースにより、**getGroupVersionKindForResource** は null セーフになり、**apiVersion** または **kind** が未定義の場合は **undefined** を返します。さらに、**useDeleteModal** のランタイムエラーは発生しなくなりましたが、**undefined** リソースでは機能しないことに注意してください。(OCPBUGS-28856)

- 以前は、**Expand PersistentVolumeClaim** モーダルは、**pvc.spec.resources.requests.stroage** 値に単位が含まれていることを前提としていました。このリリースにより、サイズが 2GiB に更新され、永続ボリューム要求 (PVC) の値を変更できます。(OCPBUGS-27779)

- 以前は、OpenShift Container Platform Web コンソールで報告されるイメージの脆弱性の値に一貫性がありませんでした。このリリースにより、**Overview** ページのイメージの脆弱性が削除されました。(OCPBUGS-27455)

- 以前は、最近承認されたノードに対して証明書署名要求 (CSR) が表示されることがありました。このリリースにより、重複が検出され、承認されたノードの CSR は表示されなくなりました。(OCPBUGS-27399)

- 以前は、**MachineHealthCheck detail** ページの条件テーブルで、**タイプ** 列が最初にありませんでした。このリリースにより、**タイプ** が条件テーブルの最初にリストされるようになりました。(OCPBUGS-27246)

- 以前は、コンソールプラグインプロキシーはプラグインサービスの応答からステータスコードをコピーしていませんでした。これにより、プラグインサービスからのすべての応答のステータスが **200** になり、特にブラウザーのキャッシュに関して予期しない動作が発生しました。このリリースにより、コンソールプロキシーロジックが更新され、プラグインサービスプロキシー応答ステータスコードを転送するようになりました。プロキシーされたプラグイン要求が、期待どおりに動作するようになりました。(OCPBUGS-26933)

- 以前は、永続ボリューム要求 (PVC) を複製する場合、モーダルは **pvc.spec.resources.requests.storage** 値にユニットが含まれていると想定していました。このリリースにより、**pvc.spec.resources.requests.storage** にユニット接尾辞が含まれ、**Clone PVC** モーダルが期待どおりに動作するようになりました。(OCPBUGS-26772)

- 以前は、VMware vSphere 接続を編集するときにエスケープ文字列が適切に処理されず、VMware vSphere 設定が壊れていました。このリリースにより、エスケープ文字列が期待どおりに機能し、VMware vSphere 設定が壊れなくなりました。(OCPBUGS-25942)

- 以前は、VMware vSphere 接続を設定するときに、**resourcepool-path** キーが VMware vSphereconfig map に追加されなかったため、VMware vSphere への接続で問題が発生する可能性がありました。このリリースでは、VMware vSphere への接続に関する問題は発生しなくなりました。(OCPBUGS-25927)

- 以前は、**Customer feedback** モーダルのテキストが欠落していました。このリリースにより、リンクテキストが復元され、正しい Red Hat イメージが表示されます。(OCPBUGS-25843)

- 以前は、**Cluster Settings** ページから **Select a version** をクリックしても、**Update cluster** モーダルは開きませんでした。このリリースにより、**Select a version** をクリックすると、**Update cluster** モーダルが表示されるようになりました。(OCPBUGS-25780)

- 以前は、モバイルデバイスでは、**Search** ページのリソースセクションのフィルター部分がモバイルデバイスでは機能しませんでした。このリリースにより、モバイルデバイスでフィルタリングが期待どおりに機能するようになりました。(OCPBUGS-25530)

- 以前は、コンソール Operator はクラスターリソースを取得するためにリスナーではなくクライアントを使用していました。これが原因で、Operator は古いリビジョンのリソースに対して操作を実行していました。このリリースにより、コンソール Operator はリストを使用して、クライアントではなくクラスターからデータを取得するようになりました。(OCPBUGS-25484)

- 以前は、コンソールは、復元のボリュームスナップショットからの復元サイズ値を新しい永続ボリューム要求 (PVC) モーダルとして誤って解析していました。このリリースにより、モーダルは復元サイズを正しく解析するようになりました。(OCPBUGS-24637)

- 以前は、ルーティングライブラリーの変更により、コンソールで **Alerting**、**Metrics**、および **Target** ページは使用できませんでした。このリリースにより、ルートが正しく読み込まれるようになりました。(OCPBUGS-24515)

- 以前は、条件のない **MachineHealthCheck** が存在する場合、**Node details** ページでランタイムエラーが発生していました。このリリースにより、**Node details** ページが期待どおりに読み込まれるようになりました。(OCPBUGS-24408)

- 以前は、コンソールバックエンドがオペランドリスト要求をパブリック API サーバーエンドポイントにプロキシーしていたため、状況によっては CA 証明書の問題が発生していました。このリリースにより、プロキシー設定が更新され、内部 API サーバーエンドポイントを指すようになり、この問題が修正されました。(OCPBUGS-22487)

- 以前は、**HorizontalPodAutoscaler** が存在する場合、デプロイメントをスケールアップまたはスケールダウンすることができませんでした。このリリースにより、**HorizontalPodAutoscaler** を使用したデプロイメントが **zero** にスケールダウンされると、**Enable Autoscale** ボタンが表示され、Pod の自動スケーリングを有効にできるようになります。(OCPBUGS-22405)

- 以前は、ファイルを編集する際に、**Info alert:Non-printable file detected. File contains non-printable characters.Preview is not available.** というエラーが発生していました。このリリースにより、ファイルがバイナリーであるかを判断するためのチェックが追加され、期待どおりにファイルを編集できるようになりました。(OCPBUGS-18699)

- 以前は、コンソール API 変換 Webhook サーバーはランタイム時に提供する証明書を更新できず、署名キーを削除してこれらの証明書を更新すると失敗していました。これが原因で、CA 証明書がローテーションされたときにコンソールが回復しなくなりました。このリリースにより、コンソール変換 Webhook サーバーが更新され、CA 証明書の変更を検出し、ランタイム時に処理できるようになりました。CA 証明書がローテーションされた後、サーバーは引き続き使用可能となり、コンソールは期待どおりに回復します。(OCPBUGS-15827)

- 以前は、コンソールフロントエンドバンドルの実稼働環境でのビルドで、ソースマップが無効になっていました。その結果、ソースコードを分析するためのブラウザーツールを実稼働環境でのビルドで使用することができませんでした。このリリースにより、コンソールの Webpack 設定が更新され、プロダクションビルドでソースマップが有効になりました。ブラウザーツールは、開発環境および実稼働環境でのビルドの両方で、期待どおりに動作するようになりました。(OCPBUGS-10851)

- 以前は、コンソールリダイレクトサービスには、コンソールサービスと同じサービス認証局 (CA) コントローラーアノテーションがありました。このため、サービス CA コントローラーがこれらのサービスの CA 証明書を誤って同期することがあり、削除および再インストール後にコンソールが正しく機能しなくなりました。このリリースにより、コンソール Operator が更新され、コンソールリダイレクトサービスからこのサービス CA アノテーションが削除されました。Operator が削除状態から管理状態に移行したときに、コンソールサービスと CA 証明書が期待どおりに機能するようになりました。(OCPBUGS-7656)

- 以前は、**Form view** を使用してルートを編集するときに代替サービスを削除しても、ルートから代替サービスが削除されませんでした。この更新により、代替サービスは削除されました。(OCPBUGS-33011)

- 以前は、クラスターの更新を実行すると、一時停止された **MachineConfigPools** のノードが誤って一時停止を解除される可能性がありました。このリリースでは、クラスターの更新を実行するときに、一時停止された **MachineConfigPools** のノードが正しく一時停止されたままになります。(OCPBUGS-23319)

モニタリング

- 以前は、特定のファイバーチャネルデバイスドライバーがすべての属性を公開しなかった場合、**node-exporter** エージェントのファイバーチャネルコレクターが失敗していました。このリリースにより、ファイバーチャネルコレクターはこれらのオプション属性を無視し、問題は解決されました。(OCPBUGS-20151)

- 以前は、**oc get podmetrics** コマンドと **oc get nodemetrics** コマンドが正しく機能していませんでした。このリリースでは、この問題は解決されました。(OCPBUGS-25164)

- 以前は、**ServiceMonitor** リソースに無効な **.spec.endpoints.proxyUrl** 属性を設定すると、Prometheus が破損し、再読み込みされて再起動していました。この更新により、**proxyUrl** 属性を無効な構文に対して検証することで問題が修正されます。(OCPBUGS-30989)

ネットワーク

- 以前は、Ingress API の **status.componentRoutes.currentHostnames** フィールドの API ドキュメントに開発者メモが含まれていました。**oc explain ingresses.status.componentRoutes.currentHostnames --api-version=config.openshift.io/v1** コマンドを入力すると、意図された情報とともに開発者メモが出力に表示されます。このリリースにより、開発者メモが **status.componentRoutes.currentHostnames** フィールドから削除され、コマンドを入力すると、出力にルートで使用されている現在のホスト名がリストされるようになりました。(OCPBUGS-31058)

- 以前の負荷分散アルゴリズムでは、重みを決定する際にアクティブなサービスと非アクティブなサービスを区別していなかったため、非アクティブなサービスが多い環境や、重み **0** でバックエンドをルーティングする環境では、random アルゴリズムが過度に使用されていました。これにより、メモリー使用量が増加し、過剰なメモリー消費のリスクが高まりました。このリリースにより、アクティブなサービスのみへのトラフィックの方向を最適化し、重み付けの高い random アルゴリズムの不必要な使用を防ぐように変更が加えられ、過剰なメモリー消費の可能性が軽減されます。(OCPBUGS-29690)

- 以前は、同じ証明書に複数のルートが指定されている場合、またはルートがデフォルトの証明書をカスタム証明書として指定し、ルーターで HTTP/2 が有効になっている場合、HTTP/2 クライアントはルートで接続の結合を実行できました。Web ブラウザーなどのクライアントは接続を再利用し、間違ったバックエンドサーバーに接続する可能性がありました。このリリースにより、OpenShift Container Platform ルーターは、同じ証明書が複数のルートで指定されているか、ルートがデフォルトの証明書をカスタム証明書として指定しているかをチェックするようになりました。これらの条件のいずれかが検出されると、ルーターは HAProxy ロードバランサーを設定して、これらの証明書を使用するルートへの HTTP/2 クライアント接続を許可しないようにします。(OCPBUGS-29373)

- 以前は、**routingViaHost** パラメーターを **true** に設定してデプロイメントを設定すると、トラフィックが IPv6 **ExternalTrafficPolicy=Local** ロードバランサーサービスに到達できませんでした。本リリースでは、この問題が修正されています。(OCPBUGS-27211)

- 以前は、セカンダリーネットワークインターフェイスコントローラー (NIC) でホストされている **EgressIp** オブジェクトによって選択された Pod により、ノード IP アドレスへの接続がタイムアウトしていました。本リリースでは、この問題が修正されています。(OCPBUGS-26979)

- 以前は、OpenShift Container Platform Precision Time Protocol (PTP) Operator によってインストールされた leap ファイルパッケージは、パッケージの有効期限が切れていたため、**ts2phc** プロセスで使用できませんでした。このリリースにより、leap ファイルパッケージが更新され、全地球測位システム (GPS) 信号から leap イベントを読み取り、オフセットを動的に更新するようになったため、期限切れのパッケージ状況が発生しなくなりました。(OCPBUGS-25939)

- 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 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。このリリースにより、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-24608)

- 以前は、シングルスタックおよびデュアルスタックのデプロイメントを含む IPv6 の OpenShift Container Platform 上の 2 つのスクリプト間で競合が発生していました。1 つのスクリプトはホスト名を完全修飾ドメイン名 (FQDN) に設定しましたが、もう 1 つのスクリプトはホスト名を早い段階で短い名前に設定する可能性があります。この競合は、ホスト名を FQDN に設定する

イベントが、ホスト名を短い名前に設定するスクリプトの後に実行される可能性があるために発生しました。これは非同期ネットワークイベントが原因で発生しました。このリリースにより、FQDN が適切に設定されることを確認するための新しいコードが追加されました。この新しいコードにより、ホスト名の設定を許可する前に、特定のネットワークイベントを待機するようになります。(OCPBUGS-22324)

- 以前は、セカンダリーインターフェイスを介して **EgressIP** によって選択された Pod のラベルが削除されると、同じ namespace 内の別の Pod も **EgressIP** の割り当てを失い、外部ホストとの接続が切断されていました。このリリースでこの問題が修正され、Pod ラベルが削除され、**EgressIP** の使用が停止しても、一致するラベルを持つ他の Pod は中断することなく **EgressIP** を引き続き使用します。(OCPBUGS-20220)

- 以前は、Global Navigation Satellite Systems (GNSS) モジュールは、GPS **fix** 位置と、GNSS モジュールとコンステレーション間のオフセットを表す GNSS **offset** 位置の両方を報告することができました。以前の T-GM では、**offset** 位置と **fix** 位置の読み取り用に **ublox** モジュールをプローブするために **ubloxtool** CLI ツールを使用していませんでした。代わりに、GPSD 経由でのみ GPS **fix** 情報を読み取ることができました。これは、**ubloxtool** CLI ツールの以前の実装では応答の受信に 2 秒かかり、呼び出しごとに CPU 使用率が 3 倍に増加していたためです。このリリースにより、**ubloxtool** リクエストが最適化され、GPS **オフセット** 位置が利用できるようになりました。(OCPBUGS-17422)

- 以前は、競合状態のため、セカンダリーインターフェイスによってホストされている **EgressIP** Pod はフェイルオーバーしませんでした。既存の IP アドレスと競合しているため、**EgressIP** Pod を割り当てることができないことを示すエラーメッセージがユーザーに表示されました。このリリースにより、**EgressIP** Pod は Egress ノードに移動します。(OCPBUGS-20209)

- 以前は、OVN-Kubernetes で使用されている物理インターフェイスで MAC アドレスが変更された場合、OVN-Kubernetes 内で正しく更新されず、トラフィックの中断やノードからの Kube API の停止が長時間発生する可能性がありました。これは、ボンドインターフェイスが使用されている場合に最も一般的であり、どのデバイスが最初に起動したかに応じてボンドの MAC アドレスが入れ替わる可能性がありました。このリリースより、問題が修正され、OVN-Kubernetes が MAC アドレスの変更を動的に検出し、正しく更新するようになりました。(OCPBUGS-18716)

- 以前は、プライマリーネットワークインターフェイスではないネットワークインターフェイスに Egress IP を割り当てる場合、IPv6 はサポートされていませんでした。この問題は解決されており、Egress IP は IPv6 にすることができます。(OCPBUGS-24271)

- 以前は、デバッグツールである **network-tools** イメージに、Wireshark ネットワークプロトコルアナライザーが含まれていました。Wireshark は **gstreamer1** パッケージに依存しており、このパッケージには特定のライセンス要件があります。このリリースにより、**gstreamer1** パッケージが network-tools イメージから削除され、イメージに **wireshark-cli** パッケージが含まれるようになりました。(OCPBUGS-31699)

- 以前は、ノードのデフォルトゲートウェイが **vlan** に設定され、複数のネットワークマネージャー接続の名前が同じである場合、デフォルトの OVN-Kubernetes ブリッジを設定できなかったため、ノードは失敗していました。このリリースにより、**configure-ovs.sh** シェルスクリプトには、同じ名前の接続が多数存在する場合に正しいネットワークマネージャー接続を取得する **nmcli connection show uuid** コマンドが含まれるようになりました。(OCPBUGS-24356)

- Microsoft Azure 上の OpenShift Container Platform クラスターでは、Container Network Interface (CNI) として OVN-Kubernetes を使用する場合、**externalTrafficPolicy: Local** でロードバランサーサービスを使用すると、Pod によって認識されるソース IP がノードの OVN ゲートウェイルーターになるという問題が発生しました。これは、UDP パケットにソースネットワークアドレス変換 (SNAT) が適用されたために発生しました。
この更新により、アフィニティータイムアウトを **86400** 秒 (24 時間) などのより高い値に設定

することで、タイムアウトのないセッションアフィニティーが可能になります。その結果、エンドポイントやノードのダウンなどのネットワークの中断が発生しない限り、アフィニティーは永続的なものとして扱われます。これにより、セッションアフィニティーはより永続的になります。(OCPBUGS-24219)

Node

- 以前は、Ansible の OpenShift Container Platform のアップグレードでは、IPsec 設定がべき等ではなかったためエラーが発生していました。この更新により、この問題は解決されました。現在、OpenShift Ansible Playbook のすべての IPsec 設定はべき等になりました。(OCPBUGS-30802)

- 以前は、CRI-O は、古いペイロードイメージがノード上のスペースを占有しないように、OpenShift Container Platform のマイナーバージョンアップグレード間でインストールされたすべてのイメージを削除していました。しかし、これはパフォーマンスの低下を招くと判断され、この機能は削除されました。この修正により、ディスク使用量が一定のレベルに達した後も、kubelet は古いイメージを引き続きガベージコレクションします。その結果、OpenShift Container Platform はマイナーバージョン間のアップグレード後にすべてのイメージを削除しなくなりました。(OCPBUGS-24743)

Node Tuning Operator (NTO)

- 以前は、**net.core.busy_read**、**net.core.busy_poll**、**kernel.numa_balancing sysctls** がリアルタイムカーネルに存在しなかったため、シングルノードの OpenShift Container Platform 上の分散ユニットプロファイルが degraded になっていました。このリリースにより、Tuned プロファイルは degraded にならなくなり、この問題は解決されました。(OCPBUGS-23167)

- 以前は、**PerformanceProfile** が適用された後、Tuned プロファイルによって **Degraded** 状態が報告されていました。このプロファイルは、デフォルトの受信パケットステアリング (RPS) マスクの **sysctl** 値の設定を試みましたが、マスクは **/etc/sysctl.d** ファイルを使用してすでに同じ値で設定されていました。この更新により、Tuned プロファイルで **sysctl** 値が設定されなくなり、問題は解決されました。(OCPBUGS-24638)

- 以前は、Performance Profile Creator (PPC) が、Day 0 パフォーマンスプロファイルマニフェストの **metadata.ownerReferences.uid** フィールドに誤った入力をしていました。その結果、手動による介入なしに Day 0 のパフォーマンスプロファイルを適用することは不可能でした。このリリースにより、PPC は Day 0 マニフェストの **metadata.ownerReferences.uid** フィールドを生成しなくなりました。その結果、期待どおりに Day 0 のパフォーマンスプロファイルマニフェストを適用できるようになりました。(OCPBUGS-29751)

- 以前は、TuneD デーモンは、Tuned カスタムリソース (CR) の更新後に不必要に再ロードする可能性がありました。このリリースにより、Tuned オブジェクトが削除され、TuneD (デーモン) プロファイルが Tuned プロファイル Kubernetes オブジェクトに直接組み込まれるようになりました。その結果、問題は解決されました。(OCPBUGS-32469)

OpenShift CLI (oc)

- 以前は、互換性のないセマンティックバージョン管理を持つ Operator イメージをミラーリングすると、oc-mirror プラグイン v2 (テクノロジープレビュー) が失敗して終了していました。この修正により、コンソールに警告が表示され、スキップされたイメージが示されて、ミラーリングプロセスが中断されることなく続行できるようになります。(OCPBUGS-34587)

- これまで、oc-mirror プラグイン v2 (テクノロジープレビュー) は、**tag** と **digest** の両方の形式を持つイメージ参照を含む特定の Operator カタログをミラーリングできませんでした。この問題により、**ImageDigestMirrorSource** (IDMS) や **ImageTagMirrorSource** (ITMS) などのクラ

スターリソースを作成できませんでした。この更新により、oc-mirror は、**tag** と **digest** の両方の参照を持つイメージをスキップし、コンソール出力に適切な警告メッセージを表示することで、この問題を解決します。(OCPBUGS-33196)

- 以前の oc-mirror プラグイン v2 (テクノロジープレビュー) では、ミラーリングエラーはコンソール出力にのみ表示され、ユーザーが他の問題を分析してトラブルシューティングすることが困難でした。たとえば、不安定なネットワークでは再実行が必要になる場合がありますが、マニフェストの不明なエラーの場合は、イメージまたは Operator をスキップするためにさらに分析することを推奨します。この更新により、ワークスペースの **working-dir/logs** フォルダー内のすべてのエラーを含むファイルが生成されます。ミラーリングプロセス中に発生するすべてのエラーは、**mirroring_errors_YYYYMMdd.txt** に記録されるようになりました。(OCPBUGS-33098)

- 以前は、Cloud Credential Operator ユーティリティー (**ccoctl**) は、FIPS が有効になっている RHEL 9 ホストでは実行できませんでした。このリリースにより、ユーザーは、RHEL 9 を含むホストの RHEL バージョンと互換性のある **ccoctl** ユーティリティーのバージョンを実行できます。(OCPBUGS-32080)

- 以前は、Operator カタログをミラーリングする場合、**oc-mirror** はカタログを再ビルドし、**imagesetconfig** カタログフィルタリング仕様に基づいて、内部キャッシュを再生成していました。このプロセスには、カタログ内の **opm** バイナリーが必要でした。バージョン 4.15 以降、Operator カタログには **opm** RHEL 9 バイナリーが含まれており、RHEL 8 システムで実行するとミラーリングプロセスが失敗していました。このリリースにより、**oc-mirror** はデフォルトでカタログを再ビルドしなくなり、代わりにカタログを宛先レジストリーにミラーリングするだけになりました。
  カタログ再ビルド機能を保持するには、**--rebuild-catalog** を使用します。ただし、現在の実装には変更が加えられていないため、このフラグを使用すると、キャッシュが生成されなかったり、カタログがクラスターにデプロイされなかったりする可能性があります。このコマンドを使用すると、**OPM_BINARY** をエクスポートして、OpenShift Container Platform にあるカタログバージョンとプラットフォームに対応するカスタム **opm** バイナリーを指定できます。カタログイメージのミラーリングは、署名の検証なしで実行されるようになりました。ミラーリング中に署名検証を有効にするには、**--enable-operator-secure-policy** を使用します。(OCPBUGS-31536)

- 以前は、**CloudCredential** クラスター機能を含む **install-config.yaml** ファイルを使用して **oc adm release extract --credentials-requests** コマンドを実行すると、一部の認証情報要求が適切に抽出されませんでした。このリリースにより、**CloudCredential** 機能が OpenShift CLI (**oc**) に正しく組み込まれ、このコマンドが認証情報要求を適切に抽出できるようになりました。(OCPBUGS-24834)

- 以前は、ユーザーが oc-mirror プラグインで **tar.gz** アーティファクトを使用すると、シーケンスエラーが発生しました。この問題を解決するために、oc-mirror プラグインは、**--skip-pruning** フラグを使用して実行された場合、これらのエラーを無視するようになりました。この更新により、ミラーリングにおける **tar.gz** の使用順序に影響を与えなくなるシーケンスエラーが効果的に処理されるようになります。(OCPBUGS-23496)

- 以前は、oc-mirror プラグインを使用して、隠しフォルダーにあるローカルの Open Container Initiative Operator カタログをミラーリングすると、oc-mirror はエラー ".hidden_folder/data/publish/latest/catalog-oci/manifest-list/kubebuilder/kube-rbac-proxy@sha256:db06cc4c084dd0253134f156dddaaf53ef1c3fb3cc809e5d81711baa4029ea4c is not a valid image reference: invalid reference format" で失敗していました。このリリースにより、oc-mirror はローカルの Open Container Initiative カタログ内のイメージへの参照を別の方法で計算するようになり、非表示のカタログへのパスがミラーリングプロセスを妨げなくなりました。(OCPBUGS-23327)

- 以前は、ミラーリングが失敗したときに oc-mirror は停止せず、有効なエラーコードを返していませんでした。このリリースにより、**--continue-on-error** フラグが使用されない限り、oc-

mirror は “operator not found” に遭遇したときに正しいエラーコードで終了するようになりました。(OCPBUGS-23003)

- 以前は、Operator をミラーリングするときに、**minVersion** と **maxVersion** の 両方が指定されている場合、oc-mirror は **imageSetConfig** の **maxVersion** 制約を無視していました。その結果、すべてのバンドルがチャネルヘッドまでミラーリングされました。このリリースにより、oc-mirror は **imageSetConfig** で指定されたように **maxVersion** 制約を考慮するようになりました。(OCPBUGS-21865)

- 以前は、oc-mirror は、**eus-*** チャネルが偶数番号のリリースのみに指定されていることを認識しなかったため、**eus-*** チャネルを使用したリリースのミラーリングに失敗していました。このリリースにより、oc-mirror プラグインは、**eus-*** チャネルが偶数番号のリリースを対象としていることを適切に確認し、ユーザーがこれらのチャネルを使用してリリースを正常にミラーリングできるようになりました。(OCPBUGS-19429)

- 以前は、**mirror.operators.catalog.packages** ファイルに **defaultChannel** フィールドを追加することで、ユーザーは優先チャネルを指定し、Operator に設定された **defaultChannel** を上書きできました。このリリースにより、oc-mirror プラグインは **defaultChannel** フィールドが設定されている場合に初期チェックを強制するようになりました。ユーザーは **ImageSetConfig** のチャネルセクションでもこれを定義する必要があります。この更新により、指定された **defaultChannel** が Operator のミラーリング中に適切に設定され、適用されるようになります。(OCPBUGS-385)

- 以前は、FIPS が有効になっているクラスターを実行している場合、RHEL 9 システムで OpenShift CLI (**oc**) を実行すると、**FIPS mode is enabled, but the required OpenSSL backend is unavailable** というエラーが発生する場合がありました。このリリースにより、OpenShift CLI (**oc**) のデフォルトバージョンが Red Hat Enterprise Linux (RHEL) 9 でコンパイルされ、RHEL 9 で FIPS が有効になっているクラスターを実行すると正常に動作します。さらに、RHEL 8 でコンパイルされた **oc** のバージョンも提供されており、RHEL 8 で FIPS を有効にしてクラスターを実行している場合は、このバージョンを使用する必要があります。(OCPBUGS-23386、OCPBUGS-28540)

- 以前は、機能が無効になっている場合でも、**ImageRegistry** および **Build** 機能に関連するロールバインディングが、すべての namespace に作成されていました。このリリースにより、クラスター上でそれぞれのクラスター機能が有効になっている場合にのみ、ロールバインディングが作成されます。(OCPBUGS-34384)

- 以前は、完全な非接続環境でのディスクからミラーへのプロセス中に、Red Hat レジストリーへのアクセスがブロックされていた場合、oc-mirror プラグイン v1 はカタログイメージのミラーリングに失敗していました。さらに、**ImageSetConfiguration** がミラーリングされたカタログに **targetCatalog** を使用した場合、ワークフローに関係なく、カタログイメージ参照が正しくないためにミラーリングが失敗していました。この問題は、ミラーリング用のカタログイメージソースをミラーレジストリーに更新することで解決されました。(OCPBUGS-34646)

Operator Lifecycle Manager (OLM)

- 以前は、インデックスイメージの **imagePullPolicy** フィールドが **IfNotPresent** に設定されていたため、Operator カタログが適切に更新されていませんでした。このバグ修正により、OLM が更新され、カタログに適切なイメージプルポリシーが使用されるようになり、結果としてカタログが適切に更新されるようになります。(OCPBUGS-30132)

- 以前は、OLM が **CrashLoopBackOff** 状態で停止したために、クラスターのアップグレードがブロックされる可能性がありました。これは、リソースに複数の所有者参照があるという問題が原因でした。このバグ修正により、OLM が更新され、重複した所有者参照が回避され、所有する関連リソースのみが検証されます。その結果、クラスターのアップグレードは期待どおりに進行します。(OCPBUGS-28744)

- 以前は、**CatalogSource** オブジェクトによってサポートされるデフォルトの OLM カタログ Pod は、実行されているノードが停止すると続行できませんでした。Pod を移動するはずの容認が設定されているにもかかわらず、Pod は終了状態のままでした。これにより、関連するカタログから Operator をインストールまたは更新できなくなりました。このバグ修正により、OLM が更新され、この状態のままになっているカタログ Pod が削除されます。その結果、カタログ Pod は計画的または計画外のノードメンテナンスから適切に回復するようになりました。(OCPBUGS-32183)

- 以前は、ある Operator が以前にインストールおよびアンインストールされていた場合、その Operator のインストールが失敗することがありました。これはキャッシュの問題が原因でした。このバグ修正により、OLM が更新され、このシナリオで Operator が正しくインストールされるようになり、結果としてこの問題は発生しなくなりました。(OCPBUGS-31073)

- 以前は、etcd の復元後に **catalogd** コンポーネントがクラッシュループを起こす可能性がありました。これは、API サーバーに到達できない場合に、ガベージコレクションプロセスによってループ障害状態が発生したことが原因でした。このバグ修正により、**catalogd** が更新されて再試行ループが追加され、その結果、このシナリオで **catalogd** がクラッシュしなくなりました。(OCPBUGS-29453)

- 以前は、デフォルトのカタログソース Pod は更新を受信できなかったため、更新を取得するにはユーザーが手動で再作成する必要がありました。これは、カタログ Pod のイメージ ID が正しく検出されなかったために発生しました。このバグ修正により、OLM が更新され、カタログ Pod イメージ ID が正しく検出されるようになり、その結果、デフォルトのカタログソースが期待どおりに更新されます。(OCPBUGS-31438)

- 以前は、OLM が既存の **ClusterRoleBinding** または **Service** リソースを見つけられず、それらを再度作成するため、Operator のインストールエラーが発生する可能性がありました。このバグ修正により、OLM が更新され、これらのオブジェクトが事前に作成されるようになり、結果としてこれらのインストールエラーは発生しなくなりました。(OCPBUGS-24009)

Red Hat Enterprise Linux CoreOS (RHCOS)

- 以前は、**kdump** サービスが特別な **initramfs** を生成する前に、OVS ネットワークが設定されていました。**kdump** サービスが起動すると、network-manager 設定ファイルを取得し、それらを **kdump initramfs** にコピーしていました。ノードが **kdump initramfs** に再起動すると、OVN が **initramfs** に実行されず、仮想インターフェイスが設定されていなかったため、ネットワーク経由のカーネルクラッシュダンプのアップロードが失敗しました。このリリースにより、順序が更新され、OVS ネットワーク設定がセットアップされる前に **kdump** が起動して **kdump initramfs** がビルドされるようになり、問題は解決されました。(OCPBUGS-30239)

スケーラビリティーおよびパフォーマンス

- 以前は、シングルノードの OpenShift Container Platform 上の Machine Config Operator (MCO) は Performance Profile がレンダリングされた後にレンダリングされていたため、コントロールプレーンとワーカーマシン設定プールが適切なタイミングで作成されませんでした。このリリースにより、Performance Profile が正しくレンダリングされ、問題は解決されました。(OCPBUGS-22095)

- 以前は、TuneD デーモンと **irqbalanced** デーモンが割り込み要求 (IRQ) CPU アフィニティー設定を変更したため、IRQ CPU アフィニティー設定で競合が発生し、シングルノードの OpenShift ノードの再起動後に予期しない動作が発生していました。このリリースにより、**irqbalanced** デーモンのみが IRQ CPU アフィニティー設定を決定します。(OCPBUGS-26400)

- 以前は、パフォーマンス調整されたクラスターでの OpenShift Container Platform の更新中に、**MachineConfigPool** リソースを再開すると、プール内のノードがさらに再起動していました。このリリースでは、プールが再開される前にコントローラーが最新の計画されたマシン設

定と調整し、追加のノードの再起動が阻止されます。(OCPBUGS-31271)

- 以前は、ARM インストールではカーネルで 4k ページが使用されていました。このリリースにより、インストール時にのみカーネルに 64k ページをインストールするためのサポートが追加され、NVIDIA CPU のパフォーマンスが向上しました。Driver Tool Kit (DTK) も更新され、64k ページサイズの ARM カーネル用のカーネルモジュールをコンパイルできるようになりました。(OCPBUGS-29223)

ストレージ

- 以前は、**LVMCluster** カスタムリソース (CR) の削除中に、クラスター上の一部の **LVMVolumeGroupNodeStatus** オペランドが削除されませんでした。このリリースにより、**LVMCluster** CR を削除すると、すべての **LVMVolumeGroupNodeStatus** オペランドが削除されます。(OCPBUGS-32954)

- 以前は、LVM Storage のアンインストールは、**LVMVolumeGroupNodeStatus** オペランドの削除を待機してスタックしていました。この修正により、すべてのオペランドが削除され、LVM Storage を遅延なくアンインストールできるようになるため、動作が修正されます。(OCPBUGS-32753)

- 以前は、LVM Storage は永続ボリューム要求 (PVC) の最小ストレージサイズをサポートしていませんでした。これにより、PVC のプロビジョニング中にマウントが失敗する可能性があります。このリリースにより、LVM Storage は PVC の最小ストレージサイズをサポートします。以下は、各ファイルシステムタイプに対して要求できる最小ストレージサイズです。

  - **block**: 8 MiB
  - **xfs**: 300 MiB
  - **ext4**: 32 MiB

  PersistentVolumeClaim オブジェクトの **request.storage** フィールドの値が最小ストレージサイズより小さい場合、要求されたストレージサイズは最小ストレージサイズに切り上げられます。**limits.storage field** の値が最小ストレージサイズより小さい場合、PVC の作成はエラーを表示して失敗します。(OCPBUGS-30266)

- 以前は、LVM Storage は、ディスクセクターサイズの倍数ではないストレージサイズ要求を持つ永続ボリューム要求 (PVC) を作成していました。これにより、LVM2 ボリュームの作成中に問題が発生する可能性がありました。この修正により、PVC によって要求されたストレージサイズを 512 の最も近い倍数に切り上げることで動作が修正されました。(OCPBUGS-30032)

- 以前は、**LVMCluster** カスタムリソース (CR) には、正しくセットアップされているデバイスの除外ステータス要素が含まれていました。この修正により、正しく設定されたデバイスが除外ステータス要素の対象から除外され、準備完了デバイスにのみ表示されるようになります。(OCPBUGS-29188)

- 以前は、Amazon Web Services (AWS) Elastic File Store (EFS) Container Storage Interface (CSI) ドライバーコンテナーの CPU 制限により、AWS EFS CSI Driver Operator によって管理されるボリュームのパフォーマンスが低下する可能性がありました。このリリースでは、潜在的なパフォーマンスの低下を防ぐために、AWS EFS CSI Driver コンテナーの CPU 制限が削除されました。(OCPBUGS-28551)

- 以前は、Microsoft Azure Disk CSI ドライバーは、特定のインスタンスの種類で割り当て可能なボリュームを適切にカウントせず、最大値を超えていました。その結果、Pod を起動できませんでした。このリリースでにより、Microsoft Azure Disk CSI ドライバーのカウントテーブルが更新され、新しいインスタンスタイプが追加されました。Pod が実行され、適切に設定されたボリュームにデータを読み書きできるようになります。(OCPBUGS-18701)

- 以前は、CLI のバグのため、Hosted Control Plane 上のシークレットストア Container Storage Interface ドライバーはシークレットをマウントできませんでした。このリリースでは、ドライバーがボリュームをマウントできるようになり、問題は解決されました。(OCPBUGS-34759)

- 以前は、ドライバーのバグにより、Microsoft Azure Workload アイデンティティークラスターの静的永続ボリューム (PV) を設定できず、PV マウントが失敗していました。このリリースにより、ドライバーが正しく動作し、静的 PV が正しくマウントされるようになりました。(OCPBUGS-32785)

1.7. テクノロジープレビュー機能のステータス

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1.18 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	4.14	4.15	4.16
Ingress Node Firewall Operator	一般公開 (GA)	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	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
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	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
インターフェイス固有の安全な sysctls リストの更新	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	4.14	4.15	4.16
Egress サービスのカスタムリソース	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
BGPPeer カスタムリソースの VRF 仕様	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
NodeNetworkConfigurationPolicy カスタムリソースの VRF 仕様	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
管理ネットワークポリシー (**AdminNetworkPolicy**)	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)
IPsec 外部トラフィック (north-south)	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
MetalLB と FRR-K8 のインテグレーション	利用不可	利用不可	テクノロジープレビュー
PTP 境界クロックとしてのデュアル NIC ハードウェア	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
デュアル NIC Intel E810 PTP 境界クロックと高可用性システムクロック	利用不可	利用不可	一般公開 (GA)
PTP グランドマスタークロックとしての Intel E810 Westport Channel NIC	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 グランドマスタークロックとしてのデュアル NIC Intel E810 Westport Channel	利用不可	テクノロジープレビュー	一般公開 (GA)
NMState を使用して OVN-Kuberenetes に必要な **br-ex** ブリッジを設定する	利用不可	利用不可	テクノロジープレビュー
外部管理証明書を使用したルートの作成	利用不可	利用不可	テクノロジープレビュー
OpenShift SDN から OVN-Kubernetes へのライブマイグレーション	利用不可	利用不可	一般公開 (GA)

機能	4.14	4.15	4.16
Whereabouts を使用したマルチテナントネットワークの IP 設定の重複	利用不可	利用不可	一般公開 (GA)
CoreDNS と egress ファイアウォールの統合の改善	利用不可	利用不可	テクノロジープレビュー

ストレージテクノロジープレビュー機能

表1.19 ストレージテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
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
Google Filestore CSI Driver Operator	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
IBM Power® Virtual Server Block CSI Driver Operator	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
Read Write Once Pod アクセスモード	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)
OpenShift ビルドでの CSI ボリュームのビルド	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
OpenShift ビルドの共有リソース CSI Driver	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
Secrets Store CSI Driver 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
CIFS/SMB CSI Driver Operator	利用不可	利用不可	テクノロジープレビュー

インストールテクノロジープレビュー機能

表1.20 インストールテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
仮想マシンを使用した Oracle® Cloud Infrastructure (OCI) への OpenShift Container Platform のインストール	開発者プレビュー	テクノロジープレビュー	テクノロジープレビュー
ベアメタル上の Oracle® Cloud Infrastructure (OCI) への OpenShift Container Platform のインストール	開発者プレビュー	開発者プレビュー	開発者プレビュー
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
SR-IOV デバイスの NIC パーティショニングの有効化	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 (GCP) のユーザー定義ラベルとタグ	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
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	利用不可
Assisted Installer を使用して Alibaba Cloud にクラスターをインストールする	利用不可	利用不可	テクノロジープレビュー
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
OpenShift Container Platform on Oracle® Cloud Infrastructure (OCI)	開発者プレビュー	テクノロジープレビュー	テクノロジープレビュー
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
VMware vSphere の静的 IP アドレス (IPI のみ)	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)
RHCOS での iSCSI デバイスのサポート	利用不可	テクノロジープレビュー	一般公開 (GA)

機能	4.14	4.15	4.16
Cluster API 実装を使用して GCP にクラスターをインストールする	利用不可	利用不可	テクノロジープレビュー
RHCOS での Intel® VROC 対応 RAID デバイスのサポート	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)

ノードテクノロジープレビュー機能

表1.21 ノードテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
MaxUnavailableStatefulSet featureset	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テクノロジープレビュー機能

表1.22 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	4.14	4.15	4.16
installer-provisioned infrastructure を使用する IBM Power® Virtual Server	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
arm64 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
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
Multiarch Tuning Operator	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1.23 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	4.14	4.15	4.16
Driver Toolkit	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
Kernel Module Management Operator	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
Kernel Module Management Operator - ハブアンドスポーククラスターのサポート	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
ノード機能の検出	一般公開 (GA)	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	4.14	4.15	4.16
factory-precaching-cli ツール	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
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
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	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)
マウント namespace のカプセル化	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	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
etcd レイテンシー許容値の調整	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)
etcd データベースサイズの増加	利用不可	利用不可	テクノロジープレビュー

機能	4.14	4.15	4.16
RHACM **PolicyGenerator** リソースを使用して GitOps ZTP クラスターポリシーを管理する	利用不可	利用不可	テクノロジープレビュー

Operator のライフサイクルと開発テクノロジープレビュー機能

表1.25 Operator のライフサイクルと開発テクノロジープレビュートラッカー

機能	4.14	4.15	4.16
Operator Lifecycle Manager (OLM) v1	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
RukPak	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
Platform Operator	テクノロジープレビュー	テクノロジープレビュー	削除済み
ハイブリッド Helm ベースの Operator プロジェクト用のスキャフォールディングツール	テクノロジープレビュー	テクノロジープレビュー	非推奨
Java ベースの Operator プロジェクト用のスキャフォールディングツール	テクノロジープレビュー	テクノロジープレビュー	非推奨

OpenShift CLI (oc) テクノロジープレビュー機能

表1.26 OpenShift CLI (oc) テクノロジープレビュートラッカー

機能	4.14	4.15	4.16
oc-mirror プラグイン v2	利用不可	利用不可	テクノロジープレビュー
エンクレーブのサポート	利用不可	利用不可	テクノロジープレビュー
削除機能	利用不可	利用不可	テクノロジープレビュー

モニタリングテクノロジープレビュー機能

表1.27 モニタリングテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
メトリクス収集プロファイル	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
Metrics Server	利用不可	テクノロジープレビュー	一般公開 (GA)

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

表1.28 RHOSP テクノロジープレビュートラッカー

機能	4.14	4.15	4.16
installer-provisioned infrastructure でのデュアルスタックネットワーキング	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
ユーザーによってプロビジョニングされるインフラストラクチャーを備えたデュアルスタックネットワーキング	利用不可	一般公開 (GA)	一般公開 (GA)
クラスター CAPI Operator への CAPO の統合	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
ローカルディスク上の **rootVolumes** と **etcd** を備えた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

Hosted Control Plane のテクノロジープレビュー機能

表1.29 Hosted Control Plane のテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
Amazon Web Services (AWS) 上の OpenShift Container Platform の Hosted Control Plane	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
ベアメタル上の OpenShift Container Platform の Hosted Control Plane	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
OpenShift Virtualization 上の OpenShift Container Platform の Hosted Control Plane	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)

機能	4.14	4.15	4.16
非ベアメタルエージェントマシンを使用した OpenShift Container Platform の Hosted Control Plane	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 上の ARM64 OpenShift Container Platform クラスター用の Hosted Control Plane	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 Power 上の OpenShift Container Platform の Hosted Control Plane	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 上の OpenShift Container Platform の Hosted Control Plane	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

マシン管理テクノロジープレビュー機能

表1.30 マシン管理テクノロジープレビュートラッカー

機能	4.14	4.15	4.16
Amazon Web Services の Cluster API を使用したマシン管理	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
Google Cloud Platform の Cluster API を使用したマシン管理	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
VMware vSphere の Cluster API を使用したマシンの管理	利用不可	利用不可	テクノロジープレビュー
コントロールプレーンマシンセットの vSphere 障害ドメインの定義	利用不可	テクノロジープレビュー	一般公開 (GA)
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
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	一般公開 (GA)	一般公開 (GA)

機能	4.14	4.15	4.16
IBM Power® Virtual Server 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

認証と認可のテクノロジープレビュー機能

表1.31 認証と認可のテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
Pod セキュリティーアドミッションの制限付き適用	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

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

表1.32 Machine Config Operator のテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
MCO 状態レポートの改善	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
クラスター上の RHCOS イメージのレイヤー化	利用不可	利用不可	テクノロジープレビュー
ノード中断ポリシー	利用不可	利用不可	テクノロジープレビュー
ブートイメージの更新	利用不可	利用不可	テクノロジープレビュー

エッジコンピューティングのテクノロジープレビュー機能

表1.33 エッジコンピューティングのテクノロジープレビュートラッカー

機能	4.14	4.15	4.16
GitOps ZTP の高速プロビジョニング	利用不可	利用不可	テクノロジープレビュー

機能	4.14	4.15	4.16
GitOps ZTP と RHACM を使用してマネージドクラスターに IPsec 暗号化をデプロイする	利用不可	利用不可	テクノロジープレビュー

1.8. 既知の問題

- **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)

- Run Once Duration Override Operator (RODOO) は、Hypershift Operator によって管理されるクラスターにはインストールできません。(OCPBUGS-17533)

- シークレットまたはトップシークレットリージョンの AWS への OpenShift Container Platform 4.16 のインストールは、これらのリージョンの Network Load Balancers (NLBs) とセキュリティーグループの問題により失敗します。(OCPBUGS-33311)

- OpenShift Container Platform クラスターで Cloud-native Network Functions (CNF) レイテンシーテストを実行すると、**oslat** テストで 20 マイクロ秒を超える結果が返されることがあります。これにより、**oslat** テストが失敗します。(RHEL-9279)

- Local Zones を使用して Amazon Web Services (AWS) にクラスターをインストールする場合、エッジノードが **us-east-1-iah-2a** リージョンにデプロイされていると、デプロイに失敗します。(OCPBUGS-35538)

- ACM バージョン 2.10.3 以前を使用して、Infrastructure Operator、Central Infrastructure Management、または ZTP 方式で OpenShift Container Platform 4.16 をインストールすることはできません。これは、動的にリンクされたインストーラーバイナリー **openshift-baremetal-install** の変更によるもので、OpenShift Container Platform 4.16 では、これを正常に実行するには Red Hat Enterprise Linux (RHEL) 9 ホストが必要です。この問題を回避するために、ACM の今後のバージョンでは静的にリンクされたバイナリーを使用する予定です。(ACM-12405)

- AWS にクラスターをインストールする場合、ロードバランサーの DNS の Time-To-Live (TTL) 値が非常に高いと、インストールがタイムアウトすることがあります。(OCPBUGS-35898)

- **br-ex** ブリッジデバイスを保持するボンディングネットワークインターフェイスの場合、ノードネットワーク設定で **mode=6 balance-alb** ボンディングモードを設定しないでください。このボンドモードは OpenShift Container Platform ではサポートされていないため、Open vSwitch (OVS) ブリッジデバイスがネットワーク環境から切断される可能性があります。(OCPBUGS-34430)

- **HostFirmwareComponents** リソースを編集して、**BareMetalHosts** (BMH) リソースのファームウェアを更新しないでください。それ以外の場合、BMH は **Preparing** 状態のままになり、ファームウェアの更新を繰り返し実行します。回避策はありません。(OCPBUGS-35559)

- プロキシーを使用すると、インストーラーによってプロビジョニングされたクラスターをベアメタルにデプロイする操作が失敗します。リグレッションバグのため、ブートストラップ仮想マシンのサービスはプロキシー経由で IP アドレス **0.0.0.0** にアクセスできません。回避策として、**noProxy** リストに **0.0.0.0** を追加します。詳細は、プロキシーの設定 を参照してください。(OCPBUGS-35818)

- 複数の CIDR ブロックを含む VPC 内の Amazon Web Services (AWS) にクラスターをインストールする場合、マシンネットワークが **install-config.yaml** ファイルでデフォルト以外の CIDR ブロックを使用するように設定されていると、インストールは失敗します。(OCPBUGS-35054)

- マルチパスが設定された IBM Power® 上の仮想 SCSI ストレージを備えた単一の VIOS ホストに、インストール後のアクティビティーとして OpenShift Container Platform 4.16 クラスターがインストールまたは設定されると、マルチパスが有効になっている CoreOS ノードが起動に失敗します。ノードに使用できるパスは 1 つだけなので、これは想定内の動作です。(OCPBUGS-32290)

- cgroupv2 で CPU 負荷分散を使用する場合、排他的 CPU にアクセスできる別の Pod がすでに存在すると、Pod の起動に失敗する可能性があります。これは、Pod が削除され、それを置き換えるために別の Pod がすぐに作成された場合に発生する可能性があります。回避策として、新しい Pod を作成する前に、古い Pod が完全に終了していることを確認してください。(OCPBUGS-34812)

- 512 エミュレーションディスクを使用するシステムで LUKS 暗号化を有効にすると、プロビジョニングが失敗し、システムは initramfs で緊急シェルを起動します。これは、パーティションを拡張するときに **sfdisk** のアライメントバグが原因で発生します。回避策として、代わりに Ignition を使用してサイズ変更を実行できます。(OCPBUGS-35410)

- OpenShift Container Platform バージョン 4.16 の切断されたインストールは、IBM Power® Virtual Server 上で失敗します。(OCPBUGS-36250)

- 現在の PTP グランドマスタークロック (T-GM) 実装には、バックアップ NMEA センテンスジェネレーターなしで GNSS から供給される単一の National Marine Electronics Association (NMEA) センテンスジェネレーターがあります。NMEA センテンスが e810 NIC に到達する前に失われた場合、T-GM はネットワーク同期チェーン内のデバイスを同期できず、PTP Operator はエラーを報告します。修正案は、NMEA 文字列が失われたときに **FREERUN** イベントを報告することです。この制限が解決されるまで、T-GM は PTP クロックの holdover 状態をサポートしません。(OCPBUGS-19838)

- ワーカーノードの Topology Manager ポリシーが変更されると、NUMA 対応のセカンダリー Pod スケジューラーはこの変更を考慮しないため、誤ったスケジューリング決定や予期しないトポロジーアフィニティーエラーが発生する可能性があります。回避策として、NUMA 対応スケジューラー Pod を削除して、NUMA 対応スケジューラーを再起動します。(OCPBUGS-34583)

- Kubernetes の問題により、CPU マネージャーは、ノードに許可された最後の Pod から利用可能な CPU リソースのプールに CPU リソースを戻すことができません。これらのリソースは、後続の Pod がノードに許可された場合は、割り当てることができます。ただし、この Pod が最後の Pod になり、CPU マネージャーはこの Pod のリソースを使用可能なプールに戻すことができなくなります。
  この問題は、CPU マネージャーが利用可能なプールに CPU を解放することに依存する CPU 負荷分散機能に影響します。その結果、保証されていない Pod は、少ない CPU 数で実行される可能性があります。回避策として、影響を受けるノード上で **best-effort** CPU マネージャーポリシーを使用して、Pod をスケジュールします。この Pod は最後に許可された Pod となり、これによりリソースが使用可能なプールに正しく解放されます。(OCPBUGS-17792)

- **SriovNetworkNodePolicy** リソースを適用した後、SR-IOV Network Operator の Webhook の調整中に CA 証明書が置き換えられる可能性があります。その結果、SR-IOV ネットワークノードポリシーを適用するときに、**unknown authority** エラーが表示される場合があります。回避策として、失敗したポリシーを再度適用してみてください。(OCPBUGS-32139)

- **vfio-pci** ドライバータイプを持つ Virtual Function の **SriovNetworkNodePolicy** リソースを削除すると、SR-IOV Network Operator はポリシーを調整できなくなります。その結果、**sriov-**

device-plugin Pod は継続的な再起動ループに入ります。回避策として、物理機能に影響する残りのポリシーをすべて削除してから、再作成します。(OCPBUGS-34934)

- クローン作成の進行中にコントローラー Pod が終了した場合、Microsoft Azure ファイルクローンの永続ボリューム要求 (PVC) は保留状態のままになります。この問題を解決するには、影響を受けるクローン PVC をすべて削除してから、PVC を再作成します。(OCPBUGS-35977)

- Microsoft Azure では、azcopy (コピージョブを実行する基盤ツール) でログプルーニングが利用できないため、最終的にはコントローラー Pod のルートデバイスがいっぱいになる可能性があり、手動でクリーンアップする必要があります。(OCPBUGS-35980)

- **openshift-network-operator** namespace の **ConfigMap** オブジェクトの **mtu** パラメーターが見つからない場合、制限付きライブマイグレーションメソッドは停止します。
ほとんどの場合、**ConfigMap** オブジェクトの **mtu** フィールドは、インストール中に **mtu-prober** ジョブによって作成されます。ただし、クラスターが OpenShift Container Platform 4.4.4 などの以前のリリースからアップグレードされた場合、**ConfigMap** オブジェクトが存在しない可能性があります。

  一時的な回避策として、制限付きライブマイグレーションプロセスを開始する前に、**ConfigMap** オブジェクトを手動で作成することができます。以下に例を示します。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: mtu
  namespace: openshift-network-operator
data:
  mtu: "1500" 1
```

  1 **mtu** 値は、ノードインターフェイスの MTU と一致する必要があります。

  (OCPBUGS-35316)

1.9. 非同期エラータの更新

OpenShift Container Platform 4.16 のセキュリティー、バグ修正、機能拡張の更新は、Red Hat Network を通じて非同期エラータとしてリリースされます。すべての OpenShift Container Platform 4.16 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。

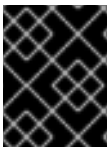
Red Hat カスタマーポータルのユーザーは、Red Hat Subscription Management (RHSM) のアカウント設定で、エラータ通知を有効にできます。エラータ通知を有効にすると、登録されたシステムに関連するエラータが新たに発表されるたびに、メールで通知が送信されます。

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。

このセクションは、これからも継続して更新され、OpenShift Container Platform 4.16 の今後の非同期エラータリリースの機能拡張とバグ修正に関する情報を追加していきます。OpenShift Container Platform 4.16.z 形式などのバージョン管理された非同期リリースについては、サブセクションで詳しく

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 リリースの場合、クラスターの更新 の手順を必ず確認してください。

1.9.1. RHSA-2024:0041 - OpenShift Container Platform 4.16.0 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: 2024-06-27

セキュリティー更新を含む OpenShift Container Platform リリース 4.16.0 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リストは、RHSA-2024:0041 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-2024:0045 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 4.16.0 --pullspecs
```

1.9.2. RHSA-2024:4156 - OpenShift Container Platform 4.16.1 のバグ修正とセキュリティー更新

発行日：2024-07-03

セキュリティー更新を含む OpenShift Container Platform リリース 4.16.1 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リストは、RHSA-2024:4156 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-2024:4159 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 4.16.1 --pullspecs
```

1.9.2.1. バグ修正

- 以前は、**growpart** のエラーが原因でデバイスがロックされ、Linux Unified Key Setup-on-disk-format (LUKS)デバイスを開くことができませんでした。その結果、ノードは起動できず、緊急モードになりました。このリリースでは、**growpart** への呼び出しが削除され、この問題は修正されています。(OCPBUGS-35973)

- 以前は、systemd のバグが原因で、**coreos-multipath-trigger.service** ユニットが無期限にハングする可能性がありました。その結果、システムが起動を完了することはありません。今回のリリースにより、systemd ユニットが削除され、問題が修正されました。(OCPBUGS-35748)

- 以前は、KMS キーが空の文字列として適用されていたため、キーが無効になりていました。このリリースでは、空の文字列が削除され、KMS キーは **install-config.yaml** から存在する場合にのみ適用されます。(OCPBUGS-35531)

- 以前は、機密コンピュートおよびユーザーが設定するホストのメンテナンスの値の検証はありませんでした。このリリースでは、ユーザーに機密コンピューティングが有効になっている場合、**onHostMaintenance** の値を **onHostMaintenance: Terminate** に設定する必要があります。(OCPBUGS-35493)

- 以前は、ユーザーがプロビジョニングしたインフラストラクチャー(CtxDN)クラスターまたは古いバージョンからアップグレードされたクラスターで、Infrastructure オブジェクトに **failureDomains** が欠落している可能性があり、特定のチェックが失敗しました。このリリースでは、**infrastructures.config.openshift.io** で使用できない場合は、**failureDomains** フォールバックが **cloudConfig** から調整されるようになりました。(OCPBUGS-35446)

- 以前のバージョンでは、新しいバージョンのカスタムリソース定義(CRD)が新規変換ストラテジーを指定する場合、この変換ストラテジーはリソースを正常に変換することと予想されていました。実際に更新操作を実行しないと、Operator Lifecycle Manager (OLM)は CRD 検証の新しい変換ストラテジーを実行できないため、これは当てはまりませんでした。今回のリリースにより、CRD の検証が既存の変換ストラテジーで失敗し、新規変換ストラテジーが CRD の新規バージョンに指定される場合に、OLM は更新プロセス中に警告メッセージを生成します。(OCPBUGS-35373)

- 以前は、Amazon Web Services (AWS) HyperShift クラスターは、Amazon Virtual Private Cloud (VPC)のプライマリークラスレスドメイン間ルーティング(CIDR)範囲を利用して、データプレーンにセキュリティーグループルールを生成していました。その結果、複数の CIDR 範囲を持つ AWS VPC に AWS HyperShift クラスターをインストールすると、生成されたセキュリティーグループルールが不十分な可能性があります。今回の更新により、提供されたマシンの CIDR 範囲に基づいてセキュリティーグループルールが生成され、この問題が解決されました。(OCPBUGS-35056)

- 以前は、Serverless 関数を作成するために、Source-to-Image (S2I)ビルドストラテジーを明示的に **func.yaml** に追加する必要がありました。さらに、エラーメッセージは問題を示しませんでした。このリリースでは、S2I が追加されていない場合でも、ユーザーは Serverless 機能を作成できます。ただし、S2I でない場合、ユーザーはその機能を作成できません。さらに、エラーメッセージが更新され、詳細情報が提供されるようになりました。(OCPBUGS-34717)

- 以前のバージョンでは、**MachineOSConfig** オブジェクトの **CurrentImagePullSecret** フィールドは、新規のクラスター上のレイヤー作成イメージのロールアウト時に使用されませんでした。今回のリリースにより、**MachineOSConfig** オブジェクトの **CurrentImagePullSecret** フィールドは、イメージのロールアウトプロセスで使用できるようになりました。(OCPBUGS-34261)

- 以前は、複数の失敗したポート転送要求を送信する場合、CRI-O メモリーの使用量はノードが停止するまで増加します。今回のリリースにより、障害のあるポート転送リクエストを送信する際のメモリーリークが修正され、この問題は解決されています。(OCPBUGS-30978)

- 以前は、**oc get podmetrics** コマンドと **oc get nodemetrics** コマンドが正しく機能していませんでした。今回の更新でこの問題が修正されています。(OCPBUGS-25164)

1.9.2.2. 更新

既存の OpenShift Container Platform 4.16 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。