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: 2025-12-12

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

Legal Notice

Abstract

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、および一般提供バージョンの既知の問題をまとめています。

Table of Contents

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を説明します。

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 および OpenShift Container Platform 4.16 のライフサイクル終了前にリリースされるそれ以降のバージョンの Red Hat Enterprise Linux (RHEL) 8 でサポートされます。OpenShift Container Platform 4.16 は、Red Hat Enterprise Linux CoreOS (RHCOS) 4.16 でもサポートされています。RHCOS で使用される RHEL バージョンを理解するには、RHEL Versions Utilized by Red Hat Enterprise Linux CoreOS (RHCOS) and OpenShift Container Platform (ナレッジベース記事) を参照してください。

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 の検証プログラムの詳細は、Cryptographic Module Validation Program を参照してください。検証用に提出された 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、Compliance Activities and Government Standards 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

クラスターで user-provisioned infrastructure を使用している場合は、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 の設定に関する詳細は、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 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、Google Cloud 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. 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。

1.3.2.6. 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。

1.3.2.7. 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 暗号化のサポート を参照してください。

1.3.2.8. 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、installer-provisioned 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。

1.3.2.9. 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。

1.3.2.10. 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。

1.3.2.11. 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。

1.3.2.12. 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。

1.3.2.13. 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 Google Cloud 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 にデプロイできます。詳細は、 サポートされている Google Cloud リージョン を参照してください。

1.3.2.14. Google Cloud 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、Google Cloud へのクラスターのインストール時に、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、Google Cloud 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 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する

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する を参照してください。

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 **Administrator** パースペクティブに次の更新が導入されています。

- Google Cloud 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 **Container list** ページと **Container details** 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。
- **Getting started** セクションの折りたたみと展開が可能です。

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。

1.3.4.4.1. コンソールテレメトリー

このリリースでは、クラスターテレメトリーが有効になっている場合、匿名ユーザー分析も有効になります。これはほとんどのクラスターのデフォルト設定であり、Web コンソールの使用状況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、各クラスターでこの設定を更新し、フロントエンドテレメトリーをオプトイン、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。

1.3.6.1. 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。

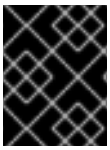
このリリースにより、IBM Z® および IBM® LinuxONE 上で次の機能がサポートされます。

- 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。

1.3.7.1. 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

1.3.7.2. 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
水平 Pod 自動スケーリング	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
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
シングル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

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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
不揮発性メモリーエクスプレスドライブ (NVMe)	サポート対象	サポート対象外
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
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

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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 Operators

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

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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. IPVLAN CNI プラグインでの IPv6 自発的ネイバーアドバタイズメント

ipvlan CNI プラグインを使用して作成された Pod (IP アドレス管理 CNI プラグインによって IP が割り当てられている) は、デフォルトで IPv6 の自発的ネイバーアドバタイズメントをネットワークに送信するようになりました。この機能は、OpenShift Container Platform 4.16 で一般提供ステータスになりました。

1.3.9.2. クラスターの OVS balance-slb モードを有効にする

2 つ以上の物理インターフェイスがネットワークトラフィックを共有できるように、クラスターが実行されるインフラストラクチャー上で Open vSwitch (OVS) **balance-slb** モードを有効化できます。この機能は、OpenShift Container Platform 4.16 で一般提供ステータスになりました。詳細は、クラスターの OVS balance-slb モードの有効化 を参照してください。

1.3.9.3. SR-IOV ネットワークメトリクスエクスポーターを有効にする

4.16.38 以降では、OpenShift Container Platform Web コンソールを使用して Single Root I/O Virtualization (SR-IOV) Virtual Function (VF) メトリクスをクエリーし、SR-IOV Pod のネットワークアクティビティーを監視できます。Web コンソールを使用して SR-IOV VF メトリクスをクエリーすると、SR-IOV ネットワークメトリクスエクスポーターは、VF が接続されている Pod の名前と namespace とともに、VF ネットワーク統計を取得して返します。

詳細は、SR-IOV ネットワークメトリクスエクスポーターの有効化 を参照してください。

1.3.9.4. 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
```

1.3.9.5. Border Gateway Protocol の MetalLB 更新

このリリースでは、MetalLB に Border Gateway Protocol (BGP) ピアカスタムリソース用の新しいフィールドが含まれています。**dynamicASN** フィールドを使用して、BGP セッションのリモートエンドに使用する自律システム番号 (ASN) を検出できます。これは、**spec.peerASN** フィールドに ASN を明示的に設定する代わりに使用できます。

1.3.9.6. 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。

1.3.9.7. 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。

1.3.9.8. 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。

1.3.9.9. 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。

1.3.9.10. 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。

1.3.9.11. 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。

1.3.9.12. 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。

1.3.9.13. 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。

1.3.9.14. 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。

1.3.9.15. 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。

1.3.9.16. 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。

1.3.9.17. 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クス を参照してください。

1.3.9.18. 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。

1.3.9.19. 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。

1.3.9.20. 外部管理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、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 OpenShift Container Platform ルートを設定できるようになりました。これにより、シークレットを介して外部で管理されている TLS 証明書を参照できるようになり、手動による証明書管理が不要になり、プロセスが合理化されます。外部で管理される証明書を使用することで、エラーが削減され、証明書の更新プロセスがスムーズになり、OpenShift ルーターが更新された証明書を迅速に提供できるようになります。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。

1.3.9.21. 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、**ネットワークセキュリティー** の AdminNetworkPolicy を参照してください。

1.3.9.22. OVN-Kubernetes ネットワークプラグインへの限定的な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、制限付きの **ライブ** マイグレーションメソッドが導入されています。限定的な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。OpenShift Container Platform で利用できます。Hosted Control Plane 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制限付きライブマイグレーションの概要 を参照してください。

1.3.9.23. 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。

1.3.9.24. 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、クラスターのインストール中に transit、join、および masquerade サブネットを設定できます。インストール後に join および transit の CIDR 範囲を変更できます。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。

1.3.9.25. IPsec テレメトリー

Telemetry および Insights Operator は、IPsec 接続に関するテレメトリーを収集します。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. thick-provisioned ストレージ設定のサポート

この機能は、thick-provisioned 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 thick-provisioned となります。thick-provisioned 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。thick-provisioned 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

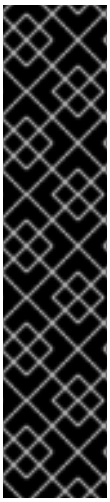
1.3.11.1. Operator API の名前が ClusterExtension (テクノロジープレビュー) に変更される

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します。
- 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ター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ター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

OLM 1.0 は依存関係の解決をサポートしていません。拡張機能が他の API またはパッケージへの依存関係を宣言する場合、拡張機能をインストールする前に、その依存関係がクラスター上に存在している必要があります。

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. Builds

1.3.12.1. 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. Nodes

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構成されます。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の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
- prom-label-proxy to 0.8.1
- 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。

1.3.18.6. AMD EPYC Zen 4 CPU を搭載したコンピュートノードのサポート

リリース 4.16.30 以降では、**PerformanceProfile** カスタムリソース (CR) を使用して、AMD EPYC Zen 4 CPU (Genoa および Bergamo など) を搭載したマシンでコンピュートノードを設定できます。単一の

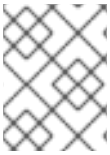
NUMA ドメイン (NPS=1) 設定のみがサポートされます。現在、AMD では Pod ごとの電源管理はサポートされていません。

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.y.z> 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. イメージベースのアップグレードの機能拡張

このリリースでは、イメージベースのアップグレードに次の機能拡張が導入されています。

- ハブクラスターに **ImageBasedGroupUpgrade** API を追加することで、マネージドクラスターの大規模なグループのアップグレードプロセスを簡素化しました。
- **ImageBasedGroupUpgrade** API を使用するときに、マネージドクラスターにアクション完了のラベルを付けます。
- シードイメージ生成前のシードクラスター検証を改善しました。
- マネージドクラスターの使用量が一定のしきい値に達した場合、コンテナーストレージディスクを自動的にクリーンします。
- **ImageBasedUpgrade** CR の新しい **status.history** フィールドに包括的なイベント履歴を追加します。

ImageBasedGroupUpgrade API の詳細は、ハブ上で ImageBasedGroupUpgrade CR を使用してイメージベースのアップグレードを大規模に管理する を参照してください。

1.3.19.6. 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

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. Hosted Control Plane

1.3.20.1. Hosted Control Plane は Amazon Web Services (AWS) で一般公開されています

OpenShift Container Platform 4.16 の Hosted Control Plane が AWS プラットフォームで一般提供されました。

1.3.21. 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。

1.4.1. HAProxy バージョン 2.8

OpenShift Container Platform 4.16 は HAProxy 2.8 を使用します。

1.4.2. 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。

1.4.3. etcd チューニングパラメーター

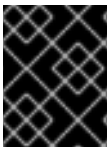
このリリースにより、etcd チューニングパラメーターを、次のようにパフォーマンスを最適化し、レイテンシーを短縮する値に設定できるようになりました。

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

1.4.4. 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。

1.4.5. 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。

1.4.6. 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。

1.4.7. 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。

1.4.8. 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、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。

1.4.9. 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。

1.4.10. 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。

1.4.11. 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。

1.4.12. 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。

1.4.13. 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。

1.4.14. IBM Power (R) Virtual Server が Cluster API Provider IBM Cloud 0.8.0 を使用するように更新されました

このリリースでは、IBM Power® Virtual Server が更新され、Cluster API Provider IBM Cloud バージョン 0.8.0 を使用するようになりました。

1.4.15. 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。

1.4.16. kube-apiserver のループバック証明書の有効期間が 3 年に延長される

以前は、Kubernetes API Server の自己署名ループバック証明書が 1 年で期限切れになりました。このリリースにより、証明書の有効期限が 3 年に延長されました。

1.4.17. VMware vSphere 7 および VMware Cloud Foundation 4 の一般サポートの終了

Broadcom は、VMware vSphere 7 および VMware Cloud Foundation (VCF) 4 の一般サポートを終了しました。既存の OpenShift Container Platform クラスターがこれらのいずれかのプラットフォームで実行されている場合は、VMware インフラストラクチャーをサポート対象バージョンに移行またはアップグレードすることを計画する必要があります。OpenShift Container Platform は、vSphere 8 Update 1 以降、または VCF 5 以降へのインストールをサポートしています。

1.5. 非推奨の機能と削除された機能

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、この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。

- **利用不可**

- **テクノロジープレビュー**
- **一般提供**
- **非推奨**
- **削除済み**

1.5.1. Operator のライフサイクルと開発の非推奨機能と削除された機能

表1.6 Operator のライフサイクルと開発に関する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	一般提供	一般提供	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	一般提供	一般提供	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	一般提供	一般提供	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	一般提供	一般提供	非推奨
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

1.5.2. イメージの非推奨機能と削除された機能

表1.7 Cluster Samples Operator の非推奨トラッカーと削除されたトラッカー

機能	4.14	4.15	4.16
Cluster Samples Operator	一般提供	一般提供	非推奨

1.5.3. モニタリングの非推奨機能と削除された機能

表1.8 モニタリングの非推奨トラッカーと削除されたトラッカー

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	一般提供	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	一般提供	非推奨	削除済み

1.5.4. インストールの非推奨機能と削除された機能

表1.9 インストールに関する非推奨および削除されたトラッカー

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
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	一般提供	一般提供	非推奨
Amazon Web Services (AWS) の **platform.aws.preserveBootstrapIgnition** パラメーター	一般提供	一般提供	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	一般提供	一般提供	削除済み
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。

1.5.5. クラスターの更新の非推奨機能と削除された機能

表1.10 クラスターの更新に関する非推奨および削除されたトラッカー

機能	4.14	4.15	4.16

1.5.6. マシン管理の非推奨機能と削除された機能

表1.11 マシン管理の非推奨トラッカーと削除されたトラッカー

機能	4.14	4.15	4.16
Alibaba Cloud の Machine API でのマシン管理	テクノロジープレビュー	テクノロジープレビュー	削除済み
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	削除済み

1.5.7. ストレージの非推奨機能と削除された機能

表1.12 ストレージに関する非推奨および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	一般提供	一般提供	削除済み

1.5.8. ネットワークの非推奨機能と削除された機能

表1.13 ネットワーキングに関する非推奨および削除されたトラッカー

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

1.5.9. Web コンソールの非推奨機能と削除された機能

表1.14 Web コンソールに関する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	一般提供	非推奨	非推奨
React Router 5	一般提供	非推奨	非推奨

1.5.10. ノードに関する非推奨機能と削除された機能

表1.15 ノードに関する非推奨および削除されたトラッカー

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	一般提供	一般提供	非推奨

1.5.11. ワークロードの非推奨機能と削除された機能

表1.16 ワークロードに関する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

1.5.12. ベアメタルモニタリングの非推奨機能と削除された機能

表1.17 Bare Metal Event Relay Operator トラッカー

機能	4.14	4.15	4.16
Bare Metal Event Relay Operator	削除済み	削除済み	削除済み

1.5.13. 非推奨の機能

1.5.13.1. Linux Control Groups バージョン 1 の非推奨化

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。

1.5.13.2. 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。

1.5.13.3. 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。

1.5.13.4. 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 は、Operator SDK (Operator Framework) を参照してください。

1.5.13.5. 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。

1.5.14. 削除された機能

1.5.14.1. 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。

1.5.14.2. 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。

1.5.14.3. Bare Metal Event Relay Operator が削除される

Bare Metal Event Relay Operator は以前はテクノロジープレビュー機能でしたが、現在は OpenShift Container Platform から削除されています。Bare Metal Event Relay Operator の完全なライフサイクル情報については、製品ライフサイクル: Bare Metal Event Relay を参照してください。

1.5.14.4. 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。

1.5.14.5. 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。

1.5.14.6. 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。

1.5.14.7. 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。

1.5.14.8. 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。

1.5.14.9. 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。

1.5.14.10. 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 の移行の詳細は、Kubernetes documentation を参照してください。

表1.18 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

1.5.14.11. Alibaba Cloud の Machine API でのマシン管理

OpenShift Container Platform 4.16 で、Alibaba Cloud クラスターの Machine API を使用したマシン管理のサポートが削除されました。この変更に伴い、テクノロジープレビュー機能であった Alibaba Cloud のクラウドコントローラーマネージャーのサポートが削除されました。

1.6. バグ修正

1.6.1. 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)

1.6.2. 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 Manager リソースが使用されていたため、RedFish Virtual Media API の Uniform Resource Identifier (URI) が非推奨になっていました。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)

1.6.3. Builds

- 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)

1.6.4. 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 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、Google Cloud 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。この問題はこの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 taint 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 taint 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 taint 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 taint 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)

1.6.5. 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。この問題はこの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 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。この問題はこの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)

1.6.6. 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)

1.6.7. 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** は認識されないか、**Pending** 状態のままでした。この更新により、Pipelines の **List** および **Details** ページから **CustomTasks** を簡単に特定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 **PipelineRuns** を区別するためのインジケーターが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)

1.6.8. エッジコンピューティング

- 以前は、プロキシー設定を使用するクラスターにおけるイメージベースのアップグレードの問題により Operator のロールアウトが発生し、そのために起動時間が長くなっていました。このリリースでは問題が修正され、アップグレード時間が短縮されました。(OCPBUGS-33471)

1.6.9. 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)

1.6.10. 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)

1.6.11. 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)

1.6.12. インストーラー

- 以前は、Google Cloud 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 Google Cloud 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、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、Google Cloud 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 Google Cloud 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 Google Cloud 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、エージェントベース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、エージェントベース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。このリリースにより、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エージェントベース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。n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。このリリースにより、この問題は解決されました。(OCPBUGS-29425)

1.6.13. 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)

1.6.14. 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)

1.6.15. 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)

1.6.16. 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.storage** 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 vSphere config 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)

1.6.17. 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。このリリースにより、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)

1.6.18. 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。このリリースにより、この問題は修正されました。(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。このリリースにより、この問題は修正されました。(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 System (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 **offset** 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)

1.6.19. ノード

- 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)

1.6.20. 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)

1.6.21. 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と、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)

1.6.22. 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 toleration 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)

1.6.23. 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)

1.6.24. 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)

1.6.25. 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 **requests.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、要求されるストレージサイズが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、こ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。

- **利用不可**
- **テクノロジープレビュー**
- **一般提供**
- **非推奨**
- **削除済み**

1.7.1. ネットワークのテクノロジープレビュー機能

表1.19 ネットワーク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
Ingress Node Firewall Operator	一般提供	一般提供	一般提供
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	一般提供	一般提供
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	一般提供	一般提供	一般提供
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
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	一般提供
IPsec 外部トラフィック (north-south)	テクノロジープレビュー	一般提供	一般提供
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	一般提供	一般提供	一般提供
追加のネットワークインターフェイス上の Egress IP	一般提供	一般提供	一般提供

機能	4.14	4.15	4.16
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	一般提供
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	一般提供
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	一般提供
OVN-Kubernetes が NMState を使用するために必要な **br-ex** ブリッジの設定	利用不可	利用不可	一般提供
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	一般提供
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	一般提供
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

1.7.2. ストレージのテクノロジープレビュー機能

表1.20 ストレージ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
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	一般提供	一般提供	一般提供
IBM Power® Virtual Server Block CSI Driver Operator	テクノロジープレビュー	一般提供	一般提供
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	一般提供

機能	4.14	4.15	4.16
OpenShift ビルドでの CSI ボリュームのビルド	一般提供	一般提供	一般提供
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

1.7.3. インストールのテクノロジープレビュー機能

表1.21 インストール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
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	一般提供	一般提供	一般提供
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 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

機能	4.14	4.15	4.16
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
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	一般提供
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	一般提供
Cluster API 実装を使用して Google 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
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	一般提供

1.7.4. ノードテクノロジープレビュー機能

表1.22 ノード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
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

1.7.5. 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1.23 マルチアーキテクチャー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
installer-provisioned infrastructure を使用する IBM Power® Virtual Server	テクノロジープレビュー	一般提供	一般提供

機能	4.14	4.15	4.16
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	一般提供

1.7.6. 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1.24 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	一般提供	一般提供	一般提供
Kernel Module Management Operator	一般提供	一般提供	一般提供
Kernel Module Management Operator - ハブアンドスポーククラスターのサポート	一般提供	一般提供	一般提供
ノード機能の検出	一般提供	一般提供	一般提供

1.7.7. 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1.25 スケーラビリティとパフォーマンス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
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

機能	4.14	4.15	4.16
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	一般提供
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	一般提供
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
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

1.7.8. 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1.26 Operator のライフサイクルおよび開発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
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

機能	4.14	4.15	4.16
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

1.7.9. OpenShift CLI (oc) テクノロジープレビュー機能

表1.27 OpenShift CLI (oc) 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
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

1.7.10. モニタリングのテクノロジープレビュー機能

表1.28 モニタリ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
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	一般提供

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

表1.29 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	一般提供	一般提供

機能	4.14	4.15	4.16
user-provisioned infrastructure を備えたデュアルスタックネットワーキング	利用不可	一般提供	一般提供
Cluster CAPI Operator への RHOSP 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

1.7.12. Hosted Control Plane のテクノロジープレビュー機能

表1.30 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	一般提供
ベアメタル上の OpenShift Container Platform の Hosted Control Plane	一般提供	一般提供	一般提供
OpenShift Virtualization 上の OpenShift Container Platform の Hosted Control Plane	一般提供	一般提供	一般提供
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

1.7.13. マシン管理テクノロジープレビュー機能

表1.31 マシン管理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 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 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
IBM Power® Virtual Server 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	テクノロジープレビュー	テクノロジープレビュー
RHOSP の Cluster API を使用したマシンの管理	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
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	一般提供
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	削除
Google 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	一般提供	一般提供
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

1.7.14. 認証と認可のテクノロジープレビュー機能

表1.32 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

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

表1.33 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
node disruption policy	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

1.7.16. 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1.34 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

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)

- プロキシーを使用すると、installer-provisioned 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)

- クラスター上で IPsec が有効になっている場合、north-south IPsec 接続をホストしているノード上で、**ipsec.service** systemd ユニットを再起動するか、**ovn-ipsec-host** Pod を再起動すると、IPsec 接続が失われます。(RHEL-26878)

- **baselineCapabilitySet** フィールドを **None** に設定する場合、Ingress 機能が無効になっているとクラスターのインストールが失敗するため、Ingress 機能を明示的に有効にする必要があります。(OCPBUGS-33794)

- 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)

- NUMA Resources Operator をデプロイする予定の場合は、OpenShift Container Platform バージョン 4.16.25 または 4.16.26 を使用しないでください。(OCPBUGS-45983)

- 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)

- ホストされたクラスターでは、API からの自己署名証明書を置き換えることはできません。(OCPSTRAT-1516)
- 高解像度タイマーに依存してスレッドをウェイクアップする低遅延アプリケーションでは、想定よりも長いウェイクアップ遅延が発生する可能性があります。予想されるウェイクアップレイテンシーは 20µs 未満ですが、**cyclictest** ツールを長時間実行すると、この時間を超えるレイテンシーが発生することがあります。テストの結果、99.99999% 以上のサンプルで、ウェイクアップ遅延が 20µs 未満であることが示されました。(OCPBUGS-34022)

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. RHBA-2025:21825 - OpenShift Container Platform 4.16.53 のバグ修正アドバイザリー

発行日: 2025 年 11 月 26 日

OpenShift Container Platform リリース 4.16.53 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:21825 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:21823 アドバイザリーで提供されています。

以下のコマンドを実行して、この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 4.16.53 --pullspecs
```

1.9.2. バグ修正

このリリースでは次のバグが修正されました。

- この更新前は、ユーザー管理のロードバランサーが使用されている場合でも、API および Ingress 仮想 IP (VIP) アドレスが自動的に割り当てられていました。このリリースでは、API および Ingress VIP が自動的に割り当てられなくなりました。これらの値が **install-config.yaml** で明示的に指定されていない場合、インストールはエラーで失敗し、値を指定するように求められます。(OCPBUGS-53237)

- この更新前は、インストールプログラムによってサポートされていないセキュリティーグループがロードバランサーに追加されていたため、Commercial Cloud Services (C2S) リージョンまたは Secret Commercial Cloud Services (SC2S) リージョンに AWS クラスターをインストールすると失敗していました。このリリースでは、インストールプログラムは、C2S リージョンまたは SC2S リージョンのいずれかでインストールする必要があるクラスターのロードバランサーに、サポート対象外のセキュリティーグループを追加しなくなりました。(OCPBUGS-54165)

- この更新前は、OVNKube-controller が Kubernetes API サーバーからの更新を処理しておらず、各ノードでオープン仮想ネットワーク (OVN) データベースを設定していない場合、このデータベースを使用する OVN コントローラーは、OVNKube-controller が設定を完了する前にデータベースに接続する可能性がありました。その結果、OVN コントローラーは古い OVN データベースと同期し、関連付けられた IP が別のノードに移動した可能性があるにもかかわらず、Egress IP をサポートするように設定された送信元ネットワークアドレス変換 (SNAT) を使用して、IP の Gratuitous Address Resolution Protocol (GARP) に進みました。このリリースでは、OVNKube-controller が更新を処理していない場合、これらの GARP はブロックされます。(OCPBUGS-63155)

- この更新前は、ドキュメント化されたセキュリティー手順に従ってユーザーが意図的に公開鍵のみを提供した場合でも、秘密鍵が見つからない場合、ccoctl ユーティリティーによって新しい鍵ペアが自動的に生成されていました。この動作により問題が発生していました。新しく生成された鍵がクラスターの鍵と一致しなくなるためです。その結果、正しいプロセスに従ったユーザーにサービス停止が発生していました。このリリースでは、**--public-key-file** パラメーターが指定されたときに新しい鍵ペアが生成されないようにユーティリティーが変更されました。また、一貫性を確保するために、このパラメーターがすべての **create-all** 関数に追加されました。その結果、公開鍵ファイルを指定した場合に、指定した鍵が確実に使用されるようになりました。そのため、クラスターが中断することなく期待どおりに機能し続けます。(OCPBUGS-63550)

- この更新前は、**/auth/error** ページが正しくレンダリングされませんでした。その結果、ページが空になり、エラーの詳細が表示されませんでした。このリリースでは、フロントエンドのエラーページコンテンツが **/auth/error** ページに表示されるようになりました。その結果、予想通りのエラー内容が表示されます。(OCPBUGS-64649)

- この更新前は、フェイルオーバー中に、システムの重複アドレス検出 (DAD) により、Egress IPv6 アドレスが両方のノードに一時的に存在する場合に、アドレスが誤って無効にされ、接続が切断されることがありました。このリリースでは、Egress IPv6 はフェイルオーバー中に

DAD チェックをスキップするように設定されます。これにより、Egress IP アドレスが別のノードに正常に移動した後も Egress IPv6 トラフィックが中断されなくなり、ネットワークの安定性が向上します。(OCPBUGS-64944)

1.9.3. 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。

1.9.4. RHBA-2025:19901 - OpenShift Container Platform 4.16.52 のバグ修正とセキュリティー更新

発行日: 2025 年 11 月 12 日

OpenShift Container Platform リリース 4.16.52 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:19901 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:19899 アドバイザリーによって提供されます。

以下のコマンドを実行して、この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 4.16.52 --pullspecs
```

1.9.4.1. バグ修正

- この更新前は、Machine Config Operator (MCO) が、クラスターに追加されたすべての新しいノードに **Upgradeable=False** 条件を誤って設定していました。**Upgradeable=False** 条件には、理由として **PoolUpdating** が指定されていました。このリリースでは、MCO がクラスターに追加されるすべての新しいノードに **Upgradeable=True** 条件を正しく設定するようになり、問題が解決されました。(OCPBUGS-57423)

- この更新前は、コントローラーは Amazon Web Services (AWS) へのセッションを設定するときにランダムな名前でファイルを作成および削除していたため、コントローラーはセッションをキャッシュするために継続的にメモリーを割り当てていました。このリリースでは、コントローラーはランダムなファイル名ではなく同じファイル名を使用するようになり、カーネルはセッションごとに新しいファイル名を要求する代わりに **dentry** オブジェクトを再利用できるようになりました。その結果、過剰なメモリー割り当ての問題が解消されました。(OCPBUGS-63140)

- この更新前は、Domain Name System (DNS) の Egress ファイアウォールルールに対応する **address_set** リスト内の古い IP アドレスが削除されませんでした。その結果、**address_set** リストが際限なく増え続け、メモリーリークの問題が発生していました。このリリースでは、5 秒間の猶予期間後に古い IP アドレスが **address_set** リストから削除されます。(OCPBUGS-63230)

- この更新前は、**--dry-run=server** オプションを指定して **istag** リソースを削除すると、サーバーからイメージが誤って実際に削除されていました。この予期しない削除は、dry-run オプションが **oc delete istag** コマンドに誤って実装されていたために発生していました。このリリースでは、dry-run オプションが **oc delete istag** コマンドに正しく関連付けられました。その結果、**--dry-run=server** オプションの使用時に、イメージオブジェクトの誤った削除が防止され、**istag** オブジェクトがそのまま残るようになりました。(OCPBUGS-63394)

- この更新前は、**ironic-inspector** コンテナーには共有ボリュームにアクセスして **ramdisk** ログを保存するための適切な権限がありませんでした。のため、ironic エージェント側で問題をトラブルシューティングできませんでした。このリリースでは、共有ボリュームへのアクセスが

可能になり、**ramdisk** ログを保存できるようになりました。(OCPBUGS-63417)

- この更新前は、OpenShift Container Platform 4.12 より前に作成されたコントロールプレーンノードに、**node-role.kubernetes.io/control-plane** ラベルがありませんでした。このリリースでは、ラベルが欠落している場合、Machine Config Operator (MCO) が、コントロールプレーンノードに対して uncordon を実行するたびにラベルを追加します。(OCPBUGS-63553)

1.9.4.2. 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。

1.9.5. RHSA-2025:19017 - OpenShift Container Platform 4.16.51 のバグ修正とセキュリティー更新

発行日: 2025 年 10 月 29 日

OpenShift Container Platform リリース 4.16.51 が公開されました。この更新に含まれるバグ修正のリストは、RHSA-2025:19017 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.51 --pullspecs
```

1.9.5.1. バグ修正

このリリースで注目すべきバグ修正はありません。

1.9.5.2. 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。

1.9.6. RHSA-2025:17690 - OpenShift Container Platform 4.16.50 のバグ修正とセキュリティー更新

発行日: 2025 年 10 月 15 日

OpenShift Container Platform リリース 4.16.50 が公開されました。この更新に含まれるバグ修正のリストは、RHSA-2025:17690 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.50 --pullspecs
```

1.9.6.1. 機能拡張

- 以前は、同じサブスクリプション内の Azure Compute Gallery (ACG) イメージに仮想マシン (VM) をインポートする場合、仮想マシンに対する読み取りアクセスが必要でした。また、同じサブスクリプション内の ACG イメージに Blob をインポートするには、ストレージアカウントへの書き込みアクセスが必要でした。2025 年 10 月 8 日以降、Microsoft では、同じサブスクリプションワークフローでの仮想マシンイメージ作成中にソース仮想マシンへの書き込みアクセスが必要になります。ACG イメージへの仮想マシンおよび Blob のインポート時に仮想マシ

ンイメージバージョンの作成が失敗しないためには、ユーザーは **properties.storageProfile.source.virtualMachineId** プロパティーを使用する必要があります。ACG イメージバージョンを作成するためのソースとして Blob を使用する場合は、**properties.storageProfile.osDiskImage.source.storageAccountId** プロパティーを使用します。(OCPBUGS-62653)

1.9.6.2. バグ修正

- この更新前は、OpenShift Container Platform 4.x のプロキシーを使用して接続されたシングルスタック IPv6 クラスターで **routingViaHost** パラメーターを **true** に設定すると、デプロイメント中にクラスターが停止していました。このリリースでは、これらのクラスターで **routingViaHost** パラメーターが **true** に設定されておらず、問題は解決しました。その結果、クラスターのデプロイメントは失敗しません。(OCPBUGS-60079)

- この更新前は、**kubectl apply** を実行する前に提供された YAML ファイルのフォーマットが不適切だったため、デプロイメントが失敗していました。その結果、エラーの誤処理により、Pod の再スケジュール中にユーザーデータが失われました。このリリースでは、taint と toleration に関する Pod のスケジューリングの問題が修正されました。その結果、エンドユーザーは、間違ったリソースの割り当てによる Pod 退避に遭遇しなくなりました。(OCPBUGS-61582)

- この更新前は、OpenShift イメージレジストリーを無効にすると、従来のプルシークレットファイナライザーフィールドが残り、namespace の削除中にシークレットの削除が停止していました。その結果、ユーザーは OpenShift イメージレジストリーを無効化する際に **Dockercfg** シークレットを削除できませんでした。このリリースでは、レジストリーの削除中に、従来のプルシークレットで残ったファイナライザーフィールドが削除されます。その結果、レジストリーの削除は停止せず、シームレスなシークレットのクリーンアップが可能になりました。(OCPBUGS-61707)

- この更新前は、**NetworkManager-wait-online** サービスへの依存関係により、ベアメタルデプロイメントで NMState サービスの障害が発生していました。この依存関係が原因で、NMState サービスの非アクティブ化によりユーザーデプロイメントが失敗していました。このリリースでは、NMState 依存関係の問題が解決され、**br-ex** 設定に **NetworkManager-wait-online** サービスが不要になりました。その結果、OpenShift Container Platform デプロイメントにおける NMState サービスの安定性が向上し、デプロイメントの失敗が減少します。(OCPBUGS-61869)

- この更新前は、OpenShift Container Platform バージョン 4.16 でアップストリームの修正済みの問題を使用すると、エラーメッセージバッファーのオーバーフローによりユーザーデータが失われていました。このリリースでは、**external-resizer** プロセスのアップストリームの問題が修正されたことで、ダウンストリームの潜在的な使用が減少し、ユーザーデータの損失が防止されます。その結果、ユーザーは、修正済みのアップストリームリソースを消費する問題に遭遇することがなくなります。(OCPBUGS-62465)

1.9.6.3. 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。

1.9.7. RHBA-2025:16726 - OpenShift Container Platform 4.16.49 のバグ修正とセキュリティー更新

発行日: 2025 年 10 月 1 日

OpenShift Container Platform リリース 4.16.49 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:16726 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.49 --pullspecs
```

1.9.7.1. 機能拡張

- この更新により、Kubernetes クラスター内の **virt-launcher** Pod からのコマンドラインログが収集され、JSON でエンコードされ、パス **aggregated/virt-launcher/logs** に保存されるようになりました。この機能拡張により、ログの場所が一元化され、仮想マシンのトラブルシューティングとデバッグが改善し、ユーザーのプロセスが効率化します。この機能は、多くの OpenShift Container Platform バージョンと互換性があります。(OCPBUGS-61973)

- この更新により、強化された **etcdDatabaseQuotaLowSpace** アラートが導入され、OpenShift Container Platform プラットフォームの **cluster-etcd-operator** がよりプロアクティブになりました。etcd クォータの使用量が 95% に近づくにつれて、複数のレベル (情報提供、警告、重大) のアラートがトリガーされます。このプロアクティブなアラートシステムにより、API サーバーが影響を受ける前にクラスター管理者が潜在的な問題を解決するための時間を十分に確保できるため、OpenShift Container Platform 環境の安定性と管理性が向上します。(OCPBUGS-61505)

1.9.7.2. バグ修正

- この更新前は、クラスターの自動スケーリング中にマシンの削除処理が不適切だったため、最後のノードに **ToBeDeletedByClusterAutoscaler** taint が残っていました。その結果、クラスターのスケーリング中にリソースの割り当てが影響を受けていました。このリリースでは、マシンセットをスケールダウンした後、**ToBeDeletedByClusterAutoscaler** taint が削除されます。その結果、マシンセットをスケールダウンした後、最後のノードに不要な taint が残りません。(OCPBUGS-60915)

- この更新前は、非接続クラスターで **ImageTagMirrorSet** リソースが **NeverContactSource** に設定されていると、**ImageStream** リソースがイメージタグをインポートできませんでした。その結果、イメージのインポートが失敗していました。このリリースでは、非接続クラスターがこのように設定されていても、**ImageStream** リソースがイメージタグをインポートします。その結果、**ImageTagMirrorSet** リソースが **NeverContactSource** に設定された非接続クラスターで、イメージのインポート機能が復元されました。(OCPBUGS-61474)

- この更新前は、再ラベル付け設定でサンプルがドロップされたために、Prometheus の **remote-write** アラートがアクティブ化されていました。その結果、ユーザーアラートが誤ってトリガーされていました。このリリースでは、Prometheus のリモート **write drop** ルールが調整され、アラートに影響しなくなりました。その結果、Prometheus の **RemoteWriteBehind** アラートのアクティブ化によってサンプルがドロップされなくなりました。(OCPBUGS-61856)

1.9.7.3. 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。

1.9.8. RHSA-2025:15680 - OpenShift Container Platform 4.16.48 のバグ修正とセキュリティー更新

発行日: 2025 年 9 月 17 日

OpenShift Container Platform リリース 4.16.48 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:15680 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.48 --pullspecs
```

1.9.8.1. 機能拡張

- この更新前は、**cluster-policy-controller** コンテナーはすべてのネットワークに対して **10357** ポートを公開し、バインドアドレスは **0.0.0.0** に設定されていました。**kube-controller-manager** (KCM) Pod マニフェストによって **hostNetwork** パラメーターが **true** に設定されているため、ポートはノードのホストネットワーク外部に公開されました。このポートはコンテナープローブにのみ使用されます。この機能拡張により、バインドアドレスは localhost のみをリッスンするように更新されました。その結果、ポートがノードネットワークの外部に公開されなくなり、ノードのセキュリティーが向上しました。(OCPBUGS-60834)

1.9.8.2. バグ修正

- この更新前は、古いバージョンの Azure API が原因で、サーバーの作成元のサブスクリプションとは異なるサブスクリプションに Capacity Reservation グループが存在する場合、そのグループを **MachineSet** に指定できませんでした。このリリースでは、最新バージョンの Azure API が使用されるため、サーバーの作成ポイントとは異なるサブスクリプションに Capacity Reservation グループがある場合でも、そのグループを **MachineSet** に指定できます。(OCPBUGS-56169)

- この更新前は、Cluster Operator のアップグレードに長い時間がかかった場合、Cluster Version Operator (CVO) はアップグレードがまだ進行中か、すでに停止しているかを判断できなかったため、何も報告しませんでした。このリリースでは、CVO によって報告されるクラスターバージョンのステータスの障害状態に対して新しい不明ステータスが追加され、クラスター管理者にクラスターを確認するよう通知します。その結果、管理者は Cluster Operator のアップグレードがブロックされるまで待つ必要がなくなります。(OCPBUGS-58452)

- この更新前は、Operator Lifecycle Management (OLM) の **OperatorGroup** の **ClusterRole** パラメーターでセレクターの順序を変更すると、不要な etcd 書き込みと認証キャッシュの無効化によってパフォーマンスが低下していました。このリリースでは、OLM の更新により、**ClusterRole** パラメーターでセレクターの順序を変更したときに、不要な etcd 書き込みと認証キャッシュの無効化が防止されます。(OCPBUGS-58881)

- この更新前は、**Machine Set** がスケールダウンされ、最小サイズに達すると、クラスターオートスケーラーによって、最後に残ったノードに **NoSchedule** taint が残され、ノードの使用が妨げられることがありました。この問題は、クラスターオートスケーラーのカウントエラーが原因で発生していました。このリリースでは、カウントエラーが修正され、**Machine Set** がスケールダウンされて最小サイズに達したときに、クラスターオートスケーラーが期待どおりに動作するようになりました。(OCPBUGS-59267)

- この更新前は、ユーザーインターフェイスと API の不一致により、vSphere 接続の設定を含むリソースが壊れていました。このリリースでは、更新された API 定義がユーザーインターフェイスで使用されるため、リソースが壊れることはありません。(OCPBUGS-60175)

- この更新前は、S3 互換ストレージプロバイダーから失敗したアップロードをパージしようとすると、イメージレジストリーがパニックを起こす場合がありました。この問題は、イメージレジストリーの s3 ドライバーが空のディレクトリーパスを誤って処理したために発生しました。このリリースでは、イメージレジストリーが空のディレクトリーパスを適切に処理し、パニックが修正されました。(OCPBUGS-60183)

- この更新前は、Hosted Control Plane の新しいネットワークデータタイプの難読化が不十分だったため、ユーザーデータが公開されていました。その結果、機密情報は保護されませんでした。このリリースでは、新しいネットワークデータタイプの難読化が実装されています。その結果、Hosted Control Plane の難読化されたネットワークデータにより、データのプライバシーが向上しています。(OCPBUGS-60520)

- この更新前は、Vertical Pod Autoscaler (VPA) に複数のレコメンダーを使用すると、デフォルトの VPA レコメンダーが、デフォルト以外のレコメンダーに関連付けられた VPA に属する **VPACheckpoint** オブジェクトを誤ってガーベッジコレクションしていました。このリリースでは、デフォルトのレコメンダーが、デフォルト以外のレコメンダーの **VPACheckpoint** オブジェクトのガベージコレクションを実行できなくなりました。(OCPBUGS-60609)

1.9.8.3. 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。

1.9.9. RHSA-2025:14859 - OpenShift Container Platform 4.16.47 のバグ修正とセキュリティー更新

発行日: 2025 年 9 月 3 日

OpenShift Container Platform リリース 4.16.47 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:14859 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.47 --pullspecs
```

1.9.9.1. バグ修正

- この更新前は、ビルドコントローラーはイメージプルシークレットではなく、リンクされた汎用シークレットを使用していました。このリリースでは、デフォルトのイメージプルシークレットは、サービスアカウントにリンクされている **ImagePullSecrets** Kubernetes シークレットを使用するビルドを検索します。(OCPBUGS-60233)

- この更新前は、**Microsoft Azure Files Container Storage Interface**(CSI) ドライバーは既存のストレージアカウントを再使用しようとしていました。このリリースでは、**Azure Files CSI** は動的プロビジョニング中にストレージアカウントを作成します。以前にプロビジョニングされた永続ボリュームは、クラスターの更新前に使用されていたものと同じストレージアカウントを引き続き使用します。(OCPBUGS-60248)

- この更新前は、Hosted Control Plane クラスターでネットワーク **obfuscation** 属性が有効になっている場合、入力/出力 (I/O) アーカイブにホスト名が含まれていました。このリリースでは、この問題が解決され、難読化された I/O アーカイブにはホスト名は含まれません。(OCPBUGS-60448)

- この更新前は、スナップショットリソースが大量にあると、起動時にコントローラーがタイムアウトしていました。その結果、スナップショット操作が中断され、バックアップおよび復元機能に影響が出ました。このリリースでは、Container Storage Interface (CSI) スナップショットコントローラーが大規模なスナップショットボリュームをより効率的に処理し、起動タイムアウトを削減します。その結果、大量のスナップショットの処理が改善され、バックアップおよび復元機能が期待どおりに完了するようになりました。(OCPBUGS-60450)

- この更新前は、**openshift-ptp** Pod のサイドカーを終了すると、再起動後にクロッククラスが

exit code 7 エラーで停止していました。このエラーは、サイドカー終了プロセスの不適切な処理が原因で発生していました。その結果、クロッククラスのメトリクスが使用不可になりました。このリリースでは、サイドカーの再起動はクロッククラスのメトリクスエラーを引き起こさず、サイドカーの再起動後にメトリクスが報告されるようになりました。(OCPBUGS-60570)

- この更新前は、VMware vSphere インフラストラクチャーでの OpenShift Container Platform 4.16 のアップグレード中に、Machine Config Daemon によってドメインネームサービス (DNS) ルックアップエラーが発生していました。このエラーは、**rpm-ostree** が **quay.io** レジストリーにアクセスできないために発生しました。その結果、DNS ルックアップの失敗によりアップグレードが停止されました。このリリースでは、vSphere インフラストラクチャーでの OpenShift Container Platform 4.16 アップグレード中に DNS ルックアップが失敗する問題が解決されました。その結果、DNS ルックアップの失敗により OpenShift Container Platform 4.16 へのアップグレードが停止しなくなりました。(OCPBUGS-60621)

- この更新前は、VMware vSphere インフラストラクチャー上での OpenShift Container Platform 4.16 へのアップグレードにより、**Skopeo** プロキシーエラーが原因で **rpm-ostree** システムのリベース中にドメインネームサービス (DNS) ルックアップが失敗していました。その結果、アップグレードが停止しました。このリリースでは、Docker レジストリーの接続問題が解決され、vSphere での OpenShift Container Platform 4.16 のアップグレード中に DNS ルックアップが失敗する問題が修正されました。その結果、アップグレードプロセスは停止せず、DNS ルックアップが再開されます。(OCPBUGS-60794)

1.9.9.2. 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。

1.9.10. RHSA-2025:13336 - OpenShift Container Platform 4.16.46 のバグ修正とセキュリティー更新

発行日: 2025 年 8 月 13 日

OpenShift Container Platform リリース 4.16.46 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:13336 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.46 --pullspecs
```

1.9.10.1. バグ修正

- この更新前は、**catalog-operator** が 5 分ごとにスナップショットをキャプチャーしていたため、多数の namespace、サブスクリプション、大規模なカタログソースを処理するときに CPU スパイクが発生していました。これにより、カタログソース Pod の負荷が増加し、ユーザーは Operator をインストールまたはアップグレードできませんでした。このリリースでは、カタログスナップショットキャッシュの有効期間が 30 分に延長されました。これにより、カタログソースに過度の負荷をかけずに試行を解決するために十分な時間が確保され、Operator のインストールおよびアップグレードプロセスが安定しました。(OCPBUGS-57429)

- この更新前は、**console.tab/horizontalNav href** の値内でフォワードスラッシュが許可されていました。4.15 以降は、リグレッションにより、**href** 値でフォワードスラッシュを使用しても正しく機能しないことがわかりました。このリリースでは、**console.tab/horizontalNav** の **href** 値のスラッシュが以前のように期待どおりに機能します。(OCPBUGS-59358)

1.9.10.2. 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。

1.9.11. RHSA-2025:11681 - OpenShift Container Platform 4.16.45 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 30 日

OpenShift Container Platform リリース 4.16.45 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:11681 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.45 --pullspecs
```

1.9.11.1. バグ修正

- この更新前は、タイトルプロパティーへの不適切なアクセスが原因で、**Metrics** タブのクエリーのコンマ区切り値 (CSV) エクスポートが失敗していました。その結果、一部のメトリクスの CSV ダウンロードが失敗し、ユーザーデータのエクスポートタスクに影響が出ていました。このリリースでは、特定のメトリクスの CSV エクスポートが正しく機能し、メトリクスの CSV ファイルが正常にダウンロードされます。(OCPBUGS-54316)

- この更新前は、**iptables-alerter** Pod がローカル Pod を正しく処理していなかったために、CPU 使用率が過剰になり、リソースの枯渇が発生していました。このリリースでは、スクリプトの実行を最適化することで、**iptables-alerter** Pod の高い CPU 使用率が削減されました。その結果、**iptables-alerter** Pod が CPU 制限を超えなくなりました。(OCPBUGS-56992)

- この更新前は、共有 Virtual Private Cloud (VPC) 環境の OpenShift Container Platform クラスターのプライマリーノードに対して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが誤ったサブネットに複製されていました。その結果、プライマリーノードインスタンスに接続の問題が発生していました。このリリースでは、共有 VPC クラスター内のプライマリーインスタンスが正しいサブネットに配置されるため、プライマリーノードのサブネットが正しいものになります。(OCPBUGS-58290)

- この更新前は、コンテナーランタイムインターフェイス (CRI-O) が、永続的なコンテナープロセス参照が原因で、終了した Pod を認識できませんでした。その結果、Pod の終了プロセスが失敗し、ステートフルセットが無期限に終了状態のままになっていました。このリリースでは、終了ループの開始を示すフラグを追加することで、CRI-O におけるコンテナーの **Process not found** の問題が解決されました。(OCPBUGS-58509)

- この更新前は、**useModal** フックが再利用されていたため、複数のモーダルが上書きされていました。その結果、別々のページのモーダルが重なり合い、Red Hat OpenShift Lightspeed でユーザーインターフェイスの問題が発生していました。このリリースでは、モーダルごとに異なる識別子が使用できるため、複数のモーダルが互いに上書きされることがなくなりました。(OCPBUGS-59274)

1.9.11.2. 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。

1.9.12. RHSA-2025:10781 - OpenShift Container Platform 4.16.44 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 16 日

OpenShift Container Platform リリース 4.16.44 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:10781 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.44 --pullspecs
```

1.9.12.1. バグ修正

- この更新前は、Kubernetes API サーバーのループバック証明書の有効期限が早期に切れていました。この証明書は自己署名証明書であるため、有効期間が短いことが原因で証明書が終了し、API サーバーで通信の問題が発生していました。この更新により、自己署名ループバック証明書の有効期間が延長されました。これにより、将来の証明書の有効期限切れが防止され、Kubernetes バージョン 4.16.z の API サーバーがより安定します。(OCPBUGS-58054)

- この更新前は、OpenShift Container Platform クラスターを Amazon Web Services (AWS) にインストールする際に、プライマリーノードを複数のサブネットに分散させると、インストールが失敗していました。このエラーは、Network Load Balancer (NLB) のセキュリティーグループ設定が不適切なために発生していました。この更新により、NLB のセキュリティーグループが更新されます。AWS クラスターのインストール中は、サブネットに関係なく、すべてのプライマリーノードのセキュリティーグループトラフィックが許可されます。その結果、クラスターのインストールで、複数のプライマリーサブネットが正常にサポートされるようになりました。(OCPBUGS-57498)

- この更新前は、クラスター内の ESXi ホストの電源がオフになっているときに Open Virtual Appliance (OVA) をクラスターにインポートしようとすると、インポートが失敗していました。このリリースでは、ESXi ホストの電源がオフになっている場合でも、OVA をクラスターに正常にインポートできます。(OCPBUGS-57460)

- この更新前は、Open Virtual Network (OVN) のネットワークコンポーネントによって、2 つのクラスターノードに重複した静的ルートが作成されていました。これらの重複したルートにより、ネットワークトラフィックが断続的にドロップされ、ネットワーク通信の信頼性が低下していました。この更新により、クラスターノードの OVN データベース内で静的ルートが重複することが許容され、パケットのドロップが解消されました。(OCPBUGS-57396)

- この更新前は、高可用性プロキシー (HAProxy) が正常なシャットダウン中にアイドル接続を処理する方法を制御する直接的な API がありませんでした。そのため、接続終了動作の管理の柔軟性が限られていました。このリリースでは、正常なシャットダウン中の HAProxy 接続の管理が修正され、進行中の応答を保持するか、アイドル状態の接続を閉じるかを管理者が選択できるようになりました。(OCPBUGS-56424)

- この更新前は、API エンドポイントの証明書の問題により、クラスターのインストール中に Red Hat Advanced Cluster Management (RHACM) エージェントが起動できず、インストールがハングしたり、アンインストールが停止したりしていました。このリリースでは、API エンドポイントの証明書の問題が解決され、証明書の問題が原因で RHACM エージェントがインストール中にハングすることがなくなりました。(OCPBUGS-58505)

1.9.12.2. 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。

1.9.13. RHSA-2025:9765 - OpenShift Container Platform 4.16.43 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 2 日

OpenShift Container Platform リリース 4.16.43 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:9765 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.43 --pullspecs
```

1.9.13.1. バグ修正

- 以前は、Machine Config Daemon (MCD) Pod が、インプレースアップグレード中にプロキシー変数を適切に考慮していませんでした。調整プロセスにおけるこの見落としにより、プロキシー設定が欠落し、ユーザーのイメージのプルが失敗していました。このリリースでは、MCD Pod がインプレースアップグレードストラテジーの実行中にプロキシー変数を正しく認識します。その結果、プロキシー設定の問題が原因でイメージのプルが失敗することがなくなり、アップグレードエクスペリエンスが向上します。(OCPBUGS-57494)

- 以前は、テスト手順中に **/metrics** および **/metrics/cadvisor** エンドポイントが無視されていました。この見落としにより、**TargetDown** アラートの **Component Readiness** テストで断続的な障害が発生し、システム全体の安定性に悪影響を及ぼしていました。このリリースでは、**Google-Cadvisor** パッケージの更新により、このテストが失敗する原因となっていた問題が解決され、システムの安定性とコンポーネントの準備状況チェックの信頼性が大幅に向上しました。(OCPBUGS-57290)

- 以前は、ネットワークアタッチメント定義 (NAD) コントローラーが、複数の大規模なマルチレイヤーネットワークポリシーを処理するときに、null ポインターの逆参照が発生していました。この問題により、コントローラーが不安定になり、Open Virtual Network (OVN) Pod がクラッシュしていました。このリリースでは、null ポインターの逆参照の問題が解決されています。この修正により、今後の OVN Pod のクラッシュが防止され、OVN Pod の安定性とクラスターの機能が向上しました。(OCPBUGS-56242)

- 以前は、**hc.spec.services.servicePublishingStrategy** パラメーターで定義された Kubernetes API サーバー (KAS) ホスト名と競合するサブジェクト代替名 (SAN) を持つカスタム証明書を追加すると、KAS 証明書が新しいペイロード生成に含まれませんでした。Hosted Control Plane クラスターに参加しようとするすべての新しいノードで、証明書の検証の問題が発生していました。このリリースでは、検証ステップによってこの競合が防止され、ユーザーに問題が通知されます。(OCPBUGS-55697)

- 以前は、マシン設定プール (MCP) がノードの drain (Pod の退避) を適切に実行できなかったため、OpenShift SDN から OVN-Kubernetes への限定的なライブマイグレーションが停止していました。その結果、ノードの Container Network Interface (CNI) が混在した状態のままとなり、アプリケーションが利用できなくなる、DNS 解決が失敗するなどの重大な問題が発生していました。このリリースでは、限定的なライブマイグレーションで、MCP が正しく使用されてノードが drain され、シームレスに移行が実行されます。この改善により、移行プロセス中にユーザーがスムーズにアプリケーションを利用でき、サービスの通信が一貫して提供されます。(OCPBUGS-55282)

- 以前は、Secure Hash Algorithm (SHA-1) 認証局 (CA) 証明書を持つルートにより、高可用性プ

ロキシー (**HAProxy**) のリロードが失敗していました。その結果、リロード操作中にサービスの中断が発生していました。このリリースでは、検証が更新され、SHA-1 CA 証明書を持つルートが拒否されるようになりました。その結果、**HAProxy** のリロードの失敗が防止され、スムーズに動作するようになりました。(OCPBUGS-49391)

- 以前は、4,000 個の Egress ファイアウォールポリシーを持つ大規模な OpenShift Container Platform クラスターで、移行中に ovn-kube コントローラーで障害が発生していました。これは、同期時間が長すぎるために移行プロセスがブロックされ、ワーカーノードの再起動が必要になることが原因でした。このリリースでは、高負荷の状況に対応するために、**EgressFirewall** インフォーマーの **InformerSyncTimeout** パラメーターが引き上げられました。その結果、大規模な OpenShift Container Platform クラスターの移行がワーカーノードの再起動によって停止することがなくなり、よりスムーズで信頼性の高い移行操作が行われるようになりました。(OCPBUGS-48121)

1.9.13.2. 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。

1.9.14. RHSA-2025:8556 - OpenShift Container Platform 4.16.42 のバグ修正とセキュリティー更新

発行日: 2025 年 6 月 11 日

OpenShift Container Platform リリース 4.16.42 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:8556 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.42 --pullspecs
```

1.9.14.1. バグ修正

- 以前は、コントロールプレーンのみの更新を実行する場合、Web コンソールで、コンピュートノードを 60 日以内に更新する必要があるというアラートがユーザーに表示されていました。この更新により、この無効なアラートが Web コンソールに表示されなくなりました。(OCPBUGS-56858)

- 以前、バグ修正により可用性セットの設定が変更されました。その際に、障害ドメイン数が固定値の **2** ではなく、利用可能な最大値を使用するように変更されました。これにより、バグ修正前に作成されたコンピュートマシンセットでスケーリングの問題が発生しました。これはコントローラーがイミュータブルな可用性セットの変更を試みることが原因でした。このリリースでは、可用性セットが作成後に変更されなくなり、影響を受けるコンピュートマシンセットが適切にスケーリングできるようになりました。(OCPBUGS-56656)

- 以前は、Operator Lifecycle Manager (OLM) によって管理される OpenShift Container Platform バージョン 4.15 以降のバージョンに、**olm.managed: "true"** ラベルが必要でした。場合によっては、ラベルが見つからないと OLM が起動に失敗し、**CrashLoopBackOff** 状態になることがありました。この状況に関するログは、Info レベルのログとして表示されていたため、根本原因の特定が困難でした。このリリースでは、ラベルが見つからない場合に問題を明確化して診断しやすくなるよう、ログレベルがエラーに変更されました。(OCPBUGS-56358)

- 以前は、ビルドコンテナーでデフォルトのプロキシー環境変数が null に設定されている場合、コンテナー内の一部のアプリケーションが実行されませんでした。このリリースでは、プロキ

シー環境変数が定義されており、デフォルト値が null でない場合にのみ、プロキシー環境変数はビルドコンテナーに追加されます。(OCPBUGS-56354)

- 以前は、機能の移行を無効にすると、Cluster Network Operator (CNO) がソフトウェア定義ネットワーク (SDN) のライブマイグレーションを開始できなくなりました。このリリースでは、機能の移行を無効にしても、CNO が SDN のライブマイグレーションをトリガーできるようになりました。(OCPBUGS-56195)

- 以前は、Ingress からルートへの変換が失敗した後にエラーが発生した場合、イベントがログに記録されませんでした。この更新により、このエラーがイベントログに表示されるようになりました。(OCPBUGS-56152)

- 以前は、ノードが準備完了になる前に削除された Azure スポットマシンが、**provisioned** 状態のままになることがありました。このリリースでは、Azure スポットインスタンスで delete エビクションポリシーが使用されるようになりました。このポリシーにより、プリエンプション時にマシンが **failed** 状態に正しく移行するようになります。(OCPBUGS-56092)

- 以前は、Zscaler のトラフィックスキャンが原因で、CRI-O コンテナーエンジンでプル進行のタイムアウトが発生し、無限ループが発生してイメージのプルが失敗していました。その結果、ユーザーがイメージをプルできませんでした。このリリースでは、プル進行のタイムアウトが 20 秒になり、イメージプルのタイムアウトと進行に関する出力が無効になり、Zscaler におけるお客様のイメージプルタイムアウトの問題が軽減されました。(OCPBUGS-54665)

- 以前は、Azure 上の MAC バインディングフローの有効期限が切れると、Open vSwitch (OVS) がコントローラーアクションを実行してそのフローを再インストールしていました。フローが削除された直後に OVN コントローラーが低速になると、新しいフローが時間内にインストールされませんでした。この遅延により、データプレーンのトラフィックが減少していました。このリリースでは、新しいフローがコントローラーアクションによって正しくインストールされるため、データプレーンのトラフィックが減少しません。(OCPBUGS-53151)

- 以前は、OVN-Kubernetes コンテナーの再起動中に、内部 **ovn-k8-mp0** インターフェイスのルートが削除されて再追加されたため、一時的なトラフィック停止が発生していました。このリリースでは、**ovn-k8s-mp0** インターフェイスを通過するトラフィックパスが遮断されなくなり、**ovn-kubernetes** Pod の再起動中にルートが削除されなくなりました。(OCPBUGS-52503)

1.9.14.2. 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。

1.9.15. RHBA-2025:8116 - OpenShift Container Platform 4.16.41 のバグ修正

発行日: 2025 年 5 月 28 日

OpenShift Container Platform リリース 4.16.41 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:8116 アドバイザリーに記載されています。

以下のコマンドを実行して、この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 4.16.41 --pullspecs
```

1.9.15.1. バグ修正

- 以前は、インストール済みの Operator のリストを表示すると、リストに Operator が 2 回表示

されていました。これは、コピーされたクラスターサービスバージョン (CSV) が Operator Lifecycle Manager (OLM) で無効になっている場合、現在選択中のプロジェクトが Operator のデフォルトの namespace と一致するために発生していました。このリリースでは、Operator が 1 回だけ表示されるようになりました。(OCPBUGS-55644)

- 以前は、Assisted Installer は、ファイバーチャネルマルチパスボリュームのハードウェア検出中に World Wide Name (WWN) の詳細を検出できませんでした。その結果、ファイバーチャネルマルチパスディスクを WWN ルートデバイスと一致させることができませんでした。そのため、WWN ルートデバイスヒントを指定すると、ヒントによってすべてのファイバーチャネルマルチパスディスクが除外されていました。このリリースでは、ファイバーチャネルマルチパスディスク検出中に Assisted Installer が WWN の詳細を検出するようになりました。複数のファイバーチャネルマルチパスディスクが存在する場合は、WWN ルートデバイスヒントを使用して、クラスターのプライマリーディスクを選択できます。(OCPBUGS-55443)

- 以前は、サービスの依存関係が欠落していたため、**nmstate** を使用して **br-ex** ブリッジを管理すると、**mtu-migration** サービスが正しく機能しませんでした。このリリースでは、サービスの依存関係が追加され、移行プロセスの開始前に、**nmstate** を使用して **br-ex** を管理するネットワーク設定の正確性が確保されるようになりました。(OCPBUGS-54831)

1.9.15.2. 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。

1.9.16. RHSA-2025:4731 - OpenShift Container Platform 4.16.40 のバグ修正とセキュリティー更新

発行日: 2025 年 5 月 15 日

OpenShift Container Platform リリース 4.16.40 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:4731 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:4733 アドバイザリーによって提供されます。

以下のコマンドを実行して、この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 4.16.40 --pullspecs
```

1.9.16.1. 既知の問題

- グランドマスタークロック (T-GM) が **Locked** 状態に遷移するのが早すぎます。これは、Digital Phase-Locked Loop (DPLL) が **Locked-HO-Acquired** 状態への変更を完了する前、および Global Navigation Satellite Systems (GNSS) タイムソースが復元された後に発生する既知の問題です。(OCPBUGS-49826)

1.9.16.2. バグ修正

- 以前は、ノードの表示権限はあるが証明書署名要求 (CSR) の表示権限がない場合、**Nodes list** ページにアクセスできませんでした。このリリースでは、**Nodes list** ページにアクセスするために CSR の表示権限は不要になりました。(OCPBUGS-55378)

- 以前は、**IngressWithoutClassName** アラートを持つ Ingress リソースの場合、リソースが削除されても Ingress Controller によってアラートが削除されませんでした。アラートは、引き続き OpenShift Container Platform Web コンソールに表示されていました。このリリースでは、Ingress Controller は、Ingress リソースを削除する前

に、**openshift_ingress_to_route_controller_ingress_without_class_name** メトリクスを **0** にリセットします。アラートは削除され、Web コンソールで開かなくなりました。(OCPBUGS-55201)

- 以前は、**Go** ルーチン間の競合状態が原因で、Cluster Version Operator (CVO) の起動後に CVO の動作に一貫性がありませんでした。このリリースでは、**Go** ルーチンの同期が改善され、問題が解決されました。(OCPBUGS-55156)

- 以前は、Microsoft Azure ネットワークインターフェイスが **provisioning failed** 状態で作成されていたため、リソース割り当ての問題が発生する可能性がありました。このリリースでは、Azure ソフトウェア開発キット (SDK) を使用してネットワークインターフェイスのプロビジョニング状態を検証および再試行するコードが追加され、Azure ネットワークインターフェイスコントローラー (NIC) のプロビジョニングの信頼性が向上しました。(OCPBUGS-54990)

- 以前は、スクレイピングが失敗すると、Prometheus が誤って次回のスクレイピングからのサンプルを重複とみなし、削除していました。この問題は、障害直後のスクレイピングにのみ影響し、その後のスクレイピングは正しく処理されていました。このリリースでは、失敗後のスクレイピングが正しく処理されるようになり、有効なサンプルが誤ってドロップされなくなりました。(OCPBUGS-54942)

- 以前は、**oauth** API サーバーによって管理されているリソースの検証 Webhook を作成しようとしても、検証 Webhook が作成されませんでした。この問題は、**oauth** API サーバーとデータプレーン間の通信の問題が原因で発生しました。このリリースでは、**oauth** API サーバーとデータプレーン間の通信をブリッジする Konnectivity プロキシーサイドカーが追加され、**oauth** API サーバーが管理する任意のリソースの検証 Webhook を作成できるようになりました。(OCPBUGS-54914)

- 以前は、SELinux **container_logreader_t** ドメインを使用して **/var/log** 内のコンテナーログを表示していたコンテナーが、**/var/log/containers** サブディレクトリー内のログにアクセスできませんでした。この問題は、シンボリックリンクが見つからないために発生していました。このリリースでは、**/var/log/containers** のシンボリックリンクが作成され、コンテナーが **/var/log/containers** 内のログにアクセスできるようになりました。(OCPBUGS-54818)

- 以前は、Container Network Interface (CNI) の再デプロイが不完全だったために、限定的なライブマイグレーション中に問題が発生していました。この問題により、ユーザーの OpenShift Container Platform ソフトウェア定義ネットワーク (SDN) へのロールバック中に、ネットワーク接続の問題が発生する可能性がありました。このリリースでは、バグ修正により、Egress IP アドレスのロールバック中に非クラウドプラットフォームを処理するためのノードのプライマリー IP アドレスのアノテーションが追加されました。この修正により、OpenShift Container Platform SDN へのロールバックがスムーズに実行され、限定的なライブマイグレーション中に発生する停止の問題が解決され、ネットワーク接続が改善されました。(OCPBUGS-53317)

- 以前は、クラスターに設定された最大転送単位 (MTU) 値よりも大きい User Datagram Protocol (UDP) パケットを、サービスを使用してパケットエンドポイントに送信できませんでした。このリリースでは、パケットサイズに関係なく、サービスの IP アドレスの代わりに Pod の IP アドレスが使用され、UDP パケットがエンドポイントに送信されます。(OCPBUGS-50581)

- 以前は、内部公開ストラテジーのバグにより、プライベートクラスターのポートが欠落し、アクセスできなくなっていました。このリリースでは、プライベートクラスターに必要なポートが修正されたため、デプロイの成功率が向上し、プライベートクラスターへのシームレスなアクセスが確保されます。(OCPBUGS-35040)

- 以前は、Pod が削除されると、Single Root I/O Virtualization (SR-IOV) Virtual Function (VF) は、最大転送単位 (MTU) の予期しない値の変更を元に戻しませんでした。この問題は、Pod 内のアプリケーションの MTU 値が変更され、Pod の MTU 値も変更された場合に発生しました。

このリリースでは、SR-IOV Container Network Interface (CNI) によって予期しない MTU 値の変更が元の値に戻され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-55012)

1.9.16.3. 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。

1.9.17. RHSA-2025:4008 - OpenShift Container Platform 4.16.39 のバグ修正とセキュリティー更新

発行日: 2025 年 4 月 23 日

OpenShift Container Platform リリース 4.16.39 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:4008 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:4010 アドバイザリーで提供されています。

以下のコマンドを実行して、この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 4.16.39 --pullspecs
```

1.9.17.1. 既知の問題

- IPsec は Red Hat Enterprise Linux (RHEL) コンピュートノードではサポートされていません。これは、各コンピュートノードに存在するホストと **ovn-ipsec** コンテナー間の **libreswan** 非互換性の問題が原因です。(OCPBUGS-52952)

1.9.17.2. バグ修正

- 以前は、**openshift-install agent create pxe-files** コマンドを実行すると、**/tmp/agent** に一時ディレクトリーが作成され、コマンドが完了してもこれらのディレクトリーが削除されませんでした。このリリースでは、コマンドが完了に近づくとディレクトリーが削除されるようになり、ディレクトリーを手動で削除する必要がなくなりました。(OCPBUGS-54345)

- 以前は、イメージが作成されたにもかかわらず、非接続環境のセットアップでエージェント ISO をビルドするときに "unable to read image" というエラーメッセージが表示されていました。これは、**ImageContentSourcePolicy** (ICSP) がチェックされていないために発生しました。このリリースでは、エラーメッセージは表示されなくなりました。(OCPBUGS-54327)

- 以前は、マシンセット内のマシンに障害が発生したために、クラスターオートスケーラーがスケーリングを停止していました。この状況は、クラスターオートスケーラーがさまざまな非実行フェーズにあるマシンをカウントする方法が不正確であるために発生しました。このリリースでは、その不正確性が修正され、クラスターオートスケーラーのカウントがより正確になりました。(OCPBUGS-54326)

- 以前は、IBM Cloud® Cloud Internet Services (CIS) 実装の更新により、アップストリームの Terraform プラグインが影響を受けていました。IBM Cloud® 上に外部向けクラスターを作成しようとした場合、次のエラーが発生しました。

```
ERROR Error: Plugin did not respond
ERROR
ERROR with module.cis.ibm_cis_dns_record.kubernetes_api_internal[0],
```

```
ERROR on cis/main.tf line 27, in resource "ibm_cis_dns_record" "kubernetes_api_internal":
ERROR 27: resource "ibm_cis_dns_record" "kubernetes_api_internal"
```

このリリースでは、プラグインの問題が発生しなくなり、インストールプログラムを使用して OpenShift Container Platform 上に外部クラスターを作成できます。(OCPBUGS-54263)

- 以前は、Operator Marketplace と Operator Lifecycle Manager (OLM) で、古いバージョンの **pod-security.kubernetes.io/** ラベルが使用されていました。このリリースでは、Operator Marketplace がデプロイされている namespace で、**latest** とマークされた Pod Security Admission (PSA) ラベルが使用されるようになりました。(OCPBUGS-53395)

- 以前は、Local Zone や Wavelength Zone などのエッジゾーンにある既存のサブネットの Amazon Web Services (AWS) にクラスターをインストールすると、エッジゾーンのサブネットリソースに **kubernetes.io/cluster/<InfraID>:shared** タグがありませんでした。このリリースでは、修正により、**install-config.yaml** 設定ファイルで使用されるすべてのサブネットに必要なタグが付けられるようになりました。(OCPBUGS-50547)

- 以前は、レジストリーにアクセスするために信頼バンドルを必要とするビルドを実行すると、ビルドはクラスタープロキシーで設定されたバンドルを取得しませんでした。カスタムトラストバンドルに必要なレジストリーが参照された場合、ビルドは失敗しました。このリリースでは、プロキシー設定で指定された信頼バンドルを必要とするビルドが成功し、問題は解決されています。(OCPBUGS-49914)

1.9.17.3. 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。

1.9.18. RHSA-2025:3301 - OpenShift Container Platform 4.16.38 のバグ修正とセキュリティー更新

発行日: 2025 年 4 月 2 日

OpenShift Container Platform リリース 4.16.38 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:3301 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:3303 アドバイザリーで提供されています。

以下のコマンドを実行して、この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 4.16.38 --pullspecs
```

1.9.18.1. バグ修正

- 以前は、インストールプログラムによってサポートされていないセキュリティーグループがロードバランサーに追加されていたため、Commercial Cloud Services (C2S) リージョンまたは Secret Commercial Cloud Services (SC2S) リージョンに AWS クラスターをインストールすると失敗していました。このリリースでは、インストールプログラムはサポートされていないセキュリティーグループをロードバランサーに追加しなくなりました。(OCPBUGS-53459)

- 以前は、再起動操作中にデプロイメントがステージングの場所に移動された場合、クラスターのシャットダウン時に、競合状態により段階的な **ostree** デプロイメントが完了できませんでした。このリリースでは、修正により **ostree** デプロイメントから競合状態が除去されました。(OCPBUGS-53313)

- 以前は、**trusted-ca-bundle-managed** ConfigMap コンポーネントは必須コンポーネントでした。このリリースでは、このコンポーネントはオプションであり、カスタム PKI を使用する場合に **trusted-ca-bundle-managed** ConfigMap コンポーネントなしでクラスターをデプロイできます。(OCPBUGS-52857)

- 以前は、モニタリングに関連する特定のフラグが設定されていない限り、Web コンソールの **Observe** セクションにはプラグインから提供された項目が表示されませんでした。しかし、これらのフラグにより、ロギングやネットワーク可観測性などの他のプラグインは **Observe** セクションに項目を追加できませんでした。このリリースでは、モニタリングフラグが削除され、他のプラグインが **Observe** セクションに項目を追加できるようになりました。(OCPBUGS-52851)

- 以前は、**ClusterVersion** が **Completed** 更新を受信しなかった場合、クラスター更新中に **Cluster Settings** ページが正しくレンダリングされませんでした。このリリースにより、**ClusterVersion** が **Completed** 更新を受信していない場合でも、**Cluster Setting** ページが適切にレンダリングされるようになりました。(OCPBUGS-52450)

- 以前は、クラスターオートスケーラーは、削除中に **PreferNoSchedule** taint のあるノードを残すことがありました。このリリースでは、一括削除の上限が無効になっているため、この taint を持つノードは削除後に残らなくなります。(OCPBUGS-52329)

- 以前は、OVN-Kubernetes ネットワークプラグインと Kubernetes-NMState Operator が対話すると、予期しない接続プロファイルがディスクストレージに残っていました。これらの接続プロファイルにより、再起動時に **ovs-configuration** サービスが失敗することがありました。このリリースでは、接続プロファイルが修正され、問題は発生しなくなりました。(OCPBUGS-52310)

- 以前は、**Developer** パースペクティブの **Alert rules** ページのアラートリンクに、無効なリンクへの外部ラベルが含まれていました。これは、**Alerts** ページの URL が外部ラベルを想定していなかったために発生しました。このリリースでは、アラート URL に外部ラベルが追加されなくなったため、アラートリンクが正確になりました。(OCPBUGS-52252)

- 以前は、ワーカーノードがクラスターに参加しようとすると、プロセスが完了する前にランデブーノードが再起動していました。そのためインストールは失敗しました。このリリースでは、競合状態を修正するパッチが適用され、問題は解決されています。(OCPBUGS-51362)

- 以前は、Assisted Installer エージェントがイメージをプルしようとすると、タイムアウト時間が 30 秒と短すぎるためにインストールが失敗することがありました。このリリースでは、タイムアウト時間が延長され、問題は解決されました。(OCPBUGS-51346)

- 以前は、Agent-based Installer の場合、すべてのホスト検証ステータスログは、最初に登録されたホストの名前を参照していました。その結果、ホスト検証に失敗したときに問題のあるホストを特定できませんでした。このリリースでは、各ログメッセージで正しいホストが識別されます。(OCPBUGS-51207)

- 以前は、DNS ベースの Egress ファイアウォールは、大文字の DNS 名が含まれるファイアウォールルールの作成を誤って妨げていました。このリリースでは、修正により大文字の DNS 名が妨げられなくなりました。(OCPBUGS-51074)

- 以前は、control plane Operator は、API エンドポイントの可用性をチェックするときに、設定されている **_PROXY** 環境変数を適用しませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-50993)

- 以前は、可用性セット障害ドメイン数は **2** にハードコードされていました。この値はほとんどのリージョンで機能しますが、**centraluseuap** および **eastusstg** リージョンでは失敗しました。このリリースでは、リージョンの可用性セット障害ドメイン数が動的に設定されるため、

この問題は発生しなくなりました。(OCPBUGS-50966)

- 以前は、IPv6 アドレスの自動設定に関連する接続の問題により、LocalNet を使用したライブマイグレーション中に長時間のダウンタイムが発生していました。このリリースにより、この問題は解決されました。(OCPBUGS-50595)

- 以前は、Egress IPv6 が割り当てられたノードで Pod が実行されると、Pod はデュアルスタッククラスター内の Kubernetes サービスと通信できませんでした。その結果、IP ファミリーのトラフィックがドロップされました。このリリースにより、トラフィックがドロップされるリスクが排除されます。(OCPBUGS-50594)

- 以前は、カスタム Security Context Constraint (SCC) により、Cluster Version Operator によって生成された Pod がクラスターバージョンのアップグレードを受け取れなくなっていました。このリリースにより、OpenShift Container Platform が各 Pod にデフォルトの SCC を設定するようになったため、作成されたカスタム SCC は Pod に影響を与えません。(OCPBUGS-50590)

- 以前は、OpenShift Container Platform の内部レジストリーがサポートしていなかったため、**ap-southeast-5** リージョンまたはその他のリージョンの AWS にクラスターをインストールできませんでした。このリリースでは、次のリージョンを含むように内部レジストリーが更新されたため、この問題は発生しなくなりました。

  - **ap-southeast-5**
  - **ap-southeast-7**
  - **ca-west-1**
  - **il-central-1**
  - **mx-central-1**
    (OCPBUGS-49696)

- 以前は、コンテナーレジストリーで使用される **imagestreams** を解決できなかったため、ROSA の no-egress 機能を使用するホステッドクラスターと、Amazon Virtual Private Cloud (VPC) エンドポイントを介してアクセスされたコンテナーレジストリーのインストールに失敗していました。これは、Konnectivity プロキシーがコントロールプレーンで **openshift-apiserver** を使用して、クラウド API 接尾辞を持つレジストリー名を解決したことが原因でした。このリリースでは、Konnectivity プロキシーは、ホスト名を一貫して解決し、ルーティングします。(OCPBUGS-46466)

- 以前は、Web コンソールの **Alert Rules** ページの URL が正しくありませんでした。このリリースでは、URL が修正され、問題は解決されました。(OCPBUGS-46388)

- 以前は、仮想マシンの再起動後、ホステッドクラスターからの永続ボリューム要求 (PVC) が仮想マシンから削除されていました。ただし、**VolumeAttachment** リソースは削除されず、PVC が仮想マシンにアタッチされると想定されていたためにクラスターで問題が発生しました。このリリースでは、仮想マシンの再起動後に **VolumeAttachment** リソースが削除されるため、問題は発生しなくなりました。(OCPBUGS-44622)

1.9.18.2. 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。

1.9.19. RHSA-2025:1907 - OpenShift Container Platform 4.16.37 のバグ修正とセキュリティー更新

発行日: 2025 年 5 月 5 日

OpenShift Container Platform リリース 4.16.37 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:1907 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:1910 アドバイザリーによって提供されます。

以下のコマンドを実行して、この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 4.16.37 --pullspecs
```

1.9.19.1. バグ修正

- 以前は、セキュアプロキシーを有効にし、**configuration.proxy.trustCA** フィールドに証明書を設定して状態でクラスターを作成できませんでした。別の問題により、管理クラスタープロキシー経由でクラウド API にアクセスできませんでした。このリリースでは、これらの問題は解決されています。(OCPBUGS-51296)
- 以前は、バケット名の生成に誤ったロジックがありました。このリリースにより、この問題は解決されました。(OCPBUGS-51167)
- 以前は、IBM Power Virtual Server クラスターで Dynamic Host Configuration Protocol (DHCP) ネットワークを削除しても、サブリソースが残存していました。このリリースでは、DHCP ネットワークを削除すると、破棄操作を続行する前にサブリソースが削除されるようになりました。(OCPBUGS-51111)
- 以前は、クラスター上の Kubernetes EndpointSlice に誤ったアドレスが渡されていました。この問題により、IPv6 非接続環境のエージェントベースのクラスターに MetalLB Operator をインストールできませんでした。このリリースでは、修正によりアドレス評価方法が変更されます。Red Hat Marketplace Pod はクラスター API サーバーに正常に接続できるようになり、MetalLB Operator のインストールと IPv6 非接続環境での Ingress トラフィックの処理が可能になります。(OCPBUGS-50694)
- 以前は、**cnf-tests image** はテストの実行に古いイメージバージョンを使用していました。このリリースにより、この問題は解決されました。(OCPBUGS-50611)
- 以前は、**CSV details** ページに関連するオペランドをリストするために使用されるリソースリストページ拡張機能に、追加の名前プロパティーが渡されていました。これにより、オペランドリストが CSV 名でフィルタリングされ、通常は空のリストになります。この更新により、オペランドが期待どおりにリストされるようになりました。(OCPBUGS-46441)

1.9.19.2. 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。

1.9.20. RHSA-2025:1707 - OpenShift Container Platform 4.16.36 のバグ修正とセキュリティー更新

発行日: 2025 年 2 月 27 日

OpenShift Container Platform リリース 4.16.36 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:1707 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:1709 アドバイザリーで提供されています。

以下のコマンドを実行して、この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 4.16.36 --pullspecs
```

1.9.20.1. バグ修正

- 以前は、数百のノードとネットワークポリシーを持つ特定の OpenShift Container Platform クラスターにより、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ライブマイグレーションが失敗していました。ライブマイグレーション操作は、RAM 消費量が多すぎるため失敗しました。このリリースでは、修正により、これらのクラスター設定でライブマイグレーション操作が失敗しなくなりました。(OCPBUGS-46493)

1.9.20.2. 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。

1.9.21. RHSA-2025:1386 - OpenShift Container Platform 4.16.35 バグ修正の更新

発行日: 2025 年 2 月 19 日

OpenShift Container Platform リリース 4.16.35 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:1386 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:1390 アドバイザリーで提供されています。

以下のコマンドを実行して、この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 4.16.35 --pullspecs
```

1.9.21.1. バグ修正

- 以前は、Bare Metal Operator (BMO) は、インテリジェントプラットフォーム管理インターフェイス (IPMI) を含め、**HostFirmwareComponents** カスタムリソースをサポートしていないすべての **BareMetalHosts** (BMH) に対して **HostFirmwareComponents** カスタムリソースを作成していました。このリリースでは、BMH に対してのみ **HostFirmwareComponents** カスタムリソースが作成されます。(OCPBUGS-49703)

- 以前は、ソースレジストリーが無効なサブマニフェストの結果を返すと、マニフェストリストのインポートにより API クラッシュが発生する可能性がありました。この更新により、API はクラッシュするのではなく、インポートされたタグのエラーにフラグを付けます。(OCPBUGS-49656)

- 以前は、インストールプログラムを使用して Prism Central 環境にクラスターをインストールすると、RHCOS イメージをロードする **prism-api** 呼び出しがタイムアウトになり、インストールが失敗していました。この問題は、**prismAPICallTimeout** パラメーターが **5** 分に設定されていたために発生しました。このリリースでは、**install-config.yaml** 設定ファイルの **prismAPICallTimeout** パラメーターのデフォルトが **10** 分になりました。**prism-api** 呼び出しのタイムアウトをさらに長くする必要がある場合は、パラメーターを設定することもできます。(OCPBUGS-49416)

- 以前は、**DeploymentConfig** オブジェクトの **deploymentconfigs/scale** サブリソースのアドミッション Webhook を使用してオブジェクトをスケーリングしようとすると、**apiserver** が要求を処理できませんでした。これにより、**DeploymentConfig** オブジェクトをスケーリングできなかったため、オブジェクトに影響が出ていました。このリリースでは、修正によりこの問題が発生しなくなりました。(OCPBUGS-45010)

1.9.21.2. 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。

1.9.22. RHBA-2025:1124 - OpenShift Container Platform 4.16.34 バグ修正の更新

発行日: 2025 年 2 月 12 日

OpenShift Container Platform リリース 4.16.34 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:1124 アドバイザリーに記載されています。このリリース用の RPM パッケージはありません。

以下のコマンドを実行して、この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 4.16.34 --pullspecs
```

1.9.22.1. 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。

1.9.23. RHBA-2025:0828 - OpenShift Container Platform 4.16.33 のバグ修正とセキュリティー更新

発行日: 2025 年 2 月 6 日

OpenShift Container Platform リリース 4.16.33 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:0828 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:0830 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、この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 4.16.33 --pullspecs
```

1.9.23.1. バグ修正

- 以前は、一部のクラスターオートスケーラーメトリクスが初期化されておらず、利用できませんでした。このリリースでは、クラスターオートスケーラーメトリクスが初期化され、利用可能になりました。(OCPBUGS-48732)

- 以前は、サブスクリプションが調整されるたびに、OLM catalog Operator はサブスクリプションのカタログソース Pod からカタログメタデータの完全なビューを要求していました。この要求により、カタログ Pod のパフォーマンスに問題が生じていました。このリリースでは、OLM

catalog Operator は、定期的に更新され、すべてのサブスクリプション調整で再利用されるローカルキャッシュを使用するようになったため、カタログ Pod のパフォーマンスの問題は発生しません。(OCPBUGS-48696)

- 以前は、**ClusterResourceOverride** CR で **forceSelinuxRelabel** フィールドを指定し、その CR を後で変更すると、Cluster Resource Override Operator は関連する **ConfigMap** リソースに更新を適用しませんでした。この **ConfigMap** リソースは、SELinux の再ラベル付け機能である **forceSelinuxRelabel** にとって重要です。このリリースでは、Cluster Resource Override Operator が **ClusterResourceOverride** CR の変更を **ConfigMap** リソースに適用し、追跡します。(OCPBUGS-48690)

- 以前は、OpenShift Container Platform クラスターから Pod を削除した後、crun コンテナーランタイムは Pod 内に存在する実行中のコンテナーを停止できませんでした。そのため、Pod は **terminating** 状態のままになりました。このリリースでは、修正により、Pod を削除した場合に、Pod を永続的に "terminating" 状態にすることなく、crun が実行中のコンテナーを停止するようになりました。(OCPBUGS-48564)

- 以前は、Cluster Version Operator (CVO) が、**ClusterVersion Failing** 状態メッセージに伝播される内部エラーをフィルタリングしていませんでした。その結果、更新に悪影響を与えないエラーが ClusterVersion Failing 状態メッセージに表示されていました。このリリースでは、**ClusterVersion Failing** 状態メッセージに伝播されるエラーがフィルタリングされます。(OCPBUGS-46408)

1.9.23.2. 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。

1.9.24. RHSA-2025:0650 - OpenShift Container Platform 4.16.32 のバグ修正とセキュリティー更新

発行日: 2025 年 1 月 29 日

OpenShift Container Platform リリース 4.16.32 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:0650 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:0652 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.32 --pullspecs
```

1.9.24.1. バグ修正

- 以前は、Operator Lifecycle Manager (OLM) がクラスター内の同じ namespace を同時に解決することがありました。これにより、2 つの同時プロセスがサブスクリプションと対話し、CSV ファイルの関連付けが解除されたため、サブスクリプションが **ConstraintsNotSatisfiable** の終了状態に達しました。今回のリリースにより、OLM は namespace を同時に解決しなくなったため、OLM は CSV ファイルを関連付けられていない状態のままにせず、サブスクリプションを正しく処理できるようになりました。(OCPBUGS-48661)

- 以前は、Google Cloud はゾーン API エラーメッセージを更新し、この更新により Google Cloud に関連する一時的なエラーメッセージが生成されたため、OpenShift Container Platform マシンコントローラーは誤ってマシンを有効とラベル付けしていました。この状況により、無効なマシンが障害発生状態に遷移できませんでした。このリリースでは、マシンコントローラーは、マシン設定に無効なゾーンや **projectID** が存在しないかチェックすることで、エラーを正しく処理するようになりました。その後、マシンコントローラーはマシンを正しく障害状態にします。(OCPBUGS-48484)

- 以前は、**RendezvousIP** がコンピュートノード設定の **next-hop-address** フィールド内のサブ文字列と一致すると、検証エラーが発生しました。**RendezvousIP** は、コントロールプレーンホストアドレスのみと一致する必要があります。このリリースでは、**RendezvousIP** の部分文字列比較がコントロールプレーンホストアドレスに対してのみ使用されるため、エラーが発生しなくなりました。(OCPBUGS-48442)

- 以前は、IBM Power® Virtual Server にインストールされたクラスターのゾーンで使用可能なすべてのマシンタイプを使用することができませんでした。この問題は、リージョン内のすべてのゾーンが同じマシンタイプのセットを持つと想定されていたために発生しました。このリリースでは、IBM Power® Virtual Server にインストールされたクラスターのゾーンで使用可能なマシンタイプをすべて使用できます。(OCPBUGS-47663)

- 以前は、リゾルバーを使用する **PipelineRuns** CR を OpenShift Container Platform Web コンソールで再実行できませんでした。CR を再実行しようとすると、**Invalid PipelineRun configuration, unable to start Pipeline.** が生成されていました。このリリースでは、この問題が発生することなく、リゾルバーを使用する **PipelineRuns** CR を再実行できるようになりました。(OCPBUGS-46602)

- 以前は、OpenShift Container Platform Web コンソールで **Form View** を使用して **Deployment** または **DeploymentConfig** API オブジェクトを編集すると、どちらかのオブジェクトの YAML 設定に重複した **ImagePullSecrets** パラメーターが追加されていました。このリリースにより、どちらのオブジェクトにも重複した **ImagePullSecrets** パラメーターが自動的に追加されないように修正されました。(OCPBUGS-45948)

- 以前は、インストールプログラムが Microsoft Azure 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によってテナント間オブジェクトが有効にされ、それらがレプリケートされていました。これらのレプリケートされたオブジェクトは、Payment Card Industry Data Security Standard (PCI DSS) および Federal Financial Supervisory Authority (BaFin) の規制に準拠していません。このリリースでは、インストールプログラムによってオブジェクトが無効になり、クラスターが前述のデータガバナンス規制に厳密に準拠するようになります。(OCPBUGS-45999)

- 以前は、Machine Config Operator (MCO) と出荷された Red Hat Enterprise Linux (RHEL) CoreOS テンプレートが原因で、Red Hat OpenStack Platform (RHOSP) でのノードのスケーリングが失敗していました。この問題は、**systemd** の問題と、古い OpenShift Container Platform バージョンのレガシーブートイメージの存在が原因で発生しました。このリリースでは、パッチによって **systemd** の問題が修正され、レガシーのブートイメージが削除されるため、ノードのスケーリングが期待どおりに継続されます。(OCPBUGS-43765)

- 以前は、OpenShift Container Platform Web コンソールで、ネットワークエラーまたは検証エラーのために VMware vSphere 設定ダイアログボックスが停止していました。このリリースでは、修正により、ダイアログの停止を引き起こすエラーは発生せず、ダイアログを閉じたり、設定の変更をキャンセルしたり、設定を編集したりできるようになりました。(OCPBUGS-29823)

- 以前は、OpenShift Container Platform Web コンソールの VMware vSphere 設定ダイアログボックスでは、vSphere プラグインの問題により、フィールドに入力された値はいずれも検証されませんでした。設定を保存した後、出力されたデータが論理的にフォーマットされません

でした。このリリースでは、vSphere プラグインは入力されたデータに対して検証チェックを実行するようになり、プラグインは論理的な形式でデータを出力するようになりました。(OCPBUGS-29616)

1.9.24.2. 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。

1.9.25. RHSA-2025:0140 - OpenShift Container Platform 4.16.30 bug fix and security update

発行日: 2025 年 1 月 15 日

OpenShift Container Platform release 4.16.30 is now available.The list of bug fixes that are included in the update is documented in the RHSA-2025:0140 advisory.更新に含まれる RPM パッケージは、RHBA-2025:0143 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.30 --pullspecs
```

1.9.25.1. バグ修正

- 以前は、Operator Lifecycle Manager (OLM) カタログレジストリー Pod が、**TerminationByKubelet** エラーで kubelet によって終了され、カタログ Operator はそれらの Pod を再作成しませんでした。このリリースでは、レジストリー Pod が再作成され、エラーは発生しません。(OCPBUGS-47738)

- 以前は、証明書署名要求 (CSR) 承認者は、過負荷状態になっていないか判断するために、他のシステムからの証明書を計算に含めていました。この状況が発生すると、CSR 承認者は証明書の承認を停止しました。このリリースでは、CSR 承認者は、**signerName** プロパティーをフィルターとして使用して、承認できる CSR のみを含めるようになりました。CSR 承認者は、多数の CSR がある場合、監視対象の **signerName** 値がある場合、および承認していない証明書の場合に限り、新しい承認を防止します。(OCPBUGS-47704)

- 以前は、論理プロセッサーのコア ID 番号 (ソケットあたりのコア) が異なり、同じノードプールに存在するコンピュートノードのパフォーマンスプロファイルを、Performance Profile Creator (PPC) が構築できませんでした。このリリースでは、論理プロセッサーのコア ID 番号が異なるコンピュートノードを持つクラスターのパフォーマンスプロファイルを、PPC が作成できます。そのため、PPC がパフォーマンスプロファイルの作成に失敗しません。PPC は、生成されたパフォーマンスプロファイルを注意して使用する必要があることを示す警告メッセージを出力します。コア ID 番号が異なると、システムの最適化や分離されたタスク管理に影響が生じる可能性があるためです。(OCPBUGS-47701)

- 以前は、インフォーマーウォッチストリームでイベントが見逃されていました。この切断が発生している間にオブジェクトが削除されると、インフォーマーは異なるタイプを返し、無効状態であることを報告し、オブジェクトは削除されました。このリリースでは、一時的な切断の可能性が正しく処理されるようになりました。(OCPBUGS-47645)

- 以前は、**SiteConfig** カスタムリソース (CR) を使用してクラスターまたはノードを削除すると、**BareMetalHost** CR が **Deprovisioning** 状態のままになりました。このリリースでは、

オーダーの削除が正しく行われ、**SiteConfig** CR によってクラスターまたはノードが正常に削除されます。この修正には、Red Hat OpenShift GitOps 1.13 以降のバージョンが必要です。(OCPBUGS-46524)

1.9.25.2. 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。

1.9.26. RHBA-2025:0018 - OpenShift Container Platform 4.16.29 のバグ修正とセキュリティー更新

発行日: 2025 年 1 月 9 日

OpenShift Container Platform リリース 4.16.29 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:0018 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:0021 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.29 --pullspecs
```

1.9.26.1. 機能拡張

1.9.26.1.1. Node Tuning Operator によるアーキテクチャー検出

Node Tuning Operator が、Intel および AMD CPU のカーネル引数と管理オプションを適切に選択できるようになりました。(OCPBUGS-46496)

1.9.26.2. バグ修正

- 以前は、デフォルトの **sriovOperatorConfig** カスタムリソース (CR) を削除すると、最初に **ValidatingWebhookConfiguration** が削除されないため、デフォルトの **sriovOperatorConfig** CR を再作成できませんでした。このリリースでは、**sriovOperatorConfig** CR を削除すると、Single Root I/O Virtualization (SR-IOV) Network Operator が検証 Webhook を削除するため、新しい **sriovOperatorConfig** CR を作成できます。(OCPBUGS-44727)

- 以前は、パフォーマンスプロファイル内の CPU セットに対して無効な文字列を入力すると、クラスターが壊れる可能性がありました。このリリースでは、修正により、入力できる文字列が有効なものだけになり、クラスターが破損するリスクが排除されました。(OCPBUGS-47678)

- 以前は、**MachineSet** オブジェクトの **publicIp** パラメーターが明示的に **false** に設定されていると、既存のサブネット上の特定の環境で AWS 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が特定の環境で AWS クラスターのマシンをプロビジョニングする際に、**publicIp** に設定された設定値が問題を引き起こさないよう修正されました。(OCPBUGS-46508)

- 以前は、ダッシュボードテーブルの行数を決定するために使用される ID が一意ではなく、行の ID が同じ場合に一部の行が結合されていました。このリリースでは、ID の重複を防ぐために、より多くの情報が ID に使用され、テーブルに予想される各行が表示されるようになりました。(OCPBUGS-45334)

1.9.26.3. 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。

1.9.27. RHBA-2024:11502 - OpenShift Container Platform 4.16.28 のバグ修正とセキュリティー更新

発行日: 2025 年 1 月 2 日

OpenShift Container Platform リリース 4.16.28 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2024:11502 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:11505 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.28 --pullspecs
```

1.9.27.1. 既知の問題

- **libreswan** の動作のリグレッションが原因となり、一部の IPsec 対応ノードが、同じクラスター内の他のノード上の Pod との通信を喪失します。この問題を解決するには、クラスターの IPsec を無効にします。(OCPBUGS-43715)

1.9.27.2. バグ修正

- 以前は、Webhook トークンオーセンティケーターが有効になっていて、認可タイプが **None** に設定されている場合、OpenShift Container Platform Web コンソールが常にクラッシュしていました。このリリースでは、バグ修正により、この設定によって OpenShift Container Platform Web コンソールがクラッシュすることがなくなりました。(OCPBUGS-46481)

- 以前は、Operator Lifecycle Manager (OLM) を使用して Operator をアップグレードしようとすると、アップグレードがブロックされ、**error validating existing CRs against new CRD's schema** というメッセージが生成されていました。OLM が既存のカスタムリソース (CR) を新しい Operator バージョンのカスタムリソース定義 (CRD) に照らして検証する際に、非互換性の問題が誤って特定されるという問題がありました。このリリースでは、検証が修正され、Operator のアップグレードがブロックされなくなりました。(OCPBUGS-46434)

- 以前は、パフォーマンスプロファイルに個々の CPU の長い文字列が含まれている場合、マシン設定が処理されませんでした。このリリースでは、カーネルコマンドラインで数字のシーケンスまたは数字の範囲を使用できるようにユーザー入力プロセスが更新されました。(OCPBUGS-46074)

- 以前は、末尾にピリオドがあるカスタムドメイン名で Amazon Web Services (AWS) DHCP オプションセットを設定し、EC2 インスタンスのホスト名を Kubelet ノード名に変換した場合、末尾のピリオドは削除されませんでした。末尾のピリオドは Kubernetes オブジェクト名には使用できません。このリリースでは、DHCP オプションセット内のドメイン名の末尾にピリオドを含めることが可能です。(OCPBUGS-45974)

- 以前は、kdump の送信先がローカルマシンにアクセスする必要のないリモートマシンである場合でも、ローカルの暗号化されたディスクを開くと、kdump **initramfs** が応答しなくなりました。このリリースでは、この問題が修正され、kdump **initramfs** が暗号化されたローカルディ

スクを正常に開くようになりました。(OCPBUGS-45837)

- 以前は、**aws-sdk-go-v2** ソフトウェア開発キット (SDK) が、Amazon Web Services (AWS) Security Token Service (STS) クラスターで **AssumeRoleWithWebIdentity** API 操作の認証に失敗していました。このリリースにより、**pod-identity-webhook** にデフォルトのリージョンが含まれるようになったため、この問題が発生しなくなりました。(OCPBUGS-45939)

- 以前は、AWS クラスターのセキュリティーグループに対して、**30000-32767** の範囲のノードポートへの **0.0.0.0/0** Classless Inter-Domain Routing (CIDR) アドレスアクセスを許可する Ingress ルールが作成されていました。このリリースでは、AWS クラスターのインストール中にこのルールが削除されます。(OCPBUGS-45669)

- 以前は、ビルドコントローラーは、イメージプル専用ではなく、一般的な使用のためにリンクされたシークレットを見つけようとしていました。このリリースでは、デフォルトのイメージプルシークレットを検索するときに、ビルドはサービスアカウントにリンクされている **ImagePullSecrets** を使用します。(OCPBUGS-31213)

- 以前は、1 つの machine config pool (MCP) が一時停止されている場合、SDN-OVN ライブマイグレーションの最大転送単位 (MTU) 移行フェーズが何度も実行される可能性がありました。これにより、ライブマイグレーションが正常に終了しませんでした。このリリース以降は発生しなくなるはずです。(OCPBUGS-44338)

- 以前は、OpenShift Container Platform 4.12 から 4.14 にアップグレードした後、**NetworkAttachmentDefinition** が設定されていると Pod がサービスに到達できないことが報告されていました。このリリースでは、Pod はアップグレード後にサービスにアクセスできるようになります。(OCPBUGS-44457)

1.9.27.3. 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。

1.9.28. RHBA-2024:10973 - OpenShift Container Platform 4.16.27 のバグ修正とセキュリティー更新

発行日: 2024 年 12 月 19 日

OpenShift Container Platform リリース 4.16.27 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2024:10973 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:10976 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.27 --pullspecs
```

1.9.28.1. バグ修正

- 以前は、OpenShift Container Platform のアップグレードプロセス中に **openshift-sdn** Pod がデプロイされると、Open vSwitch (OVS) ストレージテーブルがクリアされていました。この問題は、OpenShift Container Platform 4.16.19 以降のバージョンで発生しました。既存の Pod の

ポートを再作成する必要があり、これにより多数のサービスに中断が発生しました。このリリースでは、修正により、クラスターのアップグレード操作中に OVS テーブルはクリアされず、Pod も切断されません。(OCPBUGS-45806)

- 以前は、finally タスクを 1 つだけ含むパイプラインを作成した場合、**edit Pipeline** フォームから finally パイプラインタスクを削除できませんでした。このリリースでは、**edit Pipeline** フォームから finally タスクを削除できるようになり、問題が解決されました。(OCPBUGS-45229)

- 以前は、インストールプログラムは Red Hat Enterprise Linux CoreOS (RHCOS) 上のカスタム IPv6 ネットワークの最大転送単位 (MTU) を検証しませんでした。MTU に低い値を指定した場合、クラスターのインストールは失敗します。このリリースでは、IPv6 ネットワークの最小 MTU 値は **1380** オクテットに設定されています。この場合の **1280** オクテットは IPv6 プロトコルの最小 MTU であり、残りの **100** オクテットは OVN-Kubernetes カプセル化のオーバーヘッド用です。このリリースでは、インストールプログラムが Red Hat Enterprise Linux CoreOS (RHCOS) 上のカスタム IPv6 ネットワークの MTU を検証するようになりました。(OCPBUGS-41813)

- 以前は、**Display Admission Webhook** 警告の実装で、誤ったコードが一部表示される問題がありました。この更新により、不要な警告メッセージが削除されました。(OCPBUGS-43750)

- 以前は、OpenShift Container Platform バージョン 4.16.25、4.16.26、または 4.16 以降の z-stream バージョンでは、クラスターに NUMA Resources Operator をデプロイできませんでした。このリリースでは、OpenShift Container Platform4.16 の OpenShift Container Platform 4.16.27 以降のバージョンで NUMA Resources Operator のデプロイメントがサポートされるようになりました。この問題は 4.16.25 および 4.16.26 では未解決のままです。(OCPBUGS-45983)

1.9.28.2. 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。

1.9.29. RHSA-2024:10823 - OpenShift Container Platform 4.16.26 のバグ修正とセキュリティー更新

発行日: 2024 年 12 月 12 日

OpenShift Container Platform リリース 4.16.26 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2024:10823 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:10826 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.26 --pullspecs
```

1.9.29.1. 機能拡張

- 以前は、ClusterTasks は **Pipelines builder** ページと、**Tasks** ナビゲーションメニューの **ClusterTask list** ページにリストされていました。現在、ClusterTasks は Pipelines 1.17 から非推奨となっており、ClusterTask の依存関係は静的プラグインから削除されていま

す。**Pipelines builder** ページには、namespace に存在するタスクとコミュニティータスクのみが表示されます。(OCPBUGS-45015)

1.9.29.2. バグ修正

- 以前は、日付が正しくないノードに Agent-based Installer 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は失敗しました。このリリースでは、Agent-based Installer のライブ ISO 時刻同期にパッチが適用されます。このパッチは、追加 Network Time Protocol (NTP) サーバーのリストを使用して **/etc/chrony.conf** ファイルを設定するため、これらの追加 NTP サーバーのいずれかを **agent-config.yaml** に設定しても、クラスターのインストール問題は発生しません。(OOCPBUGS-45181)

- 以前は、カスタムテンプレートを使用した場合、秘密鍵などの複数行のパラメーターを入力できませんでした。このリリースでは、単一行モードと複数行モードを切り替えることができ、テンプレートフィールドに複数行を入力できます。(OOCPBUGS-45124)

- OpenShift Container Platform 4.15 までは、**Getting started with resources** セクションを閉じるオプションがありました。OpenShift Container Platform 4.15 以降、**Getting started with resources** セクションが展開可能なセクションに変換され、セクションを閉じる方法がありませんでした。このリリースでは、**Getting started with resources** セクションを閉じることができます。(OOCPBUGS-45181)

- 以前の Red Hat OpenShift Container Platform では、**Edit BuildConfig** ページで **start lastrun** オプションを選択すると、エラーが発生して **lastrun** 操作を実行できませんでした。このリリースでは、修正により **start lastrun** オプションが正常に完了するようになりました。(OOCPBUGS-44875)

1.9.29.3. 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。

1.9.30. RHSA-2024:10528 - OpenShift Container Platform 4.16.25 のバグ修正とセキュリティー更新

発行日: 2024 年 12 月 4 日

OpenShift Container Platform リリース 4.16.25 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2024:10528 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:10531 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.25 --pullspecs
```

1.9.30.1. バグ修正

- 以前は、Web コンソールの **Notifications** セクションで、サイレントにしたアラートが通知ドロワーに表示されていました。これはアラートに外部ラベルが含まれていなかったためです。このリリースでは、アラートに外部ラベルが含まれるようになり、サイレントにしたアラートが通知ドロワーに表示されなくなりました。(OCPBUGS-44885)

- 以前は、インストールプログラムは **cloudControllerManager** フィールドを正しく解析できず、空の文字列として Assisted Service API に渡していました。このエラーにより、Assisted Service が失敗し、Oracle® Cloud Infrastructure (OCI) でのクラスターの正常なインストールがブロックされていました。このリリースでは解析ロジックが更新され、**install-config.yaml** ファイルの **cloudControllerManager** フィールドが正しく解釈されるようになり、期待される値が Assisted Service API に適切に送信されるようになりました。(OCPBUGS-44348)

- 以前は、**Display Admission Webhook** 警告の実装により、無効なコードの問題が発生していました。このリリースでは、不要な警告メッセージが削除され、無効なコードの問題は発生しません。(OCPBUGS-44207)

- 以前は、サーバーレスインポートストラテジーを使用して Git リポジトリーをインポートすると、**func.yaml** からの環境変数がフォームに自動的にロードされませんでした。このリリースでは、Git リポジトリーのインポートプロセス中に環境変数が読み込まれます。(OCPBUGS-43447)

1.9.30.2. 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。

1.9.31. RHSA-2024:10147 - OpenShift Container Platform 4.16.24 のバグ修正とセキュリティー更新

発行日: 2024 年 11 月 26 日

OpenShift Container Platform リリース 4.16.24 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2024:10147 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:10150 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.24 --pullspecs
```

1.9.31.1. バグ修正

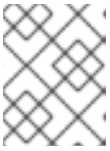
- 以前は、Operator Lifecycle Manager (OLM) がサービスアカウントに関連付けられたシークレットにアクセスできない場合、OLM は Kubernetes API サーバーに依存してベアラートークンを自動的に作成していました。Kubernetes バージョン 1.22 以降では、このアクションは自動で実行されません。そのため、このリリースの OLM は、**TokenRequest** API を使用して新しい Kubernetes API トークンを要求します。(OCPBUGS-44351)

- 以前は、証明書署名要求 (CSR) の承認メカニズムは、CSR のノード名と内部 DNS エントリーが大文字と小文字の不一致により失敗していました。このリリースでは、CSR の承認メカニズムが更新され、大文字と小文字を区別するチェックがスキップされるようになりました。これにより、ノード名と内部 DNS エントリーが一致する CSR が、大文字と小文字の不一致によりチェックに失敗することがなくなりました。(OCPBUGS-44629)

- 以前は、HyperShift ベースの ROKS クラスターは、**oc login** コマンドを使用して認証できませんでした。**Display Token** を選択した後にトークンを取得しようとすると、Web ブラウザーにエラーが表示されました。このリリースでは、**cloud.ibm.com** とその他のクラウドベースのエ

ンドポイントはプロキシーされなくなり、認証が成功します。(OCPBUGS-44277)

- OpenShift Container Platform 4.16 は Operator SDK 1.36.1 をサポートします。この最新バージョンのインストール、または最新バージョンへの更新は、Operator SDK CLI のインストール を参照してください。

  注記

  Operator SDK 1.36.1 は Kubernetes 1.29 をサポートし、Red Hat Enterprise Linux (RHEL) 9 ベースイメージを使用します。

  Operator SDK 1.31.0 で以前に作成または保守された Operator プロジェクトがある場合は、Operator SDK 1.36.1 との互換性を維持するためにプロジェクトを更新します。

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

  (OCPBUGS-44485, OCPBUGS-44486)

1.9.31.2. 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。

1.9.32. RHSA-2024:9615 - OpenShift Container Platform 4.16.23 のバグ修正とセキュリティー更新

発行日: 2024 年 11 月 20 日

OpenShift Container Platform リリース 4.16.23 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:9615 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-2024:9618 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.23 --pullspecs
```

1.9.32.1. バグ修正

- 以前は、Cluster Resource Override Operator がオペランドコントローラーの実行に失敗すると、Operator はコントローラーの再実行を試行していました。再実行操作ごとに新しいシークレットセットが生成され、これにより、最終的にクラスターの namespace リソースが制限され

ました。このリリースでは、クラスターのサービスアカウントに、クラスターにすでにシークレットが存在する場合に Operator が追加のシークレットを作成できないようにするアノテーションが含まれるようになりました。(OCPBUGS-44351)

- 以前は、VMware vSphere vCenter クラスターに標準ポートグループが定義されていない ESXi ホストが含まれていて、インストールプログラムがそのホストを選択して OVA をインポートしようとすると、インポートが失敗し、**Invalid Configuration for device 0** エラーが報告されていました。このリリースでは問題が解決され、インストールプログラムは ESXi ホストの標準ポートグループが定義されているかどうかを確認し、定義されていない場合は、定義済み標準ポートグループを持つ ESXi ホストが見つかるまで続行するか、見つからない場合はエラーメッセージを報告します。(OCPBUGS-38930)

- 以前は、IBM Cloud® 上のクラスターを既存の VPC にインストールすると、インストールプログラムがサポート対象外の VPC リージョンを取得していました。アルファベット順でサポート対象外の VPC リージョンに続くサポート対象の VPC リージョンにインストールしようとすると、インストールプログラムがクラッシュしました。このリリースでは、インストールプログラムが更新され、完全に使用可能ではない VPC リージョンをリソース検索時に無視するようになりました。(OCPBUGS-36290)

- 以前は、制限付きライブマイグレーションメソッドを使用し、クラスター内の namespace にホストネットワークとの通信を許可するネットワークポリシーが含まれていた場合、クラスター内のノードで通信の問題が発生していました。具体的には、異なる Container Network Interface によって管理されるノード上のホストネットワーク Pod は、namespace 内の Pod と通信できませんでした。このリリースでは、修正により、通信の問題が発生することなく、ホストネットワークとの通信を許可するネットワークポリシーを含む namespace でライブマイグレーションを使用できるようになりました。(OCPBUGS-43344)

1.9.32.2. 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。

1.9.33. RHBA-2024:8986 - OpenShift Container Platform 4.16.21 のバグ修正

発行日: 2024 年 11 月 13 日

OpenShift Container Platform リリース 4.16.21 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:8986 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:8989 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.21 --pullspecs
```

1.9.33.1. バグ修正

- 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-44179)

- 以前は、Open vSwitch にアタッチされたインターフェイスで IPSec を使用して ESP ハードウェアオフロードを有効にすると、Open vSwitch のバグにより接続が切断されていました。このリリースでは、OpenShift は Open vSwitch にアタッチされたインターフェイス上の ESP ハードウェアオフロードを自動的に無効にするため、問題は解決されました。(OCPBUGS-44043)

- 以前は、同期作業を初期化しているときに CVO Pod を再起動すると、ブロックされたアップグレード要求のガードが解除されていました。その結果、ブロックされたリクエストが誤って受け入れられました。このリリースでは、CVO は初期化ステップで調整を延期し、問題が解決されました。(OCPBUGS-43964)

- 以前は、**rpm-ostree-fix-shadow-mode.service** が実行されていたライブ環境で RHCOS を実行すると、**rpm-ostree-fix-shadow-mode.service** によって、デプロイメントやライブシステムに影響を与えない障害がログに記録されていました。このリリースでは、インストールされた環境から RHCOS が実行されていない場合、**rpm-ostree-fix-shadow-mode.service** は実行されず、問題が解決されました。(OCPBUGS-36806)

- 以前は、IBM Cloud® 上のクラスターを既存の VPC にインストールすると、インストールプログラムによってサポートされていない VPC リージョンが取得されていました。アルファベット順でサポート対象外の VPC リージョンに続くサポート対象の VPC リージョンにインストールしようとすると、インストールプログラムがクラッシュしました。このリリースでは、インストールプログラムが更新され、完全に使用可能ではない VPC リージョンをリソース検索時に無視するようになりました。(OCPBUGS-36290)

1.9.33.2. 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。

1.9.34. RHSA-2024:8683 - OpenShift Container Platform 4.16.20 のバグ修正とセキュリティー更新

発行日: 2024 年 11 月 6 日

OpenShift Container Platform リリース 4.16.20 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:8683 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2024:8686 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.20 --pullspecs
```

1.9.34.1. バグ修正

- 以前は、無効または到達不能なアイデンティティープロバイダー (IDP) によって Hosted Control Plane への更新がブロックされていました。このリリースでは、**HostedCluster** オブジェクトの **ValidIDPConfiguration** 条件により IDP エラーが報告されるようになりました。そのため、Hosted Control Plane の更新がエラーによりブロックされなくなりました。(OCPBUGS-43840)

- 以前は、Machine Config Operator (MCO) の vSphere **resolve-prepender** スクリプトが、OpenShift Container Platform 4 で使用されていた古いブートイメージバージョンと互換性のない **systemd** ディレクティブを使用していました。このリリースでは、ノードは新しいブートイメージバージョン 4.16 4.13 以降で、手動による介入を行うか、この修正を含むリリースに更新することでスケーリングできます。(OCPBUGS-42109)

1.9.34.2. 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。

1.9.35. RHSA-2024:8415 - OpenShift Container Platform 4.16.19 のバグ修正とセキュリティー更新

発行日: 2024 年 10 月 30 日

OpenShift Container Platform リリース 4.16.19 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:8415 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2024:8418 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.19 --pullspecs
```

1.9.35.1. バグ修正

- 以前は、Microsoft Azure で Image Registry Operator が **NetworkAccess: Internal** で設定されていた場合、Operator 設定で **managementState** を **Removed** に正常に設定できませんでした。これは、Operator がストレージコンテナーを削除しようとしたときの認証エラーが原因でした。このリリースでは、Operator がストレージアカウントの削除を引き続き実行し、それによりストレージコンテナーも自動的に削除されます。これにより、**Removed** 状態に正常に変更されます。(OCPBUGS-43555)

- 以前は、マネージドサービスでは、監査ログがローカルの Webhook サービスに送信されていました。コントロールプレーンのデプロイメントは、**konnectivity** 経由でトラフィックを送信し、**konnectivity** プロキシー (**openshift-apiserver** および **oauth-openshift**) 経由で監査 Webhook トラフィックを送信しようと試みていました。このリリースにより、**audit-webhook** は影響を受ける Pod の **no_proxy hosts** のリストに表示され、**audit-webhook** に送信される監査ログトラフィックが正常に送信されるようになりました。(OCPBUGS-43046)

- 以前は、Agent-based Installer を使用してクラスターをインストールすると、**assisted-installer-controller** は、ランデブーホストで **assisted-service** が使用不可かどうかにより、インストールプロセスがタイムアウトになっていました。このイベントにより、CSR 承認チェック中にクラスターのインストールが失敗していました。このリリースでは、**assisted-installer-**

controller が更新され、**assisted-service** が利用できない場合でも、コントローラーがタイムアウトしないようになりました。現在は、CSR 承認チェックは期待どおりに動作します。(OCPBUGS-42710)

- 以前は、IBM® Cloud Controller Manager (CCM) が、OpenShift Container Platform 4.16 のバインドアドレスとしてループバックを使用するように再設定されました。liveness プローブはループバックを使用するように設定されていなかったため、CCM は liveness プローブに常に失敗し、継続的に再起動しました。このリリースでは、IBM® CCM liveness プローブは、要求ホストのループバックを使用するように設定されています。(OCPBUGS-42125)

- 以前は、IBM Cloud の Messaging Application Programming Interface (MAPI) は、サブネットの詳細を名前で検索するときに、サブネットの最初のグループ (50) のみをチェックしていました。このリリースでは、検索ですべてのサブネットを検索するためのページネーションサポートが提供されます。(OCPBUGS-36698)

1.9.35.2. 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。

1.9.36. RHSA-2024:8260 - OpenShift Container Platform 4.16.18 のバグ修正とセキュリティー更新

発行日: 2024 年 10 月 24 日

OpenShift Container Platform リリース 4.16.18 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:8260 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2024:8263 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.18 --pullspecs
```

1.9.36.1. 機能拡張

- SR-IOV Network Operator は、Intel NetSec アクセラレーターカードと Marvell Octeon 10 DPU をサポートします。(OCPBUGS-43452)

1.9.36.2. バグ修正

- 以前は、Single-Root I/O Virtualization (SR-IOV) Operator は、Operator のシャットダウン操作中に取得したリースを期限切れにしませんでした。新規インスタンスはリースの有効期限が切れなければ動作可能にならないため、これは Operator の新規インスタンスに影響を与えました。このリリースでは、Operator シャットダウンロジックが更新され、Operator がシャットダウンするときに Operator のリースが期限切れになるようになりました。(OCPBUGS-37669)

- 以前は、新しい Pod 内に作成されたインターフェイスは非アクティブのままになり、Gratuitous Address Resolution Protocol (GARP) 通知が生成されていました。通知がクラスターに届かず、そのためにクラスター内の他の Pod の ARP テーブルが新しい Pod の MAC アドレスを更新できませんでした。この状況が原因で、ARP テーブルエントリーの有効期限が切

れるまでクラストラフィックが停止しました。このリリースでは、GARP 通知がクラスターに届くように、Pod 内のインターフェイスがアクティブになった後に GARP 通知が送信されるようになりました。その結果、周囲の Pod は以前の動作時よりも早く新しい Pod を識別できるようになります。(OCPBUGS-36735)

- 以前は、マシンコントローラーはインスタンステンプレートのクローン操作の VMware vSphere タスク ID を保存できませんでした。そのため、マシンは **Provisioning** 状態になり、電源がオフになりました。このリリースでは、VMware vSphere マシンコントローラーがこの状態を検出し、回復できるようになりました。(OCPBUGS-43433)

- 以前は、**oc import-image** コマンドを使用して Hosted Control Plane クラスターにイメージをインポートしようとすると、プライベートイメージレジストリーへのアクセスの問題によりコマンドが失敗していました。このリリースでは、Hosted Control Plane クラスター内の **openshift-apiserver** Pod が更新されてデータプレーンを使用する名前が解決され、**oc import-image** コマンドがプライベートイメージレジストリーで期待どおりに動作するようになりました。(OCPBUGS-43308)

- 以前は、**must-gather** ツールを使用すると、Multus Container Network Interface (CNI) ログファイル (**multus.log**) がノードのファイルシステムに保存されていました。この状況が原因で、ツールはノード内に不要なデバッグ Pod を生成しました。このリリースでは、Multus CNI は **multus.log** ファイルを作成しなくなり、代わりに CNI プラグインパターンを使用して、**openshift-multus** namespace 内の Multus DaemonSet Pod のログを検査するようになりました。(OCPBUGS-33959)

- 以前は、クラスターのリソースグループ以外のリソースグループに配置された Microsoft Azure ストレージアカウントを使用するようにイメージレジストリーを設定すると、Image Registry Operator のパフォーマンスが低下していました。これは検証エラーが原因で発生していました。このリリースでは Operator が更新され、ストレージアカウントキーを使用した認証のみ許可されます。その他の認証要件の検証は必要ありません。(OCPBUGS-42933)

- 以前は、ルート証明書のローテーション中に、データプレーンの **metrics-server** Pod が正しく起動しませんでした。これは証明書の問題が原因で発生しました。このリリースでは、**hostedClusterConfigOperator** リソースが正しい証明書をデータプレーンに送信するため、**metrics-server** Pod が期待どおりに起動します。(OCPBUGS-42432)

1.9.36.3. 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。

1.9.37. RHSA-2024:7944 - OpenShift Container Platform 4.16.17 のバグ修正とセキュリティー更新

発行日: 2024 年 10 月 16 日

OpenShift Container Platform リリース 4.16.17 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:7944 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:7947 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.17 --pullspecs
```

1.9.37.1. バグ修正

- 以前は、ルート証明書のローテーションが原因で、Ingress および DNS Operator が正しく起動できませんでした。このリリースでは、PKI に管理が必要になるタイミングを定義するアノテーションを使用して、Ingress および DNS Operator kubeconfigs が条件付きで管理されるようになり、問題は解決されました。(OCPBUGS-42431)

- 以前は、Hosted Control Plane (HCP) を使用した Red Hat OpenShift Service on AWS (ROSA) では、ミラーリングリリースイメージを使用するクラスターにより、既存のノードプールが **NodePool** バージョンではなく、ホストされているクラスターのオペレーティングシステムのバージョンを使用することがありました。このリリースではそれが修正され、ノードプールは独自のバージョンを使用します。(OCPBUGS-42342)

- 以前は、コーディングの問題により、RHCOS user-provisioned installation 上の Ansible スクリプトが失敗していました。これは、3 ノードクラスターで IPv6 が有効になっている場合に発生しました。このリリースでは、RHCOS 上で IPv6 が有効になっている 3 ノードクラスターをインストールするためのサポートが存在します。(OCPBUGS-41334)

- 以前は、**active-backup** モードで設定されたボンディングでは、基礎となるリンクが IPsec Encapsulating Security Payload (ESP) オフロードをサポートしていなくても、ESP オフロードがアクティブになっていました。これにより、IPsec アソシエーションが失敗しました。このリリースでは、IPsec アソシエーションが通過できるように、ボンディングの ESP オフロードが無効になっています。(OCPBUGS-41256)

- 以前は、ブロックデバイスのシリアル番号に特殊文字または無効な文字が存在する場合、Ironic 検査は失敗していました。これは、**lsblk** コマンドが文字をエスケープできなかったために発生しました。このリリースでは、コマンドが文字をエスケープするようになり、この問題は発生しなくなりました。(OCPBUGS-39017)

- 以前は、設定の問題により、**manila-csi-driver** およびノード registrar Pod のヘルスチェックが欠落していました。このリリースでは、各リソースにヘルスチェックが追加されました。(OCPBUGS-38458)

1.9.37.2. 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。

1.9.38. RHSA-2024:7599 - OpenShift Container Platform 4.16.16 のバグ修正とセキュリティー更新

発行日: 2024 年 10 月 9 日

OpenShift Container Platform リリース 4.16.16 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:7599 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:7602 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.16 --pullspecs
```

1.9.38.1. バグ修正

- 以前は、**openshift-machine-api** namespace の **metal3-ironic-inspector** コンテナーによって、クラスターのメモリー消費の問題が発生していました。このリリースでは、メモリー消費の問題が修正されました。(OCPBUGS-42113)

- 以前は、クラスターの Pod を作成するための cron ジョブを作成すると、Pod を取得するコンポーネントが失敗していました。この問題により、OpenShift Container Platform Web コンソールの **Topology** ページが失敗しました。このリリースでは、cron ジョブから生成された Pod を取得するコンポーネントに **3** 秒の遅延が設定されているため、この問題は発生しなくなりました。(OCPBUGS-42015)

- 以前は、内部バグのため、マシンに 256 個を超える CPU がある場合、Node Tuning Operator は割り込みおよびネットワーク処理 CPU アフィニティーの CPU マスクを誤って計算していました。これにより、これらのマシン上で CPU の適切な分離が妨げられ、**systemd** ユニット障害が発生しました。このリリースでは、Node Tuning Operator はマスクを正しく計算します。(OCPBUGS-39377)

- 以前は、Redfish Virtual Media を使用して xFusion ベアメタルノードをクラスターに追加すると、ノードの登録問題によりノードは追加されませんでした。この問題は、ハードウェアが Redfish に 100% 準拠していなかったために発生しました。このリリースにより、xFusion ベアメタルノードをクラスターに追加できるようになりました。(OCPBUGS-38797)

- 以前は、IPv6Classless Inter-Domain Routing (CIDR) アドレスを **no_proxy** 変数に追加すると、Ironic API はそのアドレスを無視していました。このリリースでは、Ironic API は **no_proxy** 変数に追加されたすべての IPv6 CIDR ア考慮するようになりました。(OCPBUGS-37654)

- 以前は、PatternFly 4 を使用する動的プラグインは、OpenShift Container Platform 4.15 以降では利用できない変数を参照していました。これは、ACM のダークモードでコントラストの問題を引き起こしていました。この更新により、動的プラグインで使用される PatternFly 4 のチャートをサポートするために、古いチャートスタイルが利用できるようになりました。(OCPBUGS-36816)

1.9.38.2. 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。

1.9.39. RHSA-2024:7174 - OpenShift Container Platform 4.16.15 のバグ修正とセキュリティー更新

発行日: 2024 年 10 月 2 日

OpenShift Container Platform リリース 4.16.15 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:7174 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:7177 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.15 --pullspecs
```

1.9.39.1. バグ修正

- 以前は、kube-proxy へのローカルパッチにより、OpenShift SDN は再同期するたびに特定のルールの重複コピーを iptables ルールセットに追加していました。これにより、同期が遅くなり、最終的に **NodeProxyApplySlow** アラートがトリガーされていました。このリリースでは、kube-proxy パッチが修正され、アラートは表示されなくなりました。(OCPBUGS-42159)

- 以前は、Node Tuning Operator (NTO) が PerformanceProfiles を使用して設定されると、ocp-tuned-one-shot systemd サービスが作成されていました。systemd サービスは kubelet の前に実行され、実行がブロックされていました。systemd サービスは、NTO イメージを使用する Podman を呼び出しました。しかし、NTO イメージが存在しない場合でも、Podman は引き続きイメージを取得しようとして失敗していました。このリリースでは、**/etc/mco/proxy.env** で定義されたクラスター全体のプロキシー環境変数のサポートが追加されました。Podman は、クラスター外接続にプロキシーを使用する必要がある環境で NTO イメージをプルするようになりました。(OCPBUGS-42061)

- 以前は、PatternFly v4 および v5 の TextInput パラメーターの順序が変更されたため、**until** フィールドが不適切に入力され、編集できなくなっていました。このリリースでは、**until** フィールドが編集可能になり、正しい情報を入力できるようになりました。(OCPBUGS-41996)

- 以前は、各障害ドメインにテンプレートが定義されている場合、インストールプログラムでは vSphere で OVA をダウンロードするために外部接続が必要でした。このリリースにより、この問題は解決されました。(OCPBUGS-41885)

- 以前は、Installer Provisioned Infrastructure を使用してベアメタル上にクラスターをインストールする場合、ブートストラップ仮想マシンへのネットワークが遅いとインストールがタイムアウトする可能性がありました。この更新により、タイムアウト期間が延長され、より広範なネットワークパフォーマンスの状況をカバーできるようになりました。(OCPBUGS-41845)

- 以前は、ホストされたクラスタープロキシーが設定され、http または https エンドポイントを持つアイデンティティープロバイダー (IDP) が使用されていた場合、プロキシー経由で送信される前に IDP のホスト名が解決されませんでした。その結果、データプレーンでのみ解決できるホスト名は IDP では解決できませんでした。この更新により、IPD トラフィックを **konnectivity** トンネル経由で送信する前に DNS ルックアップが実行されます。そのため、データプレーンでのみ解決できるホスト名を持つ IDP は、Control Plane Operator によって検証できるようになります。(OCPBUGS-41372)

- 以前は、内部バグのため、マシンに 256 個を超える CPU がある場合、Node Tuning Operator (NTO) は割り込みおよびネットワーク処理 CPU アフィニティーの CPU マスクを誤って計算していました。これにより、これらのマシン上で CPU の適切な分離が妨げられ、**systemd** ユニット障害が発生しました。このリリースでは、NTO がマスクを正しく計算します。(OCPBUGS-39377)

- 以前は、ユーザーが既存のサブネットを使用してプライベートクラスターを作成する際にパブリックサブネットを指定すると、インストールプログラムが、パブリックサブネット内に作成されたロードバランサーをパブリックインターネットに公開することがありました。これにより、プライベートクラスターの意味がなくなっていました。このリリースでは、プライベートインストール中に、パブリックサブネットを指定するとプライベートクラスターが破損する可能性があるという警告を表示することで問題が解決されました。警告を非表示にするには、ユーザーは入力を修正する必要があります。(OCPBUGS-38964)

1.9.39.2. 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。

1.9.40. RHSA-2024:6824 - OpenShift Container Platform 4.16.14 のバグ修正とセキュリティー更新

発行日: 2024 年 9 月 24 日

OpenShift Container Platform リリース 4.16.14 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:6824 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-2024:6827 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.14 --pullspecs
```

1.9.40.1. 機能拡張

以下の機能拡張は、この z-stream リリースに含まれています。

1.9.40.1.1. Insight Operator を使用した Red Hat OpenStack Platform (RHOSP) on OpenStack Services クラスターリソースからのデータ収集

- Insight Operator により、Red Hat OpenStack Services on OpenShift (RHOSO) クラスターリソース (**OpenStackControlPlane**、**OpenStackDataPlaneNodeSet**、**OpenStackDataPlaneDeployment**、および **OpenStackVersions**) からデータを収集できます。(OCPBUGS-38021)

1.9.40.2. バグ修正

- 以前は、Operator Lifecycle Manager (OLM) がアップグレードの可能性を評価するときに、クラスター内の全カスタムリソース (CR) インスタンスの動的クライアントリストを使用していました。多数の CR を持つクラスターの場合、API サーバーがタイムアウトし、アップグレードが停止することがありました。このリリースにより、この問題は解決されました。(OCPBUGS-41677)

- 以前は、Hosted Cluster (HC) の **controllerAvailabilityPolicy** 値が **SingleReplica** の場合、**podAntiAffinity** を持つネットワークコンポーネントによってロールアウトがブロックされていました。このリリースにより、この問題は解決されました。(OCPBUGS-41555)

- 以前は、複数の CIDR ブロックを持つ Amazon Virtual Private Cloud (VPC) にクラスターをデプロイすると、インストールプログラムが失敗していました。このリリースでは、ネットワーク設定が更新され、複数の CIDR ブロックを持つ VPC がサポートされるようになりました。(OCPBUGS-39496)

- 以前は、Ansible Playbook の順序が変更され、**metadata.json** ファイルの作成前に実行されていたため、古いバージョンの Ansible で問題が発生していました。このリリースでは、ファイルの欠落に対する Playbook の耐性が向上し、問題が解決されました。(OCPBUGS-39287)

- 以前は、同一のスクレイピング中に、Prometheus が同じ系列のサンプルを削除し、タイムスタンプが異なっていてもそのうちの 1 つだけを考慮していました。この問題が継続的に発生すると、**PrometheusDuplicateTimestamps** アラートがトリガーされていました。このリリースでは、他の条件を満たしていれば、すべてのサンプルが取り込まれるようになりました。(OCPBUGS-39179)

- 以前は、フォルダーが未定義で、データセンターがデータセンターフォルダーに配置されていた場合、vCenter Server のルートを起点とする不正なフォルダー構造が作成されていました。Govmomi **DatacenterFolders.VmFolder** を使用すると、誤ったパスが使用されていました。このリリースでは、フォルダー構造がデータセンターのインベントリーパスを使用し、それを仮想マシン (VM) およびクラスター ID 値と結合するようになり、問題が解決されました。(OCPBUGS-39082)

- 以前は、**eu-es** (スペイン、マドリード) リージョンで、**e980** システムタイプとして設定された IBM Power Virtual Server プラットフォームに OpenShift Container Platform クラスターを、インストールプログラムによってインストールできませんでした。このリリースでは、この環境でクラスターをインストールする際にインストールプログラムが失敗しなくなりました。(OCPBUGS-38502)

- 以前は、IDP 通信のプロキシーが Konnectivity エージェントで行われていました。トラフィックが Konnectivity に到達するまでに、そのプロトコルとホスト名が利用できなくなっていました。その結果、OAUTH サーバー Pod のプロキシーが正しく実行されていませんでした。プロキシーを必要とするプロトコル (HTTP/S) とプロキシーを必要としないプロトコル (LDAP) が区別されていませんでした。さらに、**HostedCluster.spec.configuration.proxy** 仕様で設定されている **no_proxy** 変数が考慮されませんでした。
  このリリースでは、OAUTH サーバーの Konnectivity サイドカーでプロキシーを設定することにより、**no_proxy** 設定を考慮しながら、トラフィックを適切にルーティングできるようになりました。その結果、ホストされたクラスターにプロキシーが設定されている場合、OAUTH サーバーがアイデンティティープロバイダーと適切に通信できるようになりました。(OCPBUGS-38058)

- 以前は、クラスターがコンピュートノードからコントロールプレーンに到達できるようにするために、プロキシーを使用してホストされたクラスターを作成した場合、クラスターでコンピュートノードを使用できませんでした。このリリースでは、ノードのプロキシー設定が更新され、ノードがプロキシーを使用してコントロールプレーンと正常に通信できるようになりました。(OCPBUGS-37937)

- 以前に導入された UPI 方式のインストールでの IPv6 サポートにより、OpenStack リソースの命名に関する問題が発生していました。この問題は、同じ OpenStack クラウド上に 2 つの UPI インストールを作成すると発生していました。その結果、ネットワーク、サブネット、ルーターの名前が同じになり、一方のセットアップが妨害され、もう一方のデプロイメントも妨げられていました。現在は、上記リソースの名前が、すべて OpenShift デプロイメントごとに一意になります。(OCPBUGS-36855)

- 以前は、一部の安全な **sysctls** が誤って許可リストから除外されていました。このリリースでは、**sysctls** が許可リストに再度追加され、問題が解決されました。(OCPBUGS-29403)

- 以前は、OpenShift Container Platform クラスターをバージョン 4.14 から 4.15 にアップグレードすると、UI の設定フォームに vCenter クラスターフィールドが入力されませんでした。インフラストラクチャークラスターリソースに、アップグレードされたクラスターの情報がありませんでした。このリリースでは、UI が vCenter クラスターの値に **cloud-provider-config** config map を使用するようになり、問題が解決されました。(OCPBUGS-41619)

1.9.40.3. 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。

1.9.41. RHSA-2024:6687 - OpenShift Container Platform 4.16.13 バグ修正の更新

発行日: 2024 年 9 月 19 日

OpenShift Container Platform リリース 4.16.13 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:6687 アドバイザリーに記載されています。この更新用の RPM パッケージはありません。

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

以下のコマンドを実行して、この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 4.16.13 --pullspecs
```

1.9.41.1. 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。

1.9.42. RHSA-2024:6632 - OpenShift Container Platform 4.16.12 のバグ修正とセキュリティー更新

発行日: 2024 年 9 月 17 日

OpenShift Container Platform リリース 4.16.12 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:6632 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:6635 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.12 --pullspecs
```

1.9.42.1. 機能拡張

この z-stream リリースには、次の機能拡張が含まれています。

1.9.42.1.1. Redfish API の TransferProtocolTypes として HTTPS をサポート

- インストーラーによってディスク上に作成された Provisioning CR ファイルに 'disableVirtualMediaTLS: false' を追加することにより、インストールプロセスのブートストラップフェーズで、Ironic とベースボード管理コントローラー (BMC) 間の通信に対して TLS を有効にできます。(OCPBUGS-39468)

1.9.42.1.2. Kubernetes バージョン 1.29.8 への更新

- このリリースには、Kubernetes バージョン 1.29.8 への更新に伴う変更点が含まれています。(OCPBUGS-39015)

1.9.42.1.3. Web コンソールでのソースコード編集時のリダイレクト

- Web コンソールの **Git Advanced** セクションには 2 つのオプションがあります。1 つはブランチ、タグ、またはコミット ID を追加するオプションで、もう 1 つはコンテキストディレクトリーを追加するオプションです。このリリースでは、特定のブランチ、タグ、またはコミット

ID のコンテキストディレクトリーを追加すると、**ソースコードの編集** アイコンを選択したときに、そのディレクトリーにリダイレクトされます。ブランチ、タグ、またはコミット ID が入力されていない場合は、以前のようにベース URL にリダイレクトされます。(OCPBUGS-38914)

1.9.42.2. バグ修正

- 以前は、クラスター内の大量のシークレットが 1 回の呼び出しで取得されると、API がタイムアウトし、CCO がエラーを出力してから再起動していました。このリリースでは、CCO がシークレットのリストを 100 個ずつ小さなバッチで取得するようになり、問題が解決されました。(OCPBUGS-41234)

- 以前は、**registryPoll** フィールドが **none** の場合、Operator Lifecycle Manager (OLM) カタログソース Pod がノード障害から回復しませんでした。このリリースでは、OLM CatalogSource レジストリー Pod がクラスターのノード障害から回復するようになり、問題が解決されました。(OCPBUGS-41217)

- 以前は、Cluster Ingress Operator が存在しない更新をログに記録していました。このリリースにより、この問題は解決されました。(OCPBUGS-39324)

- 以前は、**eu-es** (スペイン、マドリード) リージョンで、**e980** システムタイプとして設定された IBM Power Virtual Server プラットフォームに OpenShift Container Platform クラスターを、インストールプログラムによってインストールできませんでした。このリリースでは、この環境でクラスターをインストールする際にインストールプログラムが失敗しなくなりました。(OCPBUGS-38502)

- 以前は、**CanaryRepetitiveFailures** 状態の遷移時間の問題により、Ingress Controller の **Degraded** ステータスが設定されませんでした。このリリースでは、メッセージまたは理由だけが変更されたときではなく、状態のステータスが変更されたときにだけ、状態の遷移時間が更新されるようになりました。(OCPBUGS-39323)

- 以前は、Hosted Cluster イメージ設定で指定された **AdditionalTrustedCA** フィールドが、期待どおりに openshift-config namespace に調整されず、コンポーネントが利用できませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-39293)

- 以前は、インストーラーのリグレッションの問題により、Dynamic Host Configuration Protocol (DHCP) ネットワークを使用した Nutanix クラスターのデプロイで問題が発生していました。このリリースにより、この問題は解決されました。(OCPBUGS-38956)

- 以前は、CAPV セッションがまれに予期せずタイムアウトすることがありました。このリリースでは、新しいバージョンの CAPV で **Keep Alive** のサポートが無効になり、問題が解決されました。(OCPBUGS-38822)

- 以前は、Firefox のダークモードでページを表示すると、**Cluster Settings** の更新グラフのバージョン番号テキストが、暗い背景の上に黒いテキストとして表示されていました。この更新により、テキストが白いテキストとして表示されるようになりました。(OCPBUGS-38424)

- 以前は、HyperShift クラスターのコントロールプレーンで実行される Operator のプロキシーが、データプレーンで実行される konnectivity エージェント Pod のプロキシー設定によって実行されていました。その結果、アプリケーションプロトコルに基づいてプロキシーが必要かどうかを判別することができませんでした。{rh-short} との同等性を確保するために、https/http 経由の IDP 通信はプロキシーする必要がありますが、LDAP 通信はプロキシーしないでください。このリリースでは、ホストされたクラスターでのプロキシーの処理方法が変更され、**konnectivity-https-proxy** および **konnectivity-socks5-proxy** を介してコントロールプレーンでプロキシーが呼び出され、konnectivity エージェントからのトラフィックのプロキシーが停止されるようになりました。(OCPBUGS-38062)

1.9.42.3. 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。

1.9.43. RHBA-2024:6401 - OpenShift Container Platform 4.16.11 バグ修正の更新

発行日: 2024 年 9 月 11 日

OpenShift Container Platform リリース 4.16.11 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:6401 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:6404 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.11 --pullspecs
```

1.9.43.1. 既知の問題

- Red Hat OpenShift Service on AWS Hosted Control Plane (HCP) および OpenShift Container Platform クラスターは、4.15.23 より前のバージョンの MachinePool に新しいノードを追加できません。その結果、一部の更新がブロックされます。影響を受けるクラスターと推奨される回避策を確認するには、ROSA upgrade issue mitigation for HOSTEDCP-1941 を参照してください。(OCPBUGS-39447)

1.9.43.2. バグ修正

- 以前は、Platform Prometheus リモート書き込みエンドポイントのプロキシーを設定する際に、クラスター全体のプロキシーの **noProxy** フィールドが考慮されていませんでした。このリリースでは、Cluster Monitoring Operator (CMO) が、**noProxy** に基づき、プロキシーをバイパスする必要がある URL を持つリモート書き込みエンドポイントに対してプロキシーを設定しなくなりました。(OCPBUGS-39170)

- 以前は、コアオペレーティングシステムの変更により、Red Hat HyperShift の定期的な適合ジョブが失敗していました。この失敗したジョブにより、OpenShift API のデプロイメントが失敗していました。このリリースでは、更新時に 1 つのファイルがコピーされるのではなく、個々の信頼済み認証局 (CA) 証明書が再帰的にコピーされるため、定期的な適合ジョブが成功し、OpenShift API が期待どおりに実行されます。(OCPBUGS-38942)

- 以前は、Egress IP の場合、IP が Egress ノードに割り当てられ、それが削除されると、その **egressIP** によって選択された Pod に、その Egress ノードへの誤ったルーティング情報が設定されることがありました。このリリースにより、この問題は修正されました。(OCPBUGS-38705)

- 以前は、**eu-es** (スペイン、マドリード) リージョンで、**e980** システムタイプとして設定された IBM Power Virtual Server プラットフォームに OpenShift Container Platform クラスターを、インストールプログラムによってインストールできませんでした。このリリースでは、この環境でクラスターをインストールする際にインストールプログラムが失敗しなくなりました。(OCPBUGS-38502)

- 以前は、**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すると、BMH が **Preparing** 状態のままになり、ファームウェアの更新が繰り返し実行されていました。この問題は解決されています。(OCPBUGS-35559)

1.9.43.3. 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。

1.9.44. RHSA-2024:6004 - OpenShift Container Platform 4.16.10 バグ修正の更新

発行日: 2024 年 9 月 3 日

OpenShift Container Platform リリース 4.16.10 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:6004 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:6007 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.10 --pullspecs
```

1.9.44.1. 機能拡張

1.9.44.1.1. CENTOS 8 への参照を CENTOS 9 に更新

- CENTOS 8 のライフサイクルが最近終了しました。このリリースでは、CENTOS 8 への参照が CENTOS 9 に更新されています。(OCPBUGS-38627)

1.9.44.2. バグ修正

- 以前は、**egressip** コントローラーが、Virtual Routing and Forwarding (VRF) テーブルに関連付けられたネットワークインターフェイスの **EgressIP** アドレスの割り当てを正しく管理できませんでした。その結果、ネットワークインターフェイスに VRF インスタンスが設定されている場合、OVN-K が VRF のルーティングテーブルではなくメインルーティングテーブルを使用するため、パケットが正しくルーティングされませんでした。この更新により、ネットワークインターフェイスに VRF インスタンスが設定されている場合、**egressip** コントローラーが VRF のルーティングテーブルを使用するようになり、正確な **EgressIP** の割り当てと正しいトラフィックルーティングが実現するようになりました。(OCPBUGS-38704)

- 以前は、サービスアカウントの認証情報の有効期間が短い場合、内部タイムアウトが発生していました。このリリースでは、タイムアウトが削除され、親コンテキストがタイムアウトを制御できるようになりました。(OCPBUGS-38196)

- 以前は、権限が制限されたユーザーが Serveless を使用してデプロイされたアプリケーションを削除しようとすると、エラーが発生していました。このリリースでは、ユーザーに Pipeline リソースを表示する権限があるかどうかを確認するためのチェックが追加されました。(OCPBUGS-37954)

- 以前は、使用率カードに、容量と制限の関係について誤解を招くような形で **limit** が表示されていました。このリリースでは、このような誤解を排除するために **limit** の位置が変更されました。(OCPBUGS-37430)

1.9.44.3. 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。

1.9.45. RHBA-2024:5757 - OpenShift Container Platform 4.16.9 バグ修正の更新

発行日: 2024 年 8 月 29 日

OpenShift Container Platform リリース 4.16.9 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:5757 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:5760 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.9 --pullspecs
```

1.9.45.1. 機能拡張

- Insights Operator (IO) が、**haproxy_exporter_server_threshold** メトリクスからデータを収集できるようになりました。(OCPBUGS-38230)

1.9.45.2. 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。

1.9.46. RHSA-2024:5422 - OpenShift Container Platform 4.16.8 のバグ修正とセキュリティー更新

発行日: 2024 年 8 月 20 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.16.8 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:5422 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:5425 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.8 --pullspecs
```

1.9.46.1. バグ修正

- 以前は、OpenShift Container Platform クラスターの **Settings** ページで Red Hat OpenShift Lightspeed のリンクをクリックしても、Operator Hub の OpenShift Lightspeed モーダルが開きませんでした。この更新により、OpenShift Lightspeed モーダルが期待どおりに開くようになりました。(OCPBUGS-38093)

- 以前は、**--rebuild-catalogs** 引数を使用して Operator カタログをミラーリングすると、カタロ

グキャッシュがローカルマシンで再作成されていました。そのため、カタログイメージから **opm** バイナリーを抽出して使用する必要があり、ミラーリング操作またはカタログソースの障害が発生していました。この障害は、サポートされているオペレーティングシステムと **opm** バイナリーのプラットフォームが、**oc-mirror** のオペレーティングシステムおよびプラットフォームと一致しないために発生していました。このリリースでは、デフォルトで **--rebuild-catalogs** 引数に **true** の値が適用され、カタログの再構築時に内部キャッシュが再作成されなくなりました。さらに、このリリースでは、イメージが **opm serve /configs --cache-dir=/tmp/cache** から **opm serve /configs** に更新され、Pod の起動時にキャッシュが作成されるようになりました。起動時にキャッシュすると、Pod の起動時間が長くなる可能性があります。(OCPBUGS-38035)

- 以前は、Prometheus が **remote-write** エンドポイントに 1 回以上データを送信しないと、**PrometheusRemoteWriteBehind** アラートがトリガーされませんでした。このリリースでは、**remote-write** エンドポイント設定に追加した時点からエンドポイント URL にエラーが存在する場合など、エンドポイントとの接続を確立できなかった場合にもアラートがトリガーされるようになりました。(OCPBUGS-36918)

- 以前は、ビルドコントローラーが同じシークレットを使用する複数の **MachineOSBuild** オブジェクトを適切に処理できませんでした。このリリースでは、ビルドコントローラーがこれらのオブジェクトを期待どおりに処理できるようになりました。(OCPBUGS-36171)

- 以前は、機能が無効になっている場合でも、**ImageRegistry**、**Build**、**DeploymentConfig** 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。このリリースでは、クラスターで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)

1.9.46.2. 既知の問題

- SR-IOV ネットワークデバイスを使用する Pod を削除すると、エラーが発生する可能性があります。このエラーは、ネットワークインターフェイスの名前が変更されると、以前の名前が代替名リストに追加されるという RHEL 9 の変更によって発生します。その結果、SR-IOV Virtual Function (VF) にアタッチされた Pod が削除されると、VF は元の名前 (**ensf0v2** など) ではなく、予期しない新しい名前 (**dev69** など) でプールに戻ります。このエラーは致命的なものではありませんが、システムの再起動中に Multus および SR-IOV ログにエラーが表示される場合があります。このエラーにより、Pod の削除に追加で数秒かかる場合があります。(OCPBUGS-11281, OCPBUGS-18822, RHEL-5988)

1.9.46.3. 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。

1.9.47. RHSA-2024:5107 - OpenShift Container Platform 4.16.7 のバグ修正とセキュリティー更新

発行日: 2024 年 8 月 13 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.16.7 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:5107 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:5110 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.7 --pullspecs
```

1.9.47.1. バグ修正

- 以前は、ブートストラップ収集ログを収集するときに、**openshift-install** CLI がブートストラップノードへの接続に失敗することがありました。インストールプログラムにより、**The bootstrap machine did not execute the release-image.service systemd unit** などのエラーメッセージが報告されていました。このリリースでは、ブートストラップ収集ログの問題が発生すると、インストールプログラムにより、**Invalid log bundle or the bootstrap machine could not be reached and bootstrap logs were not collected** と報告されます。これは、より正確なエラーメッセージです。(OCPBUGS-37838)

- 以前は、**HostFirmwareComponents** リソースを介してファームウェアを更新した後、**Status.Components** にインストールされたファームウェアに関する新しい情報がこのリソースに表示されませんでした。このリリースでは、ファームウェアの更新が実行され、**BareMetalHosts** (BMH) オブジェクトが **provisioning** に移行すると、ファームウェアに関する新しい情報が **Status.Components** の下の **HostFirmwareComponents** リソースに入力されます。(OCPBUGS-37765)

- 以前は、タグ用の oc-mirror プラグイン v2 が、OpenShift Container Platform リリースイメージ用に作成されていませんでした。一部のコンテナーレジストリーでは、このタグが必須タグとして使用されます。このリリースでは、このタグがすべてのリリースイメージに追加されます。(OCPBUGS-37757)

- 以前は、Cluster API Machine オブジェクトから IP アドレスを抽出しても、単一のアドレスのみが返されていました。VMware vSphere では、返されるアドレスが常に IPv6 アドレスとなり、アドレスがルーティング不可能な場合は **must-gather** 実装で問題が発生していました。このリリースでは、Cluster API Machine オブジェクトが IPv4 を含むすべての IP アドレスを返すため、VMware vSphere で **must-gather** 問題が発生しなくなりました。(OCPBUGS-37607)

- 以前は、すでにアイデンティティーおよびアクセス管理 (IAM) ロールがある OpenShift Container Platform クラスターの IAM ロールを作成するために、インストールプログラムが Amazon Web Services (AWS) の権限を誤って要求していました。このリリースでは、インストールプログラムはまだ作成されていないロールの権限のみを要求します。(OCPBUGS-37494)

- 以前は、Red Hat OpenStack Platform (RHOSP) にクラスターをインストールするときに、クラスター名にハッシュ記号 (**#**) などの特殊文字を使用すると、Neutron API がクラスターの名前でセキュリティーグループをタグ付けできませんでした。このため、クラスターのインストールが失敗していました。このリリースでは、インストールプログラムが別のエンドポイントを使用してセキュリティーグループにタグを付けます。このエンドポイントは、タグ名での特殊文字の使用をサポートしています。(OCPBUGS-37492)

- 以前は、Redfish プロトコルを使用する Dell iDRAC ベースボード管理コントローラー (BMC) により、Dell iDRAC サーバー上のクラスターが失敗していました。このリリースでは、**idrac-redfish** 管理インターフェイスを更新して **ipxe** パラメーターを設定解除することで、この問題が修正されています。(OCPBUGS-37262)

- 以前は、**assisted-installer** がコントロールプレーンノードの準備状況をチェックしたときに、**assisted-installer-controller** からの書き込み操作と競合があった場合、**assisted-installer** は **assisted-service** から新しいデータを再ロードしませんでした。この競合により、**assisted-installer** が古い情報に依拠していため、**assisted-installer** は **assisted-**

installer-controller によって **Ready** とマークされたノードを検出できませんでした。このリリースでは、**assisted-installer** が **assisted-service** から最新の情報を受信できるようになり、**assisted-installer** が各ノードのステータスを正確に検出できるようになりました。(OCPBUGS-37167)

- 以前は、DNS ベースの Egress ファイアウォールにより、複数の再試行操作が原因で、クラスターで実行されているノードのメモリーが誤って増加していました。このリリースでは、再試行ロジックが修正され、DNS Pod がノードに余分なメモリーをリークしなくなりました。(OCPBUGS-37078)

- 以前は、ユーザーが **HostedCluster** オブジェクトから **ImageContentSources** フィールドを削除した後、**HostedClusterConfigOperator** リソースが **ImageDigestMirrorSet** (IDMS) オブジェクトを削除しませんでした。そのため、IDMS オブジェクトが **HostedCluster** オブジェクト内に残っていました。このリリースでは、**HostedClusterConfigOperator** が **HostedCluster** オブジェクト内のすべての IDMS リソースを削除するため、この問題は発生しなくなりました。(OCPBUGS-36766)

- 以前は、Telco RAN DU リファレンス設定を使用して OpenShift Container Platform 4.16 を実行するクラスターで、**20** マイクロ秒を超える最大レイテンシーが検出されたため、長時間の **cyclictest** または **timerlat** テストが失敗することがありました。この問題は、cgroup v2 が有効な場合に、**psi** カーネルコマンドライン引数がデフォルトで **1** に設定されていたために発生しました。このリリースでは、cgroup v2 を有効にするときにカーネル引数に **psi=0** を設定することで、この問題が修正されました。OCPBUGS-34022 で報告された **cyclictest** のレイテンシーの問題も修正されました。(OCPBUGS-37271)

1.9.47.2. 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。

1.9.48. RHSA-2024:4965 - OpenShift Container Platform 4.16.6 のバグ修正

発行日: 2024 年 8 月 6 日

OpenShift Container Platform リリース 4.16.6 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:4965 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:4968 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.6 --pullspecs
```

1.9.48.1. 機能拡張

この z-stream リリースには、次の機能拡張が含まれています。

1.9.48.1.1. Ingress Controller 証明書の有効期限が収集される

- Insights Operator は、すべての Ingress Controller 証明書の有効期限に関する情報を収集するようになりました。情報は、パス **aggregated/ingress_controllers_certs.json** の JSON ファイルに格納されます。(OCPBUGS-37671)

1.9.48.1.2. デバッグログレベルの有効化

- 以前は、クラスターノードの IP アドレスを選択する内部コンポーネントのログレベルを制御することはできませんでした。このリリースでは、デバッグログレベルを有効にして、必要に応じてログレベルを上げたり下げたりできるようになりました。ログレベルを調整するには、次のような設定を持つ config map マニフェストファイルを作成する必要があります。

```
apiVersion: v1
data:
  enable-nodeip-debug: "true"
kind: ConfigMap
metadata:
  name: logging
  namespace: openshift-vsphere-infra
# ...
```

(OCPBUGS-35891)

1.9.48.1.3. Ironic と Inspector の **htpasswd** の改善

- 以前は、Ironic および Inspector **htpasswd** は環境変数を使用して **ironic-image** に提供されていましたが、これは安全ではありませんでした。このリリースから、セキュリティー強化のため、**/auth/ironic/htpasswd** ファイルを使用して Ironic **htpasswd** が **ironic-image** に提供され、**/auth/inspector/htpasswd** ファイルを使用して Inspector **htpasswd** が **ironic-image** に提供されるようになりました。(OCPBUGS-36285)

1.9.48.2. バグ修正

- 以前は、インストーラーによって作成されたサブネットには **kubernetes.io/cluster/<clusterID>: shared** タグが付けられていました。このリリースでは、サブネットに **kubernetes.io/cluster/<clusterID>: owned** タグが付けられるようになりました。(OCPBUGS-37510)

- 以前は、同じノードがドレインコントローラーで複数回キューに入れられ、同じノードが 2 回ドレインされていました。このリリースでは、ノードは 1 回だけドレインされます。(OCPBUGS-37470)

- 以前は、使用不可ノードよりも **maxUnavailable** が高いマシン設定プール (MCP) 内の隔離されたノードが更新候補として選択される場合がありました。このリリースでは、隔離されたノードは更新のためにキューに入れられることはありません。(OCPBUGS-37460)

- 以前は、oc-mirror プラグイン v2 は、システムプロキシー設定が設定されたプロキシーの背後で実行している場合は、システムプロキシー設定を使用せずにリリースの署名を回復しようとしていました。このリリースでは、署名の回復時にシステムプロキシー設定も考慮されるようになり、問題は解決されました。(OCPBUGS-37445)

- 以前は、**OVNKubernetesNorthdInactive** のアラートは、発生する必要がある状況で発生しませんでした。このリリースでは問題が修正され、**OVNKubernetesNorthdInactive** のアラートが期待どおりに発生するようになりました。(OCPBUGS-37362)

- 以前は、Load Balancer の Ingress ルールが継続的に取り消され、承認されていたため、不要な Amazon Web Services (AWS) アプリケーションプログラミングインターフェイス (API) 呼び出しとクラスターのプロビジョニングの遅延が発生していました。このリリースでは、Load Balancer は適用する必要がある Ingress ルールをチェックし、問題は解決されます。(OCPBUGS-36968)

- 以前は、OpenShift Container Platform Web コンソールで、非アクティブまたはアイドル状態のブラウザータブが 1 つあると、他のすべてのタブのセッションが期限切れになっていました。このリリースでは、どのタブでもアクティビティーによってセッションの有効期限が切れることがなくなります。(OCPBUGS-36864)

- 以前は、Open vSwitch (OVS) ピンニング手順によってメインスレッドの CPU アフィニティーが設定されていましたが、他の CPU スレッドがすでに作成されている場合、このアフィニティーは取得されませんでした。その結果、一部の OVS スレッドが正しい CPU セットで実行されず、Quality of Service (QoS) クラスが **Guaranteed** の Pod のパフォーマンスに影響する可能性があります。この更新により、OVS ピンニング手順によってすべての OVS スレッドのアフィニティーが更新され、すべての OVS スレッドが正しい CPU セットで実行されるようになります。(OCPBUGS-36608)

- 以前は、etcd Operator は、単一メンバーのタイムアウトと一致する全メンバーのタイムアウトを使用して、etcd メンバーの健全性を順番にチェックしていました。これにより、1 つの低速メンバーチェックでタイムアウト全体が消費され、それ以降のメンバーの健全性に関係なく、それ以降のメンバーチェックが **deadline-exceeded** エラーで失敗する原因となっていました。現在、etcd はメンバーの健全性を並行してチェックするため、あるメンバーのチェックの健全性と速度は他のメンバーのチェックに影響を与えません。(OCPBUGS-36489)

- 以前は、VMware vSphere Container Storage Interface (CSI) ドライバーのスナップショット制限を変更するには、**TechPreviewNoUpgrade** フィーチャーゲートを有効にする必要がありました。これは、API の欠落により Cluster Storage Operator にバグが発生していたためです。このリリースでは、欠落していた API が追加され、**TechPreviewNoUpgrade** フィーチャーゲートを有効にしなくてもスナップショットの制限を変更できるようになりました。スナップショットの制限を変更する方法の詳細は、vSphere のスナップショットの最大数の変更 (OCPBUGS-36969) を参照してください。

1.9.48.3. 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。

1.9.49. RHBA-2024:4855 - OpenShift Container Platform 4.16.5 のバグ修正

発行日: 2024 年 7 月 31 日

OpenShift Container Platform リリース 4.16.5 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:4855 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-2024:4858 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.5 --pullspecs
```

1.9.49.1. バグ修正

- 以前は、oc-mirror プラグイン v2 (テクノロジープレビュー) では、生成されたアーカイブを別のマシンに移動すると、アーカイブからミラーレジストリーへのミラーリング操作が失敗し、次のエラーメッセージが出力されました。

  ```
  [ERROR]: [ReleaseImageCollector] open ${FOLDER}/working-dir/hold-release/ocp-
  ```

```
release/4.15.17-x86_64/release-manifests/image-references: no such file or directory
```

このリリースでは、oc-mirror を実行するマシンは、ターゲットの場所を作業ディレクトリーに変更するための自動更新を受け取ります。(OCPBUGS-37040)

- 以前は、OpenShift CLI (**oc**) コマンド **openshift-install destroy cluster** が停止し、次のエラーメッセージが表示されていました。

```
VM has a local SSD attached but an undefined value for 'discard-local-ssd' when using A3 instance types
```

このリリースでは、コマンドを発行するとローカル SSD が削除されるため、このバグは発生しなくなります。(OCPBUGS-36965)

- 以前は、Cloud Credential Operator がパススルーモードのパーミッションが正しいかどうかを確認するときに、Operator は Google Cloud API からプロジェクトの無効なパーミッションに関する応答を受け取ることがありました。このバグにより、Operator が劣化状態になり、クラスターのインストールに影響が出ました。このリリースでは、Cloud Credential Operator がこのエラーを具体的にチェックし、クラスターのインストールに影響を与えずに個別に診断します。(OCPBUGS-36834)

- 以前は、oc-mirror プラグイン v2 (テクノロジープレビュー) では、生成されたアーカイブを別のマシンに移動すると、アーカイブからミラーレジストリーへのミラーリング操作が失敗し、次のエラーメッセージが出力されました。

```
[ERROR]: [ReleaseImageCollector] open ${FOLDER}/working-dir/hold-release/ocp-release/4.15.17-x86_64/release-manifests/image-references: no such file or directory
```

このリリースでは、oc-mirror を実行するマシンは、ターゲットの場所を作業ディレクトリーに変更するための自動更新を受け取ります。(OCPBUGS-37040)

1.9.49.2. 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。

1.9.50. RHSA-2024:4613 - OpenShift Container Platform 4.16.4 のバグ修正とセキュリティー更新

発行日: 2024 年 7 月 24 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.16.4 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:4613 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-2024:4616 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.4 --pullspecs
```

1.9.50.1. バグ修正

- 以前は、Ingress Operator への変更により、canary ルートで **clear spec.host** を行い、**spec.subdomain** を設定するロジックが追加されていました。ただし、Operator のサービスアカウントには、既存のルート上の **spec.host** または **spec.subdomain** を更新するために必要な **routes/custom-host** 権限がありませんでした。このリリースでは、Operator のサービスアカウントの **ClusterRole** リソースに権限が追加され、問題が解決されました。(OCPBUGS-32887)

- 以前は、Console Operator からのサブスクリプションの **fetchOrganization** エンドポイントへの呼び出し回数が多すぎたため、インストールで問題が発生していました。このリリースでは、組織 ID がキャッシュされ、問題は解決されました。(OCPBUGS-34012)

- 以前は、それぞれの機能が無効になっている場合でも、**ImageRegistry**、**Build**、**DeploymentConfig** 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、MetalLB Operator は、MetalLB の Border Gateway Protocol (BGP) バックエンドである FRR-K8s を使用してデプロイするときに、ダウンストリームイメージをデプロイしていました。このリリースでは、MetalLB Operator はダウンストリームイメージではなくアップストリームイメージをデプロイします。(OCPBUGS-35864)

- 以前は、512 エミュレーション (512e) 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、**ignition-ostree-growfs** ステップで暗号化が失敗し、アライメントの問題によりエラーが報告されていました。このリリースでは、この状況を検出し、アライメントの問題を解決するための回避策が **ignition-ostree-growfs** ステップに追加されました。(OCPBUGS-36147)

- 以前は、localhost の **--bind-address** パラメーターにより、IBM Power Virtual Server クラスターの liveness テストが失敗していました。このリリースでは、localhost の **--bind-address** パラメーターが削除され、問題は解決されました。(OCPBUGS-36317)

- 以前は、Operator のインストール時に、すでに作成されている Operator バンドルアンパックジョブが Operator Lifecycle Manager (OLM) によって検出されませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-36450)

- 以前は、Cluster API-provisioned installation に使用される etcd データストアは、ブートストラップノードまたはクラスターのいずれかが破棄された場合にのみ削除されていました。このリリースでは、インフラストラクチャーのプロビジョニング中にエラーが発生した場合、データストアが削除され、不要なディスク領域を占有しなくなります。(OCPBUGS-36463)

- 以前は、カスタムフィーチャーゲートを有効にすると、フィーチャーゲート **ClusterAPIInstallAWS=true** が有効になっていない場合に AWS でインストールが失敗する可能性がありました。このリリースでは、**ClusterAPIInstallAWS=true** フィーチャーゲートは不要になりました。(OCPBUGS-36720)

- 以前は、**destroy cluster** コマンドの後に **create cluster** を実行すると、ローカルインフラストラクチャープロビジョニングアーティファクトがすでに存在するというエラーが報告されていました。このリリースでは、残ったアーティファクトは **destroy cluster** によって削除され、問題は解決されます。(OCPBUGS-36777)

- 以前は、**OperandDetails** ページには、名前が一致した最初のカスタムリソース定義 (CRD) の情報が表示されていました。このリリースでは、**OperandDetails** ページに、名前とオペランドのバージョンが一致する CRD の情報が表示されます。(OCPBUGS-36841)

- 以前は、**openshift.io/internal-registry-pull-secret-ref** アノテーションが **ServiceAccount** リソースから削除されると、OpenShift Container Platform は削除されたアノテーションを再作

成し、新しい管理対象イメージプルシークレットを作成しました。この競合により、クラスターがイメージプルシークレットで過負荷になる可能性があります。このリリースでは、OpenShift Container Platform は、以前参照された管理対象イメージプルシークレットの再利用を試み、調整後に孤立したままになっている管理対象イメージプルシークレットを削除します。(OCPBUGS-36862)

- 以前は、セットアップの失敗によりインストールプログラムが停止した後も、一部のプロセスは実行されたままになっていました。このリリースでは、インストールプログラムの実行が停止すると、すべてのインストールプロセスが停止します。(OCPBUGS-36890)
- 以前は、**ClusterMonitoringOperatorDeprecatedConfig** アラートの Runbook はありませんでした。このリリースでは、**ClusterMonitoringOperatorDeprecatedConfig** アラートの Runbook が追加され、問題が解決されました。(OCPBUGS-36907)
- 以前は、**クラスターの概要ページ** に **ドキュメントのすべての手順を表示** リンクが含まれていましたが、ROSA および OSD クラスターでは 404 エラーが発生していました。この更新により、ROSA および OSD クラスターのリンクは表示されなくなります。(OCPBUGS-37063)
- 以前は、OpenShift Container Platform で使用される Machine Config Operator ツールの OpenSSL バージョンと、Hosted Control Plane で実行する OpenSSL バージョンの間に不一致がありました。このリリースにより、この問題は解決されました。(OCPBUGS-37241)

1.9.50.2. 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。

1.9.51. RHSA-2024:4469 - OpenShift Container Platform 4.16.3 のバグ修正とセキュリティー更新

発行日: 2024 年 7 月 16 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.16.3 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:4469 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:4472 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.3 --pullspecs
```

1.9.51.1. 機能拡張

この z-stream リリースには、次の機能拡張が含まれています。

1.9.51.1.1. マシンセットを使用した Capacity Reservation の設定

- OpenShift Container Platform リリース 4.16.3 では、Microsoft Azure クラスター上の Capacity Reservation グループを使用したオンデマンド Capacity Reservation のサポートが導入されています。詳細は、コンピュート のマシンセットまたは コントロールプレーン マシンセットについて、**マシンセットを使用した Capacity Reservation の設定** を参照してください。(OCPCLOUD-1646)

1.9.51.1.2. 無効な Ingress クラスターに代替 Ingress を追加する

- このリリースでは、コンソール Operator 設定 API により、Ingress クラスター機能が無効になっている環境に代替 Ingress を追加できるようになりました。(OCPBUGS-33788)

1.9.51.2. バグ修正

- 以前は、PodSecurityAdmission の "restricted" レベルが適用された namespace 内の CatalogSource オブジェクトに **spec.grpcPodConfig.securityContextConfig** が設定されていないと、デフォルトの securityContext が **restricted** に設定されていました。このリリースでは、OLM Catalog Operator は、PSA 検証に合格するために必要な securityContexts を使用してカタログ Pod を設定するため、問題は解決されました。(OCPBUGS-34979)

- 以前は、**HighOverallControlPlaneCPU** アラートは、高可用性を備えたマルチノードクラスターの基準に基づいて警告をトリガーしていました。その結果、設定が環境基準と一致しなかったため、シングルノードの OpenShift クラスターで誤解を招くアラートがトリガーされました。この更新では、アラートロジックが改良され、シングルノードの OpenShift 固有のクエリーとしきい値が使用され、ワークロードのパーティション設定が考慮されるようになりました。その結果、シングルノードの OpenShift クラスターの CPU 使用率アラートは正確になり、シングルノードの設定に関連したものになります。(OCPBUGS-35831)

- 以前は、localhost への **--bind-address** により、PowerVS クラスターの liveness テストが失敗していました。このリリースでは、localhost への **--bind-address** が削除され、問題は解決されました。(OCPBUGS-36317)

- 以前は、**machine-config-daemon-firstboot.service** に互換性のない machine-config-daemon バイナリーコードがあったため、OpenShift Container Platform の 4.1 および 4.2 ブートイメージを使用してブートされたノードは、プロビジョニング中に停止していました。このリリースでは、バイナリーが更新され、問題は解決されました。(OCPBUGS-36330)

- 以前は、完全に非接続環境で **diskToMirror** アクションを実行した場合、ソースレジストリーにアクセスできませんでした。**MirrorToDisk** で **oc-mirror v2** を使用する場合、カタログイメージとコンテンツは、イメージのダイジェストに対応する **working-dir** の下のサブフォルダーに保存されます。次に、**DiskToMirror** を使用しているときに、oc-mirror はソースレジストリーを呼び出してカタログイメージタグをダイジェストに解決し、ディスク上の対応するサブフォルダーを見つけようとします。このリリースでは、**oc-mirror** は **diskToMirror** プロセス中にローカルキャッシュを照会してこのダイジェストを決定します。(OCPBUGS-36386)

- 以前は、現在のデプロイメントと同一だが別の stateroot にあるホスト上で OSTree レベルで新しいデプロイメントが実行されると、OSTree はそれらを同等と認識していました。この動作により、OSTree は 2 つの stateroot をデプロイメントの差別化要因として認識しなかったため、**set-default** が呼び出されたときにブートローダーの更新が誤って妨げられました。このリリースでは、OSTree のロジックが変更され、stateroot を考慮するようになり、OSTree はデフォルトのデプロイメントを異なる stateroot を持つ新しいデプロイメントに適切に設定できるようになりました。(OCPBUGS-36386)

- 以前は、AWS クラスターのインストーラーログに、混乱を招く可能性のある Elastic Kubernetes Service (EKS) に関する不要なメッセージが含まれていました。このリリースでは、EKS ログラインが無効になり、問題は解決されました。(OCPBUGS-36447)

- 以前は、OpenShift Container Platform 4.14 で依存関係ターゲットの変更が導入され、切断された ARO インストールが影響を受けるバージョンにアップグレードした後に新しいノードをスケールアップできなくなりました。このリリースでは、切断された ARO インストールで、OpenShift Container Platform 4.16 にアップグレードした後に新しいノードをスケールアップできます。(OCPBUGS-36536)

- 以前は、CRIO は Windows ノードでは実行されないため、**port 9637** で接続が拒否されると、Windows ノードで **Target Down** と報告されていました。このリリースでは、Windows ノードは Kubelet Service Monitor から除外されます。(OCPBUGS-36717)

1.9.51.3. 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。

1.9.52. RHSA-2024:4316 - OpenShift Container Platform 4.16.2 のバグ修正とセキュリティー更新

発行日: 2024 年 7 月 9 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.16.2 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:4316 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:4319 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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 4.16.2 --pullspecs
```

1.9.52.1. バグ修正

- 以前は、OpenShift Container Platform の古いバージョンからアップグレードされたクラスターの場合、OVN 対応のクラスターで **kdump** を有効にすると、ノードがクラスターに再参加したり、**Ready** 状態に戻ったりできなくなることがありました。このリリースにより、古い OpenShift Container Platform バージョンから古いデータが削除され、この古いデータが常にクリーンアップされるようになりました。ノードが正常に起動し、クラスターに再参加できるようになりました。(OCPBUGS-36198)

- 以前は、installer-provisioned infrastructure (IPI) クラスターを作成するときに、予期しない出力がターミナルに表示されていました。このリリースにより、問題が解決され、予期しない出力は表示されなくなりました。(OCPBUGS-36156)

- 以前は、OpenShift Container Platform コンソールのノードリストにファイルシステムメトリクスが表示されませんでした。このリリースにより、ファイルシステムメトリクスがノードテーブルに表示されるようになりました。(OCPBUGS-35946)

- 以前は、マルチクラスター以外の環境で Prometheus ダッシュボードを表示すると空となっていました。このリリースにより、ダッシュボードは両方のケースで期待どおりにダッシュボードパネルに情報を入力します。(OCPBUGS-35904)

- 以前は、4.16.0 でのリグレッションにより、プロキシーが使用されている場合に新しいベアメタル installer-provisioned infrastructure (IPI) インストールが失敗していました。これは、ブートストラップ仮想マシン (VM) 内のサービスの 1 つがプロキシー経由で IP アドレス 0.0.0.0 にアクセスしようとしたことが原因でした。このリリースにより、このサービスは 0.0.0.0 にアクセスしなくなりました。(OCPBUGS-35818)

- 以前は、クラスター API プロバイダー IBM Cloud は、IBM Power Virtual Server クラスター上にロードバランサーを作成する前に、いくつかのリソースが作成されるのを待機していました。この遅延により、15 分のタイムアウト前にロードバランサーが作成されないことがありま

した。このリリースでは、タイムアウトが延長されました。(OCPBUGS-35722)

- 以前は、Cluster API 実装を使用して Red Hat OpenStack Platform (RHOSP) にクラスターをインストールすると、コンパクトクラスターのコントロールプレーンノードに追加された追加のセキュリティーグループルールによって IPv4 プロトコルが強制され、デュアルスタッククラスターのデプロイが妨げられていました。これは、Terraform を使用したインストールからのリグレッションでした。このリリースにより、ルールは要求された IP バージョンに基づいて正しいプロトコルを使用するようになりました。(OCPBUGS-35718)

- 以前は、内部イメージレジストリーは、外部 OpenID Connect (OIDC) ユーザーで設定されたクラスター上のユーザーを正しく認証しなかったため、ユーザーが内部イメージレジストリーにイメージをプッシュしたり、内部イメージレジストリーからイメージをプルしたりすることができませんでした。このリリースにより、内部イメージレジストリーが SelfSubjectReview API の使用を開始し、外部 OIDC ユーザーで設定されたクラスターでは利用できない OpenShift Container Platform 固有のユーザー API の使用を中止したことで、再度イメージレジストリーで正常に認証できるようになりました。(OCPBUGS-35567)

- 以前は、誤ったコード変更により、**Global Configuration** ページで **oauth.config.openshift.io** 項目が重複していました。この更新により、重複したアイテムが削除されます。(OCPBUGS-35565)

- 以前の **oc-mirror** v2 では、ネットワークエラーや無効な Operator カタログコンテンツなどのさまざまな理由によりミラーリングが失敗すると、**oc-mirror** はクラスターリソースを生成しませんでした。このバグ修正により、**oc-mirror** v2 は次のアクションを実行します。

  - Operator イメージおよび追加イメージでエラーが発生した場合は他のイメージのミラーリングを続行し、リリースイメージでエラーが発生した場合はミラーリングを中止します。

  - 正しくミラーリングされたイメージのサブセットに基づいて、クラスターのクラスターリソースを生成します。

  - すべてのミラーリングエラーをログファイルに収集します。

  - すべてのミラーリングエラーを別のログファイルに記録します。(OCPBUGS-35409)

- 以前は、設定の問題により、OpenShift Container Platform コンソールで pseudolocalization が機能していませんでした。このリリースにより、問題が解決され、pseudolocalization が再び機能するようになりました。(OCPBUGS-35408)

- 以前は、各ノードでデータを順番に収集していたため、ノードの CPU 関連のパフォーマンスデータを収集する際に、**must-gather** プロセスの実行時間が長すぎました。このリリースにより、ノードデータが並列に収集されるため、**must-gather** データの収集時間が大幅に短縮されます。(OCPBUGS-35357)

- 以前は、ビルドで **GIT_LFS_SKIP_SMUDGE** 環境変数を設定できず、ソースコードのクローン作成時にその値を使用できませんでした。このため、LFS ファイルを含む一部の git リポジトリーのビルドが失敗していました。このリリースにより、ビルドでこの環境変数を設定し、ビルドの git clone ステップ中に使用できるようになりました。(OCPBUGS-35283)

- 以前は、関連のないデータプレーンイメージにレジストリーオーバーライドが存在していました。このリリースにより、OpenShift Container Platform がオーバーライドレジストリーを伝播する方法が変更され、問題が修正されました。(OCPBUGS-34602)

- 以前は、RegistryMirrorProvider が内部エントリーではなくキャッシュされたイメージを直接変更していたため、調整中に RegistryMirrorProvider イメージは更新されませんでした。このリリースにより、イメージの更新方法が変更され、キャッシュを回避してエントリー内で直接更新が行われるようになったため、バグは発生しなくなりました。(OCPBUGS-34569)

- 以前は、**alertmanager-trusted-ca-bundle ConfigMap** がユーザー定義の Alertmanager コンテナーに注入されていなかったため、アラート通知を受信する HTTPS Web サーバーの検証ができませんでした。この更新により、信頼された CA バンドル **ConfigMap** が **/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem** パスの Alertmanager コンテナーにマウントされます。(OCPBUGS-34530)

- 以前は、Security Token Service (STS) を使用する Amazon Web Services (AWS) クラスターの場合、Cloud Credential Operator (CCO) は **CredentialsRequest** カスタムリソースの **awsSTSIAMRoleARN** の値をチェックしてシークレットを作成していました。**awsSTSIAMRoleARN** が存在しない場合、CCO はエラーを記録しました。この問題はこのリリースで解決されています。(OCPBUGS-34117)

- 以前は、routing-via-host の OVN-Kubernetes 設定がデフォルト値の共有ゲートウェイモードに設定されていたため、OVN-Kubernetes はクラスター Ingress の IP レイヤーからの非断片化パケットと断片化パケットが混在するトラフィックストリームを正しく処理していませんでした。これにより、接続がリセットされたり、パケットがドロップされたりしました。このリリースでは、OVN-Kubernetes は、Ingress 時に外部トラフィックの IP パケットフラグメントを正しく再設定して処理します。(OCPBUGS-29511)

1.9.52.2. 既知の問題

- **ConfigMap** 最大転送単位 (MTU) が **openshift-network-operator** namespace に存在しない場合は、ユーザーはライブマイグレーションを開始する前に、マシン MTU 値を使用して **ConfigMap** を手動で作成する必要があります。そうしないと、ライブマイグレーションがスタックして失敗します。(OCPBUGS-35829)

1.9.52.3. 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。

1.9.53. 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 年 7 月 3 日

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-2024:4159 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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
```

1.9.53.1. バグ修正

- 以前は、**growpart** のエラーにより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、ノードは起動できなくなり、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ました。(OCPBUGS-35973)

- 以前は、systemd のバグにより、**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、システムの起動が完了しなくなります。このリリースでは、systemd ユニットが削除され、問題は修正されました。(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、キーが無効になっていました。このリリースでは、空の文字列が削除され、**install-config.yaml** から KMS キーが存在する場合にのみ KMS キーが適用されます。(OCPBUGS-35531)

- 以前は、ユーザーが設定した機密コンピュートとホストメンテナンスの値は検証されていませんでした。このリリースでは、ユーザーが機密コンピュートを有効にすると、**onHostMaintenance** の値を **onHostMaintenance: Terminate** に設定する必要があります。(OCPBUGS-35493)

- 以前は、user-provisioned infrastructure (UPI) 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は、インフラストラクチャーオブジェクトに **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ていました。このリリースでは、**infrastructures.config.openshift.io** に利用可能なドメインがない場合に、**failureDomains** フォールバックが **cloudConfig** から合成されます。(OCPBUGS-35446)

- 以前は、カスタムリソース定義 (CRD) の新しいバージョンで新しい変換ストラテジーが指定されると、この変換ストラテジーによってリソースが正常に変換されることが期待されていました。これは、Operator Lifecycle Manager (OLM) が実際に更新操作を実行せずに CRD 検証の新しい変換ストラテジーを実行できないために当てはまりませんでした。このリリースでは、既存の変換ストラテジーで CRD 検証が失敗し、新しいバージョンの CRD で新しい変換ストラテジーが指定されていると、OLM が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 Classless Inter-Domain Routing (CIDR) 範囲を活用して、データプレーンで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になる可能性があります。この更新により、提供された Machine 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す。(OCPBUGS-35056)

- 以前は、Serverless 関数を作成するには、Source-to-Image (S2I) ビルドストラテジーを **func.yaml** に明示的に追加する必要がありました。さらに、エラーメッセージには問題が示されていませんでした。このリリースでは、S2I が追加されていなくても、ユーザーは Serverless 関数を作成できます。ただし、それが S2I でないと、ユーザーは関数を作成することができません。さらに、エラーメッセージが更新され、より多くの情報が提供されるようになりました。(OCPBUGS-34717)

- 以前は、新しいオンクラスター階層化ビルドイメージをロールアウトするときに、**MachineOSConfig** オブジェクトの **CurrentImagePullSecret** フィールドは使用されていませんでした。このリリースでは、**MachineOSConfig** オブジェクトの **CurrentImagePullSecret** フィールドをイメージ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、失敗したポート転送要求を複数送信すると、ノードが停止するまで CRI-O メモリーの使用量が増加していました。このリリースでは、失敗したポート転送要求を送信する際のメモリーリークが修正され、問題が解決されました。(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。この更新でこの問題が修正されています。(OCPBUGS-25164)

1.9.53.2. 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。

1.9.54. 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 年 6 月 27 日

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 アドバイザリーで提供されています。

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

以下のコマンドを実行して、この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
```