OpenShift Container Platform 4.14

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: 2025-10-14

OpenShift Container Platform 4.14 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 4.14 リリースノート

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

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

1.1. このリリースについて

OpenShift Container Platform (RHSA-2023:5006) が使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 1.27 を使用します。以下では、OpenShift Container Platform 4.14 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 4.14 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 4.14 は、Red Hat Enterprise Linux (RHEL) 8.6 および OpenShift Container Platform 4.14 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 4.14 は、Red Hat Enterprise Linux CoreOS (RHCOS) 4.14 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。

x86_64 アーキテクチャー上の OpenShift Container Platform 4.12 では、6 カ月の Extended Update Support (EUS) フェーズを追加し、利用可能なライフサイクルを合計 18 カ月から 24 カ月に延長しました。64 ビット ARM (**aarch64**)、IBM Power® (**ppc64le**)、および IBM Z® (**s390x**) アーキテクチャーで実行される OpenShift Container Platform 4.12 では、EUS ライフサイクルは 18 カ月のままです。

OpenShift Container Platform 4.14 以降、すべてのサポート対象アーキテクチャー (**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) の偶数リリースで、各 EUS フェーズの利用可能なライフサイクルが合計 24 カ月になります。

OpenShift Container Platform 4.14 以降、Red Hat は、**Additional EUS Term 2** と呼ばれる 12 カ月間の追加 EUS アドオンを提供しています。これにより、利用可能なライフサイクルが合計 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。

こ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。

バージョン 4.12 のメンテナンスサポートは、2024 年 7 月 17 日に終了し、Extended Update Support フェーズに移行します。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。

4.14 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 は RHEL 9.2 を使用するようになりました

RHCOS は、OpenShift Container Platform 4.14 で Red Hat Enterprise Linux (RHEL) 9.2 パッケージを使用するようになりました。これ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、拡張機能、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 4.12 は、ライフサイクル全体にわたって RHEL 8.6 延長更新サポート (EUS) パッケージを引き続き使用する EUS リリースです。

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

OpenShift Container Platform 4.14 では RHEL 9.2 ベースの RHCOS が使用されるため、アップグレードする前に次の点を考慮してください。

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

- 一部のデバイスドライバーは非推奨になりました。詳細は、RHEL ドキュメント を参照してください。

1.3.2. インストールおよび更新

1.3.2.1. 共有 VPC を使用した Amazon Web Services (AWS) へのクラスターのインストール

OpenShift Container Platform 4.14 では、クラスターとは別のアカウントのプライベートホスト型ゾーンを持つ共有 Virtual Private Cloud (VPC) を使用するクラスターを AWS にインストールできます。詳細は、AWS 上のクラスターを既存の VPC へインストールする を参照してください。

1.3.2.2. AWS でのクラスターのブートストラップ中に S3 バケットを保持するように有効化する

この更新により、AWS でのクラスターのブートストラップ中に、S3 バケットの自動削除をオプトアウトできるようになりました。このオプションは、S3 バケットの削除を阻止するセキュリティーポリシーがある場合に便利です。

1.3.2.3. NAT ゲートウェイを使用した Microsoft Azure 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)

OpenShift Container Platform 4.14 では、アウトバウンドネットワーキングに NAT ゲートウェイを使用するクラスターをインストールできます。これはテクノロジープレビュー (TP) として利用できます。詳細は、追加の Azure 設定パラメーター を参照してください。

1.3.2.4. pd-balanced ディスクタイプを使用した Google Cloud Platform (GCP) へのクラスターのインストール

OpenShift Container Platform 4.14 では、**pd-balanced** ディスクタイプを使用して GCP にクラスターをインストールできます。このディスクタイプはコンピュートノードでのみ使用可能であり、コントロールプレーンノードでは使用できません。詳細は、追加の GCP 設定パラメーター を参照してください。

1.3.2.5. OpenShift Container Platform 4.14 のオプション機能

OpenShift Container Platform 4.14 では、インストール中に **Build**、**DeploymentConfig**、**ImageRegistry**、および **MachineAPI** の機能を無効にすることができます。**MachineAPI** 機能を無効にできるのは、ユーザーがプロビジョニングしたインフラストラクチャーを使用してクラスターをインストールする場合のみです。詳細は、クラスター機能 を参照してください。

1.3.2.6. Azure AD Workload Identity を使用したクラスターのインストール

インストール中に、Azure AD Workload Identity を使用するように Microsoft Azure クラスターを設定できるようになりました。Azure AD Workload Identity を使用すると、クラスターコンポーネントはクラスターの外部で管理される短期のセキュリティー認証情報を使用します。

Azure 上の OpenShift Container Platform クラスターの短期認証情報の実装に関する詳細は、Azure AD Workload Identity を参照してください。

インストール時にこの認証情報管理ストラテジーを設定する方法は、短期認証情報を使用するように Azure クラスターを設定する を参照してください。

1.3.2.7. Microsoft Azure のユーザー定義タグが一般提供に

Microsoft Azure のユーザー定義タグは、以前は OpenShift Container Platform 4.13 でテクノロジープレビューとして導入され、現在は、OpenShift Container Platform 4.14 で一般提供が開始されました。詳細は、Azure のユーザー定義タグの設定 を参照してください。

1.3.2.8. Azure の Confidential VM (テクノロジープレビュー)

Azure にクラスターをインストールするときに、Confidential VM を有効にできます。機密コンピューティングを使用して、インストール中に仮想マシンのゲスト状態ストレージを暗号化できます。この機能は、このページの既知の問題セクションに記載されている既知の問題により、テクノロジープレビューとなっています。詳細は、Confidential VM の有効化 を参照してください。

1.3.2.9. Azure のトラステッド起動 (テクノロジープレビュー)

クラスターをテクノロジープレビューとして Azure にインストールする際に、トラステッド起動機能を有効化できます。これらの機能には、セキュアブートと仮想化された Trusted Platform Module が含まれます。詳細は、Azure 仮想マシンのトラステッド起動の有効化 を参照してください。

1.3.2.10. Google Cloud Platform のユーザー定義のラベルとタグ (テクノロジープレビュー)

Google Cloud Platform (GCP) でユーザー定義のラベルとタグを設定して、リソースをグループ化し、リソースのアクセスとコストを管理できるようになりました。ユーザー定義のラベルは、OpenShift Container Platform インストールプログラムとそのコアコンポーネントによって作成されたリソースにのみ適用できます。ユーザー定義のタグは、OpenShift Container Platform Image Registry Operator で作成されたリソースにのみ適用できます。詳細は、GCP のユーザー定義のラベルとタグの管理 を参照してください。

1.3.2.11. 制限されたネットワーク内での Microsoft Azure への OpenShift Container Platform クラスターのインストール

OpenShift Container Platform 4.14 では、インストーラーがプロビジョニングしたインフラストラクチャー (IPI) およびユーザーがプロビジョニングしたインフラストラクチャー (UPI) 用に、制限されたネットワーク内の Microsoft Azure にクラスターをインストールできます。IPI の場合、既存の Azure Virtual Network (VNet) 上にインストールリリースコンテンツの内部ミラーを作成できます。UPI の場合、独自に提供するインフラストラクチャーを使用して Microsoft Azure にクラスターをインストールできます。詳細は、制限されたネットワークでの Azure へのクラスターのインストール および user-provisioned infrastructure を使用した制限されたネットワークでの Azure へのクラスターのインストール を参照してください。

1.3.2.12. バイパスデバイスエイリアスを使用したインストールディスクの指定

インストーラーがプロビジョニングしたインフラストラクチャーを使用して、ベアメタルにクラスターをインストールする場合、バイパスデバイスエイリアス (**deviceName: "/dev/disk/by-path/pci-0000:01:00.0-scsi-0:0:0:0"** など) を使用してインストールディスクを指定できるようになりました。このパラメーターは、エージェントベースのインストール中に指定することもできます。このタイプのディスクエイリアスは、再起動後も保持されます。詳細は、ベアメタル用の install-config.yaml ファイルの設定 または Agent-based インストールのルートデバイスヒントについて を参照してください。

1.3.2.13. 既存の AWS セキュリティーグループをクラスターに適用する

デフォルトでは、インストールプログラムは、セキュリティーグループを作成し、コントロールプレーンとコンピュートマシンに接続します。デフォルトのセキュリティーグループに関連付けられたルールは変更できません。

OpenShift Container Platform 4.14 では、クラスターを既存の Amazon Virtual Private Cloud (VPC) にデプロイする場合、追加の既存の AWS セキュリティーグループをコントロールプレーンとコンピュートマシンに適用できます。これらのセキュリティーグループは、クラスターのデプロイ先となる VPC に関連付ける必要があります。カスタムセキュリティーグループを適用すると、これらのマシンの受信トラフィックまたは送信トラフィックを制御する必要がある場合に、組織のセキュリティーニーズを満たすことができます。詳細は、既存の AWS セキュリティーグループのクラスターへの適用 を参照してください。

1.3.2.14. OpenShift Container Platform 4.13 から 4.14 に更新する場合に必要な管理者の承認

OpenShift Container Platform 4.14 は、非推奨の API を削除した Kubernetes 1.27 を使用します。

クラスター管理者は、クラスターを OpenShift Container Platform 4.13 から 4.14 にアップグレードする前に、手動で確認を行う必要があります。これは、OpenShift Container Platform 4.14 への更新後に、削除された API が、クラスター上で実行されている、またはクラスターと対話しているワークロード、ツール、または他のコンポーネントによって引き続き使用されている問題を防ぐ際に役立ちます。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 4.13 クラスターは、OpenShift Container Platform 4.14 に更新する前に、この管理者の承認を必要とします。

詳細は、OpenShift Container Platform 4.14 への更新の準備 を参照してください。

1.3.2.15. Nutanix の 3 ノードクラスターのサポート

3 ノードクラスターのデプロイは、OpenShift Container Platform 4.14 以降の Nutanix でサポートされています。このタイプの OpenShift Container Platform クラスターは、よりリソース効率の高いクラスターです。これは、コンピュートマシンとしても機能する 3 台のコントロールプレーンマシンのみで構成されます。詳細は、Nutanix への 3 ノードクラスターのインストール を参照してください。

1.3.2.16. Confidential 仮想マシンを使用した GCP へのクラスターのインストールが一般提供に

OpenShift Container Platform 4.14 では、Confidential 仮想マシンを使用したクラスターのインストールが一般提供になりました。現在、Confidential 仮想マシンは 64 ビット ARM アーキテクチャーではサポートされていません。詳細は、Confidential VM の有効化 を参照してください。

1.3.2.17. RHOSP のルートボリュームタイプパラメーターが利用可能に

rootVolume.types パラメーターを使用して、RHOSP で 1 つ以上のルートボリュームタイプを指定できるようになりました。このパラメーターは、コントロールプレーンとコンピュートマシンの両方で使用できます。

1.3.2.18. vSphere ノードの静的 IP アドレス

Dynamic Host Configuration Protocol (DHCP) が存在しない環境では、静的 IP アドレスを使用してブートストラップ、コントロールプレーン、およびコンピュートノードをプロビジョニングできます。

重要

vSphere ノードの静的 IP アドレスは、テクノロジープレビューのみの機能です。テクノロジープレビュー機能は、Red Hat 製品サポートのサービスレベルアグリーメント (SLA) の対象外であり、機能的に完全ではない場合があります。Red Hat は、実稼働環境でこれらを使用することを推奨していません。テクノロジープレビュー機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行い、フィードバックを提供していただくことを目的としています。

Red Hat のテクノロジープレビュー機能のサポート範囲に関する詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

静的 IP アドレスを持つノードを実行するようにクラスターをデプロイした後、これらの静的 IP アドレスのいずれかを使用するようにマシンをスケーリングできます。さらに、マシンセットを使用して、設定済みの静的 IP アドレスの 1 つを使用するようにマシンを設定できます。

詳細は、vSphere へのクラスターのインストール ドキュメントの「vSphere ノードの静的 IP アドレス」セクションを参照してください。

1.3.2.19. ベアメタルホスト CR の追加検証

ベアメタルホストのカスタムリソース (CR) に **ValidatingWebhooks** パラメーターが含まれるようになりました。このパラメーターを使用すると、ベアメタル Operator は CR を受け入れる前に設定エラーを把握し、設定エラーを含むメッセージをユーザーに返すようになりました。

1.3.2.20. AWS Local Zones にクラスターを迅速にインストールする

OpenShift Container Platform 4.14 の場合、Amazon Web Services (AWS) にクラスターをすばやくインストールして、コンピュートノードを Local Zone の場所に拡張できます。インストール設定ファイルにゾーン名を追加すると、インストールプログラムによって、各 Local Zone で必要なリソース、ネットワーク、およびコンピュートの作成が完全に自動化されます。詳細は、AWS Local Zones へのクラスターの迅速なインストール を参照してください。

1.3.2.21. クラウド認証情報を手動で維持することで、クラスターのインストールと更新のエクスペリエンスが簡素化される

このリリースには、クラウドプロバイダー認証に手動モードで Cloud Credential Operator (CCO) を使用するクラスターのインストールおよび更新のエクスペリエンスを向上させる変更が含まれています。**oc adm release extract** コマンドの次のパラメーターにより、クラウド認証情報の手動設定が簡素化されます。

--included

このパラメーターを使用して、特定のクラスター設定に必要なマニフェストのみを展開します。クラスター機能を使用して 1 つ以上のオプションコンポーネントを無効にすると、クラスターをインストールまたは更新する前に、無効になったコンポーネントの **CredentialsRequest** CR を削除する必要がなくなります。

今後のリリースでは、このパラメーターにより CCO ユーティリティー (**ccoctl**) **--enable-tech-preview** パラメーターが不要になる可能性があります。

--install-config

このパラメーターを使用して、クラスターをインストールするときに **install-config.yaml** ファイルの場所を指定します。

install-config.yaml ファイルを参照することにより、extract コマンドは、作成しようとしているクラスターのクラスター設定の側面を決定できます。**oc** は、クラスターに接続してその設定を決定できるため、クラスターの更新中にこのパラメーターは必要ありません。

この変更により、インストール先のクラウドプラットフォームを **--cloud** パラメーターで指定する必要がなくなりました。その結果、**--cloud** パラメーターは OpenShift Container Platform 4.14 以降では非推奨になります。

これらのパラメーターの使用方法を理解するには、設定のインストール手順と、手動で維持された認証情報によるクラスターの更新の準備 の手順を参照してください。

1.3.2.22. 既存の RHCOS イメージテンプレートを使用して、vSphere ホストに RHCOS を迅速にインストールする

OpenShift Container Platform 4.14 には、インストーラーがプロビジョニングしたインフラストラクチャーで使用するための新しい VMware vSphere 設定パラメーター **template** が含まれています。このパラメーターを使用すると、インストール設定ファイル内の既存の Red Hat Enterprise Linux CoreOS (RHCOS) イメージテンプレートまたは仮想マシンへの絶対パスを指定できるようになります。その後、インストールプログラムはイメージテンプレートまたは仮想マシンを使用して、vSphere ホストに RHCOS を迅速にインストールできます。

このインストール方法は、vSphere ホストに RHCOS イメージをアップロードする代替方法です。

重要

template パラメーターのパス値を設定する前に、OpenShift Container Platform リリースのデフォルトの RHCOS ブートイメージが RHCOS イメージテンプレートまたは仮想マシンのバージョンと一致していることを確認してください。そうしないと、クラスターのインストールが失敗する可能性があります。

1.3.2.23. 64-bit ARM での OpenShift Container Platform

OpenShift Container Platform 4.14 は、64 ビット ARM アーキテクチャーベースの Google Cloud Platform インストーラープロビジョニングおよびユーザーがプロビジョニングしたインフラストラクチャーでサポートされるようになりました。64 ビット ARM クラスター上で、**oc mirror** CLI プラグインの切断された環境も使用できるようになりました。インスタンスの可用性やインストールに関する詳細は、各種プラットフォームのサポートされるインストール方法 を参照してください。

1.3.2.24. Microsoft Azure クラスターのカスタム RHCOS イメージの使用

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

- **compute.platorm.azure.osImage.publisher**
- **compute.platorm.azure.osImage.offer**
- **compute.platorm.azure.osImage.sku**
- **compute.platorm.azure.osImage.version**

- **controlPlane.platorm.azure.osImage.publisher**
- **controlPlane.platorm.azure.osImage.offer**
- **controlPlane.platorm.azure.osImage.sku**
- **controlPlane.platorm.azure.osImage.version**
- **platform.azure.defaultMachinePlatform.osImage.publisher**
- **platform.azure.defaultMachinePlatform.osImage.offer**
- **platform.azure.defaultMachinePlatform.osImage.sku**
- **platform.azure.defaultMachinePlatform.osImage.version**

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

1.3.2.25. クラウドプロバイダーへのシングルノード OpenShift のインストール

OpenShift Container Platform 4.14 では、クラウドプロバイダーへのシングルノード OpenShift のインストールに対するサポートが拡張されています。シングルノード OpenShift のインストールオプションには、Amazon Web Services (AWS)、Google Cloud Platform (GCP)、および Microsoft Azure が含まれます。サポートされているプラットフォームの詳細は、シングルノード openshift でサポートされているクラウドプロバイダー を参照してください。

1.3.3. インストール後の設定

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

マルチアーキテクチャーのコンピュートマシンを備えた OpenShift Container Platform 4.14 クラスターが、Google Cloud Platform (GCP) で Day 2 操作としてサポートされるようになりました。ベアメタルインストール上のマルチアーキテクチャーコンピュートマシンを備えた OpenShift Container Platform クラスターが一般提供されるようになりました。マルチアーキテクチャーコンピュートマシンを備えたクラスターとサポートされているプラットフォームの詳細は、マルチアーキテクチャーコンピュートマシンを備えたクラスターについて を参照してください。

1.3.4. Web コンソール

1.3.4.1. 管理者パースペクティブ

今回のリリースにより、Web コンソールの **Administrator** パースペクティブに複数の更新が追加されました。これで、次のアクションを実行できるようになります。

- 正確な検索機能を使用して、リストビューまたは検索ページでリソースのリストを絞り込みます。このアクションは、類似した名前のリソースがあり、標準の検索機能では検索を絞り込めない場合に便利です。
- ツールバーの **Help** ボタンをクリックし、ドロップダウンリストから **Share Feedback** をクリックして、機能に関するフィードバックを直接提供し、バグを報告します。
- YAML エディターでツールチップを表示または非表示にします。ツールチップは保持されるため、ページに移動するたびにツールチップを変更する必要はありません。

- すべてのユーザーの Web ターミナルイメージを設定します。詳細は、Web ターミナルの設定 を参照してください。

1.3.4.1.1. 動的なプラグインの機能拡張

この更新により、カスタムメトリックダッシュボードを追加し、**QueryBowser** エクステンションを使用して、クラスターの **Overview** ページを拡張できるようになりました。OpenShift Container Platform リリースでは、エクステンションポイントが追加されているため、さまざまなタイプのモーダルの追加、アクティブな namespace の設定、カスタムエラーページの提供、動的プラグインのプロキシータイムアウトの設定が可能です。

詳細は、OpenShift Container Platform コンソール API の 動的プラグインリファレンス および **QueryBrowser** を参照してください。

1.3.4.1.2. OperatorHub でのオペレーティングシステムベースのフィルタリング

この更新により、クラスターには異種ノードが含まれる可能性があるため、OperatorHub の Operator は、ノードのオペレーティングシステムに基づいてフィルターされるようになりました。

1.3.4.1.3. Web コンソールでの特定の Operator バージョンのインストールサポート

この更新により、コンソールの **OperatorHub** ページで選択したチャネルに基づいて、Operator の利用可能なバージョンのリストから選択できるようになりました。さらに、利用可能な場合は、そのチャネルとバージョンのメタデータを表示できます。古いバージョンを選択する場合は、手動による承認更新ストラテジーが必要です。そうでない場合、Operator はすぐにチャネル上の最新バージョンに更新されます。

詳細は、Web コンソールでの Operator の特定バージョンのインストール を参照してください。

1.3.4.1.4. OperatorHub による AWS STS のサポート

このリリースでは、Amazon Web Services (AWS) クラスターが Security Token Service (STS) を使用している場合、OperatorHub はこれを検出します。検出すると、"Cluster in STS Mode" という通知が表示され、Operator をインストールする前に正しく実行されることを確認するための追加の指示が表示されます。**Operator Installation** ページも変更され、必要な **ロール ARN** フィールドが追加されます。詳細は、クラウドプロバイダー上の Operator のトークン認証 を参照してください。

1.3.4.2. Developer パースペクティブ

今回のリリースにより、Web コンソールの **Developer** パースペクティブに複数の更新が含まれるようになりました。これで、次のアクションを実行できるようになります。

- 現在のセッションで、Web ターミナルのデフォルトタイムアウト期間を変更します。詳細は、セッションの Web ターミナルタイムアウトの設定 を参照してください。
- Web コンソールの **Topology** ビュー、および Serverless Service **List** ページと **Detail** ページから Serverless 関数をテストして、CloudEvent または HTTP リクエストで Serverless 関数を使用できるようにします。
- **BuildConfigs** および Shipwright ビルドの最新ビルドのステータス、開始時間、期間を表示します。この情報は、**Details** ページでも確認できます。

1.3.4.2.1. 新しいクイックスタート

このリリースでは、Cryostat Operator のインストールや Helm チャートを使用した JBoss EAP の開始などの開発者ツールを見つけることができる新しいクイックスタートが存在します。

1.3.4.2.2. OpenShift パイプラインページの改善

OpenShift Container Platform 4.14 では、**パイプライン** ページで次のナビゲーションの改善が見られます。

- Git インポートフローにおける Pipelines as Code (PAC) の自動検出。
- サンプルカタログ内の Serverless 関数。

1.3.5. OpenShift CLI (oc)

1.3.5.1. oc-mirror を使用したカタログの multi-arch OCI ローカルイメージのサポート

OpenShift Container Platform 4.14 では、oc-mirror はカタログの multi-arch OCI ローカルイメージをサポートします。

OCI レイアウトは、ディスク上に保持されているイメージを識別する **index.json** ファイルで構成されます。この **index.json** ファイルは、任意の数の単一または multi-arch イメージを参照できます。ただし、oc-mirror は、特定の OCI レイアウトで一度に単一つのイメージのみを参照します。OCI レイアウトに格納されるイメージは、single-arch イメージ (イメージマニフェスト) または multi-arch イメージ (マニフェストリスト) のいずれかになります。

ImageSetConfiguration に OCI イメージが保存されます。カタログの処理後、カタログコンテンツには、レイアウト内のすべてのイメージのコンテンツを表す新しいレイヤーが追加されます。ImageBuilder は、single-arch イメージと multi-arch イメージの両方のイメージ更新を処理できるように変更されています。

1.3.5.2. Web ブラウザーを使用した CLI へのログイン

OpenShift Container Platform 4.14 では、新しい **oc** コマンドラインインターフェイス (CLI) フラグである **--web** が、**oc login** コマンドで使用できるようになりました。

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

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

1.3.5.3. oc new-build の機能拡張

新しい **oc** CLI フラグ、**--import-mode** が **oc new-build** コマンドに追加されました。この機能拡張により、**--import-mode** フラグを **Legacy** または **PreserverOriginal** に設定できるようになり、単一のサブマニフェストまたはすべてのマニフェストを使用して、ビルドをトリガーできるようになります。

1.3.5.4. oc new-app の機能拡張

新しい **oc** CLI フラグ、**--import-mode** が、**oc new-app** コマンドに追加されました。この機能拡張により、**--import-mode** フラグを **Legacy** または **PreserverOriginal** に設定し、続いて単一のサブマニフェストまたはすべてのマニフェストを使用して、新しいアプリケーションを作成できるようになります。

詳細は、インポートモードの設定 を参照してください。

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 4.14 と互換性を持つようになりました。インストールは、z/VM または Red Hat Enterprise Linux (RHEL) Kernel-based Virtual Machine (KVM) を使用して実行できます。インストール手順は、以下のドキュメントを参照してください。

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

重要

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

1.3.6.1. IBM Z および IBM LinuxONE の主な機能拡張

OpenShift Container Platform 4.14 以降、延長更新サポート (EUS) は 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。

OpenShift Container Platform 4.14 の IBM Z® および IBM® LinuxONE リリースでは、OpenShift Container Platform のコンポーネントと概念に、改良点と新機能が追加されました。

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

- z/VM を使用した Assisted Installer
- 単一ノードへのインストール
- Hosted Control Plane (テクノロジープレビュー)
- マルチアーキテクチャーコンピュートノード
- oc-mirror プラグイン

1.3.6.2. IBM Secure Execution

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

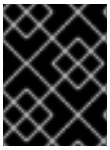
インストール手順は、以下のドキュメントを参照してください。

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

1.3.7. IBM Power

IBM Power® は OpenShift Container Platform 4.14 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 4.14 以降、延長更新サポート (EUS) は IBM Power® 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。

OpenShift Container Platform 4.14 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。

- IBM Power® Virtual Server Block CSI Driver Operator (テクノロジープレビュー)
- 単一ノードへのインストール
- Hosted Control Plane (テクノロジープレビュー)
- マルチアーキテクチャーコンピュートノード
- oc-mirror プラグイン

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

表1.1 OpenShift Container Platform の機能

機能	IBM Power®	IBM Z® および IBM® LinuxONE
代替の認証プロバイダー	サポート対象	サポート対象
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

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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
IBM Secure Execution	サポート対象外	サポート対象
IBM Power® Virtual Server Block CSI Driver Operator (テクノロジープレビュー)	サポート対象	サポート対象外
IBM Power® Virtual Server の installer-provisioned infrastructure の有効化 (テクノロジープレビュー)	サポート対象	サポート対象外
単一ノードへのインストール	サポート対象	サポート対象
IPv6	サポート対象	サポート対象
ユーザー定義プロジェクトのモニタリング	サポート対象	サポート対象
マルチアーキテクチャーコンピュートノード	サポート対象	サポート対象
マルチパス化	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
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

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

表1.2 永続ストレージのオプション

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

1. 永続共有ストレージは、Red Hat OpenShift Data Foundation またはその他のサポートされているストレージプロトコルを使用してプロビジョニングする必要があります。

2. 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
Cluster Logging Operator	サポート対象	サポート対象
Cluster Resource Override Operator	サポート対象	サポート対象
Compliance Operator	サポート対象	サポート対象
File Integrity Operator	サポート対象	サポート対象
HyperShift Operator	テクノロジープレビュー	テクノロジープレビュー
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

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

1.3.9. 認証および認可

1.3.9.1. SCC プリエンプション防止

このリリースでは、特定の Security Context Constraints (SCC) を使用するようワークロードに要求できるようになりました。特定の SCC を設定すると、必要な SCC が、クラスター内の別の SCC によってプリエンプトされるのを防ぐことができます。詳細は、特定の SCC を必要とするためのワークロードの設定 を参照してください。

1.3.9.2. Pod セキュリティーアドミッション特権 namespace

このリリースでは、次のシステム namespace が常に **privileged** Pod セキュリティーアドミッションプロファイルに設定されます。

- **default**
- **kube-public**
- **kube-system**

詳細は、特権付き namespace を参照してください。

1.3.9.3. 変更された namespace で、Pod のセキュリティーアドミッション同期が無効になる

このリリースでは、ユーザーがラベル同期された namespace で自動的にラベル付けされた値から Pod セキュリティーアドミッションラベルを手動で変更すると、そのラベルの同期は無効になります。ユーザーは、必要に応じて、同期を再度有効にすることができます。詳細は、Pod のセキュリティーアドミッション同期 namespace の除外 を参照してください。

1.3.9.4. AWS STS の OLM ベース Operator サポート

このリリースでは、Amazon Web Services (AWS) クラスター上の Operator Lifecycle Manager (OLM) によって管理される一部の Operator は、Security Token Service (STS) を使用して手動モードで Cloud Credential Operator (CCO) を使用できるようになります。これらの Operator は、クラスターの外部で管理される限定された権限の短期認証情報を使用して認証します。詳細は、クラウドプロバイダー上の Operator のトークン認証 を参照してください。

1.3.9.5. Authentication Operator は接続チェック中に noProxy を受け入れる

このリリースでは、**noProxy** フィールドが設定されており、クラスター全体のプロキシーなしでルートに到達できる場合、Authentication Operator はプロキシーをバイパスし、設定された Ingress ルートを通じて直接接続チェックを実行します。以前は、Authentication Operator は、**noProxy** 設定に関係なく、常にクラスター全体のプロキシーを介して接続チェックを実行していました。詳細は、クラスター全体のプロキシーの設定 を参照してください。

1.3.10. ネットワーク

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

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

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

1.3.10.2. OVN-Kubernetes ネットワークプラグインに対する複数の外部ゲートウェイのサポート

OVN-Kubernetes ネットワークプラグインは、特定のワークロードに対する追加のデフォルトゲートウェイの定義をサポートします。IPv4 と IPv6 の両方のアドレスファミリーがサポートされています。各デフォルトゲートウェイは、**AdminPolicyBasedExternalRoute** オブジェクトを使用して定義します。このオブジェクトでは、静的と動的の 2 種類のネクストホップを指定できます。

- 静的ネクストホップ: 外部ゲートウェイの 1 つ以上の IP アドレス
- 動的ネクストホップ: Pod を選択するための Pod と namespace セレクターの組み合わせ、および選択した Pod に以前に関連付けられたネットワークアタッチメント定義名。

定義するネクストホップは、指定する namespace セレクターによってスコープが設定されます。その後、namespace セレクターに一致する特定のワークロードに外部ゲートウェイを使用できるようになります。

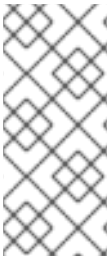
詳細は、セカンダリーネットワークインターフェイスを介した外部ゲートウェイの設定 を参照してください。

1.3.10.3. Ingress Node Firewall Operator が一般提供に

Ingress Node Firewall Operator は、OpenShift Container Platform 4.12 のテクノロジープレビュー機能に指定されました。このリリースでは、Ingress Node Firewall Operator が一般提供されました。ノードレベルでファイアウォールルールを設定できるようになりました。詳細は、Ingress Node Firewall Operator を参照してください。

1.3.10.4. OVS 用の予約されていない CPU の動的使用

このリリースでは、Open vSwitch (OVS) ネットワークスタックが、予約されていない CPU を動的に使用できるようになりました。予約されていない CPU のこの動的な使用は、パフォーマンスプロファイルが適用されているマシン config プール内のノードでデフォルトで発生します。利用可能な予約されていない CPU を動的に使用することで、OVS のコンピュートリソースが最大化され、需要が高い期間のワークロードのネットワーク遅延が最小限に抑えられます。OVS は、**Guaranteed** QoS Pod 内のコンテナーに割り当てられた分離された CPU を動的に使用できないままとなります。この分離により、重要なアプリケーションのワークロードの中断が回避されます。



注記

Node Tuning Operator が、予約されていない CPU の使用をアクティブにするパフォーマンス条件を認識すると、OVN-Kubernetes が CPU 上で実行されている OVS デーモンの CPU アフィニティー調整を設定する間に数秒の遅延が発生します。この期間中に、**Guaranteed** QoS Pod が開始されると、遅延スパイクが発生する可能性があります。

1.3.10.5. 複数の IP アドレスに対するデュアルスタック設定

Whereabouts IPAM CNI プラグインの以前のリリースでは、ネットワークインターフェイスごとに 1 つの IP アドレスのみを割り当てることができました。

現在、Whereabouts は、デュアルスタック IPv4/IPv6 機能をサポートするために、任意の数の IP アドレスの割り当てをサポートしています。デュアルスタック IP アドレスを動的に割り当てるための設定の作成 を参照してください。

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

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

たとえば、シナリオによっては、単一 NUMA ノード上の Pod の CPU およびメモリーリソースを最大化することが優先されます。Topology Manager に Pod の SR-IOV ネットワークリソースの NUMA ノードに関するヒントを提供しないことで、Topology Manager は SR-IOV ネットワークリソースと Pod の CPU およびメモリーリソースを異なる NUMA ノードにデプロイできます。以前の OpenShift Container Platform リリースでは、Topology Manager はすべてのリソースを同じ NUMA ノードに配置しようとしていました。

NUMA 対応の Pod スケジューリングにおける、より柔軟な SR-IOV ネットワークデプロイメントの詳細は、NUMA 対応スケジューリング用 SR-IOV ネットワークトポロジーの除外 を参照してください。

1.3.10.7. HAProxy 2.6 への更新

このリリースでは、OpenShift Container Platform が HAProxy 2.6 に更新されました。

1.3.10.8. Ingress コントローラーでのサイドカーロギングによる最大長の設定のサポート

以前は、Ingress コントローラーの syslog メッセージの最大長は 1024 バイトでした。現在は、最大値を増やすことができるようになりました。詳細は、サイドカーの使用時に Ingress コントローラーによる HAProxy ログの長さの変更を許可する を参照してください。

1.3.10.9. NMstate Operator がコンソールで更新される

このリリースでは、NMstate Operator と、**NodeNetworkState** (NNS)、**NodeNetworkConfigurationPolicy** (NNCP)、および **NodeNetworkConfigurationEnhancement** (NNCE) などのリソースに、Web コンソールからアクセスできるようになりました。**Networking** ページのコンソールの **Administrator** パースペクティブでは、**NodeNetworkConfigurationPolicy** ページの NNCP と NNCE に、そして **NodeNetworkState** ページの NNS にアクセスできます。NMState リソースの詳細と、コンソールでこれを更新する方法の詳細は、ノードネットワーク設定の更新 を参照してください。

1.3.10.10. IBM Cloud 上の IPsec に対する OVN-Kubernetes ネットワークプラグインのサポート

IPsec は、OpenShift Container Platform 4.14 のデフォルトである OVN-Kubernetes ネットワークプラグインを使用するクラスターの IBM Cloud 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、IPsec 暗号化の設定 を参照してください。

1.3.10.11. 外部トラフィックの IPsec 暗号化に対する OVN-Kubernetes ネットワークプラグインのサポート (テクノロジープレビュー)

OpenShift Container Platform は、**north-south トラフィック** とも呼ばれる外部トラフィックの暗号化をサポートするようになりました。IPsec は、**east-west トラフィック** と呼ばれる Pod 間のネットワークトラフィックの暗号化を、すでにサポートしています。両方の機能を組み合わせて使用すると、OpenShift Container Platform クラスターに完全な転送中の暗号化を提供できます。これはテクノロジープレビュー機能として利用できます。

この機能を使用するには、使用するネットワークインフラストラクチャーに合わせて調整された IPsec 設定を定義する必要があります。詳細は、外部 IPsec エンドポイントの IPsec 暗号化の有効化 を参照してください。

1.3.10.12. Kubernetes NMstate のシングルスタック IPv6 サポート

このリリースでは、シングルスタック IPv6 クラスターで Kubernetes NMState Operator を使用できるようになりました。

1.3.10.13. ロードバランサーの背後にある Pod の Egress トラフィックを管理するための Egress サービスリソース (テクノロジープレビュー)

この更新により、**EgressService** カスタムリソース (CR) を使用して、ロードバランサーサービスの背後にある Pod の Egress トラフィックを管理できるようになりました。これはテクノロジープレビュー機能として利用できます。

EgressService CR を使用して、次の方法で Egress トラフィックを管理できます。

- ロードバランサーサービスの IP アドレスを、ロードバランサーサービスの背後にある Pod の Egress トラフィックの送信元 IP アドレスとして割り当てます。
- ロードバランサーの背後にある Pod の Egress トラフィックを、デフォルトノードネットワークとは異なるネットワークに割り当てます。

詳細は、egress サービスの設定 を参照してください。

1.3.10.14. MetalLB の BGPPeer リソースの VRF 仕様 (テクノロジープレビュー)

この更新により、**BGPPeer** カスタムリソースで、仮想ルーティングおよび転送 (VRF) インスタンスを指定できるようになりました。MetalLB は、VRF に属するインターフェイスを通じてサービスをアドバタイズできます。これはテクノロジープレビュー機能として利用できます。詳細は、ネットワーク VRF を介したサービスの公開 を参照してください。

1.3.10.15. NMState の NodeNetworkConfigurationPolicy リソースの VRF 仕様 (テクノロジープレビュー)

この更新により、**NodeNetworkConfigurationPolicy** カスタムリソースを使用して、仮想ルーティングおよび転送 (VRF) インスタンスをネットワークインターフェイスに関連付けることができます。VRF インスタンスをネットワークインターフェイスに関連付けることにより、トラフィックの分離、独立し

たルーティングの決定、およびネットワークリソースの論理的な分離をサポートできます。この機能は、テクノロジープレビューとしてのみ利用できます。詳細は、例: VRF インスタンスノードのネットワーク設定ポリシーを使用したネットワークインターフェイス を参照してください。

1.3.10.16. Broadcom BCM57504 のサポートが一般提供に

Broadcom BCM57504 ネットワークインターフェイスコントローラーのサポートが、SR-IOV Network Operator で利用できるようになりました。詳細は、サポートされるデバイス を参照してください。

1.3.10.17. OVN-Kubernetes はセカンダリーネットワークとして利用可能

このリリースでは、Red Hat OpenShift Networking OVN-Kubernetes ネットワークプラグインで、Pod のセカンダリーネットワークインターフェイスを設定できます。OVN-Kubernetes は、セカンダリーネットワークとして、レイヤー 2 スイッチおよび localnet スイッチトポロジーネットワークの両方をサポートします。セカンダリーネットワークとしての OVN-Kubernetes の詳細は、OVN-Kubernetes 追加ネットワークの設定 を参照してください。

1.3.10.18. OVN-Kubernetes ベースのクラスターデプロイメントではグローバル IP 転送が無効になっています。

このリリース以降、OVN-Kubernetes ベースのクラスターデプロイメントでグローバル IP アドレス転送が無効になります。これは、ルーターとして機能するノードによる、クラスター管理者にとって望ましくない影響を防ぐためです。OVN-Kubernetes では、マネージドインターフェイスごとに転送を有効化および制限できるようになりました。

Network リソースの **gatewayConfig.ipForwarding** 仕様を使用して、OVN-Kubernetes マネージドインターフェイス上のすべてのトラフィックの IP 転送を制御できます。OVN-Kubernetes に関連するすべてのトラフィックのみを転送するには、**Restricted** を指定します。すべての IP トラフィックの転送を許可するには、**Global** を指定します。新規インストールの場合、デフォルトは **Restricted** です。4.14 にアップグレードされたクラスターはこの変更の影響を受けません。IP 転送の動作は変更されず、引き続きグローバルに有効になります。IP 転送をグローバルに有効にする方法の詳細は、IP 転送をグローバルに有効にする を参照してください。

1.3.10.19. 管理ネットワークポリシー (テクノロジープレビュー)

管理ネットワークポリシーは、テクノロジープレビュー機能として利用できます。OVN-Kubernetes CNI プラグインを実行しているクラスターで、Network Policy V2 API に含まれる **AdminNetworkPolicy** リソースと **BaselineAdminNetworkPolicy** リソースを有効化できます。クラスター管理者は、namespace が作成される前に、クラスター範囲のポリシーと保護措置をクラスター全体に適用できます。ネットワーク管理者は、ユーザーが上書きできないネットワークトラフィック制御を強制することで、クラスターを保護できます。ネットワーク管理者は、必要に応じて、クラスター内のユーザーが上書きできる任意のベースラインネットワークトラフィック制御を強制できます。現在、これらの API はクラスター内トラフィックのポリシーの表現のみをサポートしています。

1.3.10.20. Pod の MAC-VLAN、IP-VLAN、および VLAN サブインターフェイスの作成

このリリースでは、コンテナー namespace 内のマスターインターフェイスに基づいて MAC-VLAN、IP-VLAN、および VLAN サブインターフェイスを作成する機能が一般提供になりました。この機能を使用すると、別のネットワークアタッチメント定義で、Pod ネットワーク設定の一部としてマスターインターフェイスを作成できます。これにより、ノードのネットワーク設定を知らなくても、このインターフェイスに基づいて VLAN、MACVLAN、または IPVLAN を作成できます。詳細は、コンテナーネットワーク namespace でのマスターインターフェイスの設定について を参照してください。

1.3.10.21. all-multicast モードのサポート

OpenShift Container Platform リリースでは、チューニング CNI プラグインを使用した all-multicast モードの設定がサポートされるようになりました。この更新により、Pod の Security Context Constraints (SCC) に **NET_ADMIN** 機能を付与する必要がなくなり、Pod の潜在的な脆弱性を最小限に抑えてセキュリティーが強化されます。

all-multicast モードの詳細は、all-multicast モードについて を参照してください。

1.3.10.22. TAP デバイスプラグインを使用してネットワークの柔軟性を強化する

このリリースでは、新しい Container Network Interface (CNI) ネットワークプラグインタイプである TAP デバイスプラグインが導入されています。このプラグインを使用すると、コンテナー内に TAP デバイスを作成できます。これにより、ユーザー空間プログラムがネットワークフレームを処理し、従来のネットワークインターフェイスを介する代わりに、ユーザー空間アプリケーションとの間でフレームを送受信するインターフェイスとして機能できるようになります。詳細は、TAP 追加ネットワークの設定 を参照してください。

1.3.10.23. TAP CNI プラグインを使用した、カーネルアクセスによるルートレス DPDK ワークロードの実行のサポート

OpenShift Container Platform バージョン 4.14 以降では、カーネルにトラフィックを注入する必要がある DPDK アプリケーションは、TAP CNI プラグインを利用して非特権 Pod で実行できます。詳細は、TAP CNI を使用してカーネルアクセスでルートレス DPDK ワークロードを実行する を参照してください。

1.3.10.24. Ingress コントローラーまたは Route オブジェクトを使用して特定の HTTP ヘッダーを設定または削除する

特定の HTTP リクエストおよびレスポンスヘッダーは、Ingress コントローラーを使用してグローバルに、または特定のルートに対して、設定または削除できるようになりました。次のヘッダーを設定または削除できます。

- X-Frame-Options
- X-Cache-Info
- X-XSS-Protection
- X-Source
- X-SSL-Client-Cert
- X-Target
- Content-Location
- Content-Language

詳細は、Ingress コントローラーでの HTTP 要求ヘッダーと応答ヘッダーの設定または削除 および ルートでの HTTP 要求ヘッダーと応答ヘッダーの設定または削除 を参照してください。

1.3.10.25. 追加のネットワークインターフェイス上の Egress IP が一般提供になる

追加のネットワークインターフェイスで Egress IP アドレスを使用できる機能が一般提供になりました。この機能により、OpenShift Container Platform 管理者は、ルーティング、アドレス指定、セグメンテーション、セキュリティーポリシーなどのネットワーク側面をより高度に制御できるようになりま

す。トラフィックのセグメント化や特殊な要件を満たすなどの目的で、ワークロードトラフィックを特定のネットワークインターフェイス経由でルーティングすることもできます。

詳細は、追加のネットワークインターフェイスで Egress IP を使用する場合の考慮事項 を参照してください。

1.3.10.26. 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

この更新により、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。

1.3.11. レジストリー

1.3.11.1. オプションの Image Registry Operator

このリリースでは、Image Registry Operator がオプションのコンポーネントになりました。この機能は、Image Registry Operator が必要ない場合に、通信環境における OpenShift Container Platform の全体的なリソースフットプリントを削減する際に役立ちます。Image Registry Operator の無効化の詳細は、クラスター機能の選択 を参照してください。

1.3.12. ストレージ

1.3.12.1. LVMS での OR ロジックのサポート

このリリースでは、論理ボリュームマネージャー (LVM) クラスターのカスタムリソース (CR) が、**deviceSelector** 設定で **OR** ロジックを提供します。以前のリリースでは、デバイスパスの **paths** 設定の指定には、**AND** ロジックのみが使用されていました。このリリースでは、**OR** ロジックをサポートする **optionalPaths** 設定を指定することもできます。詳細は、論理ボリュームマネージャーストレージを使用した永続ストレージ の CR の例を参照してください。

1.3.12.2. LVMS での ext4 のサポート

このリリースでは、論理ボリュームマネージャー (LVM) クラスターのカスタムリソース (CR) が、**deviceClasses** の下の **fstype** 設定を持つ **ext4** ファイルシステムのサポートを提供します。デフォルトのファイルシステムは **xfs** です。詳細は、論理ボリュームマネージャーストレージを使用した永続ストレージ の CR の例を参照してください。

1.3.12.3. 標準化された STS 設定ワークフロー

OpenShift Container Platform 4.14 は、AWS Elastic File Storage (EFS) Container Storage Interface (CSI) Driver Operator を使用して、Security Token Service (STS) を設定するための合理化および標準化された手順を提供します。

詳細は、Security Token Service のロール Amazon リソースネームの取得 を参照してください。

1.3.12.4. Read Write Once Pod アクセスモード (テクノロジープレビュー)

OpenShift Container Platform 4.14 では、ReadWriteOncePod (RWOP) と呼ばれる永続ボリューム (PV) および永続ボリューム要求 (PVC) の新しいアクセスモードが導入されています。これは、単一ノード上の単一 Pod でのみ使用できます。これは、シングルノード上で多数の Pod によって PV または PVC を使用できる既存の ReadWriteOnce アクセスモードと比較されます。これはテクノロジープレビュー機能として利用できます。

詳細は、アクセスモード を参照してください。

1.3.12.5. GCP Filestore ストレージ CSI Driver Operator が一般提供に

OpenShift Container Platform は、Google Compute Platform (GCP) Filestore Storage の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。GCP Filestore CSI Driver Operator は、OpenShift Container Platform 4.12 に導入され、テクノロジープレビュー機能としてサポートされていました。GCP Filestore CSI Driver Operator は現在、一般提供されています。詳細は、Google Compute Platform Filestore CSI Driver Operator を参照してください。

1.3.12.6. VMware vSphere の自動 CSI 移行

VMware vSphere の自動 CSI 移行機能は、in-tree オブジェクトを対応する CSI 表現に自動的に変換します。理想的には、ユーザーに対して完全に透過的である必要があります。in-tree ストレージプラグインを参照するストレージクラスは引き続き機能しますが、デフォルトのストレージクラスを CSI ストレージクラスに切り替えることを検討してください。

OpenShift Container Platform 4.14 では、vSphere の CSI 移行はあらゆる状況においてデフォルトで有効になっており、管理者によるアクションは必要ありません。

ただし、vSphere in-tree 永続ボリューム (PV) を使用していて、OpenShift Container Platform 4.12 または 4.13 から 4.14 にアップグレードする場合は、vSphere vCenter および ESXI ホストを 7.0 Update 3L または 8.0 Update 2 に更新します。更新しない場合、OpenShift Container Platform のアップグレードがブロックされます。vSphere を更新したくない場合は、管理者承認を実行して、OpenShift Container Platform のアップグレードを続行できます。ただし、管理者承認を使用すると、既知の問題が発生する可能性があります。管理者承認に進む前に、こちらの ナレッジベースの記事 をよくお読みください。

詳細は、CSI 自動移行 を参照してください。

1.3.12.7. Secrets Store CSI ドライバー Operator (テクノロジープレビュー)

Secrets Store Container Storage Interface (CSI) Driver Operator である **secrets-store.csi.k8s.io** を使用すると、OpenShift Container Platform がエンタープライズグレードの外部シークレットストアに保存されている複数のシークレット、キー、証明書をインラインの一時ボリュームとして Pod にマウントできます。Secrets Store CSI Driver Operator は、gRPC を使用してプロバイダーと通信し、指定された外部シークレットストアからマウントコンテンツを取得します。ボリュームがアタッチされると、その中のデータがコンテナーのファイルシステムにマウントされます。これはテクノロジープレビュー機能として利用できます。Secrets Store CSI Driver の詳細は、Secrets Store CSI Driver を参照してください。

Secrets Store CSI Driver Operator を使用して外部シークレットストアから CSI ボリュームにシークレットをマウントする方法は、外部シークレットストアを使用した機密データの Pod への提供 を参照してください。

1.3.12.8. NFS をサポートする Azure File が一般提供に

OpenShift Container Platform 4.14 は、一般提供として Network File System (NFS) を備えた Azure File Container Storage Interface (CSI) Driver Operator をサポートします。

詳細は、NFS サポート を参照してください。

1.3.13. Oracle® クラウドインフラストラクチャー

Assisted Installer またはエージェントベースのインストーラーを使用して、Oracle® Cloud Infrastructure (OCI) に OpenShift Container Platform クラスターをインストールできるようになりました。OCI に OpenShift Container Platform クラスターをインストールするには、次のインストールオプションのいずれかを選択します。

- Assisted Installer を使用した Oracle® Cloud Infrastructure (OCI) へのクラスターのインストール
- エージェントベースのインストーラーを使用した Oracle® Cloud Infrastructure (OCI) へのクラスターのインストール

1.3.14. Operator ライフサイクル

1.3.14.1. Operator Lifecycle Manager (OLM) 1.0 (テクノロジープレビュー)

Operator Lifecycle Manager (OLM) は、最初のリリースから OpenShift Container Platform 4 に含まれています。OpenShift Container Platform 4.14 では、OLM の次世代イテレーションのためのコンポーネントがテクノロジープレビュー機能として導入されており、このフェーズでは **OLM 1.0** として知られています。この更新されたフレームワークは、OLM の以前のバージョンの一部であった概念の多くを進化させ、新しい機能を追加します。

OpenShift Container Platform 4.14 の OLM 1.0 のテクノロジープレビューフェーズ中に、管理者は以下の機能を試すことができます。

GitOps ワークフローをサポートする完全な宣言型モデル

OLM 1.0 は、次の 2 つの主要な API を通じて Operator 管理を簡素化します。

- 新しい Operator Controller コンポーネントによって **operators.operators.operatorframework.io** として提供される新しい **Operator** 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、インストールされた Operator の管理を合理化します。これにより、管理者と SRE は、GitOps 原則を使用してプロセスを自動化し、望ましい状態を定義できるようになります。
- 新しい catalogd コンポーネントによって提供される **Catalog** API は、OLM 1.0 の基盤として機能し、クラスター上のクライアント用にカタログを展開して、ユーザーが Operator や Kubernetes エクステンションなどのインストール可能なコンテンツを検出できるようにします。これにより、詳細、チャネル、更新エッジなど、利用可能なすべての Operator バンドルバージョンの可視性が向上します。

詳細は、Operator Controller と Catalogd を参照してください。

Operator 更新に対する制御の向上

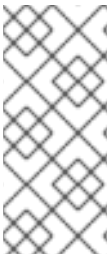
カタログの内容に対する洞察が向上したため、管理者はインストールと更新のターゲットバージョンを指定できます。これにより、管理者は Operator 更新のターゲットバージョンをより詳細に制御できるようになります。詳細は、カタログからの Operator のインストール を参照してください。

柔軟な Operator パッケージ形式

管理者は、ファイルベースのカタログを使用して、次のタイプのコンテンツをインストールおよび管理できます。

- 既存の OLM エクスペリエンスと同様の OLM ベースの Operator
- **プレーンバンドル** (任意の Kubernetes マニフェストの静的コレクション)

さらに、バンドルサイズは etcd 値のサイズ制限によって制限されなくなりました。詳細は、OLM 1.0 でのプレーンバンドルの管理 を参照してください。



注記

OpenShift Container Platform 4.14 の場合、OLM 1.0 の文書化された手順は CLI ベースのみになります。別の方法として、管理者は、**Import YAML** ページや **Search** ページなどの通常の方法を使用して、Web コンソールで関連オブジェクトを作成および表示することもできます。ただし、既存の **OperatorHub** および **Installed Operators** ページでは、OLM 1.0 コンポーネントはまだ表示されません。

詳細は、Operator Lifecycle Manager 1.0 について を参照してください。

1.3.15. Operator の開発

1.3.15.1. クラウドプロバイダー上の Operator のトークン認証: AWS STS

このリリースでは、Operator Lifecycle Manager (OLM) によって管理される Operator は、Security Token Service (STS) を使用する Amazon Web Services (AWS) クラスター上で実行する際のトークン認証をサポートできるようになりました。Cloud Credential Operator (CCO) は、Operator の作成者が Operator による AWS STS のサポートを有効にしている場合、特定の権限が限定された短期認証情報のプロビジョニングを半自動化するように更新されています。OLM ベースの Operator を有効化して、AWS STS で CCO ベースのワークフローをサポートする方法の詳細は、クラウドプロバイダー上の Operator のトークン認証 を参照してください。

1.3.15.2. 複数のプラットフォームをサポートする Operator プロジェクトの設定

このリリースでは、Operator の作成者は、複数のアーキテクチャーとオペレーティングシステム、または **プラットフォーム** をサポートするように Operator プロジェクトを設定できます。Operator の作成者は、次のアクションを実行して、複数のプラットフォームのサポートを設定できます。

- Operator がサポートするプラットフォームを指定するマニフェストリストをビルドします。
- マルチアーキテクチャーのコンピュートマシンをサポートするように Operator のノードアフィニティーを設定します。

詳細は、マルチプラットフォームサポートのための Operator プロジェクトの設定 を参照してください。

1.3.16. Builds

- 今回の更新により、Source-to-Image (S2I) ツールが OpenShift Container Platform 4.14 で一般提供されるようになりました。S2I ツールを使用すると、ソースコードからコンテナーイメージをビルドし、アプリケーションコードをすぐにデプロイできるコンテナーイメージに変換できます。この機能により、再現可能なコンテナー化されたアプリケーション開発をサポートするプラットフォームの機能が強化されます。詳細は、Source-to-Image (S2I) ツールの使用 を参照してください。

- この更新により、Build CSI Volumes 機能が OpenShift Container Platform 4.14 で一般提供されるようになりました。

1.3.17. Machine Config Operator

1.3.17.1. レジストリー認証局の処理

Machine Config Operator は、イメージレジストリーの認証局の配布を処理するようになりました。この変更によるエンドユーザーへの影響はありません。

1.3.17.2. Prometheus で利用可能な追加のメトリクス

このリリースでは、追加のメトリクスをクエリーして、マシンとマシン config プールの状態をより詳しく監視できるようになりました。

Prometheus の使用方法に関する詳細は、利用可能なメトリクスのリストの表示 を参照してください。

1.3.17.3. オフライン Tang プロビジョニングのサポート

このリリースでは、初回起動時にアクセスできない Tang サーバーを使用し、Tang が有効化された Network-Bound Disk Encryption (NBDE) を使用して、OpenShift Container Platform クラスターをプロビジョニングできるようになりました。

詳細は、暗号化しきい値の設定 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。

1.3.17.4. 証明書が Machine Config Daemon によって処理されるようになる

以前の OpenShift Container Platform バージョンでは、MCO はマシン設定ファイルから証明書を直接読み取り、処理していました。これにより、ローテーションの問題が発生し、証明書が一時停止したマシン config プールの背後でスタックされるなど、望ましくない状況が発生しました。

このリリースでは、証明書はブートストラップからマシン設定ファイルにテンプレート化されなくなりました。代わりに、これらは Ignition オブジェクトに直接置かれ、コントローラー config を使用してディスクに書き込まれ、通常のクラスター操作中に Machine Config Daemon (MCD) によって処理されます。その後、**ControllerConfig** リソースを使用して、証明書を表示できるようになります。

Machine Config Controller (MCC) は、次の証明書データを保持します。

- **/etc/kubernetes/kubelet-ca.crt**
- **/etc/kubernetes/static-pod-resources/configmaps/cloud-config/ca-bundle.pem**
- **/etc/pki/ca-trust/source/anchors/openshift-config-user-ca-bundle.crt**

MCC は、イメージレジストリー証明書とそれに関連するユーザーバンドル証明書も処理します。これは、証明書がマシン config プールのステータスにバインドされず、よりタイムリーにローテーションされることを意味します。マシン設定ファイルに保存されている以前にリストされた CA は削除され、クラスターのインストール中に見つかったテンプレート化されたファイルは存在しなくなります。これらの証明書にアクセスする方法の詳細は、証明書の表示と操作 を参照してください。

1.3.18. マシン API

1.3.18.1. Nutanix クラスターでのコントロールプレーンマシンセットのサポート

このリリースでは、Nutanix クラスターでコントロールプレーンマシンセットがサポートされています。詳細は、Control Plane Machine Set Operator のスタートガイド を参照してください。

1.3.18.2. RHOSP クラスター上のコントロールプレーンマシンセットへのサポート

このリリースでは、RHOSP 上で実行されるクラスターでコントロールプレーンマシンセットがサポートされます。

詳細は、Control Plane Machine Set Operator のスタートガイド を参照してください。

注記

ルートボリュームのアベイラビリティーゾーンがあり、4.14 にアップグレードする RHOSP で実行されているクラスターの場合、コントロールプレーンマシンセットを有効にする前に、コントロールプレーンマシンを 1 つのサーバーグループに統合する必要があります。必要な変更を加えるには、OpenShift on OpenStack with Availability Zones: Invalid Compute ServerGroup setup during OpenShift deployment の手順に従ってください。

少なくとも 1 つのゾーンで設定されたコンピュートゾーンがあり、バージョン 4.14 にアップグレード可能な RHOSP 上で実行されているクラスターの場合、ルートボリュームも少なくとも 1 つのゾーンで設定する必要があります。この設定変更が行われない場合、クラスター用のコントロールプレーンマシンセットを生成できません。必要な変更を加えるには、関連する OpenShift on OpenStack with compute Availability Zones: Missing rootVolume availability zone の手順に従ってください。

1.3.18.3. AWS マシンの配置グループへの割り当てのサポート

このリリースにより、既存の AWS 配置グループ内にマシンをデプロイするようにマシンセットを設定できるようになりました。この機能を Elastic Fabric Adapter (EFA) インスタンスで使用すると、指定した配置グループ内のマシンのネットワークパフォーマンスを向上させることができます。この機能は、コンピュート と コントロールプレーン のマシンセットで使用できます。

1.3.18.4. Azure Confidential VM と信頼された起動 (テクノロジープレビュー)

このリリースでは、Azure Confidential VM、トラステッド起動、またはその両方を使用するマシンをデプロイするように、マシンセットを設定できるようになりました。これらのマシンは、セキュアブートや専用の virtual Trusted Platform Module (vTPM) インスタンスなどの Unified Extensible Firmware Interface (UEFI) セキュリティー機能を使用できます。

この機能は、コンピュート と コントロールプレーン のマシンセットで使用できます。

1.3.19. Nodes

1.3.19.1. 大規模クラスターの descheduler リソース制限

このリリースでは、descheduler オペランドのリソース制限が削除されました。これにより、メモリー不足エラーによって失敗することなく、多くのノードと Pod を含む大規模なクラスターに対して、descheduler を使用できるようになります。

1.3.19.2. Pod トポロジーの分散制約 matchLabelKeys パラメーターが一般提供に

Pod トポロジー分散制約を設定するための **matchLabelKeys** パラメーターが、OpenShift Container Platform 4.14 で一般提供されるようになりました。以前は、**TechPreviewNoUpgrade** 機能セットを有

効にすることで、パラメーターをテクノロジープレビュー機能として利用できました。**matchLabelKeys** パラメーターは、Pod ラベルキーのリストを取得して、分散を計算する Pod を選択します。

詳細は、Pod トポロジー分散制約を使用した Pod 配置の制御 を参照してください。

1.3.19.3. MaxUnavailableStatefulSet の有効化 (テクノロジープレビュー)

このリリースでは、**TechPreviewNoUpgrade** 機能セットを有効にすることで、**MaxUnavailableStatefulSet** 機能セット設定パラメーターがテクノロジープレビュー機能として利用できるようになります。更新中に使用できなくなる **StatefulSet** Pod の最大数を定義できるようになりました。これにより、アップグレード時のアプリケーションのダウンタイムが短縮されます。

詳細は、フィーチャーゲートについて を参照してください。

1.3.19.4. Pod Disruption Budget (PDB) の正常でない Pod エビクションポリシー。

このリリースでは、Pod Disruption Budget (PDB) に対する異常な Pod エビクションポリシーの指定が、OpenShift Container Platform で一般提供され、**TechPreviewNoUpgrade** featureSet から削除されました。これは、ノードドレイン中に誤動作しているアプリケーションを排除するのに役立ちます。

詳細は、異常な Pod のエビクションポリシーの指定 を参照してください。

1.3.19.5. Linux Control Groups バージョン 2 がデフォルトに

OpenShift Container Platform 4.14 以降、新規インストールではデフォルトで Control Groups バージョン 2 (cgroup v2、cgroup2、または cgroupsv2 とも呼ばれる) が使用されます。この機能拡張には、多くのバグ修正、パフォーマンスの向上、新機能との統合機能が含まれています。cgroup v1 は、初期インストール日が OpenShift Container Platform 4.14 より前の、アップグレードされたクラスターで引き続き使用されています。cgroup v1 は、**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、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。

1.3.19.6. cron ジョブのタイムゾーンの一般提供

cron ジョブスケジュールのタイムゾーンの設定が一般提供されるようになりました。タイムゾーンが指定されていない場合、Kubernetes コントローラーマネージャーは、ローカルタイムゾーンを基準にしてスケジュールを解釈します。

詳細は、cron ジョブの作成 を参照してください。

1.3.20. モニタリング

このリリースの監視スタックには、次の新機能および変更された機能が含まれています。

1.3.20.1. モニタリングスタックコンポーネントおよび依存関係の更新

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

- **kube-state-metrics** to 2.9.2
- **node-exporter** to 1.6.1

- **prom-label-proxy** to 0.7.0
- Prometheus to 2.46.0
- **prometheus-operator** to 0.67.1

1.3.20.2. 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。

- New
  - デプロイメントのロールアウトが 15 分間進行していないかどうかを監視する **KubeDeploymentRolloutStuck** アラートを追加しました。
  - ノード上のリソースの飽和状態を監視するための **NodeSystemSaturation** アラートを追加しました。
  - ノード上の systemd サービスを監視するための **NodeSystemdServiceFailed** アラートを追加しました。
  - ノード上のメジャーページフォールトを監視するための **NodeMemoryMajorPagesFaults** アラートを追加しました。
  - 失敗した Prometheus サービス検出を監視するための **PrometheusSDRefreshFailure** アラートを追加しました。
- **変更済み**
  - **apiserver** ジョブからのメトリクスのみを評価するように、**KubeAggregatedAPIDown** アラートと **KubeAggregatedAPIErrors** アラートを変更しました。
  - **kube-state-metrics** ジョブからのメトリクスのみを評価するように、**KubeCPUOvercommit** アラートを変更しました。
  - **node-exporter** ジョブからのメトリクスのみを評価するように、**NodeHighNumberConntrackEntriesUsed**、**NodeNetworkReceiveErrs**、および **NodeNetworkTransmitErrs** アラートを変更しました。
- **削除済み**
  - 実行可能でない **MultipleContainersOOMKilled** アラートを削除しました。メモリー不足に陥っているノードは、他のアラートによってカバーされます。

1.3.20.3. コアプラットフォームのメトリクスに基づいてアラートを作成する新しいオプション

管理者はこのリリースにより、コアプラットフォームのメトリクスに基づいて、新しいアラートルールを作成できます。しきい値を調整したりラベルを変更したりして、既存のプラットフォームアラートルールの設定を変更できるようになりました。また、**openshift-monitoring** namespace のコアプラットフォームメトリクスに基づいてクエリー式を構築することで、新しいカスタムアラートルールを定義および追加することもできます。この機能は、OpenShift Container Platform 4.12 リリースではテクノ

ロジープレビューとして含まれていましたが、現在は、OpenShift Container Platform 4.14 で一般提供されています。詳細は、コアプラットフォームモニタリングのアラートルールの管理 を参照してください。

1.3.20.4. すべての監視コンポーネントのリソース制限を指定する新しいオプション

このリリースでは、以下を含むすべての監視コンポーネントのリソース要求と制限を指定できるようになりました。

- Alertmanager
- **kube-state-metrics**
- **monitoring-plugin**
- **node-exporter**
- **openshift-state-metrics**
- Prometheus
- Prometheus アダプター
- Prometheus Operator とそのアドミッション Webhook サービス
- Telemeter クライアント
- Thanos Querier
- Thanos Ruler

OpenShift Container Platform の以前のバージョンでは、Prometheus、Alertmanager、Thanos Querier、および Thanos Ruler のオプションのみを設定できました。

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

このリリースでは、追加の **node-exporter** コレクターの Cluster Monitoring Operator (CMO) config map 設定をカスタマイズできます。次の **node-exporter** コレクターはオプションになり、config map 設定で、それぞれを個別に有効または無効にできます。

- **ksmd** コレクター
- **mountstats** コレクター
- **processes** コレクター
- **systemd** コレクター

さらに、**netdev** および **netclass** コレクターの関連コレクター設定から、ネットワークデバイスを除外できるようになりました。また、**maxProcs** オプションを使用して、node-exporter を実行できるプロセスの最大数を設定できるようになりました。

1.3.20.6. 監視 Web コンソールプラグインリソースをデプロイするための新しいオプション

このリリースでは、OpenShift Container Platform Web コンソールの **Observe** セクションのモニタリングページが、動的プラグイン としてデプロイされます。この変更により、Cluster Monitoring

Operator (CMO) が、OpenShift Container Platform Web コンソール監視プラグインリソースをデプロイするコンポーネントになりました。CMO 設定を使用して、コンソール監視プラグインリソースの次の機能を設定できるようになりました。

- ノードセレクター
- toleration
- トポロジー分散制約
- リソース要求
- リソース制限

1.3.21. 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。

1.3.22. スケーラビリティーおよびパフォーマンス

1.3.22.1. PAO の must-gather イメージがデフォルトの must-gather イメージに追加される

このリリースでは、Performance Addon Operator (PAO) の must-gather イメージは、低遅延チューニングに関連するデバッグデータをキャプチャーするための **must-gather** コマンドの引数として必要とされなくなりました。PAO must-gather イメージの機能は、イメージ引数なしで **must-gather** コマンドによって使用されるデフォルトのプラグインイメージの下に置かれるようになりました。低遅延チューニングに関連するデバッグ情報の収集の詳細は、Red Hat Support 用の低遅延チューニングデバッグデータの収集 を参照してください。

1.3.22.2. Operator の must-gather イメージを使用した NUMA Resources Operator のデータの収集

このリリースでは、Operator の **must-gather** イメージを使用して NUMA Resources Operator のデータを収集するように、**must-gather** ツールが更新されました。NUMA Resources Operator のデバッグ情報の収集に関する詳細は、NUMA Resources Operator データの収集 を参照してください。

1.3.22.3. 各 Pod の C ステートをより詳細に制御できるようにする

このリリースでは、Pod の C ステートをより詳細に制御できるようになりました。C ステートを完全に無効にする代わりに、C ステートの最大遅延をマイクロ秒単位で指定できるようになりました。このオプションは、**cpu-c-states.crio.io** アノテーションで設定できます。これは、より浅い C ステートを完全に無効にするのではなく、一部を有効にすることで、優先度の高いアプリケーションの節電を最適化するのに役立ちます。Pod の C 状態の制御に関する詳細は、優先度の高い Pod の省電力モードを無効にする を参照してください。

1.3.22.4. デュアルスタックハブクラスターからの IPv6 スポーククラスターのプロビジョニングのサポート

この更新により、デュアルスタックハブクラスターから IPv6 アドレススポーククラスターをプロビジョニングできるようになります。Zero Touch Provisioning (ZTP) 環境では、ブート ISO をホストする

ハブクラスター上の HTTP サーバーが、IPv4 ネットワークと IPv6 ネットワークの両方をリッスンするようになりました。プロビジョニングサービスは、ターゲットスポーククラスター上のベースボード管理コントローラー (BMC) アドレススキームもチェックし、インストールメディアに一致する URL を提供します。これらの更新により、デュアルスタックハブクラスターから、シングルスタックの IPv6 スポーククラスターをプロビジョニングできる機能が提供されます。

1.3.22.5. RHOSP クラスター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)

RHOSP 上で実行されるクラスターでデュアルスタックネットワーク設定が利用できるようになりました。これはテクノロジープレビューの機能です。インストーラーがプロビジョニングしたインフラストラクチャーにクラスターをデプロイメントするときに、デュアルスタックネットワークを設定できます。

詳細は、デュアルスタックネットワークを使用したクラスターの設定 を参照してください。

1.3.22.6. RHOSP クラスターのセキュリティーグループ管理

OpenShift Container Platform 4.14 では、RHOSP 上で実行されるクラスターのセキュリティーが強化されています。デフォルトでは、OpenStack クラウドプロバイダーは、ロードバランサーの **manage-security-groups** オプションを **true** に設定し、クラスターの操作に必要なノードポートのみが開かれるようにします。以前は、コンピュートプレーンマシンとコントロールプレーンマシンの両方のセキュリティーグループが、すべての受信トラフィックに対して、広範囲のノードポートを開くように設定されていました。

ロードバランサーの設定で **manage-security-groups** オプションを **false** に設定し、セキュリティーグループルールがノードポート範囲 30000 から 32767 までの **0.0.0.0/0** からのトラフィックを許可するようにすることで、以前の設定を使用することを選択できます。

4.14 にアップグレードされたクラスターの場合は、デプロイメントをすべてのトラフィックに開放する permissive セキュリティーグループルールを手動で削除する必要があります。たとえば、ノードポート範囲 30000 から 32767 までの **0.0.0.0/0** からのトラフィックを許可するルールを削除する必要があります。

1.3.22.7. GitOps Zero Touch Provisioning (ZTP) パイプラインでの PolicyGenTemplate CR でのカスタム CR の使用

GitOps ZTP を使用して、**ztp-site-generate** コンテナーの GitOps ZTP プラグインによって提供されるベースソース CR に加えて、カスタム CR を含めることができるようになりました。詳細は、GitOps ZTP パイプラインへのカスタムコンテンツの追加 を参照してください。

1.3.22.8. GitOps ZTP のマネージドクラスターバージョンからの独立性

GitOps ZTP を使用して、OpenShift Container Platform のさまざまなバージョンを実行しているマネージドクラスターをプロビジョニングできるようになりました。これは、ハブクラスターと GitOps ZTP プラグインのバージョンが、マネージドクラスター上で実行されている OpenShift Container Platform のバージョンに依存しないことを意味します。詳細は、バージョンに依存しないように GitOps ZTP サイト設定リポジトリーを準備する を参照してください。

1.3.22.9. Topology Aware Lifecycle Manager を使用したユーザー指定のイメージの事前キャッシュ

このリリースにより、Topology Aware Lifecycle Manager を使用してシングルノード OpenShift クラスター上のアプリケーションをアップグレードする前に、アプリケーションのワークロードイメージを事前キャッシュできるようになりました。詳細は、シングルノード OpenShift クラスターでの TALM を

使用したユーザー指定イメージの事前キャッシュ を参照してください。

1.3.22.10. SiteConfig および GitOps ZTP によるディスククリーニングオプション

このリリースでは、**SiteConfig** CR の **automatedCleaningMode** フィールドを使用して、インストール前にパーティションテーブルを削除できます。詳細は、シングルノード OpenShift SiteConfig CR インストールリファレンス を参照してください。

1.3.22.11. GitOps ZTP を介した SiteConfig CR でのカスタムノードラベルの追加へのサポート

この更新により、**SiteConfig** CR に **nodeLabels** フィールドを追加して、マネージドクラスター内のノードのカスタムロールを作成できるようになりました。カスタムラベルを追加する方法の詳細は、SiteConfig および GitOps ZTP を使用したマネージドクラスターのデプロイ 、GitOps ZTP インストールおよび設定 CR の手動生成、および シングルノード OpenShift SiteConfig CR インストールリファレンス を参照してください。

1.3.22.12. etcd レイテンシー許容値の調整のサポート (テクノロジープレビュー)

このリリースでは、コントロールプレーンのハードウェア速度を **"Standard"**、**"Slower"**、またはデフォルトの **""** のいずれかに設定できます。これにより、システムが使用する速度を決定できます。これはテクノロジープレビューの機能です。詳細は、etcd のチューニングパラメーターの設定 を参照してください。

1.3.22.13. SiteConfig のフィールドの非推奨化

この更新により、**SiteConfig** カスタムリソース定義 (CRD) の **apiVIP** フィールドと **ingressVIP** フィールドは非推奨となり、代わりに複数形の **apiVIPs** と **ingressVIPs** が使用されるようになりました。

1.3.23. Hosted Control Plane

1.3.23.1. ベアメタルおよび OpenShift Virtualization で Hosted Control Plane を一般提供

OpenShift Container Platform の Hosted Control Plane が、ベアメタルおよび OpenShift Virtualization プラットフォームで一般提供されるようになりました。AWS 上の Hosted Control Plane は、引き続きテクノロジープレビュー機能として提供されます。

1.3.23.2. AWS のホストされたクラスター上で ARM NodePool オブジェクトを作成する (テクノロジープレビュー)

このリリースでは、同一の Hosted Control Plane から 64 ビット ARM および AMD64 上のアプリケーションワークロードをスケジュールできます。詳細は、AWS のホストされたクラスターで ARM NodePool オブジェクトを作成する を参照してください。

1.3.23.3. IBM Z 上の Hosted Control Plane (テクノロジープレビュー)

このリリースでは、IBM Z 上で Hosted Control Plane をテクノロジープレビュー機能として使用できます。詳細は、64 ビット x84 ベアメタルで IBM Z コンピュートノード用のホスティングクラスターを設定する (テクノロジープレビュー) を参照してください。

1.3.23.4. IBM Power 上の Hosted Control Plane (テクノロジープレビュー)

このリリースでは、IBM Power 上で Hosted Control Plane をテクノロジープレビュー機能として使用できます。詳細は、IBM Power コンピュートノードの Hosted Control Plane を作成するために 64 ビッ

ト x86 OpenShift Container Platform クラスターでホスティングクラスターを設定する (テクノロジープレビュー) を参照してください。

1.3.24. Insights Operator

1.3.24.1. オンデマンドのデータ収集 (テクノロジープレビュー)

OpenShift Container Platform 4.14 では、Insights Operator がオンデマンドで収集操作を実行できるようになりました。オンデマンドでの収集操作の実行に関する詳細は、Insights Operator の収集操作の実行 を参照してください。

1.3.24.2. 個別の Pod として収集操作を実行する (テクノロジープレビュー)

OpenShift Container Platform 4.14 テクノロジープレビュークラスターでは、Insights Operator は個々の Pod で収集操作を実行します。これは、新しいオンデマンドデータ収集機能をサポートします。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.14 では、次の注目すべき技術的な変更が導入されています。

1.4.1. 追加のクラウドプロバイダー向けのクラウドコントローラーマネージャー

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

このリリースでは、Amazon Web Services と Microsoft Azure のクラウドコントローラーマネージャーの使用が一般提供されるようになりました。

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

クラウドコントローラーマネージャーおよびクラウドノードマネージャーのデプロイメントおよびライフサイクルを管理するには、Cluster Cloud Controller Manager Operator を使用します。詳細は、**Platform Operators リファレンス** の Cluster Cloud Controller Manager Operator を参照してください。

1.4.2. Pod セキュリティーアドミッションの今後の限定的な適用

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

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

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

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

- Pod のセキュリティー違反の原因となっているワークロードを見つける方法の詳細は、Pod のセキュリティー違反の特定 を参照してください。
- Pod セキュリティーアドミッションラベルの同期のタイミングに関する詳細は、Pod セキュリティー標準との Security Context Constraint の同期 を参照してください。Pod セキュリティーアドミッションラベルは、次のような特定の状況では同期されません。
  - ワークロードは、**openshift-** で始まるシステム作成の namespace で実行されています。
  - ワークロードは、Pod コントローラーなしで直接作成された Pod で実行されています。
- 必要に応じて、**pod-security.kubernetes.io/enforce** ラベルを設定して、namespace または Pod にカスタムアドミッションプロファイルを設定できます。

1.4.3. SSH キーの場所の変更

OpenShift Container Platform 4.14 では、RHEL 9.2 ベースの RHCOS が導入されています。この更新前は、SSH キーは RHCOS の **/home/core/.ssh/authorized_keys** にありました。この更新により、RHEL 9.2 ベースの RHCOS では SSH キーが **/home/core/.ssh/authorized_keys.d/ignition** に配置されます。

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

1.4.4. cert-manager Operator の一般提供

Red Hat OpenShift 1.11 の cert-manager Operator は、OpenShift Container Platform 4.14、OpenShift Container Platform 4.13、OpenShift Container Platform 4.12 で一般提供されるようになりました。

1.4.5. Open Virtual Network (OVN) 最適化によるスケーリングと安定性の向上

OpenShift Container Platform 4.14 では、Open Virtual Network Kubernetes (OVN-K) の最適化が導入されており、内部アーキテクチャーが変更されて運用遅延が短縮され、ネットワーキングコントロールプレーンのスケールとパフォーマンスに対する障壁が取り除かれています。ネットワークフローデータは、コントロールプレーンに情報を集中させるのではなく、クラスターノードにローカライズされるようになりました。これにより、操作遅延が短縮され、ワーカーノードとコントロールノード間のクラスター全体のトラフィックが削減されます。その結果、ノードが追加されるたびにネットワーク容量が追加され、大規模なクラスターが最適化されるため、クラスターネットワークのノード数は線形にスケールします。ネットワークフローはすべてのノードでローカライズされるため、コントロールプレーンノードの RAFT リーダー選出は必要なくなり、不安定性の主な原因が除去されました。ローカライズされたネットワークフローデータのさらなる利点は、ネットワーク上のノード損失の影響が障害が発生したノードに限定され、クラスターの残りのネットワークには影響を及ぼさないため、クラスターの障害シナリオに対する回復力が高まることです。詳細は、OVN-Kubernetes アーキテクチャー を参照してください。

1.4.6. Operator SDK 1.31.0

OpenShift Container Platform 4.14 は Operator SDK 1.31.0 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 1.31.0 は Kubernetes 1.26 をサポートします。

Operator SDK 1.28.0 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 1.31.0 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

1.4.7. oc コマンドは、デフォルトで Podman 設定の場所から認証情報を保存および取得するようになりました。

以前は、レジストリー設定を使用する OpenShift CLI (**oc**) コマンド (**oc adm release** や **oc image** コマンドなど) は、最初に ~/**.docker/config.json** などの Docker 設定ファイルの場所から認証情報を取得していました。Docker 設定の場所でレジストリーエントリーが見つからなかった場合、**oc** コマンドは、**${XDG_RUNTIME_DIR}/containers/auth.json** などの Podman 設定ファイルの場所から認証情報を取得しました。

このリリースでは、**oc** コマンドはデフォルトで最初に Podman 設定の場所から認証情報を取得するようになりました。Podman 設定の場所でレジストリーエントリーが見つからない場合、**oc** コマンドは Docker 設定の場所から認証情報を取得します。

さらに、**oc registry login** コマンドは、Docker 設定ファイルの場所ではなく、Podman 設定の場所に認証情報を保管するようになりました。

1.4.8. 長時間実行される Pod リクエストは、CONNECT リクエストとして記録されるようになりました。

OpenShift Container Platform メトリクスでは、pod **attach**、**exec**、**log**、**portforward**、**proxy** のリクエストが **CONNECT** リクエストとして記録されるようになりました。

1.4.9. Open Virtual Network Infrastructure Controller のデフォルト範囲

この更新により、コントローラーはトランジットスイッチサブネットのデフォルトの IP アドレス範囲として **100.88.0.0/16** を使用します。実稼働インフラストラクチャーネットワークでは、この IP 範囲を使用しないでください。(OCPBUGS-20261)

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 4.14 内で非推奨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。

- **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	4.12	4.13	4.14
Operator カタログの SQLite データベース形式	非推奨	非推奨	非推奨
operators.openshift.io/infrastructure-features アノテーション	一般提供	一般提供	非推奨

1.5.2. イメージの非推奨および削除された機能

表1.7 イメージに関する非推奨および削除されたトラッカー

機能	4.12	4.13	4.14
Cluster Samples Operator の **ImageChangesInProgress** 状態	非推奨	非推奨	非推奨
Cluster Samples Operator の **MigrationInProgress** 状態	非推奨	非推奨	非推奨

1.5.3. インストールに関する非推奨機能および削除された機能

表1.8 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	4.12	4.13	4.14
oc adm release extract の **--cloud** パラメーター	一般提供	一般提供	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	削除済み	削除済み
RHOSP の **compute.platform.openstack.rootVolume.type**	一般提供	一般提供	非推奨
RHOSP の **controlPlane.platform.openstack.rootVolume.type**	一般提供	一般提供	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
Google Cloud Provider の **platform.gcp.licenses**	非推奨	非推奨	削除済み

機能	4.12	4.13	4.14
VMware ESXi 7.0 Update 1 以前	一般提供	削除済み [1]	削除済み
vSphere 7.0 Update 1 以前	非推奨	削除済み [1]	削除済み

1. OpenShift Container Platform 4.14 の場合、使用するコンポーネントの要件を満たす VMware vSphere バージョン 8.0 を含む VMware vSphere バージョン 7.0 Update 2 以降のインスタンスに OpenShift Container Platform クラスターをインストールする必要があります。

1.5.4. ストレージに関する非推奨機能と削除された機能

表1.9 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	4.12	4.13	4.14
FlexVolume を使用した永続ストレージ	非推奨	非推奨	非推奨

1.5.5. 非推奨化および削除されたアプリケーションビルド機能

表1.10 非推奨化および削除された Service Binding Operator のトラッカー

機能	4.12	4.13	4.14
Service Binding Operator	一般提供	非推奨	非推奨

1.5.6. マルチアーキテクチャーの非推奨および削除された機能

表1.11 マルチアーキテクチャーの非推奨および削除されたトラッカー

機能	4.12	4.13	4.14
IBM Power8 の全モデル (**ppc64le**)	非推奨	削除済み	削除済み
IBM Power® AC922 (**ppc64le**)	非推奨	削除済み	削除済み
IBM Power® IC922 (**ppc64le**)	非推奨	削除済み	削除済み
IBM Power® LC922 (**ppc64le**)	非推奨	削除済み	削除済み
IBM z13 全モデル (**s390x**)	非推奨	削除済み	削除済み
IBM® LinuxONE Emperor (**s390x**)	非推奨	削除済み	削除済み
IBM® LinuxONE Rockhopper (**s390x**)	非推奨	削除済み	削除済み

機能	4.12	4.13	4.14
AMD64 (x86_64) v1 CPU	非推奨	削除済み	削除済み

1.5.7. ネットワークの非推奨機能と削除された機能

表1.12 ネットワーキングに関する非推奨および削除されたトラッカー

機能	4.12	4.13	4.14
RHOSP 上の Kuryr	非推奨	非推奨	非推奨
OpenShift SDN ネットワークプラグイン	一般提供	一般提供	非推奨

1.5.8. ノードに関する非推奨機能と削除された機能

表1.13 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	4.12	4.13	4.14
ImageContentSourcePolicy (ICSP) オブジェクト	一般提供	非推奨	非推奨
Kubernetes トポロジーラベル **failure-domain.beta.kubernetes.io/zone**	一般提供	非推奨	非推奨
Kubernetes トポロジーラベル **failure-domain.beta.kubernetes.io/region**	一般提供	非推奨	非推奨

1.5.9. OpenShift CLI (oc) の非推奨および削除された機能

機能	4.12	4.13	4.14
oc-mirror の **--include-local-oci-catalogs** パラメーター	利用不可	一般提供	削除済み
oc-mirror の **--use-oci-feature** パラメーター	一般提供	非推奨	削除済み

1.5.10. ワークロードに関する非推奨機能と削除された機能

表1.14 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	4.12	4.13	4.14
DeploymentConfig オブジェクト	一般提供	一般提供	非推奨

1.5.11. 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1.15 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

1.5.12. 非推奨の機能

1.5.12.1. OpenShift SDN ネットワークプラグインの非推奨化

OpenShift SDN CNI は、OpenShift Container Platform 4.14 以降非推奨になりました。OpenShift Container Platform の次のマイナーリリースでは、ネットワークプラグインは現時点では新規インストールのオプションにはならない予定です。今後のリリースでは、OpenShift SDN ネットワークプラグインは削除され、サポートされなくなる予定です。Red Hat は、この機能が削除されるまでバグ修正とサポートを提供しますが、この機能は機能拡張の対象外となります。OpenShift SDN CNI の代わりに、OVN Kubernetes CNI を使用できます。

1.5.12.2. Service Binding Operator

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

1.5.12.3. DeploymentConfig リソースが非推奨に

OpenShift Container Platform 4.14 以降、**DeploymentConfig** オブジェクトは非推奨になりました。**DeploymentConfig** オブジェクトは引き続きサポートされていますが、新規インストールには推奨されません。セキュリティー関連の重大な問題のみが修正されます。

代わりに、**Deployment** オブジェクトまたは別の代替手段を使用して、Pod の宣言的更新を提供します。

1.5.12.4. GitOps ZTP で使用される Operator 固有の CatalogSource CR は非推奨に

OpenShift Container Platform 4.14 以降で、Topology Aware Lifecycle Manager (TALM) を使用して Operator を更新する場合は、**DefaultCatSrc.yaml CatalogSource** CR のみを使用する必要があります。他のすべての **CatalogSource** CR は非推奨となり、今後のリリースで削除される予定です。Red Hat は、現在のリリースの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、機能拡張を受け取らず、削除されます。**DefaultCatSrc** CR の詳細は、Operator 更新の実行を参照してください。

1.5.12.5. oc adm release extract コマンドの --cloud パラメーター

OpenShift Container Platform 4.14 以降、**oc adm release extract** コマンドの **--cloud** パラメーターは非推奨になりました。**--included** パラメーターと **--install-config** パラメーターの導入により、**--cloud** パラメーターは不要になります。

詳細は、手動管理のクラウド認証情報を使用したクラスターの簡素化されたインストールと更新 を参照してください。

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

OpenShift Container Platform のホストプラットフォームとしての Red Hat Virtualization (RHV) は非推奨となり、サポートされなくなりました。このプラットフォームは、今後の OpenShift Container Platform リリースでは、OpenShift Container Platform から削除される予定です。

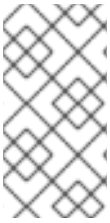
1.5.12.7. REGISTRY_AUTH_PREFERENCE 環境変数の使用が非推奨になる

REGISTRY_AUTH_PREFERENCE 環境変数を使用して、OpenShift CLI (**oc**) コマンドのレジストリー認証情報を取得するための優先場所を指定することは、非推奨になりました。

OpenShift CLI (**oc**) コマンドは、デフォルトで最初に Podman 設定の場所から認証情報を取得するようになりましたが、非推奨の Docker 設定ファイルの場所を確認するようにフォールバックします。

1.5.12.8. operators.openshift.io/infrastructure-features アノテーション

OpenShift Container Platform 4.14 以降、**operators.openshift.io/infrastructure-features** のアノテーションのグループが、**features.operators.openshift.io** namespace のアノテーションのグループによって非推奨となりました。



注記

現在、Web コンソールは引き続き、以前のアノテーションに基づいた表示とフィルタリングをサポートしています。ただし、これらは非推奨であり、このサポートは今後の OpenShift Container Platform リリースで Web コンソールから削除されるため、新しいアノテーション形式への移行が推奨されます。

アノテーションの以前のグループは、非推奨のインフラストラクチャー機能のアノテーション を、最新のグループについては インフラストラクチャー機能のアノテーション を参照してください。

1.5.13. 削除された機能

1.5.13.1. 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。

1.5.13.2. Kubernetes 1.27 からベータ API が削除される

Kubernetes 1.27 では次の非推奨の API が削除されたため、適切な API バージョンを使用するにはマニフェストと API クライアントを移行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1.16 Kubernetes 1.27 から削除された API

リソース	削除された API	移行先
CSIStorageCapacity	**storage.k8s.io/v1beta1**	**storage.k8s.io/v1**

1.5.13.3. LatencySensitive 機能セットのサポートが削除される

OpenShift Container Platform 4.14 以降、**LatencySensitive** 機能セットのサポートは削除されました。

1.5.13.4. oc レジストリーログインでは、認証情報が Docker 設定ファイルの場所に保存されなくなる

OpenShift Container Platform 4.14 以降、**oc registry login** コマンドは、**~/.docker/config.json** などの Docker ファイルの場所にレジストリー認証情報を保管しなくなりました。**oc registry login** コマンドは、**${XDG_RUNTIME_DIR}/containers/auth.json** などの Podman 設定ファイルの場所に認証情報を保存するようになりました。

1.6. バグ修正

1.6.1. API サーバーと認証

- 以前は、セキュリティーコンテキストの制約によって変更される Pod 仕様を使用して Pod コントローラーを作成すると、Pod が指定された namespace の Pod セキュリティーレベルを満たしていないという警告がユーザーに表示されることがありました。このリリースでは、Pod コントローラーがその namespace で Pod のセキュリティーに違反しない Pod を作成する場合に、Pod のセキュリティー違反に関する警告が表示されなくなりました。(OCPBUGS-7267)

- **user:check-access** スコープのトークンは、SelfSubjectAccessReview リクエストを送信するための十分なパーミッションを付与します。以前は、トークンに **user:full** スコープまたはロールスコープが含まれていない限り、クラスターはアクセスレビューを実行するための十分なパーミッションを付与しませんでした。このリリースでは、クラスターは、アクセスレビューを実行できるようにするために、完全なユーザーのパーミッション、またはリクエストに設定されたユーザーのロールのパーミッションを持っているかのように、SelfSubjectAccessReview リクエストを承認します。(OCPBUGS-7415)

- 以前は、Pod セキュリティーアドミッションコントローラーでは、サービスアカウントをロールに正常にバインドするために **.subjects[].kind** が **ServiceAccount** に設定されている場合に、**RoleBinding** オブジェクトの **.subject[].namespace** フィールドを設定する必要がありました。このリリースでは、**.subject[].namespace** が指定されていない場合、Pod セキュリティーアドミッションコントローラーは、**RoleBinding** オブジェクトの namespace を使用します。(OCPBUGS-160)

- 以前は、**ValidatingWebhookConfiguration** オブジェクトと **MutatingWebhookConfiguration** オブジェクトのすべての Webhook の **clientConfig** は、**service-ca** トラストバンドルを使用して適切に注入された **caBundle** を取得できませんでした。このリリースでは、**ValidatingWebhookConfiguration** オブジェクトと **MutatingWebhookConfiguration** オブジェクトのすべての Webhook の **clientConfig** が、**service-ca** トラストバンドルを使用して適切に注入された **caBundle** を取得するようになりました。(OCPBUGS-19318)

- 以前は、**namedCertificates** の **servingCertificate** に無効なシークレット名が指定された場合、kube-apiserver は **Degraded=True** に変更されませんでした。このリリースでは、kube-apiserver が **Degraded=True** に切り替わり、証明書が受け入れられなかった理由を表示して、トラブルシューティングを簡素化するようになりました。(OCPBUGS-8404)

- 以前は、可観測性ダッシュボードは、データを表示するために大規模なクエリーを使用していたため、多数のノードを持つクラスターで頻繁にタイムアウトが発生していました。このリリースでは、可観測性ダッシュボードは、多数のノードを含むクラスターの信頼性を確保するために、事前に計算された記録ルールを使用します。(OCPBUGS-3986)

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、ベアメタルマシンのホスト名がリバース DNS または DHCP によって提供されなかった場合、インストーラーがプロビジョニングしたインフラストラクチャーでのベアメタルクラ

スターのプロビジョニング中に、デフォルトで **localhost** が使用されていました。この問題により、Kubernetes ノード名の競合が発生し、クラスターをデプロイできなくなりました。現在は、ホスト名が **localhost** であることが検出された場合、プロビジョニングエージェントは永続的なホスト名を **BareMetalHost** オブジェクトの名前に設定します。(OCPBUGS-9072)

1.6.3. クラウドコンピュート

- 以前は、マシン API コントローラーは、複数のゾーンを使用する vSphere クラスター内のマシンのゾーンを特定できませんでした。このリリースでは、ゾーン検索ロジックは仮想マシンのホストに基づいており、その結果、マシンオブジェクトは適切なゾーンを示します。(OCPBUGS-7249)

- 以前は、**clouds.yaml** ファイル内のクラウド認証情報をローテーションした後、新しいクラウド認証情報を取得するために、OpenStack マシン API プロバイダーを再起動する必要がありました。その結果、ゼロにスケールよう設定されたマシンの機能が影響を受ける可能性があります。この変更により、クラウド認証情報はキャッシュされなくなり、プロバイダーは必要に応じて対応するシークレットを新たに読み取ります。(OCPBUGS-8687)

- 以前は、Cluster Autoscaler Operator の起動プロセス中のいくつかの条件によってロックが発生し、Operator が正常に起動して自身を使用可能にマークすることができませんでした。その結果、クラスターのパフォーマンスが低下しました。この問題は、このリリースで解決されました。(OCPBUGS-20038)

- 以前は、コントロールプレーンノードのクライアント認証情報を要求するために使用されるブートストラップ認証情報には、汎用のすべてのサービスアカウントグループが含まれていませんでした。その結果、Cluster Machine Approver は、このフェーズ中に作成された証明書署名要求 (CSR) を無視しました。特定の状況では、これによりブートストラップ中に CSR が承認されなくなり、インストールが失敗する原因となりました。このリリースでは、ブートストラップ認証情報には、Cluster Machine Approver がサービスアカウントに対して期待するグループが含まれています。この変更により、Machine Approver がクラスターのライフサイクルの早い段階でブートストラップ CSR Approver を引き継ぐことができるようになり、CSR Approver に関連するブートストラップの失敗が減少するはずです。(OCPBUGS-8349)

- 以前は、Nutanix クラスター上のマシンのスケーリングが操作を完了するために利用可能なメモリーを超えた場合、マシンは **Provisioning** 状態でスタックし、スケールアップまたはスケールダウンできませんでした。この問題はこのリリースで解決されています。(OCPBUGS-19731)

- 以前は、Control Plane Machine Set Operator が **OnDelete** 更新ストラテジーを使用するように設定されているクラスターの場合、マシンに関するキャッシュされた情報により、Operator はマシンのバランスを誤って、調整中にマシンを想定外の障害ドメインに配置していました。このリリースでは、Operator は新しいマシンを作成する直前にこの情報を更新し、マシンを配置する障害ドメインを正確に識別します。(OCPBUGS-15338)

- 以前は、Control Plane Machine Set Operator は **Infrastructure** オブジェクト仕様を使用してクラスターのプラットフォームタイプを決定していました。このプラクティスは、OpenShift Container Platform バージョン 4.5 以前からアップグレードされたクラスターの場合、クラスターが AWS で実行されていることを Operator が正しく判断できないことを意味しました。そのため、想定どおりに **ControlPlaneMachineSet** カスタムリソース (CR) を生成できませんでした。このリリースでは、Operator はステータスプラットフォームタイプを使用します。このタイプは、クラスターの作成時に関係なくすべてのクラスターに設定され、すべてのクラスターに対して **ControlPlaneMachineSet** CR を生成できるようになりました。(OCPBUGS-11389)

- 以前は、コントロールプレーンマシンセットによって作成されたマシンは、基盤となる Machine API マシンが実行されると、準備完了とみなされていました。このリリースでは、マシンにリンクされているノードの準備も完了するまで、そのマシンは準備完了とみなされなく

なりました。(OCPBUGS-7989)

- 以前は、Control Plane Machine Set Operator は、障害ドメイン全体でのマシンの可用性が改善されなかったとしても、アルファベット順に障害ドメインに優先順位を付け、アルファベット順で後方に位置する障害ドメインからアルファベット順で前方に位置する障害ドメインにマシンを移動していました。このリリースでは、既存のマシンに存在する障害ドメインを優先し、可用性を向上させる既存の障害ドメインを考慮するように Operator が更新されました。(OCPBUGS-7921)

- 以前は、コントロールプレーンマシンセットを使用する vSphere クラスター上のコントロールプレーンマシンが削除されると、2 つの代替マシンが作成されることがありました。このリリースでは、コントロールプレーンマシンセットによって余分なマシンが作成されなくなりました。(OCPBUGS-7516)

- 以前は、マシンセット内のアベイラビリティーゾーンとサブネット ID が一致しない場合、ユーザーに不一致が通知されることなく、マシンセット仕様を使用してマシンが正常に作成されました。値の不一致は、一部の設定で問題を引き起こす可能性があるため、この問題が警告メッセージとして表示される場合があります。このリリースでは、不一致に関する警告がログに記録されます。(OCPBUGS-6882)

- 以前は、IP アドレス管理 (IPAM) ネットワーク設定の代わりに Dynamic Host Configuration Protocol (DHCP) を使用する OpenShift Container Platform クラスターを Nutanix 上に作成する場合、仮想マシンのホスト名は DHCP によって設定されませんでした。このリリースでは、仮想マシンホスト名が Ignition 設定ファイルの値で設定されます。その結果、DHCP および他のネットワーク設定タイプの問題が解決されました。(OCPBUGS-6727)

- 以前は、**openshift-cluster-api** namespace に複数のクラスターを作成できました。この namespace には、クラスターを 1 つだけ含める必要があります。このリリースにより、この namespace に追加のクラスターを作成できなくなりました。(OCPBUGS-4147)

- 以前は、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の **providerSpec** フィールドから一部のパラメーターをクリアすると、コントロールプレーンマシンの削除と作成のループが発生していました。このリリースでは、これらのパラメーターがクリアされたり、空のままになったりするとデフォルト値が適用され、問題は解決されました。(OCPBUGS-2960)

1.6.4. Cloud Credential Operator

- 以前は、Cloud Credential Operator ユーティリティー (**ccoctl**) は、AWS GovCloud (米国) および AWS 中国リージョンに対して誤った Amazon Resource Names (ARN) 接頭辞を使用していました。ARN 接頭辞が正しくないため、インストール中に AWS リソースの作成に使用される **ccoctl aws create-all** コマンドが失敗していました。このリリースでは、ARN 接頭辞を正しい値に更新しました。(OCPBUGS-13549)

- 以前は、Amazon S3 バケットに対するセキュリティーの変更により、インストール中に AWS リソースを作成するために使用される Cloud Credential Operator ユーティリティー (**ccoctl**) コマンド (**ccoctl aws create-all**) が失敗していました。このリリースでは、**ccoctl** ユーティリティーが更新され、Amazon S3 セキュリティーの変更が反映されています。(OCPBUGS-11671)

1.6.5. Cluster Version Operator

- 以前は、Cluster Version Operator (CVO) が **SecurityContextConstraints** リソースを期待どおりに調整しませんでした。CVO は、リリースイメージで定義された状態に合わせて **SecurityContextConstraints** リソースを適切に調整し、サポートされていない変更をすべて元に戻します。
  以前の OpenShift Container Platform バージョンからアップグレードしたいユーザー、および

変更されたシステム **SecurityContextConstraints** リソースに応じてワークロードを操作するユーザーは、ナレッジベースの記事 の手順に従って、変更されたシステムの **SecurityContextConstraint** リソースなしでワークロードを実行できるようにする必要があります。(OCPBUGS-19465)

- 以前は、Cluster Version Operator は、どの条件付き更新リスクを最初に評価するかを決定する際に、可能性のあるターゲットに優先順位を付けていませんでした。リスクが適用されない条件付き更新は、Cluster Version Operator の検出後、これらの更新をより迅速に利用できるようになります。(OCPBUGS-5469)

1.6.6. 開発者コンソール

- 以前は、**Developer** コンソールで **Helm** に移動し、**Repositories** タブをクリックしてから、

  Helm チャートリポジトリーの  メニューから **Edit HelmChartRepository** を選択して Helm チャートリポジトリーを編集しようとした場合、**Error** ページに **404: Page Not Found** エラーが表示されました。これは、コンポーネントパスが最新ではないことが原因でした。この問題は修正されています。(OCPBUGS-14660)

- 以前は、**Samples** ページにリストされているサンプルのタイプを区別することは困難でした。この修正により、**Samples** ページに表示されるバッジで、サンプルタイプを簡単に識別できるようになります。(OCPBUGS-7446)

- 以前のパイプライン **Metrics** ページでは、**TaskRun** 期間グラフに 4 つの凡例のみが表示されていました。この更新により、**TaskRun** 期間グラフに存在するすべての凡例を確認できるようになりました。(OCPBUGS-19878)

- 以前は、Cluster Samples Operator がインストールされていない切断されたクラスターで **Import JAR** フォームを使用してアプリケーションを作成すると、問題が発生しました。この更新により、Java ビルダーイメージが存在しない場合、**Add** ページおよび **Topology** ページの **Import JAR** フォームが非表示になりました。(OCPBUGS-15011)

- 以前は、クラスターサービスバージョン (CSV) のコピーが無効になっている場合、Operator がサポートするカタログにはカタログアイテムが表示されませんでした。この修正により、CSV コピーが無効になっている場合でも、Operator がサポートするカタログがすべての namespace に表示されます。(OCPBUGS-14907)

- 以前は、**Git からインポート** および **イメージのデプロイ** フローで、**リソースタイプ** セクションが **詳細** セクションに移動されました。その結果、作成されたリソースの種類を特定することが困難になりました。この修正により、**Resource Type** セクションが **General** セクションに移動されました。(OCPBUGS-7395)

1.6.7. etcd Cluster Operator

- 以前は、**etcdctl** バイナリーがローカルマシンに無期限にキャッシュされていたため、バイナリーを更新できませんでした。バイナリーは、**cluster-backup.sh** スクリプトが呼び出されるたびに、適切に更新されるようになりました。(OCPBUGS-19499)

1.6.8. インストーラー

- 以前は、サポートされているシークレットパーティションに AWS クラスターをインストールするときに、カスタム Red Hat Enterprise Linux CoreOS (RHCOS) Amazon Machine Image (AMI) を指定しなかった場合、インストールは失敗していました。この更新により、インス

トールプログラムは、クラスターをデプロイする前に、インストール設定ファイルで RHCOS AMI の ID が指定されたことを検証します。(OCPBUGS-13636)

- 以前は、OpenShift Container Platform インストールプログラムは、共有 VPC を使用した Google Cloud Platform (GCP) へのインストール中に、ホストプロジェクト内のプライベートホスト型ゾーンを検出しませんでした。この更新により、インストールプログラムはホストプロジェクト内の既存のプライベートホスト型ゾーンを確認し、存在する場合はプライベートホスト型ゾーンを使用します。(OCPBUGS-11736)

- 以前は、プライベート Azure クラスターをインストールする際に、ユーザー定義の送信ルーティングを設定すると、クラスターがデフォルトのパブリックロードバランサーを使用して誤ってデプロイされました。この動作は、インストーラーがプロビジョニングしたインフラストラクチャーを使用してクラスターをインストールする際に発生しました。この更新により、ユーザー定義のルーティングが設定されている場合、インストールプログラムはパブリックロードバランサーを作成しなくなります。(OCPBUGS-9404)

- 以前は、RHOSP 上で実行されるクラスターの場合、インストールのプロビジョニング解除フェーズで、インストーラーはオブジェクトストレージコンテナーを連続的に削除していました。この動作により、特に大きなコンテナーの場合、オブジェクトの削除が遅くなり、非効率的になってしまいました。この問題は、Swift コンテナーを使用するイメージストリームが時間の経過とともにオブジェクトを蓄積したことが原因の 1 つとなり、発生しました。現在は、オブジェクトの一括削除は RHOSP API への最大 3 つの呼び出しと同時に行われ、呼び出しあたりにより多くのオブジェクト数を処理することで効率が向上しています。この最適化により、プロビジョニング解除中のリソースのクリーンアップが高速化されます。(OCPBUGS-9081)

- 以前は、踏み台ホストがクラスターノードと同じ VPC ネットワークで実行されている場合、ブートストラップノードとクラスターノードへの SSH アクセスが失敗していました。また、この設定が原因で、一時ブートストラップノードからクラスターノードへの SSH アクセスが失敗していました。これらの問題は、一時ブートストラップノードとクラスターノード間の SSH トラフィックと、同じ VPC ネットワーク上の bastion ホストからクラスターノードへの SSH トラフィックをサポートするように IBM Cloud **SecurityGroupRules** を更新することで修正されています。インストーラーがプロビジョニングしたインフラストラクチャーでの障害発生中に、分析用のログとデバッグ情報を正確に収集できます。(OCPBUGS-8035)

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

- 以前は、RHOSP API で無効な HTTPS 証明書をチェックするためにドキュメントで提供されているスクリプトは、最新バージョンの RHOSP クライアントを想定していました。最新バージョンのクライアントを持っていないユーザーの場合、このスクリプトは失敗しました。現在、マニュアルの手順がドキュメントに追加されており、ユーザーはこれに従って、クライアントの任意のバージョンでチェックを実行できます。(OCPBUGS-7954)

- 以前は、エージェントベースのインストールの設定のために、**agent-config.yaml** または **nmstateconfig.yaml** ファイルで静的 IP アドレスを定義する場合、設定された静的 IP アドレスがブートストラップ中に設定されていない可能性がありました。その結果、ホストインターフェイスは DHCP 経由でアドレスを選択していました。この更新により、設定された静的 IP アドレスがホストインターフェイスに正しく適用されるように、タイミングの問題が修正されました。(OCPBUGS-16219)

- 以前は、エージェントベースのインストール中に、**ImageContentSources** フィールドもミラーリングに設定されている場合にのみ、**install-config.yaml** ファイルの **AdditionalTrustBundle** フィールド内の証明書が最終イメージに伝播されました。ミラーリングが設定されていない場合、追加の証明書はブートストラップにはありましたが、最終イメージにはありませんでした。この状況は、インストール中のクラスター全体のプロキシー設定 で

説明されているように、プロキシーをセットアップして証明書を追加する場合に、問題を引き起こす可能性があります。この更新により、**ImageContentSources** フィールドも設定されているかどうかに関係なく、これらの追加の証明書が最終イメージに伝播されます。(OCPBUGS-13535)

- 以前は、**openshift-install agent create** コマンドは、無効なコマンドを実行するとヘルプ出力を返しませんでした。この更新により、無効な **openshift-install agent create** コマンドを実行したときに、ヘルプ出力が表示されるようになりました。(OCPBUGS-10638)

- 以前は、テクノロジープレビューの障害ドメインを使用する生成されたマシンに対して、プライマリーネットワークが正しく設定されませんでした。その結果、ID **control-plane** を持つポートターゲットが、マシン上のプライマリーネットワークとして設定されず、Kuryr を使用するインストールが正しく機能しない可能性がありました。このフィールドは、適切なポートターゲットが設定されている場合は、それを使用するように設定されるようになりました。生成されたマシンのプライマリーネットワークが正しく設定されるようになり、Kuryr を使用するインストールを完了できるようになりました。(OCPBUGS-10570)

- 以前は、ダイジェストを含む **releaseImage** を使用している際に **openshift-install agent create image** コマンドを実行すると、コマンドは **WARNING The ImageContentSources configuration in install-config.yaml should have at-least one source field matching the releaseImage** という警告メッセージを生成しました。このメッセージは、**ImageContentSources** の設定方法に関係なく毎回生成され、混乱を引き起こす可能性がありました。この更新により、リリースイメージに一致するソースフィールドが少なくとも 1 つ含まれるように **ImageContentSources** が適切に設定されていない場合にのみ、警告メッセージが生成されるようになりました。(OCPBUGS-10207)

- 以前は、**openshift-install agent create image** コマンドを実行してブート可能 ISO イメージを生成すると、コマンド出力にイメージが正常に生成されたことを示すメッセージが表示されていました。この出力メッセージは、エージェントベースのインストーラーが、リリースイメージからベース ISO イメージを展開できなかった場合でも存在しました。この更新により、エージェントベースのインストーラーがベース ISO イメージを見つけられない場合 (**releaseImage** の問題を示している可能性あり) に、コマンド出力でエラーメッセージが生成されるようになりました。(OCPBUGS-9949)

- 以前は、インストールプログラムがデフォルトのサービスアカウントの認証情報を使用していたため、パススルー認証情報モードを使用した GCP への共有 VPC インストールが失敗することがありました。この更新により、デフォルトの代わりにノードの作成に使用する別のサービスアカウントを指定できるようになりました。(OCPBUGS-15421)

- 以前は、**agent-config.yaml** または **nmstateconfig.yaml** 設定ファイルのいずれかで、コンピュートノードよりも多くのコントロールプレーンノードを定義すると、警告メッセージが表示されていました。現在は、いずれかのファイルでこの設定を指定すると、どちらのファイルでもコンピュートノードがコントロールプレーンノードを超えることができないことを示すエラーメッセージが表示されます。(OCPBUGS-14877)

- 以前は、**agent-config.yaml** ファイルの **RendezvousIP** フィールドに非標準 IPv6 アドレスが使用されている場合、エージェントベースのインストールは失敗していました。非標準の IPv6 アドレスには、先頭にゼロが含まれます (例: **2001:0db8:0000:0000:0000:0000:0000:0000**)。この更新により、これらの有効なアドレスが **RendezvousIP** に使用できるようになりました。(OCPBUGS-14121)

- 以前は、Operator がクラウド認証情報をキャッシュしていたため、これらの認証情報がローテーションされると認証の問題が発生していました。現在、Operator は常に最新の認証情報を使用します。Manila CSI Driver Operator は、利用可能な Manila 共有タイプごとに OpenShift ストレージクラスを自動的に作成します。この操作の一環として、Operator は Manila API にクエリーを実行します。(OCPBUGS-14049)

- 以前は、エージェントベースのインストール中に使用する **install-config.yaml** ファイルを設定する際に、**cpuPartitioning** フィールドをデフォルト以外の値に変更しても、このフィールドがエージェントベースのインストールでは無視されることをユーザーに知らせるための警告は生成されませんでした。この更新により、**cpuPartitioning** フィールドを変更すると、その設定がインストールに影響を与えないという警告がユーザーに表示されるようになりました。(OCPBUGS-13662)

- 以前は、インストールプログラムが **0.0.0.0** からのトラフィックを許可するデフォルトのネットワークセキュリティーグループを作成したため、既存の Azure Virtual Network (VNet) への Azure クラスターのインストールが失敗することがありました。この障害は、既存の VNet のテナントで、**Rule: Network Security Groups shall not allow rule with 0.0.0.0/Any Source/Destination IP Addresses - Custom Deny** というルールが有効になっている場合に発生しました。この修正により、インストールプログラムは、クラスターを既存の VNet にインストールする際にデフォルトのネットワークセキュリティーグループを作成しなくなり、インストールは成功するようになりました。(OCPBUGS-11796)

- インストール中のクラスターのステータスが **installing-pending-user-action** の場合、ステータスが解決されるまでインストールは完了しません。以前は、**openshift-install agent wait-for bootstrap-complete** コマンドを実行した場合、このステータスの原因となった問題を解決する方法が示されていませんでした。この更新により、問題解決のためにどのアクションを実行する必要があるかを示すメッセージが、コマンド出力に表示されます。(OCPBUGS-4998)
たとえば、無効なブートディスクが使用された場合の **wait-for** 出力は、次のようになります。

  ```
  "level=info msg=Cluster has hosts requiring user input
  level=debug msg=Host master-1 Expected the host to boot from disk, but it booted the
  installation image - please reboot and fix boot order to boot from disk QEMU_HARDDISK
  drive-scsi0-0-0-0 (sda, /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0)
  level=debug msg=Host master-2 Expected the host to boot from disk, but it booted the
  installation image - please reboot and fix boot order to boot from disk QEMU_HARDDISK
  drive-scsi0-0-0-0 (sda, /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0)
  level=info msg=cluster has stopped installing... working to recover installation"
  ```

- 以前は、インストールされたクラスター上の **assisted-installer-controller** は、クラスターのインストールが完了した後でも継続的に実行されていました。**assisted-service** は、クラウドではなくブートストラップノードで実行され、ブートストラップノードが再起動してクラスターに参加すると assisted-service はオフラインになるため、**assisted-installer-controller** は assisted-service との通信ができず、更新のポストやログとループのアップロードができませんでした。現在、**assisted-installer-controller** は **assisted-service** を使用せずにクラスターのインストールをチェックし、クラスターのインストールが完了すると終了します。(OCPBUGS-4240)

- 以前は、AWS Commercial Cloud Services (C2S) **us-iso-east-1** リージョンへのクラスターのインストールが失敗し、**UnsupportedOperation** を示すエラーメッセージが表示されました。この修正により、このリージョンへ正常にインストールされるようになりました。(OCPBUGS-2324)

- 以前は、インストールプログラムが必要なサービスエンドポイントを含む **cloud.conf** ファイルを作成しなかったため、AWS へのインストールが失敗することがありました。これにより、マシン config Operator がサービスエンドポイントのない空の **cloud.conf** ファイルを作成し、エラーが発生しました。この更新により、インストールが成功するように、インストールプログラムは常に **cloud.conf** ファイルを作成するようになりました。(OCPBUGS-20401)

- 以前は、エージェントベースのインストーラーを使用してクラスターをインストールし、プルシークレットに null の **auth** または **email** フィールドが含まれている場合、有用なエラーが表

示されずにインストールが失敗していました。この更新により、**openshift-install agent wait-for install-complete** コマンドがプルシークレットを検証し、null フィールドがある場合に通知するようになりました。(OCPBUGS-14405)

- 以前は、**create agent-config-template** コマンドは **INFO** のみを含む行を出力していましたが、コマンドが成功したかどうか、そしてテンプレートファイルがどこに書き込まれたかに関する詳細は出力されませんでした。コマンドが成功すると、コマンドは **INFO Created Agent Config Template in <path> directory** を出力します。(OCPBUGS-13408)

- 以前は、ユーザーが **agent-config.yaml** ファイルで **vendor** ヒントを指定すると、その値が間違ったフィールドと照合され、ヒントが一致しませんでした。この更新により、**vendor** ヒントを使用すると、ディスクが正しく選択されるようになりました。(OCPBUGS-13356)

- 以前は、AWS にクラスターをインストールするときに、**metadataService.authentication** フィールドを **Required** に設定しても、IMDSv2 認証を使用するようにブートストラップ仮想マシンが設定されませんでした。これにより、IMDSv1 認証をブロックするように AWS アカウントを設定した場合、インストールが失敗する可能性があります。この更新により、**metadataService.authentication** フィールドは、**Required** に設定されている場合、IMDSv2 認証を使用するようにブートストラップ仮想マシンを正しく設定します。(OCPBUGS-12964)

- 以前は、プライベート Azure クラスターをインストールする際に、ユーザー定義の送信ルーティングを設定すると、クラスターがデフォルトのパブリックロードバランサーを使用して誤ってデプロイされました。この動作は、インストーラーがプロビジョニングしたインフラストラクチャーを使用してクラスターをインストールする際に発生しました。この更新により、ユーザー定義のルーティングが設定されている場合、インストールプログラムはパブリックロードバランサーを作成しなくなります。(OCPBUGS-9404)

- 以前は、vSphere Terraform **vsphere_virtual_machine** リソースには、**firmware** パラメーターが含まれていませんでした。この問題により、仮想マシンのファームウェアが、**efi** ではなく、**bios** にデフォルトで設定されていました。現在、リソースには **firmware** パラメーターが含まれており、パラメーターのデフォルト値として **efi** が設定されているため、仮想マシンは Basic Input/Output System (BIOS) インターフェイスではなく、Extensible Firmware Interface (EFI) を実行します。(OCPBUGS-9378)

- 以前は、RHOSP 上で実行されるクラスターの場合、インストールのプロビジョニング解除フェーズで、インストーラーはオブジェクトストレージコンテナーを連続的に削除していました。この動作により、特に大きなコンテナーの場合、オブジェクトの削除が遅くなり、非効率的になってしまいました。この問題は、Swift コンテナーを使用するイメージストリームが時間の経過とともにオブジェクトを蓄積したことが原因の 1 つとなり、発生しました。現在、オブジェクトの一括削除は RHOSP API への最大 3 つの呼び出しと同時に行われるようになり、呼び出しあたりにより多くのオブジェクト数を処理することで効率が向上します。この最適化により、プロビジョニング解除中のリソースのクリーンアップが高速化されます。(OCPBUGS-9081)

- 以前は、サブスクリプション ID を指定せずにディスク暗号化を使用し、クラスターを Azure にインストールした場合、インストールプログラムはエラーを表示して終了しませんでした。これにより、インストールは開始しても、その後失敗していました。この更新により、インストールプログラムでは、暗号化された Azure インストールのサブスクリプション ID を指定する必要があり、指定しない場合はエラーを表示して終了するようになりました。(OCPBUGS-8449)

- 以前は、エージェントベースのインストーラーは **ping** や **nslookup** などのセカンダリーチェックの結果を表示していましたが、これはインストールが成功した場合でも、害を及ぼさない形で失敗する可能性がありました。これにより、クラスターが正常にインストールされたにもかかわらず、エラーが表示される可能性がありました。この更新により、セカンダリーチェック

は、プライマリーインストールのチェックが失敗した場合にのみ、結果を表示するようになり、セカンダリーチェックを使用して、失敗したインストールのトラブルシューティングを行うことができるようになりました。(OCPBUGS-8390)

- エージェントベースのインストーラーで IPI **install-config** を使用すると、未使用のフィールドの内容を示す警告ログメッセージが表示されます。以前は、これらの警告にはパスワードなどの機密情報が出力されていました。この更新により、**vsphere** および **baremetal** プラットフォームセクションの認証情報フィールドの警告メッセージが変更され、機密情報が記録されないようになりました。(OCPBUGS-8203)

- 以前は、デフォルトのディスクサイズを検証できなかったため、ノードにカスタムディスクサイズが設定されていない限り、Azure Stack Hub 上のクラスターは新しいコントロールプレーンノードを作成できませんでした。この更新により、デフォルトのディスクサイズが 128 GB に設定され、インストールプログラムは、128 から 1023 GB までのユーザー指定のディスクサイズ値を適用します。(OCPBUGS-6759)

- 以前は、インストーラーがプロビジョニングしたインフラストラクチャーを使用してベアメタルにインストールする場合、インストールプログラムは、ポート 80 を使用してベースボード管理コントローラー (BMC) とデプロイメントエージェントにイメージを提供していました。多くの種類の公共トラフィックではポート 80 が使用されるため、これによりセキュリティー上の懸念が生じる可能性があります。この更新では、インストールプログラムはこの目的でポート 6180 を使用します。(OCPBUGS-8509)

1.6.9. Machine Config Operator

- 以前は、AWS にインストールされた OpenShift Container Platform クラスターは、スケールアップできない 4.1 ブートイメージを使用していました。この問題は、Ignition から設定され、新しいマシンの初回起動時に MCO によってレンダリングおよび起動される 2 つの systemd ユニットが、アプリケーション Afterburn に依存しているために発生しました。OpenShift Container Platform 4.1 ブートイメージには Afterburn が含まれていないため、この問題により新しいノードがクラスターに参加できませんでした。現在、**systemd** ユニットには、Afterburn の存在に依存しないフォールバックコードとともに、Afterburn の追加チェックが含まれています。(OCPBUGS-7559)

1.6.10. 管理コンソール

- 以前は、アラートはログなどの Prometheus 以外のデータソースから読み込まれていました。これにより、すべてのアラートのソースが常に **Prometheus** として表示されるようになりました。この更新により、アラートソースが正しく表示されるようになりました。(OCPBUGS-9907)

- 以前は、Patternfly 4 には、マスターノードのログセクションでログコンポーネントを一度選択すると、それを選択または変更できないという問題がありました。この更新により、マスターノードのログセクションからログコンポーネントを変更した場合にページを更新すると、デフォルトのオプションが再ロードされるようになりました。(OCPBUGS-18727)

- 以前は、**alertmanager-main** ページの **Metrics** タブでルートの詳細を表示すると、空のページが表示されていました。この更新により、ユーザー権限が更新され、**Metrics** タブでルートの詳細を表示できるようになりました。(OCPBUGS-15021)

- 以前は、Red Hat OpenShift Service on AWS はカスタムブランディングを使用していましたが、ファビコンが表示されなくなるため、カスタムブランディングの使用中に特定のブランディングが表示されませんでした。この更新により、Red Hat OpenShift Service on AWS のブランディングが、Branding API の一部になりました。(OCPBUGS-14716)

- 以前は、プロキシーが予期されている場合、OpenShift Container Platform Web コンソールは

モニタリング **Dashboard** ページをレンダリングしませんでした。その結果、WebSocket 接続は失敗しました。この更新により、Web コンソールは環境変数からプロキシー設定も検出するようになりました。(OCPBUGS-14550)

- 以前は、**console.openshift.io/disable-operand delete: "true"** および **operator.openshift.io/uninstall-message: "some message"** アノテーションが Operator CSV で使用されている場合、アンインストール手順が Web コンソールで表示されませんでした。この更新では、インストールをオプトアウトする手順が利用可能になりました。(OCPBUGS-13782)

- 以前は、**PersistentVolumeClaims** namespace の **Details** ページのサイズが正しくありませんでした。この更新により、**PersistentVolumeClaims** namespace の **詳細** ページの Prometheus クエリーに namespace ラベルが含まれ、サイズが正しくなりました。(OCPBUGS-13208)

- 以前は、コンソールとダウンロードのルートをカスタマイズした後、**ConsoleCLIDownloads** リンク内のダウンロードルートが更新されず、デフォルトのダウンロードルートを指していました。この更新により、カスタムダウンロードルートが設定されると、**ConsoleCLIDownloads** リンクが更新されます。(OCPBUGS-12990)

- 以前は、出力プレビューにはリストビューの不完全なトポロジー情報が表示されていました。この更新により、リソースが 1 ページを超える場合、リソースの完全なリストが出力されるようになりました。(OCPBUGS-11219)

- 以前は、応答時間が長いサービスにプロキシーする動的プラグインは 30 秒でタイムアウトし、**504** エラーメッセージが表示されました。この更新により、ほとんどのブラウザーの最大タイムアウトに一致するように、5 分間の HAProxy タイムアウトアノテーションがコンソールルートに追加されました。(OCPBUGS-9917)

- 以前は、提供された API ページでは、提供された API の **displayName** が使用されていましたが、この値は常に設定されているわけではありませんでした。その結果、リストは空でしたが、すべてのインスタンスをクリックして、新しいインスタンスの YAML に引き続きアクセスすることができました。この更新により、**displayName** が設定されていない場合、リストにはテキストが表示されます。(OCPBUGS-8682)

- 以前は、**CronJobs** テーブルと詳細ビューには **suspend** の指示がありませんでした。この更新により、**spec.suspend** が **CronJobs** のリストと詳細ビューに追加されました。(OCPBUGS-8299)

- 以前は、コンソール Operator の設定でシングルプラグインを有効にすると、再デプロイされたコンソールが失敗していました。この更新により、プラグインのリストが一意になり、Pod が期待どおりに実行されるようになりました。(OCPBUGS-5059)

- 以前は、プラグインイメージをアップグレードした後も、古いプラグインファイルが引き続き要求されていました。この更新により、**plugin-entry.js** リソースが要求された際に、**?cacheBuster=${getRandomChars()}** クエリー文字列が追加されました。(OCPBUGS-3495)

1.6.11. モニタリング

- この更新前は、**node-exporter** collected がネットワークインターフェイス情報を収集する方法が原因で、メトリクスのスクレイピング中に大量の CPU リソースが消費される可能性がありました。このリリースでは、ネットワークインターフェイス情報を収集する際の **node-exporter** のパフォーマンスを向上させることでこの問題を修正し、これにより、メトリクスのスクレイピング中の過剰な CPU 使用の問題を解決します。(OCPBUGS-12714)

- この更新前は、Thanos Querier はノードのロールごとにメトリクスの重複を排除できませんでした。この問題はこの更新で修正され、Thanos Querier がノードのロールごとにメトリクスの重複を適切に排除できるようになりました。(OCPBUGS-12525)

- この更新前は、**node-exporter** の **btrfs** コレクターが常に有効になっており、Red Hat Enterprise Linux (RHEL) が **btrfs** ストレージ形式をサポートしていないため、CPU 使用量が増加していました。この更新により、**btrfs** コレクターが無効になり、問題が解決されました。(OCPBUGS-11434)

- この更新前は、**cluster:capacity_cpu_cores:sum** メトリックの場合、**infra** ロールを持つけれども **master** ロールは持たないノードには、**label_node_role_kubernetes_io** ラベルの **infra** 値が割り当てられませんでした。この更新により、**master** ロールではなく **infra** ロールを持つノードが、このメトリックに対して正しく **infra** としてラベル付けされるようになりました。(OCPBUGS-10387)

- この更新前は、起動プローブがないため、Kubernetes API に多くのカスタムリソース定義がインストールされている場合、プログラムの初期化に liveness プローブで許可されている時間よりも長い時間がかかるため、Prometheus アダプター Pod は起動できませんでした。この更新により、Prometheus アダプター Pod は、失敗するまで 5 分間待機する起動プローブを使用して設定されるようになり、問題が解決されました。(OCPBUGS-7694)

- **node_exporter** コレクターは、物理インターフェイスのみのネットワークインターフェイスメトリクスを収集することを目的としていますが、この更新前は、**node-exporter** コレクターはこれらのメトリクスを収集するときに、Calico 仮想ネットワークインターフェイスコントローラー (NIC) を除外しませんでした。この更新により、**cali[a-f0-9]*** 値が **collector.netclass.ignored-devices** リストに追加され、Calico 仮想 NIC のメトリクスが収集されないようになります。(OCPBUGS-7282)

- このリリースでは、セキュリティー対策として、Thanos Querier の Cross Origin Resource Sharing (CORS) ヘッダーがデフォルトで無効になりました。引き続き CORS ヘッダーを使用する必要がある場合は、**ThanosQuerierConfig** リソースの **enableCORS** パラメーターの値を **true** に設定して、CORS ヘッダーを有効にできます。(OCPBUGS-11889)

1.6.12. ネットワーク

- 以前は、クライアント相互 TLS (mTLS) が Ingress コントローラー上で設定されており、CA バンドル内の認証局 (CA) 証明書をダウンロードするために 1 MB を超える証明書失効リスト (CRL) を必要とする場合、サイズ制限のために CRL config map を更新できませんでした。CRL が欠落しているため、有効なクライアント証明書を使用した接続が、**unknown ca** エラーで拒否されていた可能性があります。
  この更新により、CRL は config map に配置されなくなり、ルーターは CRL を直接ダウンロードするようになりました。その結果、各 Ingress コントローラーの CRL config map は存在しなくなります。CRL が直接ダウンロードされるようになり、有効なクライアント証明書を使用した接続は拒否されなくなりました。(OCPBUGS-6661)

- 以前は、OpenShift Container Platform の指定された 512 バイトのバッファーサイズを超える UDP 応答を提供する非準拠のアップストリーム DNS サーバーにより、CoreDNS がオーバーフローエラーをスローしていました。したがって、DNS クエリーに対する応答は提供されません。
  この更新により、ユーザーは **dnses.operator.openshift.io** カスタムリソース (CR) の **protocolStrategy** フィールドを **TCP** に設定できるようになりました。このフィールドを **TCP** に設定すると、CoreDNS はアップストリーム要求に TCP プロトコルを使用し、非準拠のアップストリーム DNS サーバーによる UDP オーバーフローの問題を回避します。(OCPBUGS-6829)

- 以前は、クラスター管理者が **NoExecute** 効果を持つテイントを使用してインフラノードを設定した場合、Ingress Operator のカナリア Pod は、これらのインフラノードでスケジュールされませんでした。しばらくすると、DaemonSet 設定がオーバーライドされ、インフラノード上の Pod が終了しました。
  このリリースでは、Ingress Operator は、**NoExecute** 効果を指定する **node-role.kubernetes.io/infra** ノード taint を許容するように、カナリア DaemonSet を設定するようになりました。その結果、どのような効果が指定されているかに関係なく、カナリア Pod はインフラノード上でスケジュールされます。(OCPBUGS-9274)

- 以前は、Ingress コントローラーでクライアント相互 TLS (mTLS) が設定されている場合、クライアント認証局 (CA) 証明書のいずれかに、別の CA によって発行された CRL の証明書失効リスト (CRL) 配布ポイントが含まれており、その CRL の有効期限が切れた場合、配布 CA と発行 CA の間の不一致により、間違った CRL がダウンロードされていました。その結果、CRL バンドルが更新されて、誤ってダウンロードされた CRL の余分なコピーが含まれることになり、更新する必要のある CRL がなくなっていました。CRL がないため、有効なクライアント証明書を使用した接続が、**unknown ca** というエラーで拒否される可能性がありました。
  この更新により、ダウンロードした CRL はそれらを配布元の CA によって追跡されるようになりました。CRL の有効期限が切れると、配布 CA の CRL 配布ポイントを使用して更新された CRL がダウンロードされます。その結果、有効なクライアント証明書は拒否されなくなりました。(OCPBUGS-9464)

- 以前は、Gateway API が Red Hat OpenShift Service Mesh に対して有効になっている場合、Ingress Operator は設定に失敗し、**the spec.techPreview.controlPlaneMode field is not supported in version 2.4+; use spec.mode** というエラーを返していました。このリリースでは、**ServiceMeshControlPlane** カスタムリソース (CR) の Service Mesh **spec.techPreview.controlPlaneMode** API フィールドが、**spec.mode** に置き換えられました。その結果、Ingress Operator は **ServiceMeshControlPlane** カスタムリソースを作成でき、Gateway API は適切に動作します。(OCPBUGS-10714)

- 以前は、Gateway API ゲートウェイの DNS を設定するときに、リスナーがクラスターのベースドメインの外部にあるドメインのホスト名を指定した場合でも、Ingress Operator はゲートウェイリスナーの DNS レコードを作成しようとしていました。その結果、Ingress Operator は DNS レコードを公開しようとして失敗し、**failed to publish DNS record to zone** というエラーを返しました。
  この更新により、ゲートウェイリスナーの **DNSRecord** カスタムリソース (CR) を作成するときに、ドメインがクラスターの基本ドメイン外にある場合、Ingress Operator は、**DNSRecord's** DNS 管理ポリシーを **Unmanaged** に設定するようになりました。その結果、Ingress Operator はレコードの公開を試行しなくなり、**failed to publish DNS record to zone** というエラーのログも記録されなくなりました。(OCPBUGS-10875)

- 以前は、**oc explain route.spec.tls.insecureEdgeTerminationPolicy** コマンドで、一部のユーザーを混乱させる可能性のある不正確なオプションが記載されていました。このリリースでは、API ドキュメントが更新され、**insecureEdgeTerminationPolicy** で使用できる正しいオプションが示されるようになりました。これは API ドキュメントの修正のみです。(OCPBUGS-11393)

- 以前は、Cluster Network Operator コントローラーが必要以上に広範なリソースのセットを監視していたため、そのリコンサイラーがかなり頻繁にトリガーされていました。その結果、Cluster Network Operator と **kube-apiserver** の両方の負荷が増加しました。
  この更新により、Cluster Network Operator の **allowlist** コントローラーは、**cni-sysctl-allowlist** config map の変更を監視します。その結果、**allowlist** コントローラーのリコンサイラーは、config map が変更されたときにトリガーされるのではなく、**cni-sysctl-allowlist** config map または **default-cni-sysctl-allowlist** config map に変更が加えられた場合にのみトリガーされます。その結果、Cluster Network Operator API リクエストと config map リクエストが減少します。(OCPBUGS-11565)

- HaProxy に関連した **segfault** 障害が解決されました。ユーザーはこれらのエラーを受信しなくなります。(OCPBUGS-11595)

- 以前は、ユーザーがポート番号なしで **EndpointSlice** ポートを作成した場合、CoreDNS が予期せず終了していました。この更新により、CoreDNS が予期せず終了することを防ぐための検証が CoreDNS に追加されました。(OCPBUGS-19805)

- 以前は、バックエンドサービスが 1 つしかない場合、OpenShift ルーターは重み **0** のルートにトラフィックを送信していました。この更新により、ルーターは重み **0** の単一バックエンドを持つルートにトラフィックを送信しなくなります。(OCPBUGS-16623)

- 以前は、Ingress Operator は、ルートに **spec.subdomain** または **spec.host** パラメーターを指定せずに、カナリアルートを作成していました。通常、API サーバーはこれが原因で、デフォルトの Ingress コントローラーのドメインと一致するクラスターの Ingress ドメインを使用して、**spec.host** パラメーターのデフォルト値を設定していました。ただし、代替 Ingress ドメインを設定するために **appsDomain** オプションを使用してクラスターを設定した場合、ルートホストには代替ドメインが設定されます。さらに、カナリアルートを削除すると、デフォルトの Ingress コントローラーのドメインと一致しないドメインでルートが再作成されるため、カナリアチェックが失敗します。現在、Ingress コントローラーは、カナリアルートを作成するときに **spec.subdomain** パラメーターを指定します。**appsDomain** オプションを使用してクラスターを設定してからカナリアルートを削除しても、カナリアチェックは失敗しません。(OCPBUGS-16089)

- 以前は、Ingress Operator は、Operator のステータスを更新するときに、パブリックホスト型ゾーンの DNS レコードのステータスをチェックしませんでした。これにより、パブリックホスト型ゾーンの DNS レコードにエラーがある可能性があると、Ingress Operator が DNS ステータスを **Ready** と報告していました。現在、Ingress Operator はパブリックとプライベートの両方のホスト型ゾーンのステータスをチェックするため、問題は解決されています。(OCPBUGS-15978)

- 以前は、CoreDNS **bufsize** 設定は、512 バイトとして設定されていました。現在、OpenShift Container Platform CoreDNS のバッファーの最大サイズは 1232 バイトです。この変更により、DNS の切り捨てと再試行の発生が減り、DNS のパフォーマンスが向上します。(OCPBUGS-15605)

- 以前は、Ingress Operator は、**spec.template.spec.containers[].ports[].hostPort** を指定せずに、ルーターデプロイメントで **spec.template.spec.hostNetwork: true** パラメーターを指定していました。これにより、API サーバーは各ポートの **hostPort** フィールドにデフォルト値を設定し、続いて Ingress Operator はこれを外部更新として検出し、元に戻そうとしました。現在は、Ingress Operator がこれらの更新を誤って実行することはなくなりました。(OCPBUGS-14995)

- 以前は、起動時に DNS Operator には、**cluster-dns-operator startup has an error message: [controller-runtime] log.SetLogger(...) was never called, logs will not be displayed:** というエラーメッセージが記録されていました。これは、ユーザーに誤解を与える可能性がありました。これで、起動時にエラーメッセージが表示されなくなりました。(OCPBUGS-14395)

- 以前は、Ingress Operator は、**NodePort** および **ClusterIP** タイプのサービスに対して、**spec.internalTrafficPolicy**、**spec.ipFamilies**、および **spec.ipFamilyPolicy** フィールドを未指定のままにしていました。続いて、API はこれらのフィールドにデフォルト値を設定し、Ingress Operator はこれを元に戻そうとします。この更新により、Ingress Operator は初期値を指定し、API のデフォルト値によって引き起こされるエラーを修正しました。(OCPBUGS-13190)

- 以前は、Transmission Control Protocol (TCP) 接続はすべての DNS に対して負荷分散されていました。この更新により、TCP 接続は、ローカル DNS エンドポイントを優先するように有効化されました。(OCPBUGS-9985)

- 以前は、Intel E810 NIC の場合、Pod が削除されたときに Virtual Function (VF) を使用して SR-IOV 上の MAC アドレスをリセットすると、障害が発生していました。これにより、SR-IOV VF を使用して Pod を作成するときに長い遅延が発生しました。この更新により、Container Network Interface (CNI) はこの問題を確実に修正するようになりました。(OCPBUGS-5892)

- 以前は、OpenShift Container Platform で、一部の Pod が **terminating** 状態でスタックするという問題が確認されました。これにより、許可リストコントローラーの調整ループが影響を受け、不要な再試行が発生して複数の Pod が作成されました。この更新により、許可リストコントローラーは現在のデーモンセットに属する Pod のみを検査するようになります。その結果、1 つ以上の Pod の準備ができていないときに再試行は行われなくなります。(OCPBUGS-16019)

1.6.13. OpenShift CLI (oc)

- 以前は、タグとダイジェストの両方を持つコンテナーイメージ参照は oc-mirror プラグインによって正しく解釈されず、次のエラーが発生していました。

  > "localhost:6000/cp/cpd/postgresql:13.7@sha256" is not a valid image reference: invalid reference format

  この動作は修正され、参照が受け入れられ、正しくミラーリングされるようになりました。(OCPBUGS-11840)

- 以前は、パスコンポーネントの数が予想される最大パスコンポーネントを超えた場合に、レジストリーに対して **401 - Unauthorized** エラーが発生していました。この問題は、パスコンポーネントの数が最大パスコンポーネントを超えたときに oc-mirror が失敗するようにすることで、修正されています。整数値を受け入れる **--max-nested-paths** フラグを使用して、最大パスコンポーネントを設定できるようになりました。デフォルトでは、パスコンポーネントの最大数に制限はなく、**0** に設定されています。生成された **ImageContentSourcePolicy** には、リポジトリーレベルまでのソースおよびミラー参照が含まれます。(OCPBUGS-8111, OCPBUGS-11910, OCPBUGS-11922)

- 以前は、oc-mirror フラグの **--short**、**-v**、および **--verbose** は、誤ったバージョン情報を提供していました。oc ミラー **version** フラグを使用して、oc-mirror の正しいバージョンを確認できるようになりました。oc-mirror フラグの **--short**、**-v**、および **--verbose** は非推奨となり、サポートされなくなります。(OCPBUGS-7845)

- 以前は、イメージの複数のダイジェストがタグなしで **imageSetConfig** に指定されていた場合、レジストリーからディスクへのミラーリングが失敗していました。oc-mirror は、デフォルトのタグ **latest** をイメージに追加します。この問題は、省略されたダイジェストをタグとして使用することで修正されました。(OCPBUGS-2633)

- 以前は、oc-mirror が誤って Operator カタログを **ImageContentSourcePolicy** 仕様に追加していました。Operator カタログは **CatalogSource** リソースを通じて宛先レジストリーから直接使用されるため、これは予期しない動作です。このバグは、oc-mirror が Operator カタログを **ImageContentSourcePolicy** のエントリーとして追加しないようにすることで修正されました。(OCPBUGS-10051)

- 以前は、レジストリードメイン名がイメージ参照の一部ではない場合、Operator のイメージのミラーリングは失敗していました。この修正により、レジストリーのドメイン名が指定されていない場合、イメージは **docker.io** からダウンロードされます。(OCPBUGS-10348)

- 以前は、タグとダイジェストの両方がコンテナーイメージ参照に含まれている場合、oc-mirror がそれを誤って解釈し、**invalid reference format** エラーが発生していました。この問題は修正され、イメージは正常にミラーリングされます。(OCPBUGS-11840)

- 以前は、名前が数字で始まる場合は、**CatalogSource** リソースを作成できませんでした。この修正により、デフォルトで、**CatalogSource** リソース名が **cs-** 接頭辞を付けて生成され、RFC 1035 に準拠するようになりました。(OCPBUGS-13332)

- 以前は、**registries.conf** ファイルを使用する場合、一部のイメージがマッピングに含まれていませんでした。このバグ修正により、エラーなしでマッピングに含まれるイメージを確認できるようになりました。(OCPBUGS-13962)

- 以前は、**--oci-registries-config** フラグで参照される **registries.conf** ファイル内の安全でないミラーを使用しているときに、oc-mirror がミラーレジストリーとの HTTPS 接続を確立しようとしました。この修正により、コマンドラインで **--source-skip-tls** または **--source-use-http** を指定することで、HTTPS 接続を使用しないように oc-mirror を設定できるようになりました。(OCPBUGS-14402)

- 以前は、oc-mirror プラグインを使用して OCI インデックスをミラーリングしようとすると、イメージミラーリングが失敗していました。この修正により、oc-mirror プラグインを使用して OCI インデックスをミラーリングできるようになりました。(OCPBUGS-15329)

- 以前は、低帯域幅ネットワーク上で複数の大規模なカタログをミラーリングすると、認証トークンの期限切れによりミラーリングが中断され、結果として **HTTP 401 unauthorized** エラーが発生していました。この問題は、各カタログのミラーリングプロセスを開始する前に、認証トークンを更新することで修正されました。(OCPBUGS-20137)

1.6.14. Operator Lifecycle Manager (OLM)

- この更新前は、Operator Lifecycle Manager (OLM) は、API サーバーがビジー状態のときに、初期化エラーが原因でインストールに失敗する可能性がありました。この更新では、初期化エラーに対する 1 分間の再試行間隔を追加することで、問題が修正されています。(OCPBUGS-13128)

- この更新前は、切断された環境でカスタムカタログがデフォルトの Red Hat カタログと同じ名前を使用すると、競合状態が発生しました。デフォルトの Red Hat カタログが無効になっていた場合、カタログは開始時に作成され、OperatorHub カスタムリソース (CR) が調整された後に削除されました。その結果、カスタムカタログはデフォルトの Red Hat カタログとともに削除されました。この更新により、カタログが削除される前に OperatorHub CR が調整され、競合状態が阻止されます。(OCPBUGS-9357)

- この更新前は、一部の Operator のチャネルが OperatorHub にランダムな順序で表示されていました。この更新により、Operator チャネルが辞書式順序で表示されるようになりました。(OCPBUGS-7910)

- この更新前は、所有者参照ファイルでコントローラーフラグが true に設定されていない場合、レジストリー Pod はオートスケーラーによって正常にドレインされませんでした。この更新により、コントローラーフラグが true に設定され、ドレイン中のノードで強制的なシャットダウンが必要なくなりました。(OCPBUGS-7431)

- この更新前は、証明書の生成方法が原因で、**collect-profiles** Pod により CPU 使用率が定期的に急増していました。この更新により、証明書が毎日生成され、証明書の読み込みが最適化され、CPU 使用率が低下します。(OCPBUGS-1684)

1.6.15. OpenShift API サーバー

- 以前は、**projects** リソースへの更新リクエストとパッチリクエストで、**metadata.namespace** フィールドが自動的に設定されていました。その結果、影響を受けるリクエストにより偽の検証エラーが生成される可能性がありました。このリリースでは、**projects** リソースが自動的に設定されなくなりました。(OCPBUGS-8232)

1.6.16. Red Hat Enterprise Linux CoreOS (RHCOS)

- 以前は、論理ボリュームマネージャー (LVM) メタデータを使用してブロック永続ボリューム要求 (PVC) ストレージにアクセスする OpenShift Container Platform の Pod が終了時にスタックする可能性がありました。これは、同じ LVM デバイスがコンテナー内とホストの両方でアクティブになっていたためです。これは、仮想マシンに LVM を使用する OpenShift Virtualization を使用して、Pod 内で仮想マシンを実行する場合などに発生しました。この更新により、RHCOS はデフォルトで **/etc/lvm/devices/system.devices** ファイルにあるデバイスのセットアップとアクセスのみを試みます。これにより、仮想マシンゲスト内の LVM デバイスへの競合的なアクセスが阻止されます。(OCPBUGS-5223)

- 以前は、Google Cloud Platform (GCP) Confidential Computing インスタンス上で Pod が **ContainerCreating** 状態のままになり、ボリュームマウントが失敗していました。この修正により、Google Cloud Platform の Confidential Computing インスタンスの Persistent Disk ストレージタイプへのサポートが追加され、OpenShift Container Platform で永続ボリュームとして使用できるようになりました。その結果、Pod は **Running** 状態になり、ボリュームをマウントできるようになりました。(OCPBUGS-7582)

1.6.17. ストレージ

- 以前は、IBM Cloud® クラスターでクラスター全体のプロキシーが有効になっている場合、ボリュームのプロビジョニングに失敗しました。(OCPBUGS-18142)

- Storage Operator オブジェクトの **vsphereStorageDriver** フィールドは、非推奨になりました。このフィールドは、OpenShift Container Platform 4.13 vSphere クラスターでの CSI 移行をオプトインするために使用されましたが、OpenShift Container Platform 4.14 以降のクラスターには影響しません。(OCPBUGS-13914)

1.7. テクノロジープレビュー機能

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

テクノロジープレビュー機能のサポート範囲

次の表では、機能は次のステータスでマークされています。

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

1.7.1. ネットワーキングテクノロジープレビュー機能

表1.17 ネットワークのテクノロジープレビュートラッカー

機能	4.12	4.13	4.14
境界クロックとして設定される PTP デュアル NIC ハードウェア	テクノロジープレビュー	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	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	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
PTP グランドマスタークロックとしてのデュアル Intel E810 Westport Channel NIC	利用不可	利用不可	テクノロジープレビュー
Ingress Node Firewall Operator	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
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	テクノロジープレビュー	テクノロジープレビュー
セカンダリーネットワークとしての OVN-Kubernetes ネットワークプラグイン	利用不可	テクノロジープレビュー	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
MT2892 Family [ConnectX-6 Dx] SR-IOV 対応	テクノロジープレビュー	一般提供	一般提供
MT2894 Family [ConnectX-6 Lx] SR-IOV 対応	テクノロジープレビュー	一般提供	一般提供
MT42822 BlueField-2 in ConnectX-6 NIC mode SR-IOV 対応	テクノロジープレビュー	一般提供	一般提供

機能	4.12	4.13	4.14
Silicom STS Family SR-IOV 対応	テクノロジープレビュー	一般提供	一般提供
MT2892 Family [ConnectX-6 Dx] OvS Hardware Offload 対応	テクノロジープレビュー	一般提供	一般提供
MT2894 Family [ConnectX-6 Lx] OvS Hardware Offload 対応	テクノロジープレビュー	一般提供	一般提供
MT42822 BlueField-2 in ConnectX-6 NIC mode OvS Hardware Offload 対応	テクノロジープレビュー	一般提供	一般提供
Bluefield-2 の DPU から NIC への切り替え	テクノロジープレビュー	一般提供	一般提供
Intel E810-XXVDA4T	利用不可	一般提供	一般提供
Egress サービスのカスタムリソース	利用不可	利用不可	テクノロジープレビュー
BGPPeer カスタムリソースの VRF 仕様	利用不可	利用不可	テクノロジープレビュー
NodeNetworkConfigurationPolicy カスタムリソースの VRF 仕様	利用不可	利用不可	テクノロジープレビュー
管理ネットワークポリシー (**AdminNetworkPolicy**)	利用不可	利用不可	テクノロジープレビュー
IPsec 外部トラフィック (north-south)	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1.18 ストレージのテクノロジープレビュートラッカー

機能	4.12	4.13	4.14
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	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
CSI 自動移行 (Azure ファイル、VMware vSphere)	テクノロジープレビュー	一般提供	一般提供
CSI インラインの一時ボリューム	テクノロジープレビュー	一般提供	一般提供
IBM Power® Virtual Server Block CSI Driver Operator	利用不可	テクノロジープレビュー	テクノロジープレビュー
Azure File CSI Operator ドライバーの NFS サポート	一般提供	一般提供	一般提供
Read Write Once Pod アクセスモード	利用不可	利用不可	テクノロジープレビュー
OpenShift ビルドでの CSI ボリュームのビルド	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
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	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1.19 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	4.12	4.13	4.14
kvc を使用したノードへのカーネルモジュールの追加	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

機能	4.12	4.13	4.14
Azure Tagging	利用不可	テクノロジープレビュー	一般提供
SR-IOV デバイスの NIC パーティション設定の有効化	利用不可	テクノロジープレビュー	テクノロジープレビュー
GCP Confidential 仮想マシン	利用不可	テクノロジープレビュー	一般提供
Google Cloud Platform (GCP) のユーザー定義ラベルとタグ	利用不可	利用不可	テクノロジープレビュー
installer-provisioned infrastructure を使用した Alibaba Cloud へのクラスターのインストール	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
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
マルチアーキテクチャーコンピュートマシン	テクノロジープレビュー	一般提供	一般提供
AWS Outposts プラットフォーム	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
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	N/A	N/A	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	N/A	開発者プレビュー	開発者プレビュー
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
vSphere を使用した静的 IP アドレス (IPI のみ)	利用不可	利用不可	テクノロジープレビュー

1.7.4. ノードのテクノロジープレビュー機能

表1.20 ノードのテクノロジープレビュートラッカー

機能	4.12	4.13	4.14
Linux コントロールグループバージョン 2 (cgroup v2)	テクノロジープレビュー	一般提供	一般提供
コンテナーランタイムをクロン	テクノロジープレビュー	一般提供	一般提供
Cron ジョブのタイムゾーン	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
MaxUnavailableStatefulSet featureset	利用不可	利用不可	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1.21 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	4.12	4.13	4.14
IBM Z® および IBM® LinuxONE での IBM Secure Execution	テクノロジープレビュー	一般提供	一般提供
installer-provisioned infrastructure を使用する IBM Power® Virtual Server	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
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

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

機能	4.12	4.13	4.14
Driver Toolkit	一般提供	一般提供	一般提供
ハブアンドスポーククラスターのサポート	テクノロジープレビュー	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1.23 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	4.12	4.13	4.14
etcd レイテンシー許容値の調整	利用不可	利用不可	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
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
factory-precaching-cli ツール	利用不可	テクノロジープレビュー	テクノロジープレビュー
ワーカーノードを使用したシングルノードの OpenShift クラスターの拡張	テクノロジープレビュー	一般提供	一般提供
Topology Aware Lifecycle Manager (TALM)	テクノロジープレビュー	一般提供	一般提供
マウント namespace のカプセル化	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
NUMA Resources Operator による NUMA 対応のスケジューリング	テクノロジープレビュー	一般提供	一般提供
PTP およびベアメタルイベントの AMQP を HTTP トランスポートに置き換え	利用不可	テクノロジープレビュー	テクノロジープレビュー

機能	4.12	4.13	4.14
3 ノードクラスターと標準クラスターのワークロードパーティションの設定	利用不可	テクノロジープレビュー	一般提供

1.7.8. 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機能

表1.24 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	4.12	4.13	4.14
Operator Lifecycle Manager (OLM) v1	利用不可	利用不可	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	テクノロジープレビュー
ハイブリッド Helm Operator	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Java ベースの Operator	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

1.7.9. モニタリングのテクノロジープレビュー機能

表1.25 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	4.12	4.13	4.14
プラットフォームモニタリングメトリクスに基づいたアラートルール	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
メトリクス収集プロファイル	利用不可	テクノロジープレビュー	テクノロジープレビュー

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

表1.26 Hosted Control Plane のテクノロジープレビュー機能トラッカー

機能	4.12	4.13	4.14
Amazon Web Services (AWS) 上の OpenShift Container Platform の Hosted Control Plane	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
ベアメタル上の OpenShift Container Platform の Hosted Control Plane	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
OpenShift Virtualization 上の OpenShift Container Platform の Hosted Control Plane	利用不可	テクノロジープレビュー	一般提供
AWS 上の ARM64 OpenShift Container Platform クラスターの 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
IBM Power 上の OpenShift Container Platform の Hosted Control Plane	利用不可	利用不可	テクノロジープレビュー
IBM Z 上の OpenShift Container Platform の Hosted Control Plane	利用不可	利用不可	テクノロジープレビュー

1.7.11. マシン管理テクノロジープレビュー機能

表1.27 マシン管理のテクノロジープレビュートラッカー

機能	4.12	4.13	4.14
Amazon Web Services の Cluster API を使用したマシン管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Google Cloud Platform の Cluster API を使用したマシン管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Alibaba Cloud のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Amazon Web Services のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	一般提供

機能	4.12	4.13	4.14
Google Cloud Platform のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
IBM Cloud Power VS 用クラウドコントローラーマネージャー	利用不可	テクノロジープレビュー	テクノロジープレビュー
Microsoft Azure のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	一般提供
Nutanix 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
VMware vSphere のクラウドコントローラーマネージャー	テクノロジープレビュー	一般提供	一般提供

1.7.12. 認証と認可のテクノロジープレビュー機能

表1.28 認証と認可のテクノロジープレビュートラッカー

機能	4.12	4.13	4.14
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

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

表1.29 Machine Config Operator のテクノロジープレビュートラッカー

機能	4.12	4.13	4.14
Red Hat Enterprise Linux CoreOS (RHCOS) イメージの階層化	テクノロジープレビュー	一般提供	一般提供

1.8. 既知の問題

- **libreswan** の動作のリグレッションにより、IPsec が有効になっている一部のノードが、同じクラスター内の他のノード上の Pod との通信を失う原因となりました。この問題を解決するには、クラスターの IPsec を無効にすることを検討してください。(OCPBUGS-42952)

- OpenShift Container Platform 4.1 では、匿名ユーザーは検出エンドポイントにアクセスできました。後のリリースでは、一部の検出エンドポイントは集約された API サーバーに転送されるため、このアクセスを無効にして、セキュリティーの脆弱性の可能性を減らすことができます。ただし、既存のユースケースに支障がで出ないように、認証されていないアクセスはアップグレードされたクラスターで保持されます。
  OpenShift Container Platform 4.1 から 4.14 にアップグレードされたクラスターのクラスター管理者の場合は、認証されていないアクセスを取り消すか、許可し続けることができます。認証なしのアクセスが必要な理由が特に無い限り、無効にしてください。認証されていないアクセスを引き続き許可する場合は、それに伴ってリスクが増大することに注意してください。

  警告

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

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

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

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

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

  (BZ#1821771)

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

- インストールプログラムが Google Cloud Platform (GCP) サービスアカウントに関連付けられているすべてのプロジェクトを取得できない場合、インストールは失敗し、**context deadline exceeded** というエラーメッセージが表示されます。
  この現象は、次の条件が満たされる場合に発生します。
  - サービスアカウントが、過剰な数のプロジェクトにアクセスできる場合。
  - インストールプログラムが、次のいずれかのコマンドで実行される場合。
    - **openshift-install create install-config**

      Error message

      > FATAL failed to fetch Install Config: failed to fetch dependency of "Install Config": failed to fetch dependency of "Base Domain": failed to generate asset "Platform": failed to get projects: context deadline exceeded

    - 既存のインストール設定ファイル (**install-config.yaml**) を使用しない **openshift-install create cluster**

      Error message

      > FATAL failed to fetch Metadata: failed to fetch dependency of "Metadata": failed to fetch dependency of "Cluster ID": failed to fetch dependency of "Install Config": failed to fetch dependency of "Base Domain": failed to generate asset "Platform": failed to get projects: context deadline exceeded

    - 既存のインストール設定ファイルを使用、または使用しない **openshift-install create manifests**

      Error message

      > ERROR failed to fetch Master Machines: failed to load asset "Install Config": failed to create install config: platform.gcp.project: Internal error: context deadline exceeded

      回避策として、インストール設定ファイルがある場合は、使用する特定のプロジェクト ID (**platform.gcp.projectID**) でそれを更新します。それ以外の場合は、インストール設定ファイルを手動で作成し、特定のプロジェクト ID を入力します。ファイルを指定して、インストールプログラムを再度実行します。(OCPBUGS-15238)

- 大規模なコンピュートノードでは起動に失敗します。(OCPBUGS-20075)

- IBM Power® 上に **OVNKubernetes** のネットワークタイプを持つクラスターをデプロイすると、カーネルスタックのオーバーフローが原因で、コンピュートノードが再起動する可能性があります。回避策として、ネットワークタイプを **OpenShiftSDN** としてクラスターをデプロイできます。(RHEL-3901)

- 次の既知の問題は、リリース候補 3 または 4 を使用して OpenShift Container Platform デプロイメントを早期アクセスバージョンの 4.14 に更新したユーザーに適用されます。
  ノード識別機能の導入後、root として実行されていた一部の Pod は、特権なしで実行されるように更新されます。OpenShift Container Platform 4.14 の早期アクセスバージョンに更新したユーザーの場合、4.14 の正式バージョンにアップグレードしようとすると進まない可能性があります。このシナリオでは、Network Operator は **DaemonSet "/openshift-network-node-identity/network-node-identity" update is rolling** を報告し、更新の問題を示します。

回避策として、**oc delete --force=true -n openshift-network-node-identity --all pods** コマンドを実行して、**openshift-network-node-identify** namespace 内のすべての Pod を削除できます。このコマンドを実行すると、更新が続行されます。

早期アクセスの詳細は、candidate-4.14 チャネル を参照してください。

- ユーザーは現在、**openshift-multus** namespace の **cni-sysctl-allowlist** config map を更新して、**interface-specific** の安全な sysctl リストを変更できません。回避策として、手動または DaemonSet を使用して、ノード上の **/etc/cni/tuning/allowlist.conf** ファイルを変更できます。(OCPBUGS-11046)

- OpenShift Container Platform 4.14 では、すべてのノードが、デフォルトの RHEL 9 設定に合わせた内部リソース管理に Linux コントロールグループバージョン 2 (cgroup v2) を使用します。ただし、クラスターにパフォーマンスプロファイルを適用する場合、パフォーマンスプロファイルに関連付けられた低遅延チューニング機能は、cgroup v2 をサポートしません。
その結果、パフォーマンスプロファイルを適用すると、クラスター内のすべてのノードが再起動され、cgroup v1 設定に戻ります。この再起動には、パフォーマンスプロファイルの対象になっていないコントロールプレーンノードとワーカーノードが含まれます。

  クラスター内のすべてのノードを cgroups v2 設定に戻すには、**Node** リソースを編集する必要があります。詳細は、Linux cgroup v2 の設定 を参照してください。最後のパフォーマンスプロファイルを削除しても、クラスターを cgroups v2 設定に戻すことはできません。(OCPBUGS-16976)

- OpenShift Container Platform 4.14 を使用してインストールされたクラスターでは、AWS **M4** および **C4** インスタンスが適切に起動できない場合があります。現在のところ回避策はありません。(OCPBUGS-17154)

- このリリースには、インストーラーがプロビジョニングしたインフラストラクチャーを使用して Alibaba Cloud にクラスターをインストールできない既知の問題があります。Alibaba Cloud へのクラスターのインストールは、このリリースではテクノロジープレビュー機能になります。(OCPBUGS-20552)

- ルートボリュームのアベイラビリティーゾーンがあり、4.14 にアップグレードする RHOSP で実行されているクラスターの場合、コントロールプレーンマシンセットを有効にする前に、コントロールプレーンマシンを 1 つのサーバーグループに統合する必要があります。必要な変更を加えるには、knowledge base article の手順に従ってください。(OCPBUGS-13300)

- 少なくとも 1 つのゾーンで設定されたコンピュートゾーンがあり、バージョン 4.14 にアップグレード可能な RHOSP 上で実行されているクラスターの場合、ルートボリュームも少なくとも 1 つのゾーンで設定する必要があります。この設定変更が行われない場合、クラスター用のコントロールプレーンマシンセットを生成できません。必要な変更を加えるには、knowledge base article の手順に従ってください。(OCPBUGS-15997)

- 現時点で、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。このエラーは重大なエラーではありませんが、システムが自動修復する際に、Multus および SR-IOV ログにエラーが表示される場合があります。このエラーにより、Pod の削除に数秒かかる場合があります。(OCPBUGS-11281, OCPBUGS-18822, RHEL-5988)

- **RHEL 5.14.0-284.28.1.el9_2** 以降、特定の MAC アドレスを使用して SR-IOV Virtual Function を設定すると、i40e ドライバーで設定エラーが発生する可能性があります。その結果、Intel 7xx シリーズ NIC に接続の問題が発生する可能性があります。回避策として、Pod リソースの

metadata.annotations フィールドに MAC アドレスを指定しないようにします。代わりに、ドライバーが Virtual Function に割り当てるデフォルトのアドレスを使用してください。(RHEL-7168, OCPBUGS-19536, OCPBUGS-19407, OCPBUGS-18873)

- 現在、**Tuned** リソースの **profile** フィールドで、名前にスラッシュが含まれる設定 (ボンディングデバイスなど) の **sysctl** 値を定義すると、機能しない可能性があります。**sysctl** オプション名にスラッシュが含まれる値は、**/proc** ファイルシステムに正しくマップされません。回避策として、必要な値を使用して設定ファイルを **/etc/sysctl.d** ノードディレクトリーに配置する **MachineConfig** リソースを作成します。(RHEL-3707)

- 現在、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、これが最後の Pod となり、CPU マネージャーは再びこの 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 負荷分散機能に影響を与えます。これらの機能は、CPU マネージャーが使用可能なプールに CPU を解放することに依存しているためです。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 は許可された最後の Pod となり、リソースが使用可能なプールに適切に解放されるようにします。(OCPBUGS-17792)

- 現在、Machine Config Operator (MCO) がワーカープールとカスタムプールのマシン設定を処理する方法が原因で、MCO はカスタムプールに間違った cgroup バージョン引数を適用する可能性があります。その結果、カスタムプール内のノードに間違った cgroup カーネル引数が設定され、予測できない動作が発生する可能性があります。回避策として、ワーカーおよびコントロールプレーンプールのみに cgroup バージョンのカーネル引数を指定します。(OCPBUGS-19352)

- 現在、物理ネットワークデバイスへの **udev** ルールの適用と、すべてのネットワークデバイスへのデフォルトの 1 秒あたりのリクエスト (RPS) マスクの適用との間で競合状態が発生しているため、一部の物理ネットワークデバイスは間違った RPS マスク設定を備えている可能性があります。その結果、RPS マスク設定が正しくない物理ネットワークデバイスに、パフォーマンスの低下による影響が及ぶ可能性があります。今後の z-stream リリースには、この問題の修正が含まれる予定です。(OCPBUGS-21845)

- 従来の Single Root I/O Virtualization (SR-IOV) の Broadcom ネットワークインターフェイスコントローラーは、SRIOV VLAN の quality of service (QoS) および tag protocol identifier (TPID) 設定をサポートしていません。これは、Broadcom BCM57414、Broadcom BCM57508、および Broadcom BCM57504 に影響します。(RHEL-9881)

- デュアルスタックネットワークを使用する環境でホステッドクラスターを作成すると、次の DNS 関連の問題が発生する可能性があります。

  - **service-ca-operator** Pod の **CrashLoopBackOff** 状態: Pod が Hosted Control Plane 経由で Kubernetes API サーバーに到達しようとすると、**kube-system** namespace のデータプレーンプロキシーがリクエストを解決できないため、Pod はサーバーに到達できません。この問題は、HAProxy セットアップでフロントエンドが IP アドレスを使用し、バックエンドが Pod が解決できない DNS 名を使用するために発生します。

  - Pod が **ContainerCreating** 状態でスタックする: この問題は、**openshift-service-ca-operator** が DNS Pod が DNS 解決に必要とする **metrics-tls** シークレットを生成できないために発生します。その結果、Pod は Kubernetes API サーバーを解決できません。

  これらの問題を解決するには、デュアルスタックネットワーク用の DNS の設定 のガイドラインに従って DNS サーバー設定を指定します。(OCPBUGS-22753, OCPBUGS-23234)

- OpenShift Container Platform の Hosted Control Plane では、次の Operator とコンポーネントはテストされていません (OCPSTRAT-605)。
  - Performance Addon Operator
  - OpenShift sandboxed containers
  - Red Hat OpenShift GitOps
  - Red Hat OpenShift Service Mesh
  - Red Hat OpenShift Pipelines
  - Red Hat OpenShift Dev Spaces
  - Red Hat のシングルサインオンテクノロジー
  - OpenShift Container Platform Web コンソールの Web ターミナル
  - Migration toolkit for applications
- OpenShift Container Platform の Hosted Control Plane では、ホスト型クラスターへの File Integrity Operator のインストールが失敗します。(OCPBUGS-3410)
- OpenShift Container Platform の Hosted Control Plane では、Vertical Pod Autoscaler Operator をホスト型クラスターにインストールできません。(PODAUTO-65)
- ベアメタルおよび OpenShift Virtualization プラットフォーム上の OpenShift Container Platform の Hosted Control Plane では、自動修復機能が無効になっています。(OCPBUGS-20028)
- OpenShift Container Platform の Hosted Control Plane では、AWS Secrets Manager または AWS Systems Manager Parameter Store での Secrets Store CSI Driver Operator の使用がサポートされていません。(OCPBUGS-18711)
- OpenShift Container Platform の Hosted Control Plane では、**default**、**kube-system**、および **kube-public** namespace が Pod のセキュリティーアドミッションから適切に除外されません。(OCPBUGS-22379)
- OpenShift Virtualization 上の Hosted Control Plane では、再起動後にワーカーノードがネットワーク接続を失う可能性があります。(OCPBUGS-23208)
- OpenShift Container Platform の Hosted Control Plane では、HyperShift Operator は Operator の初期化中にリリースメタデータを 1 回しか抽出しません。管理クラスターに変更を加えたり、ホストされたクラスターを作成したりしても、HyperShift Operator はリリースメタデータを更新しません。回避策として、Pod のデプロイメントを削除して HyperShift Operator を再起動します。(OCPBUGS-29110)
- OpenShift Container Platform の Hosted Control Plane では、非接続環境で **ImageDigestMirrorSet** オブジェクトと **ImageContentSourcePolicy** オブジェクトのカスタムリソース定義 (CRD) を同時に作成すると、HyperShift Operator が **ImageContentSourcePolicy** CRD を無視して、**ImageDigestMirrorSet** CRD のみのオブジェクトを作成します。回避策として、**ImageDigestMirrorSet** CRD に **ImageContentSourcePolicies** オブジェクト設定をコピーします。(OCPBUGS-29466)
- OpenShift Container Platform の Hosted Control Plane では、非接続環境でホストされたクラスターを作成するときに、**HostedCluster** リソースで **hypershift.openshift.io/control-plane-**

operator-image アノテーションを明示的に設定しないと、ホストされたクラスターのデプロイメントがエラーで失敗します。(OCPBUGS-29494)

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

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

(OCPBUGS-20049)

- このリリースではテクノロジープレビュー機能である Azure 機密仮想マシンには、使用上の既知の問題があります。platform-managed key (PMK) または customer-managed key (CMK) を使用して、マネージドディスクと Azure VM Guest State (VMGS) Blob を暗号化するようにクラスターを設定することは、サポートされていません。この問題を回避するには、**securityEncryptionType** パラメーターの値を **VMGuestStateOnly** に設定して、VMGS Blob の暗号化のみを有効にします。(OCPBUGS-18379)

- このリリースではテクノロジープレビュー機能である Azure 機密仮想マシンには、使用上の既知の問題があります。コントロールプレーンのプロビジョニングプロセスが 30 分後にタイムアウトになるため、この機能を使用するように設定されたクラスターのインストールは失敗します。
この問題が発生した場合は、**openshift-install create cluster** コマンドを 2 回目として実行し、インストールを完了できます。

  この問題を回避するには、マシンセットを使用して既存のクラスターで Confidential VM を有効にします。(OCPBUGS-18488)

- ベアメタルプラットフォーム上で OpenShift Container Platform の Hosted Control Plane を実行する場合、ワーカーノードに障害が発生すると、他のエージェントが使用可能な場合でも、別のノードがホスト型クラスターに自動的に追加されません。回避策として、障害が発生したワーカーノードに関連付けられたマシンを手動で削除します。(MGMT-15939)

- ソースカタログにはアーキテクチャー固有の **opm** バイナリーがバンドルされているため、そのアーキテクチャーからミラーリングを実行する必要があります。たとえば、ppc64le カタログをミラーリングしている場合は、ppc64le アーキテクチャーで実行されているシステムから oc-mirror を実行する必要があります。(OCPBUGS-22264)

- 複数の OpenShift Container Platform グループが同じ LDAP グループを指している場合、1 つの OpenShift Container Platform グループのみが同期されます。**oc adm groups sync** コマンドは、複数のグループが同じ LDAP グループを指している場合、マッピングの対象となるのが 1 つのグループのみであることを示す警告を出力します。(OCPBUGS-11123)

- セキュアブートが無効になっているノード上で、**bootMode** を **UEFISecureBoot** に設定して OpenShift Container Platform をインストールすると、インストールが失敗します。セキュアブートを有効にして OpenShift Container Platform をインストールしようとすると、通常どおり続行されます。(OCPBUGS-19884)

- OpenShift Container Platform 4.14 では、Ignition バージョン 3.4 の **MachineConfig** オブジェクトが、**CrashLoopBackOff** エラーで **api-collector** Pod のスキャンに失敗し、Compliance Operator が想定どおりに動作しなくなる可能性があります。(OCPBUGS-18025)

- OpenShift Container Platform 4.14 では、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への IPv6 egress IP の割り当ては、サポートされていませ

ん。これは既知の問題であり、OpenShift Container Platform の今後のバージョンで修正される予定です。(OCPBUGS-17637)

- 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)

- OpenShift Container Platform クラスターで CNF 遅延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)

- リアルタイムカーネルで **preempt-rt** パッチを使用し、ネットワーク割り込みの SMP アフィニティーを更新すると、対応する IRQ スレッドはすぐには更新を受信しません。代わりに、次の割り込みを受信したときに更新が有効になり、その後スレッドが正しいコアに移行されます。(RHEL-9148)

- 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。想定されるウェイクアップ遅延は 20 µs 未満ですが、**cyclictest** ツールを長時間 (24 時間以上) 実行すると、これを超える遅延が発生することがあります。テストの結果、99.999999% 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。(RHELPLAN-138733)

- グランドマスタークロック (T-GM) として設定されている Intel Westport Channel e810 NIC の Global Navigation Satellite System (GNSS) モジュールは、GPS **FIX** 状態と、GNSS モジュールと GNSS コンステレーション衛生間の GNSS オフセットを報告できます。
現在の T-GM 実装では、GNSS オフセットおよび GPS **FIX** 値を読み取るために、**ubxtool** CLI を使用して **ublox** モジュールをプローブすることはしません。代わりに、**gpsd** サービスを使用して GPS **FIX** 情報を読み取ります。これは、**ubxtool** CLI の現在の実装では応答を受信するのに 2 秒かかり、呼び出しごとに CPU 使用率が 3 倍に増加するためです。(OCPBUGS-17422)

- GNSS からクロック供給される PTP グランドマスタークロックでは、GNSS 信号が失われると、Digital Phase Locked Loop (DPLL) クロック状態が 2 つの方法に変更される可能性があります。つまり、ロック解除に移行するか、ホールドオーバー状態に移行するかのいずれかになります。現在、ドライバーはデフォルトで DPLL 状態をロック解除に移行します。ホールドオーバー状態機能を処理し、どのステートマシン処理を使用するかを設定するためのアップストリームの変更が現在開発中です。(RHELPLAN-164754)

- DPLL サブシステムと DPLL サポートは現在、Intel Westport Channel e810 NIC Ice ドライバーでは有効になっていません。(RHELPLAN-165955)

- 現在の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 から提供される単一の 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 に向かう途中で失われた場合、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。(OCPBUGS-19838)

- 現在、コンテナーの cgroup 階層のセットアップの違いにより、**crun** OCI ランタイムと **PerformanceProfile** 設定を使用するコンテナーでは、パフォーマンスの低下が発生します。回避策として、**runc** OCI コンテナーランタイムを使用します。**runc** コンテナーランタイムは、コンテナーの起動中、シャットダウン操作中、**exec** プローブ中のパフォーマンスが低下しますが、**crun** コンテナーランタイムと **runc** コンテナーランタイムは機能的には同じものです。今後の z-stream リリースには、この問題の修正が含まれる予定です。(OCPBUGS-20492)

- 実行時に IPsec を有効および無効にした後に、**an unknown error has occurred: MultipleErrors** というエラーメッセージを表示して、クラスターが健全でない状態となる既知の問題があります。(OCPBUGS-19408)

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

- RHOSP 17.1 で実行され、ネットワーク機能仮想化 (NFV) を使用するクラスターの場合、RHOSP の既知の問題により、クラスターのデプロイメントが正常に行われません。この問題に対する回避策はありません。Red Hat サポートに連絡して、ホットフィックスをリクエストしてください。(BZ#2228643)

- RHOSP 17.1 での Kuryr インストールはサポートされていません。

- 現在、OpenShift Container Platform 4.14 の HAProxy バージョン 2.6.13 への更新により、再暗号化トラフィックの P99 レイテンシーが増加します。これは、Ingress トラフィックの量により、**IngressController** カスタムリソース (CR) の HAProxy コンポーネントにかなりの負荷がかかる場合に発生します。全体的なスループットは、レイテンシーの増加の影響を受けず、一貫したままになります。
  デフォルトの **IngressController** CR は、4 つの HAProxy スレッドで設定されています。Ingress トラフィック (特に再暗号化トラフィック) が多い状況で、P99 レイテンシーの上昇が発生した場合は、HAProxy スレッドの数を増やしてレイテンシーを減らすことを推奨します。(OCPBUGS-18936)

- 4.14 上のシングルノード OpenShift および Google Cloud Platform (GCP) では、Cloud Network Config Controller (CNCC) が **CrashLoopBackOff** 状態になるという既知の問題があります。これは、CNCC が GCP 内部ロードバランサーアドレスに到達しようとする初期化時に発生し、結果として生じるヘアピントラフィックが GCP 上の OVN-Kubernetes 共有ゲートウェイモードで正しく阻止されず、ドロップされてしまいます。このような場合、Cluster Network Operator は **Progressing=true** ステータスを表示します。現在、この問題に対する回避策はありません。(OCPBUGS-20554)

- CPU が保証されており、割り込み要求 (IRQ) の負荷分散が無効になっているシングルノード OpenShift では、コンテナーの起動時に大きなレイテンシースパイクが発生する可能性があります。(OCPBUGS-22901)

- 多数の Pod があり、その一部に CPU 制限が設定されているアプリケーションをデプロイすると、デプロイが失敗する可能性があります。回避策は、アプリケーションを再デプロイすることです。(RHEL-7232)

- 機能が無効になっているシングルノード OpenShift では、**openshift-controller-manager-operator** が継続的に再起動される可能性があります。回避策として、ビルド機能を有効にするか、**builds.config.openshift.io** CRD を手動で作成します。
  builds.config.openshift.io CRD を手動で作成するには、次の手順を実行します。

  1. 次のコマンドを実行して、リリースマニフェストを展開します。

     ```
     $ oc adm release extract --to manifests
     ```

  2. **manifests** ディレクトリーおよびサブディレクトリー内で **builds.config.openshift.io** を検索します。

     ```
     $ grep -r builds.config.openshift.io manifests
     ```

     予想される出力

     ```
     ```

```
manifests/0000_10_openshift-controller-manager-operator_01_build.crd.yaml:  name: builds.config.openshift.io
```

3. **0000_10_openshift-controller-manager-operator_01_build.crd.yaml** で指定された設定を適用します。

```
$ oc apply -f manifests/0000_10_openshift-controller-manager-operator_01_build.crd.yaml
```

(OCPBUGS-21778)

- Microsoft Azure Stack Hub 上の OpenShift Container Platform のこのバージョンにクラスターをインストールしたり、クラスターを更新したりできない既知の問題があります。詳細と回避策は、こちらの Red Hat ナレッジベースの記事 を参照してください。(OCPBUGS-20548)

- OpenShift Container Platform 4.14.2 より前のバージョン 4.14 で Azure AD Workload Identity を使用する Microsoft Azure クラスターには、既知の問題があります。**eastus** リージョンにおける新しい Azure ストレージアカウントのデフォルトのセキュリティー設定を最近変更したことで、そのリージョンでの Azure AD Workload Identity を使用するクラスターのインストールが阻止されます。現時点では、他のリージョンは影響を受けていないようですが、将来的に影響を受ける可能性があります。
この問題は OpenShift Container Platform 4.14.2 で解決されています。

  この問題を回避するには、短期認証情報を使用するように Azure クラスターを設定する の手順で **ccoctl azure create-all** を実行する前に、パブリックアクセスを許可するストレージアカウントを手動で作成します。

  以下の手順を実行します。

  1. 次の Azure CLI コマンドを実行して、ストレージアカウントのリソースグループを作成します。

```
$ az group create --name <oidc_resource_group_name> --location <azure_region>
```

  2. 次の Azure CLI コマンドを実行して、パブリックアクセスを許可するストレージアカウントを作成します。

```
$ az storage account create --name <storage_account_name> --resource-group <oidc_resource_group_name> --location <azure_region> --sku Standard_LRS --kind StorageV2 --allow-blob-public-access true
```

  3. 次のコマンドを実行し、**ccoctl** ツールを使用してすべての **CredentialsRequest** オブジェクトを処理する場合は、前の手順で作成したリソースを指定する必要があります。

```
$ ccoctl azure create-all \
  --name=<azure_infra_name> \
  --output-dir=<ccoctl_output_dir> \
  --region=<azure_region> \
  --subscription-id=<azure_subscription_id> \
  --credentials-requests-dir=<path_to_credentials_requests_directory> \
  --dnszone-resource-group-name=<azure_dns_zone_resource_group_name> \
  --tenant-id=<azure_tenant_id> \
  --storage-account-name=<storage_account_name> \
  --oidc-resource-group-name=<oidc_resource_group-name>
```

(OCPBUGS-22651)

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

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

     a. マニフェストを作成します。

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

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

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

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

     ip 設定は、次のように置き換えます。

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

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

6 **<fqdn>** は、ノードの完全修飾ドメイン名に置き換えます。

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

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

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

d. クラスターを作成します。

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

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

以前のネットワーク設定の場合は、次のように置き換えます。

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

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

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

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

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

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

(OCPBUGS-17895)

- このリリースには、Web Terminal Operator をインストールした後に、Web Terminal Operator にアクセスできなくなるという既知の問題があります。この問題は、今後の OpenShift Container Platform リリースで修正される予定です。(OCPBUGS-14463)

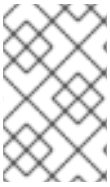
- Cluster Network Operator をバージョン 4.13 から 4.14 にアップグレードする場合、既知の問題が発生します。新しい OVN Kubernetes 相互接続マルチゾーンアーキテクチャーへの変換により、パケットドロップが発生し、短時間のネットワーク停止が発生する可能性があります。**routingViaHost** が **true** に設定されたローカルゲートウェイモードの East/West トラフィックに影響があります。(OCPBUGS-38891)

- OpenShift Container Platform 4.14 の HAProxy には、無効な **Transfer-Encoding** ヘッダーを送信するアプリケーションに関する既知の問題があります。この問題により、これらの無効なヘッダーを送信するルートを公開すると、Pod への外部アクセスが失われます。詳細は、この Red Hat ナレッジベースの記事 の情報を参照してください。(OCPBUGS-43095)

1.9. 非同期エラータの更新

OpenShift Container Platform 4.14 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 4.14 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の通知を有効にできます。エラータ通知を有効にすると、登録されたシステムに関連するエラータが新たに発表されるたびに、メールで通知が送信されます。



注記

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

このセクションは、これからも継続して更新され、OpenShift Container Platform 4.14 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 4.14.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

クラスターの更新 の手順は、OpenShift Container Platform のすべてのリリースで必ず確認してください。

1.9.1. RHSA-2025:16165 - OpenShift Container Platform 4.14.57 のバグ修正とセキュリティー更新

発行日: 2025 年 9 月 25 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.57 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-2025:16165 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-2025:16163 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 4.14.57 --pullspecs
```

1.9.1.1. バグ修正

- この更新前は、影響を受けるバージョンでアプリケーションプログラミングインターフェイス (API) エンドポイント証明書が見つからないため、クラスターのインストールが失敗していました。この現象により、証明書が応答しなくなる問題やインストールの問題が発生しました。このリリースでは、Hosted Control Plane クラスターのインストール中に発生する証明書の問題が解決され、Advanced Cluster Management (ACM) エージェントが停止しなくなりました。(OCPBUGS-61176)

1.9.1.2. 更新

既存の OpenShift Container Platform 4.14 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。

1.9.2. RHSA-2025:14855 - OpenShift Container Platform 4.14.56 のバグ修正とセキュリティー更新

発行日: 2025 年 9 月 4 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.56 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-2025:14855 アドバイザリーに記載されています。この更新に 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 4.14.56 --pullspecs
```

1.9.2.1. バグ修正

- この更新前は、**openshift-ptp** Pod のサイドカーは再起動中に停止するとクラッシュしていました。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、再起動中に **openshift-ptp** Pod のサイドカーが停止しなくなりました。その結果、クロッククラスメトリクスが使用できます。(OCPBUGS-59233)

1.9.2.2. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.3. RHSA-2025:13289 - OpenShift Container Platform 4.14.55 のバグ修正とセキュリティー更新

発行日: 2025 年 8 月 14 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.55 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-2025:13289 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 4.14.55 --pullspecs
```

1.9.3.1. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.4. RHSA-2025:11669 - OpenShift Container Platform 4.14.54 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 31 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.54 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-2025:11669 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-2025:11670 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 4.14.54 --pullspecs
```

1.9.4.1. バグ修正

- この更新前は、ポートが障害状態になったときに、Precision Time Protocol (PTP) Pod が初期のサマリーメトリクスをマスクしていませんでした。その結果、値が変更されないまま新しいインターフェイスが表示され、不正確なデータや古いデータが表示されていました。
  この更新により、PTP Pod はサマリーメトリクスを正しくマスクしてエイリアスを設定するようになりました。これにより、インターフェイスのデータが期待どおりに更新されます。
  (OCPBUGS-55309)

1.9.4.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:9759 - OpenShift Container Platform 4.14.53 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 2 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.53 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-2025:9759 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-2025:9760 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 4.14.53 --pullspecs
```

1.9.5.1. バグ修正

- 以前は、ユーザーが **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。これにより、Hosted Control Plane クラスターに参加しようとする新しいノードの証明書検証で問題が発生していました。このリリースでは、競合を事前に特定してユーザーに警告し、このバグの発生を防ぐための新しい検証が実装されています。(OCPBUGS-57321)

- 以前は、プロキシー環境変数の不適切な処理により外部バイナリーでエラーが発生し、プロキシー設定の形式が不適切であったためにビルドが失敗していました。このリリースでは、プロキシー変数が設定されていない場合は、ビルドプロセスからこの変数を除外することで問題が解決されています。この修正により、この変数が原因でビルドが失敗することがなくなりました。(OCPBUGS-56951)

- 以前は、Hosted Control Plane を使用する OpenShift Container Platform クラスターをデプロイし、検証用に **Kyverno** ポリシーエンジンをデプロイすると、**Konnectivity** サービスが API Pod のリクエストを検証 Webhook に中継することに失敗していました。これにより、クラスター内での追加グループの作成が妨げられていました。このリリースでは、**Konnectivity** サービスのプロキシーの問題が解決され、ユーザーが追加グループを正常に作成できるようになりました。(OCPBUGS-55936)

- 以前は、Time-Grandmaster (T-GM) のホールドオーバー中に、Global Navigation Satellite System (GNSS) ソースが再取得された場合、DPLL (Digital Phase-Locked Loop) がロック状態になる前に、システムが誤って **T-GM-STATUS** を **S2** と通知していました。この早すぎる通知により、T-GM の安定性が損なわれ、GNSS 再取得後のステータスの報告が不正確になっていました。このリリースでは、DPLL が GNSS ソースの可用性に照らして T-GM ステータスを検証してから、**S2** 状態を宣言するようになりました。この変更により、T-GM の安定性が向上し、GNSS の再取得後にステータスの通知が送信されるようになりました。(OCPBUGS-55467)

1.9.5.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:7702 - OpenShift Container Platform 4.14.52 のバグ修正とセキュリティー更新

発行日: 2025 年 5 月 21 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.52 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-2025:7702 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-2025:7704 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 4.14.52 --pullspecs
```

1.9.6.1. バグ修正

- 以前は、現在のプロジェクトがデフォルトの namespace と一致し、コピーされた CSV が Operator Lifecycle Manager (OLM) で無効になっている場合、インストールされた Operator リストに Operator が誤って 2 回表示されていました。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-55942)

- 以前は、OpenShift Container Platform 4.14.52 以降のリリースが、eus-4.14 チャネルに切り替わらずに、stable-4.14 チャネルのままでした。このため、更新情報を取得しようとしたときに 'VersionNotFound' エラーが発生していました。stable-4.14 チャネルではバージョンが見つからないため、推奨される更新を利用できませんでした。このリリースでは、インストーラーが 4.14.52 以降のリリースを Extended Update Support (EUS) チャネルに誘導するようになりました。これにより、各リリースが推奨される更新の通知を受け取れるようになり、**VersonNotFound** エラーが表示されなくなりました。(OCPBUGS-55193)

- 以前は、**openshift-host-network** namespace がユーザーまたはアップグレードによって変更された場合、ネットワークポリシーは VXLAN 仮想ネットワーク ID パラメーターである **VNID** を正しく **0** に設定しませんでした。このリリースでは、namespace が変更された後に VNID パラメーターが正しく設定されるようになりました。(OCPBUGS-54868)

- 以前は、Open Virtual Network (OVN)-Kubernetes による不適切なリモートポートバインディングが原因で、クラスターノードの通信が何度も失われていました。これにより、ノード間の Pod 通信に影響が発生していました。このリリースでは、リモートポートバインディング機能が更新され、OVN によって直接処理されるようになりました。その結果、クラスターノード通信の信頼性が向上しました。(OCPBUGS-48522)

- 以前は、IBM Cloud® 上のクラスターを既存の Virtual Private Cloud (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 リージョンの後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、完全には利用できない VPC リージョンをリソースの検索時に無視するようになりました。(OCPBUGS-48196)

1.9.6.2. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.7. RHSA-2025:4177 - OpenShift Container Platform 4.14.51 のバグ修正とセキュリティー更新

発行日: 2025 年 4 月 30 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.51 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-2025:4177 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 4.14.51 --pullspecs
```

1.9.7.1. バグ修正

- 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すると、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-54264)。

- 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。これらのフラグにより、ロギング、Distributed Tracing Platform、ネットワーク可観測性などの他のプラグインが **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-53437)

- 以前は、**condition.Status** で、ignition-server コントローラーがすべての調整ループで同じメッセージを使用してその条件を更新することにより、Kubernetes エージェントサーバー (KAS) に過負荷をかけていました。このリリースでは、コントローラーはメッセージをチェックし、それが既存のメッセージであるかどうかを検証して、KAS が過負荷状態にならないようにします。(OCPBUGS-53433)

- 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-50592)

- 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) パケットは、サービスを使用してパケットの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、パケットサイズにかかわらず、サービス IP アドレスの代わりに Pod IP アドレスが使用されるため、UDP パケットをエンドポイントに送信できます。(OCPBUGS-50584)

1.9.7.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:3569 - OpenShift Container Platform 4.14.50 のバグ修正とセキュリティー更新

発行日: 2025 年 4 月 9 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.50 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-2025:3569 アドバイザリーに記載されています。

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

以下のコマンドを実行して、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 4.14.50 --pullspecs
```

1.9.8.1. バグ修正

- 以前は、VMware vSphere にクラスターをインストールするには、vSphere 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へ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-54260)
- 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-54167)
- 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 非接続環境における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-53314)
- 以前は、Web コンソールの **Administrator perspective** の **Home** > **Overview** > **Status** ペインで、コード移行操作によって外部ラベルを正しく処理できませんでした。これらの外部ラベルは、サイレント化されたアラート通知が **Status** ペインに追加されるのを防ぐために必要です。**Status** ペインが外部ラベルを正しく処理しなかったため、ペインには **Alert detail** ページへのリンクが表示されましたが、リンクをクリックすると "no matching alerts found" というメッセージが生成されました。このリリースでは、**Status** ペインで外部ラベルが受け入れられるようになったため、アラートをクリックすると正しい **Alert detail** ページにリンクされます。(OCPBUGS-51118)

1.9.8.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:2710 - OpenShift Container Platform 4.14.49 のバグ修正とセキュリティー更新

発行日: 2025 年 3 月 19 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.49 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-2025:2710 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-2025:2712 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 4.14.49 --pullspecs
```

1.9.9.1. バグ修正

- 以前は、コンピュートノードがクラスターから削除された後は、**PersistentVolume** (PV) リソースのプロビジョニングが失敗し、**The object <virtual machine ID> has already been deleted or has not been completely created** というメッセージが表示されました。このリリースでは、修正により、コンピュートノードが削除されても PV リソースのプロビジョニングは影響を受けなくなりました。(OCPBUGS-51045)

- 以前は、リクエストに一致するアドミッション Webhook があると、**deploymentconfig/scale** サブリソースへのリクエストが失敗しました。このリリースでは、問題は解決され、**deploymentconfig/scale** サブリソースへのリクエストは成功します。(OCPBUGS-50477)

- 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-49753)

1.9.9.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:1451 - OpenShift Container Platform 4.14.48 のバグ修正とセキュリティー更新

発行日: 2025 年 2 月 19 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.48 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-2025:1451 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:1453 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 4.14.48 --pullspecs
```

1.9.10.1. 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-49405)

1.9.10.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:0840 - OpenShift Container Platform 4.14.46 のバグ修正とセキュリティー更新

発行日: 2025 年 2 月 6 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.46 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-2025:0840 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-2025:0842 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 4.14.46 --pullspecs
```

1.9.11.1. バグ修正

- 以前は、ターミナルセッションを開いてから切断した場合、crun はコンテナーを停止できませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-48752)
- 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-46603)

1.9.11.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:0364 - OpenShift Container Platform 4.14.45 のバグ修正とセキュリティー更新

発行日: 2025 年 1 月 22 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.45 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-2025:0364 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-2025:0367 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 4.14.45 --pullspecs
```

1.9.12.1. バグ修正

- 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** 状態のままになる可能性がありました。このバグは修正され、オーダーの削除が正しく行われるようになりました。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-48339)

- 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-48245)

- 以前は、ノードの再起動中、特に更新操作中に、再起動中のマシンと対話するノードが短時間 **Ready=Unknown** 状態になりました。この状況により、Control Plane Machine Set Operator は **UnavailableReplicas** 状態になり、その後 **Available=false** 状態になりました。**Available=false** 状態は、緊急のアクションを要求するアラートをトリガーしますが、この場合、介入が必要なのはノードが再起動するまでの短い期間のみでした。このリリースでは、ノードの非準備状態に対する猶予期間が提供されます。この期間中、ノードが非準備状態に入っても、Control Plane Machine Set Operator が即座に **UnavailableReplicas** 条件や **Available=false** 状態に入ることはありません。(OCPBUGS-48211)

- 以前は、マシン削除の優先順位を計算するために使用されていたアルゴリズムでは、一定の経過時間を超えたマシンは、削除が優先されるマシンと同等の優先順位とされていました。このリリースでは、経過時間順に並べられたマークされていないマシンの優先順位が下げられ、削除対象として明示的にマークされたマシンと競合することがなくなりました。アルゴリズムも更新され、10 年経過したマシンまでの経過時間の順序が確保されるようになりました。(OCPBUGS-47659)

- 以前は、OpenShift Container Platform クラスターを 4.14 から 4.15 にアップグレードすると、**use-connection-form.ts** 設定ファイルで **vCenterCluster** パラメーターに値が入力されませんでした。その結果、VMware vSphere GUI に VMware vSphere vCenter 情報が表示されませんでした。このリリースでは、**Infrastructure** カスタムリソース (CR) が更新され、GUI が **vCenterCluster** 値の **cloud-provider-config** config map をチェックするようになりました。(OCPBUGS-45323)

1.9.12.2. 更新

既存の OpenShift Container Platform 4.14 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-2025:0029 - OpenShift Container Platform 4.14.44 のバグ修正とセキュリティー更新

発行日: 2025 年 1 月 9 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.44 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-2025:0029 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-2025:0032 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 4.14.44 --pullspecs
```

1.9.13.1. 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。新しいインスタンスが準備される前にリースの有効期限が切れるまで待機する必要があったため、Operator の新しい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-44726)

- 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。新しい Operator バージョンの既存のカスタムリソース定義 (CRD) の検証で、OLM が非互換性の問題を誤って特定す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-46595)

- 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。このリリースでは、**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、認証の問題は発生しなくなりました。(OCPBUGS-46487)

- 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 に存在するライブ ISO 時刻同期にパッチが適用されます。このパッチは日付の問題を修正し、追加の Network Time Protocol (NTP) サーバーのリストを使用して **/etc/chrony.conf** ファイルを設定します。現在は、**agent-config.yaml** でこれらの追加の NTP サーバーを設定でき、その場合にクラスターインストール問題は発生しなくなりました。(OCPBUGS-45464)

- 以前は、リソースフィールドがペイロードに追加されたときに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、その結果、リソースが非推奨になりました。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、エラーが発生することなく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-39368)

1.9.13.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:11031 - OpenShift Container Platform 4.14.43 のバグ修正とセキュリティー更新

発行日: 2024 年 12 月 18 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.43 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-2024:11031 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-2024:11034 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 4.14.43 --pullspecs
```

1.9.14.1. バグ修正

- 以前は、DNS 1123 サブドメイン名標準により、Kubernetes オブジェクト名の末尾のピリオドは許可されていませんでした。末尾のピリオドを含むカスタムドメイン名を使用して AWS DHCP オプションセットを設定した場合、EC2 インスタンスのホスト名を抽出して Kubelet ノード名に変換するロジックでは、ホスト名の末尾のピリオドは切り捨てられません。このリリースでは、末尾のピリオドを切り捨てるロジックが更新され、DHCP オプションセット内のドメイン名内で末尾のピリオドが許可されるようになりました。(OCPBUGS-46057)

- 以前は、Hosted Control Plane ベースのクラスターは **oc login** コマンドを介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** および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-44279)

1.9.14.2. 更新

既存の OpenShift Container Platform 4.14 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. RHSA-2024:10523 - OpenShift Container Platform 4.14.42 のバグ修正とセキュリティー更新

発行日: 2024 年 12 月 5 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.42 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-2024:10523 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-2024:10526 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 4.14.42 --pullspecs
```

1.9.15.1. バグ修正

- 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-44774)

- 以前は、同期作業の初期化中に Cluster Version Operator (CVO) Pod が再起動すると、Operator はブロックされたアップグレード要求のガードを中断していました。ブロックされた要求が予期せず受け入れられました。このリリースでは、CVO の再起動後もブロックされたアップグレード要求のガードが継続されます。(OCPBUGS-44704)

- 以前は、Cluster Resource Override Operator がオペランドコントローラーを完全にデプロイできなかった場合、Operator はプロセスを再起動していました。Operator がデプロイメントプロセスを試行するたびに、Operator は新しいシークレットのセットを作成しました。その結果、Cluster Resource Override Operator がデプロイされた namespace に大量のシークレットが作成されました。このリリースでは、修正バージョンでサービスアカウントのアノテーションが正しく処理され、シークレットのセットが 1 つだけ作成されます。(OCPBUGS-44435)

1.9.15.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:9620 - OpenShift Container Platform 4.14.41 のバグ修正とセキュリティー更新

発行日: 2024 年 11 月 20 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.41 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-2024:9620 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-2024:9623 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 4.14.41 --pullspecs
```

1.9.16.1. バグ修正

- 以前は、vSphere **resolv-prepender** スクリプトの Machine Config Operator (MCO) は、OpenShift Container Platform 4 の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、OpenShift Container Platform ノードは、手動介入によるブートイメージ 4.13 以降でのスケーリング、またはこの修正を含むリリースへのアップグレードのいずれかのソリューションを使用して、古いブートイメージと互換性があります。(OCPBUGS-42111)

1.9.16.2. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.17. RHSA-2024:8697 - OpenShift Container Platform 4.14.40 のバグ修正とセキュリティー更新

発行日: 2024 年 11 月 7 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.40 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-2024:8697 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-2024:8700 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 4.14.40 --pullspecs
```

1.9.17.1. バグ修正

- 以前は、Google Cloud Platform (GCP) にインストールされたクラスターの Cloud Credential Operator (CCO) は、クラスターが手動モードの認証情報を使用しておらず、**backupdr** API が

有効になっていない場合、**Degraded=True** を入力していました。このリリースでは、更新により、クラスターがこの環境で設定されている場合にクラスターが degraded 状態にならないようにします。(OCPBUGS-43821)

- 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-43468)

- 以前の Hosted Control Plane 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では、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-43368)

- 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-43058)

- 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-42935)

1.9.17.2. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.18. RHSA-2024:8235 - OpenShift Container Platform 4.14.39 のバグ修正とセキュリティー更新

発行日: 2024 年 10 月 23 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.39 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-2024:8235 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-2024:8238 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 4.14.39 --pullspecs
```

1.9.18.1. 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。

1.9.18.1.1. Insights Operator を使用して Prometheus メトリクスからデータを収集する

- Insights Operator (IO) は、Prometheus の **haproxy_exporter_server_threshold** メトリクスからデータを収集するようになりました。(OCPBUGS-41918)

1.9.18.2. バグ修正

- 以前は、Windows ノードのポート 9637 への接続が拒否された場合、CRI-O は Windows ノードでは実行されないため、Kubelet Service Monitor は **target down** アラートをスローしていました。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-42603)

- 以前は、Node Tuning Operator (NTO) が **PerformanceProfiles** 仕様を使用して設定されていたときに、kubelet の前に実行され、NTO の実行をブロックする **ocp-tuned-one-shot systemd** サービスが作成されていました。これにより、Podman はイメージを取得できなくなりました。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利用可能となりました。これにより、Podman は、クラスター外接続に http (s) プロキシーを使用する必要がある環境に NTO イメージをプルできるようになります。(OCPBUGS-42567)

- 以前は、**Pod** リソースに **spec.securityContext.runAsGroup** 属性が設定されている場合、コンテナー内の **/etc/group** にグループ ID が追加されませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-41246)

- 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含まれている場合、検査プロセスが失敗し、**lsblk** コマンドをエスケープできませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-39019)

- 以前は、Pipelines Operator をインストールした後でも、Pipeline テンプレートが利用可能になる前に、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、選択したリソースで Pipeline テンプレートが利用できない場合は、**Import from Git** ページの **Create** ボタンが無効になります。(OCPBUGS-37353)

- 以前は、ノード登録の問題により、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ことができませんでした。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。このリリースでは、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-32266)

1.9.18.3. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.19. RHSA-2024:7184 - OpenShift Container Platform 4.14.38 のバグ修正とセキュリティー更新

発行日: 2024 年 10 月 3 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.38 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-2024:7184 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-2024:7187 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 4.14.38 --pullspecs
```

1.9.19.1. 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。

1.9.19.1.1. 設定可能なサブネットのバックポート

- このリリースには、マスカレードを設定するために使用できる設定可能なサブネットが含まれています。また、設定可能なサブネットを使用してサブネットを結合および移行し、ローカルインフラストラクチャーで使用されている IP アドレスとの重複を防ぐこともできます。(OCPBUGS-38440)

1.9.19.2. バグ修正

- 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-42184)

- 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 がクラスターノードの障害から回復し、問題が解決されます。(OCPBUGS-42150)

- 以前は、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、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した場合、クラスターでは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-42021)

- 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、クラスター内のすべてのカスタムリソース (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 を持つクラスターでは、**apiserver** のタイムアウトやアップグレードの停止が発生する可能性があります。このリリースにより、この問題は解決されました。(OCPBUGS-42017)

- 以前は、OpenShift Container Platform Web コンソールの **Topology** ビューには最大 100 個のノードしか表示できませんでした。100 を超えるノードを表示しようとすると、Web コンソールに **Loading is taking longer than expected** エラーメッセージが出力されます。このリリースでは、Web コンソールの **MAX_NODES_LIMIT** パラメーターが **200** に設定され、Web コンソールに最大 200 個のノードを表示できるようになりました。(OCPBUGS-41581)

- 以前は、**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) を使用するようにホストされたクラスターを設定すると、プロキシー経由で送信されたときに IdP ホスト名が解決されませんでした。このリリースでは、IdP トラフィックがプロキシー経由で送信される前に DNS ルックアップ操作によって IdP がチェックされるため、ホスト名を持つ IdP はデータプレーンによってのみ解決され、Control Plane Operator (CPO) によって検証されるようになります。(OCPBUGS-41374)

- 以前は、クラスター内で多数のシークレットを起動または再起動すると、Cloud Credential Operator (CCO) によってエラーが発生していました。CCO は同時にシークレットを入手しようとしました。このリリースでは、CCO はシークレットを 100 個ずつバッチで取得し、問題が解決されました。(OCPBUGS-41236)

- 以前は、ノードが準備完了になるまでの猶予期間は、アップストリームの動作と一致していませんでした。場合によっては、猶予期間により、ノードが **Ready** および **Not ready** 状態の間を循環することがありました。このリリースでは、猶予期間によってノードが 2 つの状態間を循環することがないように問題が修正されました。(OCPBUGS-39378)

- 以前は、クラスターのアップグレード後に **openvswitch** サービスは古いクラスター設定を使用していたため、**openvswitch** サービスが停止していました。このリリースでは、クラスターのアップグレード後に **openvswitch** サービスが再起動され、新しいクラスター設定を使用するようになりました。(OCPBUGS-39192)

- 以前は、ホストされた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。
  OpenShift Container Platform との互換性を保つために、HTTPS または HTTP プロトコル経由の IdP 通信はプロキシーする必要がありますが、LDAP 通信はプロキシーすることはできません。このタイプのプロキシーでは、トラフィックが Konnectivity エージェントに到達するまでに宛先 IP アドレスのみ使用可能になるため、ホスト名に依存する **NO_PROXY** エントリーも無視されます。つまり、宛先 IP アドレスのみが使用可能です。このリリースでは、ホストされたクラスターで、**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プロキシートラフィックが停止されます。その結果、LDAP サーバー宛のトラフィックはプロキシーされなくなります。その他の HTTPS または HTTPS トラフィックは正しくプロキシーされます。ホスト名を指定すると、**NO_PROXY** 設定が適用されます。(OCPBUGS-38066)

- 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ませんでした。プロキシーを必要とするプロトコル (HTTP または HTTPS) 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-38060)

1.9.19.3. 既知の問題

- **bootstrap-kubeconfig** ファイルで誤った **api-server** ポートが使用されているため、AWS に自己管理型のホストされたプライベートクラスターのデプロイが失敗します。その結果、AWS インスタンスはプロビジョニングされますが、ホストされたクラスターにノードとして参加することはできませんでした。(OCPBUGS-42221)

1.9.19.4. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.20. RHSA-2024:6689 - OpenShift Container Platform 4.14.37 のバグ修正とセキュリティー更新

発行日: 2024 年 9 月 19 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.37 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-2024:6689 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 4.14.37 --pullspecs
```

1.9.20.1. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.21. RHSA-2024:6406 - OpenShift Container Platform 4.14.36 のバグ修正とセキュリティー更新

発行日: 2024 年 9 月 11 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.36 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-2024:6406 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-2024:6412 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 4.14.36 --pullspecs
```

1.9.21.1. 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。

1.9.21.1.1. 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-39160)

1.9.21.1.2. Ingress Controller 証明書の収集

- Insights Operator は、すべての Ingress Controller 証明書 (NotBefore 日付と NotAfter 日付) に関する情報を収集するようになりました。データは 'aggregated/ingress_controllers_certs.json' パスの JSON ファイルに集約されます。(OCPBUGS-37673)

1.9.21.2. PTP グランドマスタークロックの自動うるう秒処理

PTP Operator は、Global Positioning System (GPS) のアナウンスを使用して、うるう秒ファイルを自動的に更新するようになりました。

うるう秒情報は、**openshift-ptp** namespace の **leap-configmap** という名前の自動生成された **ConfigMap** リソースに保存されます。

詳細は、PTP グランドマスタークロックの動的うるう秒処理の設定 を参照してください。

1.9.21.3. バグ修正

- 以前は、仮想マシン (VM) が削除されても、その仮想マシンのネットワークインターフェイスコントローラー (NIC) が引き続き存在する場合、Microsoft Azure 仮想マシン検証チェックがクラッシュしていました。このリリースでは、検証チェックはクラッシュすることなく問題を適切に処理します。(OCPBUGS-39413)

- 以前は、Cluster Monitoring Operator (CMO) が Prometheus リモート書き込みエンドポイントのプロキシー機能を設定するときに、クラスター全体のプロキシーの **spec.noProxy** フィールドは考慮されませんでした。このリリースでは、CMO は、**noProxy** フィールドに従ってプロキシーをバイパスする 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機能を設定しなくなりました。(OCPBUGS-39176)

- 以前は、**oc logs -f <pod>** を実行すると、ログファイルがローテーションされた後、ログは何も出力しませんでした。このリリースでは、kubelet はファイルのローテーション後にログファイルを出力するため、問題が解決されました。(OCPBUGS-38959)

- 以前は、OpenShift Container Platform Web コンソールはベアメタルノードの再起動に失敗していました。このリリースではこの問題が修正され、OpenShift Container Platform Web コンソールを使用してベアメタルノードを再起動できるようになりました。(OCPBUGS-38053)

- 以前は、Cloud Credential Operator (CCO) がパススルーモードの権限が正しいかどうかを確認すると、CCO は Google Cloud Platform (GCP) API からプロジェクトの無効な権限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、CCO が degraded 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、CCO は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-37823)

- 以前は、カスタムリソース (CR) の更新後に、TuneD プロファイルが不必要に再ロードされる可能性がありました。このリリースでは、TuneD オブジェクトが削除され、TuneD プロファイルは TuneD プロファイル Kubernetes オブジェクトに直接保持されます。その結果、問題は解決されました。(OCPBUGS-37754)

1.9.21.4. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.22. RHSA-2024:5433 - OpenShift Container Platform 4.14.35 のバグ修正とセキュリティー更新

発行日: 2024 年 8 月 22 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.35 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-2024:5433 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-2024:5436 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 4.14.35 --pullspecs
```

1.9.22.1. 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。

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

- OpenShift Container Platform リリース 4.14.35 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 または コントロールプレーン マシーンセットに関する **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)

1.9.22.1.2. Kubernetes v1.27.16 への更新

- このリリースには、Kubernetes v1.27.16 への更新による更新が含まれています。(OCPBUGS-37623)

1.9.22.2. バグ修正

- 以前は、**OVNKubernetesNorthdInactive** アラートは期待どおりに発生しませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-38073)

- 以前は、使用できないノードの数よりも高い **maxUnavailable** 値を持つマシン設定プール (MCP) により、閉鎖されたノードがノードリストの特定の位置にある場合に更新を受信していました。このリリースでは、修正により、閉鎖されたノードが更新を受信するためのキューに追加されなくなります。(OCPBUGS-37738)

- 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** 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-37175)

- 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-33590)

1.9.22.3. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.23. RHSA-2024:4960 - OpenShift Container Platform 4.14.34 のバグ修正とセキュリティー更新

発行日: 2024 年 8 月 7 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.34 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-2024:4960 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-2024:4963 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 4.14.34 --pullspecs
```

1.9.23.1. 機能拡張

1.9.23.1.1. Ingress Controller API に connectTimeout チューニングオプションを追加する

- IngressController API は、新しいチューニングオプション **ingresscontroller.spec.tuningOptions.connectTimeout** で更新されました。このオプションは、バックエンドサーバーへの接続を確立するときにルーターが応答を待機する時間を定義します。(OCPBUGS-36555)

1.9.23.1.2. Insights Operator による Prometheus および AlertManager リソースの収集

- Insights Operator は、**openshift-monitoring** namespace の外部で **Prometheus** および **AlertManager** リソースを収集するようになりました。(OCPBUGS-36380)

1.9.23.2. バグ修正

- 以前は、AWS HyperShift クラスターは VPC のプライマリー CIDR 範囲を活用して、データプレーン上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、この問題を解決するために、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るようになりました。(OCPBUGS-36159)

- 以前は、Pod が一致するノードのないノードセレクターを指定した場合、Kubernetes スケジューラーでパニックが発生、"Observed a panic: integer divide by zero" というエラーが表示されました。このリリースでは、Kubernetes スケジューラーコードベースの問題が解決され、Pod が一致するノードのないノードセレクターを指定しても、Kubernetes スケジューラーがパニックに陥らなくなりました。(OCPBUGS-36397)

- 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。このリリースでは、Operator Lifecycle Manager (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、問題が解決されました。(OCPBUGS-36452)

- 以前は、Operator に既存ルートの **spec.host** または **spec.subdomain** を更新する権限がなかったため、Ingress Operator はカナリアルートを正常に更新できませんでした。このリリースでは、Operator のサービスアカウントのクラスターロールに必要な権限が追加され、Ingress Operator はカナリアルートを更新できるようになりました。(OCPBUGS-36467)

- 以前は、routing-via-host の OVN-Kubernetes 設定が共有ゲートウェイモードのデフォルト値に設定されていた場合、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ませんでし

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、問題が解決されました。(OCPBUGS-36554)

- 以前は、Amazon Web Services (AWS) Security Token Service (STS) では、Cloud Credential Operator (CCO) が **CredentialsRequest** の **awsSTSIAMRoleARN** 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。このリリースでは、CCO はエラーをログに記録しなくなり、問題が解決されました。(OCPBUGS-36716)

- 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を及ぼす可能性があります。この更新により、OVS ピンニング手順によって各 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-37197)

1.9.23.3. 既知の問題

- SR-IOV Network Operator がインストールおよび設定されているクラスターでは、SR-IOV VF のセカンダリーインターフェイスを持つ Pod が失敗し、**SRIOV-CNI failed to configure VF "failed to set vf 0 vlan configuration - id 0, qos 0 and proto 802.1q: invalid argument"** というエラーメッセージが表示されます。この問題を解決するには、OpenShift Container Platform をアップグレードする前に、SR-IOV Network Operator をアップグレードします。これにより、この問題の修正が SR-IOV Network Operator に含まれるようになります。(OCPBUGS-38091)

1.9.23.4. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.24. RHSA-2024:4479 - OpenShift Container Platform 4.14.33 のバグ修正とセキュリティー更新

発行日: 2024 年 7 月 17 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.33 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-2024:4479 アドバイザリーに記載されています。この更新には 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 4.14.33 --pullspecs
```

1.9.24.1. バグ修正

- 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起動されたノードは、プロビジョニング中にスタックしていました。このリリースでは、バイナリーが更新され、問題が解決されました。(OCPBUGS-36776)

- 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 4.14 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-36593)

- 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完了した場合、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識別しなかったため、**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 ロジックが変更され、stateroot を分析できるようになり、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-36437)

- 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-31354)

- 以前は、DNS Operator は、クラスターに少なくとも 2 つのアベイラビリティーゾーンで使用可能な CPU を備えた準備完了ノードがあるかどうかを確認せず、DNS デーモンセットはローリング更新にサージを使用していませんでした。その結果、すべてのノードが同じアベイラビリティーゾーンにあるクラスターは、クラスター DNS サービスに対して **TopologyAwareHintsDisabled** イベントを繰り返し発行しました。このリリースでは、複数のアベイラビリティーゾーンにノードがないクラスターでは **TopologyAwareHintsDisabled** イベントが生成されなくなり、問題は解決されました。(OCPBUGS-5943)

1.9.24.2. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.25. RHSA-2024:4329 - OpenShift Container Platform 4.14.32 のバグ修正とセキュリティー更新

発行日: 2024 年 7 月 11 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.32 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-2024:4329 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-2024:4332 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 4.14.32 --pullspecs
```

1.9.25.1. 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。

1.9.25.1.1. パイプラインプラグインの新しいカスタムリソース定義

このリリースでは、パイプライン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-35723)

1.9.25.1.2. etcd のデフラグ用コントローラー

このリリースでは、Hypershift でホストされているクラスターの etcd をデフラグメントするコントローラーが導入されています。(OCPBUGS-35723)

1.9.25.2. バグ修正

- 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-36416)

- 以前は、OpenShift Container Platform の古いバージョンから更新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。この修正により、古い OpenShift Container Platform バージョンから問題のある古いデータが削除され、この種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す。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-36356)

- 以前は、**growpart** のバグによりデバイスがロックされ、LUKS で暗号化されたデバイスが開けなくなっていました。システムは正常に起動できません。このリリースでは、**growpart** がプロセスから削除され、システムは正常に起動するようになりました。(OCPBUGS-35989)

- 以前は、古いバージョンから更新された user-provisioned infrastructure 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、特定のチェックが失敗する可能性がありました。このリリースでは、**infrastructures.config.openshift.io** に利用可能なものがない場合、フォールバック **failureDomains** が **cloudConfig** から合成されます。(OCPBUGS-35913)

- 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かったため、インストールが失敗していました。この更新により、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くなり、インストールを続行できるようになります。(OCPBUGS-35827)

- 以前は、systemd のバグにより、**coreos-multipath-trigger.service** ユニットが永久にハングする可能性がありました。システムの起動が完了できません。このリリースでは、systemd が削除され、起動が成功しました。(OCPBUGS-35750)

- 以前は、管理側のクラスター管理者によって設定されたレジストリーオーバーライドが、関連のないデータプレーンコンポーネントに適用されていました。このリリースでは、レジストリーオーバーライドがこれらのコンポーネントに適用されなくなりました。(OCPBUGS-35549)

- 以前は、OpenShift Cluster Manager コンテナーには適切な 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-35482)

- 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-35401)

- 以前は、Hypershift の secrets-store CSI ドライバーは、Hypershift CLI の問題により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-35183)

- 以前は、**!ens0** などの反転ルールでは、ネットワークキューの削減が期待どおりに機能しませんでした。これは、生成された Tuned プロファイルで感嘆符記号が重複していたために発生しました。このリリースでは重複が発生しなくなり、反転したルールが意図したとおりに適用されるようになりました。(OCPBUGS-35012)

- 以前は、競合状態により、Kubelet がボリュームリサイザーからのサイズ変更の失敗に関連する誤ったエラーを報告する可能性がありました。このリリースでは、競合状態が修正され、誤ったエラーは出力されなくなりました。(OCPBUGS-33964)

- 以前は、vSphere 接続を編集するときにエスケープされた文字列が適切に処理されず、vSphere 設定が壊れていました。この更新により、エスケープ文字列が期待どおりに機能し、vSphere 設定が壊れなくなりました。(OCPBUGS-33942)

- 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-33590)

- 以前は、ノード上で **kubelet** サービスを手動で再起動すると、想定されるノードの再起動後に一部の状態ファイルが削除され、kubelet によって CPU マネージャーの状態がリセットされていました。状態がリセットされると、CPU マネージャーは実行中のワークロードへの新しい CPU 割り当てを計算します。その結果、新規かつ初期の **cpuset** 設定が異なる場合があります。この更新により、kubelet の再起動後に **cpuset** 設定が正しく復元されるようになりました。(OCPBUGS-32472)

1.9.25.3. 更新

既存の OpenShift Container Platform 4.14 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. RHSA-2024:4010 - OpenShift Container Platform 4.14.31 のバグ修正とセキュリティー更新

発行日: 2024 年 6 月 26 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.31 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-2024:4010 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-2024:4013 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 4.14.31 --pullspecs
```

1.9.26.1. バグ修正

- 以前は、ホストからノードの名前を取得するロジックは複数の値を考慮せず、スペースを含む名前に対して複数の値が返されたときに予期せず終了していました。このリリースでは、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、問題が解決されました。(OCPBUGS-34716)

1.9.26.2. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.27. RHSA-2024:3881 - OpenShift Container Platform 4.14.30 のバグ修正とセキュリティー更新

発行日: 2024 年 6 月 19 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.30 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-2024:3881 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-2024:3918 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 4.14.30 --pullspecs
```

1.9.27.1. 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。

1.9.27.1.1. プルシークレットパスワードにコロン文字を許可する

このリリースでは、OpenShift Container Platform Assisted Installer のプルシークレットパスワードにコロン文字を含める機能が追加されました。(OCPBUGS-35034)

1.9.27.1.2. Cinder CSI Driver のトポロジー機能の設定

以前は、トポロジー機能を無効にできなかったため、Cinder CSI Driver のトポロジー機能は常にアクティブでした。このリリースでは、トポロジー機能はコンピュートとストレージのアベイラビリティーゾーンに基づいており、トポロジー機能を無効にすることができます。(OCPBUGS-34792)

1.9.27.2. バグ修正

- 以前は、OpenShift Container Platform Assisted Installer はインストールされた SATA SDD を取り外し可能として報告し、いずれもインストールターゲットとして使用しませんでした。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となり、問題が解決されました。(OCPBUGS-35085)

- 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-34856)

- 以前は、クラスターまたは BareMetal Host (BMH) を削除すると、クラスターの削除中に **PreprovImage** イメージが作成されていました。その結果、クラスターリソースがスタックしました。このリリースでは、削除段階の前に電源をオフにする例外が作成され、問題が解決されました。(OCPBUGS-34814).

- 以前は、Image Registry Operator 設定で、**regionEndpoint** を使用して **virtualHostedStyle** パラメーターを有効にすると、イメージレジストリーは **virtualHostedStyle** を無視し、起動に失敗しました。このリリースでは、**virtualHostedStyle** の使用が廃止され、代わりに **ForcePathStyle** が使用されるため、問題が修正されました。(OCPBUGS-34668)

- 以前は、OpenShift Container Platform 4.15.8 から 4.15.11 にアップグレードすると、FIPS モードの有効化に関連するインストールの失敗により、**metal3-ironic** および **metal3-ironic-inspector** Pod が失敗していました。このリリースにより、この問題は解決されました。(OCPBUGS-34657).

- 以前は、OVN-Kubernetes ネットワークプラグインは、状況によっては Egress IP アドレスをあるノードから別のノードに転送できないため、新しいノードの Medium Access Control (MAC) アドレスを通知するための無償の Address Resolution Protocol (ARP) 要求をピアに送信することができませんでした。その結果、フェイルオーバーの問題が発生しました。このリリースでは、OVN-Kubernetes ネットワークプラグインは、フェイルオーバーの問題を引き起こすことなく、新しいノードの Medium Access Control (MAC) アドレスをピアに正しく通知します。(OCPBUGS-34570)

- 以前は、ブートストラッププロセス中に **wait-for-ceo** コマンドを使用した場合、失敗した場合にコマンドはエラーメッセージを報告しませんでした。このリリースでは、コマンドは **bootkube** スクリプト内でエラーメッセージを表示して報告します。(OCPBUGS-34495)

- 以前は、インストールプログラムは **ca-west-1** Amazon Web Services (AWS) リージョンをサポートしていませんでした。このリリースでは、**ca-west-1** リージョンがサポートされ、問題が解決されました。(OCPBUGS-34024)

1.9.27.3. 更新

既存の OpenShift Container Platform 4.14 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-2024:3697 - OpenShift Container Platform 4.14.29 のバグ修正とセキュリティー更新

発行日: 2024 年 6 月 13 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.29 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-2024:3697 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-2024:3700 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 4.14.29 --pullspecs
```

1.9.28.1. バグ修正

- 以前は、Red Hat OpenStack Platform (RHOSP) 上の OpenShift Container Platform デプロイメントで、**MachineSet** オブジェクトが **Port Security** パラメーターの値を正しく適用していませんでした。これは、RHOSP サーバーのポートの **port_security_enabled** パラメーターに予期しない値が含まれていることを意味しました。このリリースでは、**MachineSet** オブジェクトが **port_security_enabled** フラグを期待どおりに適用します。(OCPBUGS-32428)

- 以前は、**IngressController** オブジェクトがクライアント SSL/TLS で設定されていても、**clientca-configmap** ファイナライザーがない場合、Ingress Operator は **IngressController** オブジェクトが削除対象としてマークされているかどうかを確認せずにファイナライザーを追加しようとしました。その結果、**IngressController** がクライアント SSL/TLS で設定され、その後削除された場合、Operator はファイナライザーを正しく削除しました。その後、Operator は、ファイナライザーを追加し直すために繰り返し、そして誤って **IngressController** オブジェクトを更新しようとして失敗し、Operator のログにエラーメッセージが記録されました。この更新により、Ingress Operator は、削除対象としてマークされた **IngressController** オブジェクトに **clientca-configmap** ファイナライザーを追加しなくなりました。その結果、Ingress Operator は誤った更新を実行しようとしなくなり、関連するエラーをログに記録しなくなりました。(OCPBUGS-34410)

1.9.28.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:3523 - OpenShift Container Platform 4.14.28 のバグ修正更新とセキュリティー更新

発行日: 2024 年 6 月 10 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.28 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-2024:3523 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-2024:3526 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 4.14.28 --pullspecs
```

1.9.29.1. バグ修正

- 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-33844)

- 以前は、Hosted Control Plane (HCP) のリサイクラー Pod が非接続環境で起動していませんでした。このリリースでは、HCP recycler-pod イメージが OpenShift Container Platform ペイロード参照を指すようになり、問題が解決されました。(OCPBUGS-33843)

- 以前は、**imageRegistryOverrides** からの情報は、HyperShift Operator の初期化時に 1 回だけ抽出され、更新されませんでした。このリリースでは、HyperShift Operator が管理クラスター

から新しい **ImageContentSourcePolicy** ファイルを取得し、そのファイルを各調整ループで HyperShift Operator と Control Plane Operator に追加します。(OCPBUGS-33713)

- 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-33321)

1.9.29.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:3331 - OpenShift Container Platform 4.14.27 のバグ修正更新とセキュリティー更新

発行日: 2024 年 5 月 30 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.27 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-2024:3331 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-2024:3335 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 4.14.27 --pullspecs
```

1.9.30.1. バグ修正

- 以前は、多数の内部サービスまたはユーザー管理のロードバランサー IP アドレスを使用して OpenShift Container Platform クラスターを設定すると、OVN-Kubernetes サービスの起動時間が遅延していました。この遅延は、OVN-Kubernetes サービスがノードに **iptables** ルールをインストールしようとしたときに発生しました。このリリースでは、OVN-Kubernetes サービスは数秒で多数のサービスを処理できるようになります。さらに、新しいログにアクセスして、ノードへの **iptables** ルールのインストールのステータスを表示することもできます。(OCPBUGS-33537)

- 以前は、OpenShift Container Platform Web コンソールの **トポロジー** ビューには、仮想マシン (VM) ノードとその他の非仮想マシンコンポーネント間のビジュアルコネクターが表示されませんでした。このリリースでは、ビジュアルコネクターにコンポーネントのインタラクションアクティビティーが表示されます。(OCPBUGS-33640)

- 以前は、OpenShift Container Platform Web コンソールのマストヘッド要素のロゴの高さが 60 ピクセルを超えて大きくなる可能性がありました。これによりマストヘッドが増加しました。このリリースでは、マストヘッドロゴの **max-height** が 60 ピクセルに制限されます。(OCPBUGS-33635)

1.9.30.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:2869 - OpenShift Container Platform 4.14.26 のバグ修正更新とセキュリティー更新

発行日: 2024 年 5 月 23 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.26 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-2024:2869 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-2024:2873 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 4.14.26 --pullspecs
```

1.9.31.1. 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。

1.9.31.1.1. OperatorHub フィルターの名前が FIPS Mode から Designed for FIPS に変更されました

- 以前は、OperatorHub には **FIPS Mode** というフィルターが含まれていました。このリリースでは、そのフィルターの名前が **Designed for FIPS** になりました。(OCPBUGS-33110)

1.9.31.2. バグ修正

- 以前は、**ContainerRuntimeConfig** リソースがシングルノードの OpenShift Container Platform インストールの追加マニフェストとして作成されたときに、ブートストラップが失敗し、"more than one ContainerRuntimeConfig found that matches MCP labels" というエラーメッセージが表示されました。このリリースでは、**ContainerRuntimeConfig** リソースの誤った処理が修正され、問題が解決されました。(OCPBUGS-30153)

- 以前は、**NodePort** トラフィック転送の問題により、Transmission Control Protocol (TCP) トラフィックが終了状態の Pod に送信されていました。このリリースでは、エンドポイント選択ロジックが **KEP-1669 ProxyTerminatingEndpoints** を完全に実装し、問題が解決されました。(OCPBUGS-32319)

- 以前は、Red Hat OpenStack Platform (RHOSP) 上の OpenShift Container Platform デプロイメントで、**MachineSet** オブジェクトが **Port Security** パラメーターの値を正しく適用していませんでした。このリリースでは、**MachineSet** オブジェクトが **port_security_enabled** フラグを期待どおりに適用します。(OCPBUGS-32428)

- 以前は、ドライバーの問題により、Workload アイデンティティークラスター上の Azure ファイルの静的永続ボリュームを設定できませんでした。このリリースでは、問題は解決され、静的永続ボリュームが正しくマウントされるようになりました。(OCPBUGS-33039)

- 以前は、負荷分散アルゴリズムに不具合があり、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っていました。このリリースでは、負荷分散のサービスフィルタリングロジックが更新され、問題が解決されました。(OCPBUGS-33389)

- 以前は、Ironic Python Agent (IPA) は、間違ったバイトセクターサイズを予期していたためディスクを消去しようとして失敗し、ノードのプロビジョニングが失敗していました。このリリースでは、IPA がディスクセクターサイズをチェックし、ノードのプロビジョニングが成功します。(OCPBUGS-33452)

- 以前は、フォームビュー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ようとしても、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、代替サービスが削除され、問題が解決されました。(OCPBUGS-33462)

- 以前は、Operator に HTTP(S) プロキシーが設定されていなかったため、**vsphere-problem-detector** Operator は vCenter に接続できませんでした。このリリースでは、**vsphere-problem-detector** Operator はクラスターの残りの部分と同じ HTTP(S) プロキシーを使用するため、問題が解決されました。(OCPBUGS-33467)

1.9.31.3. 更新

既存の OpenShift Container Platform 4.14 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. RHBA-2024:2789 - OpenShift Container Platform 4.14.25 バグ修正の更新

発行日: 2024 年 5 月 16 日

OpenShift Container Platform リリース 4.14.25 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-2024:2789 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-2024:2792 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 4.14.25 --pullspecs
```

1.9.32.1. バグ修正

- 以前は、**exec** コマンドを使用して作成された一部のコンテナープロセスは、CRI-O がコンテナーを停止した後も存続していました。その結果、プロセスが長引くことで追跡の問題が発生し、プロセスリークや機能停止状態が発生しました。このリリースでは、CRI-O はコンテナーに対して処理された **exec** 呼び出しを追跡し、コンテナーが停止されたときに **exec** 呼び出しの一部として作成されたプロセスが終了するようにします。(OCPBUGS-32482)

- 以前は、Go プログラミング言語が解析できるタイムアウト値よりも大きいタイムアウト値は適切に検証されませんでした。その結果、HAProxy が解析できるタイムアウト値よりも大きいタイムアウト値により、HAProxy で問題が発生しました。今回の更新により、タイムアウトに解析できる値より大きな値が指定された場合、HAProxy が解析できる最大値に制限されます。その結果、HAProxy に関する問題は発生しなくなります。(OCPBUGS-30773)

- 以前は、ユーザーがイメージストリームタグをインポートすると、**ImageContentSourcePolicy** (ICSP) は **ImageDigestMirrorSet** (IDMS) および **ImageTagMirrorSet** (ITMS) と共存できませんでした。OpenShift Container Platform は、ユーザーが作成した IDMS/ITMS を無視し、ICSP を優先していました。このリリースでは、ICSP も存在する場合、イメージストリームタグのインポートで IDMS/ITMS が考慮されるようになったため、イメージストリームタグが共存できるようになりました。(OCPBUGS-31509)

- 以前は、マシン設定プールの一時停止と一時停止解除を伴うコントロールプレーンのみの更新を OpenShift Container Platform クラスターで実行した後、一時停止解除操作後に 2 回の再起動操作が発生していました。この追加の再起動は予期されておらず、**MachineConfigPool** オブジェクトにリストされている古い **MachineConfig** オブジェクトに対してパフォーマンスプロ

ファイルコントローラーが調整されたために発生しました。このリリースでは、パフォーマンスプロファイルコントローラーは、**MachineConfigPool** オブジェクトにリストされている最新の **MachineConfig** オブジェクトと調整し、余分な再起動が発生しないようにします。(OCPBUGS-32980)

- 以前は、OpenShift Container Platform 4.14.14 で導入されたカーネルのリグレッションにより、CephFS ストレージにマウントされたノードでノードのクラッシュや再起動などのカーネルの問題が発生していました。このリリースでは、回帰問題が修正され、カーネル回帰問題が発生しなくなりました。(OCPBUGS-33251)

- 以前は、**ovs-if-br-ex.nmconnection.*** ファイルによって **ovs-configuration.service** が失敗し、ノードが **NotReady** 状態に移行していました。このリリースでは、**ovs-if-br-ex.nmconnection.*** ファイルが **/etc/NetworkManager/system-connections** から削除されたため、この問題は発生しなくなりました。(OCPBUGS-32341)

1.9.32.2. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.33. RHSA-2024:2668 - OpenShift Container Platform 4.14.24 のバグ修正更新とセキュリティー更新

発行日: 2024 年 5 月 9 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.24 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-2024:2668 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-2024:2672 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 4.14.24 --pullspecs
```

1.9.33.1. 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。

1.9.33.1.1. IPv6 非要請近隣アドバタイズメントが macvlan CNI プラグインでデフォルトになる

- macvlan 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 アドレスが割り当てられている) は、デフォルトで IPv6 の非要請近隣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。これにより、特定の IP アドレスの新しい Pod の MAC アドレスがホストに通知され、IPv6 ネイバーキャッシュが更新されます。(OCPBUGS-33066)

1.9.33.2. バグ修正

- 以前は、プロキシーを使用してクラスターがインストールされ、プロキシー情報に **%XX** 形式のエスケープ文字が含まれていた場合、インストールは失敗していました。このリリースでは、この問題が修正されています。(OCPBUGS-33010)

- 以前は、OpenShift Container Platform の Hosted Control Plane では、非接続環境で **ImageDigestMirrorSet** オブジェクトと **ImageContentSourcePolicy** オブジェクトのカスタムリソース定義 (CRD) を同時に作成すると、HyperShift Operator が **ImageContentSourcePolicy** CRD を無視して、**ImageDigestMirrorSet** CRD のみのオブジェクトを作成していました。このリリースでは、HyperShift Operator は **ImageDigestMirrorSet** および **ImageContentSourcePolicy** CRD のオブジェクトを作成します。(OCPBUGS-32471)

- 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解除される可能性がありました。この更新により、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-32168)

- 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-31857)

- 以前は、Terraform はコントロールプレーンのポリシーセットを使用してコンピュートサーバーグループを作成していました。その結果、コンピュートサーバーグループでは **install-config.yaml** ファイルの **serverGroupPolicy** プロパティーが無視されました。このリリースでは、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、Terraform フローのインストール時に正しく適用されるようになりました。(OCPBUGS-31756)

1.9.33.3. 更新

既存の OpenShift Container Platform 4.14 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. RHBA-2024:2051 - OpenShift Container Platform 4.14.23 のバグ修正更新とセキュリティー更新

発行日: 2024 年 5 月 2 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.23 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、RHBA-2024:2051 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-2024:2054 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 4.14.23 --pullspecs
```

1.9.34.1. 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。

1.9.34.1.1. 追加ホップの Egress IP 検証ステップ

- 以前は、Egress IP がプライマリーインターフェイス以外のインターフェイスによってホストされている場合、ネクストホップが必要かどうかを判断するための検証が行われていませんでした。このリリースでは、IP によってメインのルーティングテーブルが調査され、ネクストホップが必要かどうかが判断されるようになりました。(OCPBUGS-31854)

1.9.34.1.2. サポートされていないパラメーターを削除する RT カーネルの新しいプロファイル

- 以前は、**net.core.busy_read**、**net.core.busy_poll**、**kernel.numa_balancing sysctl** パラメーターは RT カーネル内に存在しなかったため、サポートされていませんでした。このリリースでは、RT カーネルが検出された場合、**openshift-node-performance-rt** プロファイルが追加され、含まれるようになりました。これにより、サポートされていないカーネルパラメーターが適用される前に削除されます。(OCPBUGS-31905)

1.9.34.1.3. OLM デフォルトソースのオプションを無効にする

- 以前は、切断された状況で Operator Lifecycle Manager (OLM) のデフォルトソースを無効にする方法はありませんでした。このリリースでは、**OperatorHubSpec** フィールドが **hostedcluster.Spec.Configuration** API に統合され、作成時にデフォルトのソースを無効化および有効化することが容易になりました。CLI にはこの機能のフラグも含まれています。(OCPBUGS-32221)

1.9.34.2. バグ修正

- 以前は、Node Tuning Operator (NTO) は、関連付けられているノードに関係なく、同じ優先度を共有するプロファイルがあるかどうかをチェックしていました。このプロセスでは、NTO はまずプロファイルを収集し、優先順位の競合をチェックし、関連するノードをフィルタリングします。その結果、2 つの異なるノードに複数のパフォーマンスプロファイルが存在する場合、誤った優先度の警告がログにダンプされました。このリリースでは、このプロセスの手順が変更され、NTO は最初に関連付けられたノードをフィルター処理し、次に優先順位の競合をチェックするようになりました。(OCPBUGS-31735)

- 以前は、マルチネットワークインターフェイスコントローラー (NIC) を備えた Elastic IP (EIP) に対して EgressIPv6 が機能しないという根本的な問題がありました。このリリースにより、この問題は解決されました。(OCPBUGS-31853)

- 以前は、OpenShift Container Platform 4.14 にアップグレードした後、閉じられたアイドル接続が誤って再利用されると、特定の HTTP クライアントによって Ingress トラフィックが低下していました。このリリースにより、この問題は解決されました。(OCPBUGS-32437)

- 以前は、イメージレジストリーの Azure パス修正ジョブが機能するには、クライアント ID とテナント ID の存在を誤って必要としたため、有効な設定で検証エラーが発生していました。このリリースでは、不足しているクライアント ID とテナント ID へのキー入力接続を考慮するチェックが追加されました。(OCPBUGS-32450)

1.9.34.3. 更新

既存の OpenShift Container Platform 4.14 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-2024:1891 - OpenShift Container Platform 4.14.22 のバグ修正更新とセキュリティー更新

発行日: 2024 年 4 月 25 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.22 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-2024:1891 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-2024:1897 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 4.14.22 --pullspecs
```

1.9.35.1. 機能拡張

1.9.35.1.1. 設定済みコントロールプレーンレプリカの数の検証

- 以前は、コントロールプレーンのレプリカの数を **2** などの無効な値に設定することができました。このリリースでは、ISO 生成時にコントロールプレーンのレプリカの設定ミスを防ぐために、検証が追加されました。(OCPBUGS-31885)

1.9.35.2. バグ修正

- 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。このリリースでは、**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-31862)

- 以前は、クラスターがシャットダウンまたは休止状態の間に、外部ネイバーが Media Access Control (MAC) アドレスを変更する可能性がありました。Gratuitous Address Resolution Protocol (GARP) は他のネイバーにこの変更を通知することになっていましたが、クラスターは GARP を処理しませんでした。クラスターを再起動した後、古い MAC アドレスが使用されていたため、OVN-Kubernetes クラスターネットワークからネイバーが利用できなくなる可能性がありました。このリリースでは、更新によりエージングメカニズムが有効になり、ネイバーの MAC アドレスが 300 秒ごとに定期的に更新されるようになりました。(OCPBUGS-11710)

1.9.35.3. 更新

既存の OpenShift Container Platform 4.14 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-2024:1765 - OpenShift Container Platform 4.14.21 のバグ修正更新とセキュリティー更新

発行日: 2024 年 4 月 18 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.21 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、RHSA-2024:1765 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-2024:1768 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 4.14.21 --pullspecs
```

1.9.36.1. バグ修正

- 以前は、コンソールバックエンドプロキシーサーバーは、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送信していました。これにより、状況によっては認証局 (CA) の問題が発生しました。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-29783)

1.9.36.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:1681 - OpenShift Container Platform 4.14.20 のバグ修正更新とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.20 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-2024:1681 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。

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 4.14.20 --pullspecs
```

1.9.37.1. 更新

既存の OpenShift Container Platform 4.14 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.38. RHBA-2024:1564 - OpenShift Container Platform 4.14.19 のバグ修正更新とセキュリティー更新

発行日: 2024 年 4 月 3 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.19 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、RHBA-2024:1564 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-2024:1567 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 4.14.19 --pullspecs
```

1.9.38.1. バグ修正

- 以前は、ステータスに IP がない Pod は、Admin Policy Based (APP) コントローラーによって処理されるときに新しい調整ループをトリガーできず、その設定をノースバウンド DB に追加するロジックが失われていました。このリリースでは、ステータスフィールドに IP がない Pod は、IP フィールドが設定され、コントローラーが調整ループを完了できるようになるまで、イベントの変更ごとにコントローラーによって処理され続けます。(OCPBUGS-29342)

1.9.38.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:1458 - OpenShift Container Platform 4.14.18 のバグ修正更新とセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.18 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-2024:1458 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-2024:1461 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 4.14.18 --pullspecs
```

1.9.39.1. バグ修正

- 以前は、特定の条件下ではインストールプログラムが失敗し、**unexpected end of JSON input** というエラーメッセージが表示されていました。このリリースでは、エラーメッセージが明確化され、問題を解決するためには **install-config.yaml** 設定ファイルで **serviceAccount** フィールドを設定することをユーザーに提案しています。(OCPBUGS-30027)

1.9.39.2. 既知の問題

- 現在、OpenShift Container Platform クラスターのインストール時にパフォーマンスプロファイルを追加のマニフェストとして提供することはサポートされていません。(OCPBUGS-18640)

1.9.39.3. 更新

既存の OpenShift Container Platform 4.14 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. RHBA-2024:1260 - OpenShift Container Platform 4.14.17 バグ修正の更新

発行日: 2024 年 3 月 20 日

OpenShift Container Platform リリース 4.14.17 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、RHBA-2024:1260 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-2024:1263 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 4.14.17 --pullspecs
```

1.9.40.1. 更新

既存の OpenShift Container Platform 4.14 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. RHBA-2024:1205 - OpenShift Container Platform 4.14.16 バグ修正の更新

発行日: 2024 年 3 月 13 日

OpenShift Container Platform リリース 4.14.16 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、RHBA-2024:1205 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-2024:1208 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 4.14.16 --pullspecs
```

1.9.41.1. 更新

既存の OpenShift Container Platform 4.14 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. RHBA-2024:1046 - OpenShift Container Platform 4.14.15 バグ修正の更新

発行日: 2024 年 3 月 4 日

OpenShift Container Platform リリース 4.14.15 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2024:1046 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-2024:1049 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 4.14.15 --pullspecs
```

1.9.42.1. バグ修正

- 以前は、アプリケーションセレクターの名前が間違っていたため、**manila-csi-driver-controller-metrics** サービスには空のエンドポイントがありました。このリリースでは、アプリケーションセレクター名が **openstack-manila-csi** に変更され、問題は修正されました。(OCPBUGS-23443)

- 以前は、イメージ認証情報を提供していた Amazon Web Services (AWS) コードが、OpenShift Container Platform 4.14 の kubelet から削除されました。その結果、kubelet が自身を認証してコンテナーランタイムに認証情報を渡すことができなくなったため、指定されたプルシークレットがない場合、Amazon Elastic Container Registry (ECR) からのイメージのプルが失敗しました。この更新により、別の認証情報プロバイダーが設定され、kubelet に ECR 認証情報を提供するようになりました。その結果、kubelet は ECR からプライベートイメージをプルできるようになりました。(OCPBUGS-29630)

- 以前の OpenShift Container Platform 4.14 リリースでは、OpenShift Container Platform バージョン 4.13 から 4.14 に更新するときにイメージが失われたという認識をユーザーに与える変更が導入されました。デフォルトの内部レジストリーを変更したことが原因で、Microsoft Azure

オブジェクトストレージの使用時にレジストリーが誤ったパスを使用していました。このリリースでは、正しいパスが使用され、間違ったストレージパスを使用していたレジストリーにプッシュされた Blob を正しいストレージパスに移動するレジストリー Operator にジョブが追加されました。これにより、2 つの異なるストレージパスが 1 つのパスに効果的にマージされます。(OCPBUGS-29604)

注記

この修正は Azure Stack Hub では機能しません。OpenShift Container Platform バージョン 4.14.0 から 4.14.13 を使用していた Azure Stack Hub ユーザーは、4.14.14 以降のバージョンにアップグレードするときに、オブジェクト Blob を正しいストレージパスに移動するための手動の手順を実行する必要があります。Red Hat ナレッジベースのソリューション記事 を参照してください。

- 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。現在、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ません。(OCPBUGS-29152)

1.9.42.2. 更新

既存の OpenShift Container Platform 4.14 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. RHSA-2024:0941 - OpenShift Container Platform 4.14.14 のバグ修正とセキュリティー更新

発行日: 2024 年 2 月 28 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.14 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-2024:0941 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-2024:0944 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 4.14.14 --pullspecs
```

1.9.43.1. 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。

1.9.43.1.1. IPI に "eu-es" リージョンのサポートを追加する

- 以前は、インストールプログラムは、サポートされているにもかかわらず、"eu-es" リージョンの IBM Cloud VPC にクラスターをインストールできませんでした。この更新により、インストールプログラムは "eu-es" リージョンの IBM Cloud VPC にクラスターを正常にインストールします。(OCPBUGS-19398)

1.9.43.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:0837 - OpenShift Container Platform 4.14.13 のバグ修正とセキュリティー更新

発行日: 2024 年 2 月 21 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.13 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-2024:0837 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-2024:0840 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 4.14.13 --pullspecs
```

1.9.44.1. バグ修正

- 以前は、Kubelet は誤った **unconfined_service_t** ラベルで実行されていたため、SELinux に関連するエラーが発生していました。このリリースでは、問題は解決され、kubelet は **kubelet_exec_t** ラベルで実行されます。(OCPBUGS-22270)

1.9.44.2. 更新

既存の OpenShift Container Platform 4.14 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. RHSA-2024:0735 - OpenShift Container Platform 4.14.12 のバグ修正とセキュリティー更新

発行日: 2024 年 2 月 13 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.12 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-2024:0735 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-2024:0738 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 4.14.12 --pullspecs
```

1.9.45.1. 機能

この z-stream リリースには次の機能が含まれています。

1.9.45.1.1. PTP Operator を使用してデュアル Intel E810 Westport Channel NIC をグランドマスタークロックとして使用する

- 両方の NIC を設定する **PtpConfig** カスタムリソース (CR) を作成することで、**linuxptp** サービスをデュアル Intel E810 Westport Channel NIC のグランドマスタークロック (T-GM) として設定できるようになりました。ホストのシステムクロックは、GNSS タイムソースに接続されている 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。(RHBA-2024:0734)

1.9.45.2. バグ修正

- 以前は、release-to-channel ストラテジーと **oc-mirror** の動作により、パッケージの選択的なミラーリングでエラーが発生していました。パッケージの最新 (つまりデフォルト) のチャネルを選択的にミラーリングしている場合に、新しいリリースで新しいチャネルが導入されると、現在のデフォルトチャネルが無効になり、新しいデフォルトチャネルの自動割り当てが失敗しました。このリリースにより、この問題は解決されました。**ImageSetConfig** CR で、**currentDefault** チャネルをオーバーライドする **defaultChannel** フィールドを定義できるようになりました。(OCPBUGS-28871)

- 以前は、EFS CSI ドライバーコンテナーからの CPU 制限により、パフォーマンスの低下が発生することがありました。このリリースでは、EFS CSI ドライバーコンテナーの CPU 制限が削除されました。(OCPBUGS-28823)

- 以前は、**routingViaHost** モードを使用すると、**ExternalTrafficPolicy=Local** ロードバランサーサービスへのアクセスが中断されました。このリリースにより、この問題は解決されました。(OCPBUGS-28789)

- 以前は、HostedCluster がデプロイされている場合に、ユーザーが KAS の **AdvertiseAddress** を定義すると、現在のデプロイメントと競合し、サービス、クラスター、マシンネットワークなどの他のネットワークと重複して、デプロイメントの失敗が発生していました。このリリースでは、**AdvertiseAddress** のネットワーク検証が追加されました。(OCPBUGS-20547)

1.9.45.3. 更新

既存の OpenShift Container Platform 4.14 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-2024:0642 - OpenShift Container Platform 4.14.11 のバグ修正とセキュリティー更新

発行日: 2024 年 2 月 7 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.11 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、RHSA-2024:0642 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-2024:0645 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 4.14.11 --pullspecs
```

1.9.46.1. 機能

この z-stream リリースには次の機能が含まれています。

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

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

1.9.46.2. バグ修正

- 以前は、OpenShift Container Platform を更新すると、DNS クエリーが失敗することがありました。これは、CoreDNS 1.10.1 を使用する非 EDNS クエリーに対してアップストリームが 512 バイトを超えるペイロードを返すためです。このリリースでは、非準拠のアップストリームを持つクラスターが、オーバーフローエラーの発生時に TCP で再試行するようになりました。これにより、更新時の機能の停止が防止されます。(OCPBUGS-28200)

- 以前は、環境変数のタイプミスにより、**node.env** ファイルが再起動のたびに上書きされていました。このリリースでは、**node.env** への編集が再起動後も保持されるようになりました。(OCPBUGS-27362)

- 以前は、**container_t** がダイレクトレンダリングインフラストラクチャー (DRI) デバイスにアクセスできませんでした。このリリースでは、ポリシーが更新され、デバイスプラグインによって公開される DRI デバイスおよび GPU デバイスに **container_t** がデフォルトでアクセスできるようになりました。(OCPBUGS-27275)

- 以前は、Whereabouts CNI プラグインによって作成されたプールから IP アドレスが割り当てられた Pod が、ノードの強制再起動後に **ContainerCreating** 状態でスタックしていました。このリリースでは、ノードの強制再起動後の IP 割り当てに関連する Whereabouts CNI プラグインの問題が解決されました。(OCPBUGS-26553)

1.9.46.3. 更新

既存の OpenShift Container Platform 4.14 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-2024:0290 - OpenShift Container Platform 4.14.10 のバグ修正とセキュリティー更新

発行日: 2024 年 1 月 23 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.10 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2024:0290 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-2024:0293 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 4.14.10 --pullspecs
```

1.9.47.1. バグ修正

- 以前は、Cloud Credential Operator (CCO) がデフォルトモードの場合、CCO はルート認証情報のクエリーに間違ったクライアントを使用していました。CCO は、目的のシークレットを見つけることができず、**cco_credentials_mode** メトリクスで **credsremoved** モードを誤って報告していました。このリリースでは、CCO は正しいクライアントを使用するようになり、**cco_credentials_mode** メトリクスが正確にレポートされるようになりました。(OCPBUGS-26512)

1.9.47.2. 更新

既存の OpenShift Container Platform 4.14 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-2024:0204 - OpenShift Container Platform 4.14.9 のバグ修正とセキュリティー更新

発行日: 2024 年 1 月 17 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.9 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2024:0204 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-2024:0207 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 4.14.9 --pullspecs
```

1.9.48.1. バグ修正

- 以前は、Cluster Version Operator (CVO) が更新の推奨事項を継続的に取得し、現在のクラスターの状態に対して既知の条件付き更新のリスクを評価していました。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ませんでした。このバグにより、CVO は、改善されたリスク宣言を提供する更新推奨サービスを認識しませんでした。このリリースでは、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ます。(OCPBUGS-26207)

- 以前は、リリースのミラーリングに eus-* チャネルを使用すると、oc-mirror プラグインでのミラーリングに失敗していました。これは、eus-* チャネルが偶数番号のみであることを oc-mirror プラグインが認識しないことが原因でした。このリリースでは、oc-mirror プラグインのユーザーはリリースのミラーリングに eus-* チャネルを使用できます。(OCPBUGS-26065)

1.9.48.2. 更新

既存の OpenShift Container Platform 4.14 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. RHSA-2024:0050 - OpenShift Container Platform 4.14.8 のバグ修正とセキュリティー更新

発行日: 2024 年 1 月 9 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.8 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2024:0050 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-2024:0053 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 4.14.8 --pullspecs
```

1.9.49.1. 機能

この z-stream リリースには、次の機能が含まれています。

- このリリースでは、Pod セキュリティーアドミッション違反が発生しているクラスターから Telemetry データが収集されます。収集されるのは、違反した namespace が Kubernetes システム namespace、OpenShift Container Platform システム namespace、またはカスタム namespace であるかどうかを示すデータです。このデータ収集は、Red Hat が今後の Pod セキュリティーアドミッションのグローバルな制限付き適用に対する顧客クラスターの準備状況を評価するのに役立ちます。Pod セキュリティーアドミッションの詳細は、Pod セキュリティーアドミッションの理解と管理 を参照してください。(OCPBUGS-25384)

- 以前は、レイヤード製品において有効期間の短い認証トークンに OpenShift の Azure Identity 機能は利用できませんでした。このリリースでは、このサポートを有効にすることで OLM マネージドの Operator のセキュリティーが強化されました。(OCPBUGS-25275)

1.9.49.2. バグ修正

- 以前は、Secure Boot が無効になっているノード上で **bootMode** を **UEFISecureBoot** に設定して OpenShift Container Platform をインストールすると、インストールが失敗していました。このリリースでは、Secure Boot を有効にして OpenShift Container Platform をインストールしようとする後続の試行は正常に続行されます。(OCPBUGS-19884)

- 以前は、Google Cloud Platform でリージョン PD を使用する場合、インストーラーはクラスターの破棄に失敗していました。このリリースでは、レプリケートされたゾーンが検出され、ディスクが適切に削除されます。(OCPBUGS-22770)

- 以前は、コントロールプレーンノードで **additionalSecurityGroupIDs** フィールドが指定されていない場合、**defaultMachinePlatform** スタンザの **additionalSecurityGroupIDs** は使用されませんでした。このリリースでは、コントロールプレーンノードで **additionalSecurityGroupIDs** フィールドが指定されていない場合、**defaultMachinePlatform** スタンザの **additionalSecurityGroupIDs** が使用されるようになりました。(OCPBUGS-22771)

1.9.49.3. 更新

既存の OpenShift Container Platform 4.14 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-2023:7831 - OpenShift Container Platform 4.14.7 のバグ修正とセキュリティー更新

発行日: 2024 年 1 月 3 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.7 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:7831 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:7834 アドバイザリーで提供されます。

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 4.14.7 --pullspecs
```

1.9.50.1. バグ修正

- 以前は、IPsec Pod を再起動すると、既存のポリシーが強制終了されました。このリリースでは、IPsec サービスも再起動されて既存のポリシーが復元されることで、問題が解決されました。(OCPBUGS-24633)
- 以前は、無効なネットワーク名やイメージなどの無効なリソースを参照するように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を更新すると、プロビジョニング状態でスタックして削除できないコントロールプレーンマシンが作成されました。このリリースでは、この問題が解決されました。(OCPBUGS-23202)
- 以前は、パフォーマンスプロファイルを適用すると、tuned プロファイルが **DEGRADED** 状態を報告しました。これは、生成された tuned プロファイルが 2 つ目の sysctl 値を設定しようとしたためです。このリリースでは、sysctl 値は tuned によって設定されなくなり、代わりに **sysctl.d** ファイルによってのみ設定されます。(OCPBUGS-25305)

1.9.50.2. 更新

既存の OpenShift Container Platform 4.14 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-2023:7682 - OpenShift Container Platform 4.14.6 のバグ修正とセキュリティー更新

発行日: 2023 年 12 月 12 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.6 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:7682 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:7685 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 4.14.6 --pullspecs
```

1.9.51.1. 機能

この z-stream リリースには、次の PTP 機能が含まれています。

1.9.51.1.1. PTP Operator でハードウェア固有の NIC 機能を使用する

- 新しい PTP Operator ハードウェアプラグインが利用可能になり、PTP Operator でサポートされている NIC のハードウェア固有の機能を使用できるようになります。現在、Intel Westport チャネル E810 NIC がサポートされています。詳細は、E810 ハードウェア設定リファレンス を参照してください。

1.9.51.1.2. PTP グランドマスタークロックに GNSS タイミング同期を使用する

- PTP Operator は、グランドマスタークロック (T-GM) に接続された Global Navigation Satellite System (GNSS) ソースからの高精度 PTP タイミングの受信をサポートするようになりました。詳細は、linuxptp サービスを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。

1.9.51.2. バグ修正

- 以前は、デュアルスタッククラスターから IPv6 専用ホストをデプロイすると、問題が発生してベースボード管理コントローラー (BMC) が正しいコールバック URL を受信できませんでした。代わりに、BMC は IPv4 URL を受信していました。この更新により、URL の IP バージョンが BMC アドレスの IP バージョンに依存するようになり、この問題は発生しなくなります。(OCPBUGS-23903)

- 以前は、CPU が保証されており、割り込み要求 (IRQ) ロードバランシングが無効になっているシングルノード OpenShift で、コンテナーの起動時に大きなレイテンシースパイクが発生することがありました。この更新により、この問題は発生しなくなりました。(OCPBUGS-22901) (OCPBUGS-24281)

1.9.51.3. 既知の問題

- PTP タイミング同期の場合、グランドマスタークロック (T-GM) の状態を完全に判断するには、DPLL フェーズオフセットモニタリングが必要です。これは現在、ツリー内 ice ドライバー DPLL API に存在しないため、グランドマスターの状態を判断する際に盲点が生じます。

1.9.51.4. 更新

既存の OpenShift Container Platform 4.14 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-2023:7599 - OpenShift Container Platform 4.14.5 のバグ修正とセキュリティー更新

発行日: 2023 年 12 月 5 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.5 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:7599 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-2023:7603 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 4.14.5 --pullspecs
```

1.9.52.1. バグ修正

- 以前は、ビルド機能が有効になっていない場合、ビルドインフォーマーとの同期を試みると、ConfigObserver コントローラーが失敗していました。このリリースでは、ビルド機能が有効になっていない場合でも、ConfigObserver は正常に起動します。(OCPBUGS-23490) (OCPBUGS-21778)

- 以前は、Cloud Credential Operator (CCO) は、**kube-system** namespace の VMware vSphere ルートシークレット (**vsphere-creds**) の更新をサポートしていませんでした。そのため、コンポーネントのシークレットが正しく同期されませんでした。このリリースでは、CCO は vSphere ルートシークレットの更新をサポートし、同期時にシークレットデータをリセットします。(OCPBUGS-23426)

- 以前は、多数の Pod があり、その一部に CPU 制限が設定されているアプリケーションをデプロイすると、デプロイが失敗することがありました。この更新により、この問題は発生しなくなりました。(RHEL-7232)

1.9.52.2. 更新

既存の OpenShift Container Platform 4.14 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-2023:7470 - OpenShift Container Platform 4.14.4 のバグ修正とセキュリティー更新

発行日: 2023 年 11 月 29 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.4 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:7470 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-2023:7473 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 4.14.4 --pullspecs
```

1.9.53.1. バグ修正

- 以前は、Amazon Web Services (AWS) にクラスターをインストールするために **install-config.yaml** 設定ファイルの **kmsKeyARN** セクションで Key Management Service (KMS) 暗号鍵を指定すると、クラスターのインストール操作中に権限ロールが追加されませんでした。この更新により、設定ファイルで鍵を指定すると追加の鍵セットがクラスターに追加され、クラスターが正常にインストールされるようになりました。設定ファイルで **credentialsMode** パラメーターを指定すると、すべての KMS 暗号鍵が無視されます。(OCPBUGS-22774)

1.9.53.2. 更新

既存の OpenShift Container Platform 4.14 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-2023:7315 - OpenShift Container Platform 4.14.3 のバグ修正とセキュリティー更新

発行日: 2023 年 11 月 21 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.3 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:7315 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:7321 アドバイザリーによって提供されます。

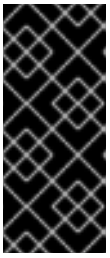
このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。

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 4.14.3 --pullspecs
```

1.9.54.1. バグ修正

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



重要

ICSP オブジェクトを使用してリポジトリーミラーリングを設定することは、非推奨の機能です。非推奨の機能は OpenShift Container Platform に引き続き含まれており、サポートが継続されます。ただし、この製品の今後のリリースでは削除される可能性があります。これは非推奨の機能であるため、新しいデプロイメントでは使用しないでください。

- 以前は、**enable_port_security** パラメーターが **false** に設定されている追加ポートがノードに含まれている場合、デプロイメント用に **LoadBalancer** サービスは作成されませんでした。このリリースでは、同じように設定された追加ポートがデプロイメントに含まれていても、**LoadBalancer** サービスが作成されます。(OCPBUGS-22974)

- 以前は、**ClusterAutoscaler** リソースは、Container Storage Interface (CSI) 実装で設定されたノードの **CrashBackoff** ループに陥っていました。このリリースでは依存関係が更新され、**ClusterAutoscaler** リソースがこの方法で設定されたノードの **CrashBackoff** に陥らなくなりました。(OCPBUGS-23270)

1.9.54.2. 更新

既存の OpenShift Container Platform 4.14 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。

1.9.55. RHSA-2023:6837 - OpenShift Container Platform 4.14.2 のバグ修正とセキュリティー更新

発行日: 2023 年 11 月 15 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.2 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:6837 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-2023:6840 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 4.14.2 --pullspecs
```

1.9.55.1. バグ修正

- 以前は、**eastus** リージョンの新しい Microsoft Azure ストレージアカウントでデフォルトのセキュリティー設定が変更されると、そのリージョンで Azure AD Workload Identity を使用する OpenShift Container Platform クラスターをインストールできなくなりました。この問題は、このリリースでは解決されています。(OCPBUGS-22651)

- 以前は、インライン Dockerfile フックがコピーされたファイルの変更時刻を保存しないため、Docker ビルド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、コンテナー間でアーティファクトをコピーする際にタイムスタンプを保持するための '-p' フラグが、**cp** コマンドに追加されました。(OCPBUGS-23006)

- 以前は、Image Registry Operator は、5 分ごとにアクセスキーを取得する一環として、ストレージアカウントリストエンドポイントへの API 呼び出しを行っていました。多くの OpenShift Container Platform (OCP) クラスターを含むプロジェクトでは、これにより API 制限に達し、新規クラスターの作成を試みると 429 エラーが発生する可能性があります。このリリースでは、呼び出し間隔が 5 分から 20 分に延長されました。(OCPBUGS-22127)

- 以前は、Azure Managed Identity ロールが cloud-controller-manager (CCM) サービスアカウントから除外されていました。これは、プライベート公開メソッドを使用して既存の VNet にデプロイされた環境では、CCM が **Service** タイプの **LoadBalancers** を適切に管理できなかったことを意味します。このリリースでは、欠落していたロールが CCO ユーティリティー (**ccoctl**) に追加されたため、プライベート公開を使用して既存の VNet に Azure Managed Identity をインストールできるようになりました。(OCPBUGS-21926)

- このパッチにより、アウトバウンド接続にアウトバウンドルールを使用する Azure セットアップの egress IP が有効になります。このようなセットアップでは、Azure が持つアーキテクチャー上の制約により、egress IP として機能するセカンダリー IP はアウトバウンド接続ができません。これは、一致する Pod がインターネットへのアウトバウンド接続を持たないことを意味しますが、インフラストラクチャーネットワーク内の外部サーバーに到達できるようになります。これは、egress IP の意図されたユースケースです。(OCPBUGS-21785)

- 以前は、IP が割り当てられているロードバランサーサービスと割り当てられていないロードバランサーサービスがある場合に MetalLB Operator のコントローラーが再起動すると、内部が空の状態で再起動され、ワークロードが中断される可能性がありました。このリリースでは、すでに IP が割り当てられているサービスを最初に処理するように MetalLB のコントローラーが変更されました。(OCPBUGS-16267)

- 以前は、OpenShift Container Platform または Kubernetes リソースで使用されているクラスターロールと同じ名前の Operator グループを作成すると、Operator Lifecycle Manager (OLM) がクラスターロールを上書きしていました。今回の修正により、OpenShift Container Platform または Kubernetes で使用されているクラスターロールと競合する Operator グループを作成すると、OLM は次の構文を使用して一意のクラスターロール名を生成します。

  命名構文

```
olm.og.<operator_group_name>.<admin_edit_or_view>-<hash_value>
```

OLM は、OpenShift Container Platform および Kubernetes で使用される定義済みのクラスターロールセットと競合する Operator グループに対してのみ一意の名前を生成します。Operator グループの名前が、クラスター上に存在する他のクラスターロールと競合しないことを確認する必要があります。

OLM は、次のクラスターロールと競合する Operator グループの一意の名前を生成します。

- **aggregate-olm**
- **alert-routing**
- **cluster**
- **cluster-monitoring**
- **monitoring**
- **monitoring-rules**
- **packagemanifests-v1**
- **registry**
- **storage**
  (OCPBUGS-19789)

1.9.55.2. 既知の問題

- このリリースには、インストーラーがプロビジョニングしたインフラストラクチャーを使用して、Alibaba Cloud にクラスターをインストールできない既知の問題があります。Alibaba Cloud へのクラスターのインストールは、このリリースではテクノロジープレビュー機能になります。(OCPBUGS-20552)

1.9.55.3. 更新

既存の OpenShift Container Platform 4.14 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。

1.9.56. RHBA-2023:6153 - OpenShift Container Platform 4.14.1 バグ修正の更新

発行日: 2023 年 11 月 1 日

OpenShift Container Platform リリース 4.14.1 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:6153 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:6152 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 4.14.1 --pullspecs
```

1.9.56.1. 更新

既存の OpenShift Container Platform 4.14 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。

1.9.57. RHSA-2023:5006 - OpenShift Container Platform 4.14.0 イメージリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2023 年 10 月 31 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.14.0 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:5006 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-2023:5009 アドバイザリーによって提供されます。更新プログラムに含まれるセキュリティー更新プログラムのリストは、RHSA-2023:6143 アドバイザリーに記載されています。

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

以下のコマンドを実行して、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 4.14.0 --pullspecs
```