OpenShift Container Platform 4.15

リリースノート

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

Last Updated: 2024-04-23

OpenShift Container Platform 4.15 リリースノート

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

法律上の通知

概要

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

目次

第1章 OPENSHIFT CONTAINER PLATFORM 4.15 リリースノート

Red Hat OpenShift Container Platform は、開発者と IT 組織に、最小限の設定と管理で新規および既存のアプリケーションの両方を安全でスケーラブルなリソースにデプロイするためのハイブリッドクラウドアプリケーションプラットフォームを提供します。OpenShift Container Platform は、Java、Javascript、Python、Ruby および PHP など、幅広いプログラミング言語およびフレームワークをサポートしています。

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

1.1. このリリースについて

OpenShift Container Platform (RHSA-2023:7198) 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 1.28 を使用します。以下では、OpenShift Container Platform 4.15 に関連する新機能、変更点および既知の問題について説明します。

OpenShift Container Platform 4.15 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 4.15 は、Red Hat Enterprise Linux (RHEL) 8.8 と 8.9、および Red Hat Enterprise Linux CoreOS (RHCOS) 4.15 でサポートされています。

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

OpenShift Container Platform 4.12 以降、偶数番号のリリースの Extended Update Support (EUS) フェーズが 6 カ月間延長され、これまでの 1 年半から 2 年になりました。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。

OpenShift Container Platform 4.14 以降、Extended Update Support (EUS) は 64 ビット ARM、IBM Power® (ppc64le)、および IBM Z®(s390x) 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。

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。

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

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

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

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

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

1.3. 新機能および機能拡張

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

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

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

RHCOS は、OpenShift Container Platform 4.15 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、機能拡張、ハードウェアサポート、およびドライバーの更新を確実に受け取ることができます。

1.3.1.2. iSCSI デバイスのサポート (テクノロジープレビュー)

RHCOS は **iscsi_bft** ドライバーをサポートするようになり、iSCSI Boot Firmware Table (iBFT) で動作する iSCSI デバイスから直接ブートできるようになります (テクノロジープレビュー)。これにより、iSCSI デバイスをインストールのルートディスクとしてターゲットにすることができます。

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. インストール中の Azure ストレージアカウントの暗号化

お客様が管理する暗号鍵をインストールプログラムに提供することで、インストール中に Azure ストレージアカウントを暗号化できるようになりました。Azure ストレージアカウントの暗号化に必要なパラメーターに関する説明は、インストール設定パラメーター を参照してください。

1.3.2.2. クラスター CAPI Operator への CAPO の統合 (テクノロジープレビュー)

TechPreviewNoUpgrade 機能フラグを有効にすると、Cluster API (CAPI) Operator は Cluster API Provider for OpenStack (CAPO) をデプロイし、そのライフサイクルを管理します。CAPI Operator は、現在の OpenShift Container Platform クラスターの **Cluster** リソースおよび **OpenStackCluster** リソースを自動的に作成します。

Machine API (MAPI) リソースの設定方法と同様の方法で、CAPI **Machine** リソースと CAPO **OpenStackMachine** リソースを設定できるようになりました。CAPI リソースは MAPI リソースと同等ですが、同一ではないことに注意することが重要です。

1.3.2.3. IBM Cloud とユーザー管理の暗号化

インストールプロセスの一環として、独自の IBM® Key Protect for IBM Cloud® ルート鍵を指定できるようになりました。このルート鍵は、コントロールプレーンとコンピュートマシンのルート (ブート) ボリューム、およびクラスターのデプロイ後にプロビジョニングされる永続ボリューム (データボリューム) を暗号化するために使用されます。

詳細は、IBM Cloud のユーザー管理の暗号化 を参照してください。

1.3.2.4. インターネットアクセスが制限された IBM Cloud にクラスターをインストールする

切断または制限されたネットワーククラスターなど、インターネットアクセスが制限された環境の IBM Cloud® にクラスターをインストールできるようになりました。このタイプのインストールでは、OpenShift Container Platform インストールイメージの内容をミラーリングするレジストリーを作成します。このレジストリーは、インターネットと制限されたネットワークの両方にアクセスできるミラーホスト上に作成できます。

詳細は、制限されたネットワーク内の IBM Cloud へのクラスターのインストール を参照してください。

1.3.2.5. AWS にクラスターをインストールしてノードを Wavelength Zone に拡張する

install-config.yaml ファイルのエッジコンピュートプールにゾーン名を設定することで、Amazon Web Services (AWS) Wavelength Zonese に OpenShift Container Platform クラスターをすばやくインストールするか、Wavelength Zone のサブネットを使用して既存の VPC にクラスターをインストールできます。

インストール後のタスクを実行して、AWS 上の既存の OpenShift Container Platform クラスターを拡張し、AWS Wavelength Zone を使用することもできます。

詳細は、AWS Wavelength Zone 上のコンピュートノードを使用して AWS にクラスターをインストールする および 既存のクラスターの拡張による AWS Local Zones または Wavelength Zones の使用 を参照してください。

1.3.2.6. AWS デプロイメントでのクラスターネットワーク MTU のカスタマイズ

AWS Local Zones インフラストラクチャーにクラスターをデプロイする前に、インフラストラクチャーのニーズを満たすようにクラスターネットワークの最大伝送単位 (MTU) をカスタマイズできます。

install-config.yaml 設定ファイルで networking.clusterNetworkMTU パラメーターを指定することにより、クラスターの MTU をカスタマイズできます。

詳細は、クラスターネットワーク MTU のカスタマイズ を参照してください。

1.3.2.7. AWS Outposts 上のコンピュートノードを使用して AWS にクラスターをインストールする

OpenShift Container Platform バージョン 4.14 では、テクノロジープレビューとして AWS Outposts で実行されているコンピュートノードを使用して、クラスターを AWS にインストールできます。OpenShift Container Platform 4.15 では、AWS 上のクラスターを既存の VPC にインストールし、インストール後の設定タスクとして AWS Outposts にコンピュートノードをプロビジョニングできます。

詳細は、AWS 上のクラスターを既存の VPC にインストールする および AWS VPC クラスターを AWS Outpost に拡張する を参照してください。

1.3.2.8. Nutanix とフォールトトレランスのデプロイメント

デフォルトでは、インストールプログラムは、コントロールプレーンとコンピュートマシンを単一の Nutanix Prism Element (クラスター) にインストールします。OpenShift Container Platform クラスターのフォールトトレランスを向上させるために、障害ドメインを設定することで、これらのマシンが複数の Nutanix クラスターに分散されるように指定できるようになりました。

詳細は、複数の Prism 要素を使用したフォールトトレランスのデプロイメント を参照してください。

1.3.2.9. 64-bit ARM での OpenShift Container Platform

OpenShift Container Platform 4.15 は、Machine Config Operator (MCO) を使用して、RHCOS カーネルで 64k ページサイズを有効にする機能をサポートするようになりました。この設定は、64 ビット ARM アーキテクチャーを使用するマシンに限定されます。詳細は、マシン設定タスク のドキュメントを参照してください。

1.3.2.10. オプションの OLM クラスター機能

OpenShift Container Platform 4.15 では、インストール中に Operator Lifecycle Manager (OLM) 機能を無効にすることができます。詳細は、Operator Lifecycle Manager の機能 を参照してください。

1.3.2.11. ローカルディスク上のルートボリュームと etcd を使用した Red Hat OpenStack Platform (RHOSP) のデプロイ (テクノロジープレビュー)

Day 2 デプロイメントとして、etcd をルートボリューム (Cinder) から専用のエフェメラルローカルディスクに移動できるようになりました。このテクノロジープレビュー機能を使用すると、RHOSP インストールのパフォーマンスの問題を解決したり、阻止したりできます。

詳細は、ローカルディスク上の rootVolume および etcd を使用した OpenStack へのデプロイ を参照してください。

1.3.2.12. エージェントベースのインストーラーを使用した vSphere インテグレーションの設定

エージェントベースのインストール用の **install-config.yaml** ファイルを作成する際に、vSphere を使用するようにクラスターを設定できるようになりました。詳細は、追加の VMware vSphere 設定パラメーター を参照してください。

1.3.2.13. エージェントベースのインストール中の追加のベアメタル設定

エージェントベースのインストール用の **install-config.yaml** ファイルを作成する際に、ベアメタルプラットフォームの追加設定を行うことができるようになりました。これらの新しいオプションには、ホスト設定、ネットワーク設定、ベースボード管理コントローラー (BMC) の詳細が含まれます。

これらのフィールドは、クラスターの初期プロビジョニング中には使用されませんが、インストール後にフィールドを設定する必要がなくなります。詳細は、エージェントベースのインストーラー用の追加のベアメタル設定パラメーター を参照してください。

1.3.2.14. インストーラーがプロビジョニングするインストール中に Dell iDRAC BMC を使用して RAID を設定する

Redfish プロトコルで Dell iDRAC ベースボード管理コントローラー (BMC) を使用して、インストーラーがプロビジョニングしたインストール中にベアメタルプラットフォームの Redundant Array of Independent Disks (RAID) を設定できるようになりました。詳細は、オプション: RAID の設定 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 4.15 クラスターでは、クラスター内の 64 ビット ARM コンピュートマシン上の Red Hat Enterprise Linux CoreOS (RHCOS) カーネルで 64k ページサイズを有効にできるようになりました。このパラメーターの設定に関する詳細は、Red Hat Enterprise Linux CoreOS (RHCOS) カーネルでの 64k ページの有効化 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

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

- ロード時間を最小限に抑えるために、Pod ログビューアーへのテーリングを有効化および無効化します。
- Deployment ページで、**VerticalPodAutoscaler** の推奨値を表示します。

1.3.4.1.1. ノード稼働時間情報

この更新により、追加のノード稼働時間情報を表示して、ノードの再起動または障害を追跡する機能を有効にすることができます。**Compute → Nodes** ページに移動し、**Manage columns** をクリックして、**Uptime** を選択します。

1.3.4.1.2. 動的なプラグインの機能拡張

この更新により、**console.resource/details-item** を使用して、**Details** ページのデフォルトのリソース概要に新しい詳細アイテムを追加できるようになりました。OpenShift Container Platform リリースでは、アノテーション、ラベル、および削除モーダルの実装例も CronTab 動的プラグインに追加されています。

詳細は、動的プラグインのリファレンス を参照してください。

console.resource/details-item の詳細は、OpenShift Container Platform コンソール API を参照してください。

1.3.4.1.3. Azure AD Workload Identity の OperatorHub サポート

このリリースでは、OperatorHub は、Azure 上で実行されている OpenShift Container Platform クラスターが Azure AD Workload Identity 用に設定されている場合に検出します。検出されると、Operator が正しく実行されることを確認するために Operator をインストールする前に、追加の指示とともに "Cluster in Workload Identity / Federated Identity Mode" 通知が表示されます。**Operator Installation** ページも変更され、必要な Azure 認証情報のフィールドが追加されます。

Operator のインストール ページの更新された手順については、Web コンソールを使用した OperatorHub からのインストール を参照してください。

1.3.4.2. Developer パースペクティブ

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

- Tekton Results からのデータに基づくパイプライン履歴とログは、クラスター上で PipelineRun CR を必要とせずにダッシュボードで利用できます。

1.3.4.2.1. ソフトウェアサプライチェーンの機能拡張

Web コンソールの **開発者** または **管理者** パースペクティブの **PipelineRun Details** ページでは、プロジェクト内の PipelineRun の強化された視覚的表現を提供しています。

詳細は、Red Hat OpenShift Pipelines を参照してください。

1.3.4.2.2. Web コンソールの Red Hat Developer Hub

この更新により、Developer Hub のインストールおよび使用方法の詳細を学ぶためのクイックスタートが利用できるようになりました。

詳細は、Red Hat Developer Hub の製品ドキュメント を参照してください。

1.3.4.2.3. builds for OpenShift Container Platform が Web コンソールでサポートされる

この更新により、builds for OpenShift Container Platform 1.0 が Web コンソールでサポートされるようになりました。Builds は、Shipwright プロジェクト に基づく拡張可能なビルドフレームワークです。builds for OpenShift Container Platform を使用して、OpenShift Container Platform クラスター上にコンテナーイメージをビルドできます。

詳細は、builds for OpenShift Container Platform を参照してください。

1.3.5. 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 4.15 と互換性を持つようになりました。z/VM、LPAR、または Red Hat Enterprise Linux (RHEL) カーネルベースの仮想マシン (KVM) を使用して、インストールを実行できます。インストール手順については、以下のドキュメントを参照してください。

- IBM Z および IBM LinuxONE でのクラスターのインストール

重要

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

IBM Z および IBM LinuxONE の主な機能拡張
OpenShift Container Platform 4.15 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。

- Agent-based Installer
- cert-manager Operator for Red Hat OpenShift
- **x86_64** マルチアーキテクチャーコンピュートノードを備えた **s390x** コントロールプレーン

IBM Z および IBM LinuxONE 上の LPAR へのクラスターのインストール

OpenShift Container Platform は、IBM Z および IBM LinuxONE 上の論理パーティション (LPAR) での OpenShift Container Platform 4.15 のユーザーがプロビジョニングしたインストールをサポートするようになりました。

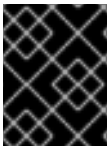
インストール手順については、以下のドキュメントを参照してください。

- IBM Z® および IBM® LinuxONE 上の LPAR へのクラスターのインストール
- 制限されたネットワーク内の IBM Z® および IBM® LinuxONE 上の LPAR へのクラスターのインストール

1.3.6. IBM Power

IBM Power® は OpenShift Container Platform 4.15 と互換性を持つようになりました。インストール手順については、以下のドキュメントを参照してください。

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



重要

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

IBM Power の主な機能拡張
OpenShift Container Platform 4.15 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。

- Agent-based Installer
- cert-manager Operator for Red Hat OpenShift
- IBM Power® Virtual Server Block CSI Driver Operator
- IBM Power® Virtual Server の installer-provisioned infrastructure の有効化
- Intel および IBM Power® ワーカーをサポートするマルチアーキテクチャー IBM Power® コントロールプレーン
- Power10 用の nx-gzip (ハードウェアアクセラレーション)
- IBM Power® 上のさまざまな SMT レベルをサポートする **openshift-install** ユーティリティー (ハードウェアアクセラレーション)

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

表1.1 OpenShift Container Platform の機能

機能	IBM Power®	IBM Z® および IBM® LinuxONE
代替の認証プロバイダー	サポート対象	サポート対象
Agent-based Installer	サポート対象	サポート対象
Assisted Installer	サポート対象	サポート対象
ローカルストレージ Operator を使用した自動デバイス検出	サポート対象外	サポート対象
マシンヘルスチェックによる障害のあるマシンの自動修復	サポート対象外	サポート対象外
IBM Cloud® 向けクラウドコントローラーマネージャー	サポート対象	サポート対象外
オーバーコミットの制御およびノード上のコンテナーの密度の管理	サポート対象外	サポート対象外
Cron ジョブ	サポート対象	サポート対象
Descheduler	サポート対象	サポート対象
Egress IP	サポート対象	サポート対象
etcd に保存されるデータの暗号化	サポート対象	サポート対象
FIPS 暗号	サポート対象	サポート対象
Helm	サポート対象	サポート対象
Horizontal Pod Autoscaling	サポート対象	サポート対象
Hosted Control Plane (テクノロジープレビュー)	サポート対象	サポート対象
IBM Secure Execution	サポート対象外	サポート対象
IBM Power® Virtual Server Block CSI Driver Operator	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	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

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

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

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

2. 永続的な非共有ストレージは、iSCSI、FC などのローカルストレージを使用するか、DASD、FCP、または EDEV/FBA での LSO を使用してプロビジョニングする必要があります。

表1.3 Operator

機能	IBM Power®	IBM Z® および IBM® LinuxONE
cert-manager Operator for Red Hat OpenShift	サポート対象	サポート対象
Cluster Logging Operator	サポート対象	サポート対象
Cluster Resource Override Operator	サポート対象	サポート対象
Compliance Operator	サポート対象	サポート対象
Cost Management Metrics Operator	サポート対象	サポート対象
File Integrity Operator	サポート対象	サポート対象
HyperShift Operator	テクノロジープレビュー	テクノロジープレビュー
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

機能	IBM Power®	IBM Z® および IBM® LinuxONE
NFD Operator	サポート対象	サポート対象
NMState Operator	サポート対象	サポート対象
OpenShift Elasticsearch Operator	サポート対象	サポート対象
Vertical Pod Autoscaler Operator	サポート対象	サポート対象

表1.4 Multus CNI プラグイン

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

表1.5 CSI ボリューム

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

1.3.7. 認証および認可

1.3.7.1. Azure AD Workload Identity に対する OLM ベースの Operator のサポート

このリリースでは、Azure 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、Azure AD Workload Identity 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短期認証情報を使用して認証します。

詳細は、Azure AD Workload Identity を使用した OLM 管理 Operator の CCO ベースのワークフロー を参照してください。

1.3.8. ネットワーク

1.3.8.1. OVN-Kubernetes ネットワークプラグインによる外部トラフィックの IPsec 暗号化の一般公開 (GA) のサポート

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。両方の機能を一緒に使用して、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。

この機能は次のプラットフォームでサポートされています。

- ベアメタル
- Google Cloud Platform (GCP)
- Red Hat OpenStack Platform (RHOSP)
- VMware vSphere

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。

1.3.8.2. macvlan CNI プラグインで IPv6 の自発的近隣広告がデフォルトに

以前は、1 つの Pod (**Pod X**) が削除され、同様の設定で 2 番目の Pod (**Pod Y**) が作成された場合、**Pod Y** は **Pod X** と同じ IPv6 アドレスを持つ可能性がありますが、MAC アドレスは異なりました。このシナリオでは、ルーターは MAC アドレスの変更を認識せず、**Pod X** の MAC アドレスにトラフィックを送信し続けます。

今回の更新により、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 が割り当てられている) は、デフォルトで IPv6 の自発的近隣広告をネットワークに送信するようになりました。この機能拡張により、IPv6 の近隣キャッシュを更新するために、特定の IP の新しい Pod の MAC アドレスがネットワークファブリックに通知されます。

1.3.8.3. Whereabouts IP リコンサイラーのスケジュールの設定

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

1.3.8.4. EgressFirewall および AdminPolicyBasedExternalRoute CR のステータス管理の更新

EgressFirewall および **AdminPolicyBasedExternalRoute** カスタムリソースポリシーのステータス管理に対して、次の更新が行われました。

- 1 つ以上のメッセージが **failure** を報告すると、**status.status** フィールドは **failure** に設定されます。
- 障害が報告されず、ステータスを報告していないノードがある場合、**status.status** フィールドは空になります。
- すべてのノードが **success** を報告すると、**status.status** フィールドは **success** に設定されます。

- **status.mesages** フィールドには、メッセージがリストされます。メッセージはデフォルトでノード名ごとにリストされ、ノード名が接頭辞として付けられます。

1.3.8.5. MetalLB の追加の BGP メトリクス

この更新により、MetalLB は、MetalLB と Border Gateway Protocol (BGP) ピア間の通信に関連する追加のメトリクスを公開します。詳細は、BGP および BFD の MetalLB メトリクス を参照してください。

1.3.8.6. all-multicast モードのサポート

OpenShift Container Platform は、チューニング CNI プラグインを使用した all-multicast モードの設定をサポートす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。

1.3.8.7. IPv6 ネットワークのマルチネットワークポリシーのサポート

この更新により、IPv6 ネットワーク用の multi-network ポリシーを作成できるようになりました。詳細は、IPv6 ネットワークでの multi-network ポリシーのサポート を参照してください。

1.3.8.8. Ingress Operator メトリクスダッシュボードが利用可能になる

このリリースでは、Ingress ネットワーキングメトリクスが OpenShift Container Platform Web コンソール内から表示できるようになりました。詳細は、Ingress Operator ダッシュボード を参照してください。

1.3.8.9. サブドメインに対する ExternalName サービスクエリーの CoreDNS フィルタリング

OpenShift Container Platform 4.15 以降、CoreDNS は 1.10.1 から 1.11.1 に更新されました。

CoreDNS のこの更新により、**com** や **org** などのトップレベルドメインと名前を共有する **ExternalName** サービスのクエリーに対して、CoreDNS が誤って応答を返す問題が解決されました。外部サービスのサブドメインのクエリーは、その外部サービスに解決されるべきではありません。詳細は、関連する CoreDNS GitHub の問題 を参照してください。

1.3.8.10. CoreDNS メトリクスの非推奨化と削除

OpenShift Container Platform 4.15 以降、CoreDNS は 1.10.1 から 1.11.1 に更新されました。

CoreDNS のこの更新により、メトリクス **coredns_forward_healthcheck_failures_total**、**coredns_forward_requests_total**、**coredns_forward_responses_total**、および **coredns_forward_request_duration_seconds** など、再配置された特定のメトリクスが非推奨になり、削除されました。詳細は、CoreDNS メトリクス を参照してください。

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

OpenShift Container Platform 4.15 では、以下の SR-IOV デバイスのサポートが追加されました。

- Mellanox MT2910 ファミリー [ConnectX-7]

詳細は、サポート対象のデバイス を参照してください。

1.3.8.12. SR-IOV ネットワーク VF のホストネットワーク設定ポリシー (テクノロジープレビュー)

このリリースでは、**NodeNetworkConfigurationPolicy** リソースを使用して、既存のクラスター内の Single Root I/O Virtualization (SR-IOV) ネットワーク Virtual Function (VF) のホストネットワーク設定を管理できるようになりました。

たとえば、ホストネットワークの Quality of Service (QoS) ポリシーを設定して、アタッチされた SR-IOV ネットワーク VF によるホストリソースへのネットワークアクセスを管理できます。詳細は、Virtual Function のノードネットワーク設定ポリシー を参照してください。

1.3.9. レジストリー

1.3.9.1. Azure 上のプライベートストレージエンドポイントのサポート

このリリースでは、Image Registry Operator を活用して Azure 上のプライベートストレージエンドポイントを使用できるようになりました。この機能を使用すると、OpenShift Container Platform がプライベート Azure クラスターにデプロイされている場合に、ストレージアカウントのプライベートエンドポイントをシームレスに設定できるため、ユーザーは公開用ストレージエンドポイントを公開せずに Image Registry をデプロイできます。

詳細は、以下のセクションを参照してください。

- Azure 上でプライベートストレージエンドポイントを設定する
- オプション: プライベート Image Registry 用のプライベート Microsoft Azure クラスターを準備する

1.3.10. ストレージ

1.3.10.1. 以前の LVM Storage インストールからのボリュームグループの復元

このリリースでは、**LVMCluster** カスタムリソース (CR) が、以前の LVM Storage インストールからボリュームグループをリカバリーするためのサポートを提供します。**deviceClasses.name** フィールドが以前の LVM Storage インストールのボリュームグループの名前に設定されている場合、LVM Storage は現在の LVM Storage インストールでそのボリュームグループに関連するリソースを再作成します。これにより、以前の LVM Storage インストールから LVM Storage の再インストールまでのデバイスを使用するプロセスが簡素化されます。

詳細は、ワーカーノードでの Logical Volume Manager クラスターの作成 を参照してください。

1.3.10.2. LVM Storage 内におけるデバイスのワイプのサポート

この機能は、選択したデバイスを強制的にワイプするために、**LVMCluster** カスタムリソース (CR) に新しいオプションのフィールド **forceWipeDevicesAndDestroyAllData** を提供します。このリリースより前は、デバイスをワイプするにはホストに手動でアクセスする必要がありました。このリリースでは、手動介入なしでディスクを強制的に消去できます。これにより、ディスクを消去するプロセスが簡素化されます。

警告

forceWipeDevicesAndDestroyAllData が **true** に設定されている場合、LVM Storage はデバイス上の以前のデータをすべて消去します。この機能の使用は、慎重に行う必要があります

詳細は、ワーカーノードでの Logical Volume Manager クラスターの作成 を参照してください。

1.3.10.3. マルチノードクラスター上での LVM Storage のデプロイメントのサポート

この機能は、LVM Storage をマルチノードクラスターにデプロイするためのサポートを提供します。以前は、LVM Storage はシングルノード設定のみをサポートしていました。このリリースでは、LVM Storage はすべての OpenShift Container Platform デプロイメントトポロジーをサポートします。これにより、マルチノードクラスター上でローカルストレージをプロビジョニングできるようになります。

警告

LVM Storage は、マルチノードクラスター上のノードローカルストレージのみをサポートします。ノード間のストレージデータレプリケーションメカニズムはサポートされません。マルチノードクラスターで LVM Storage を使用する場合は、単一障害点を回避するために、アクティブまたはパッシブレプリケーションメカニズムを通じて、ストレージデータを確実にレプリケーションする必要があります。

詳細は、LVM Storage のデプロイメント を参照してください。

1.3.10.4. RAID アレイと LVM Storage の統合

この機能は、**mdadm** ユーティリティーを使用して作成された RAID アレイを LVM Storage と統合するためのサポートを提供します。**LVMCluster** カスタムリソース (CR) は、**deviceSelector.paths** フィールドおよび **deviceSelector.optionalPaths** フィールドで、RAID アレイへのパスを追加するためのサポートを提供します。

詳細は、ソフトウェア RAID アレイと LVM Storage の統合 を参照してください。

1.3.10.5. LVM Storage の FIPS 準拠サポート

このリリースでは、LVM Storage は Federal Information Processing Standards (FIPS) に準拠するように設計されています。LVM Storage が FIPS モードで OpenShift Container Platform にインストールされている場合、LVM Storage は、x86_64 アーキテクチャー上でのみ FIPS 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。

1.3.10.6. 遡及的なデフォルトの StorageClass 割り当てが一般提供される

OpenShift Container Platform 4.13 より前では、デフォルトのストレージクラスがなかった場合、デフォルトのストレージクラスを要求するために作成された永続ボリューム要求 (PVC) は、手動で削除

して再作成しない限り、無期限に保留状態のままになりました。OpenShift Container Platform 4.14 以降では、テクノロジープレビュー機能として、デフォルトのストレージクラスがこれらの PVC に遡って割り当てられるため、保留状態に残らないようになります。デフォルトのストレージクラスが作成されるか、既存のストレージクラスの 1 つがデフォルトとして宣言されると、これらの以前に保留された PVC がデフォルトのストレージクラスに割り当てられます。現在、この機能は一般提供されています。

詳細は、デフォルトストレージクラスの欠落 を参照してください。

1.3.10.7. ローカルボリューム上の既存データの削除を容易にする Local Storage Operator オプションが一般提供される

この機能には、オプションのフィールド **forceWipeDevicesAndDestroyAllData** があり、**wipefs** を呼び出すかどうかを定義します。これにより、パーティションテーブルの署名 (マジックストリング) が削除され、ディスクを Local Storage Operator (LSO) プロビジョニングに使用できるようになります。署名以外のデータは消去されません。現在、この機能は一般提供されています。この機能は **LocalVolumeSet** (LVS) には適用されないことに注意してください。

詳細は、Local Storage Operator を使用したローカルボリュームのプロビジョニング を参照してください。

1.3.10.8. 正常ではないノードのシャットダウン後に CSI ボリュームを切断する機能が一般提供される

OpenShift Container Platform 4.13 以降、Container Storage Interface (CSI) ドライバーは、テクノロジープレビュー機能として、ノードが正常に停止しないときにボリュームを自動的にデタッチできるようになりました。ノードが正常にシャットダウンしなかった場合、ノードに out-of-service テイントを手動で追加し、ノードからボリュームを自動的にデタッチできます。現在、この機能は一般提供されています。

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

1.3.10.9. 共有 VPC が一般提供され、GCP Filestore CSI Driver Operator でサポートされる

Google Compute Platform (GCP) Container Storage Interface (CSI) Driver Operator の共有 Virtual Private Cloud (VPC) が、一般提供機能としてサポートされるようになりました。共有 VPC により、ネットワーク管理が簡素化され、一貫したネットワークポリシーが可能になり、ネットワークリソースの一元的なビューが提供されます。

詳細は、GCP Filestore Storage のストレージクラスの作成 を参照してください。

1.3.10.10. ユーザー管理の暗号化が一般提供され、IBM VPC ブロックストレージをサポートする

ユーザー管理型の暗号化機能を使用すると、インストール中に OpenShift Container Platform ノードのルートボリュームを暗号化するキーを提供でき、すべてのマネージドストレージクラスが指定された暗号化キーを使用してプロビジョニングされたストレージボリュームを暗号化できるようになります。この機能は、Google Cloud Platform (GCP) 永続ディスク (PD) ストレージ、Microsoft Azure Disk、および Amazon Web Services (AWS) Elastic Block Storage (EBS) 用の OpenShift Container Platform 4.13 で導入され、現在は IBM Virtual Private Cloud (VPC) Block ストレージでサポートされています。

1.3.10.11. マウントオプションを使用した SELinux の再ラベル付け (テクノロジープレビュー)

以前は、SELinux が有効になっていると、永続ボリューム (PV) を Pod に接続するときに永続ボリュームのファイルのラベルが変更され、PV に多くのファイルが含まれている場合にタイムアウトが発生したり、ストレージバックエンドが過負荷になったりする可能性がありました。

OpenShift Container Platform 4.15 では、この機能をサポートする Container Storage Interface (CSI) ドライバーの場合、ドライバーは正しい SELinux ラベルを使用してボリュームを直接マウントするため、ボリュームのラベルを再帰的に変更する必要がなくなり、Pod の起動が大幅に高速化されます。

これはテクノロジープレビュー機能としてサポートされています。

次の条件が当てはまる場合、この機能はデフォルトで有効になります。

- ボリュームを提供する CSI ドライバーは、CSIDriver インスタンスの **seLinuxMountSupported: true** でこの機能をサポートします。OpenShift Container Platform の一部として出荷される以下の CSI ドライバーは、SELinux マウントのサポートをアナウンスします。
    - AWS Elastic Block Storage (EBS)
    - Azure Disk
    - Google Compute Platform (GCP) 永続ディスク (PD)
    - IBM Virtual Private Cloud (VPC) ブロック
    - OpenStack Cinder
    - VMware vSphere
- 永続ボリュームを使用する Pod には、**restricted** SCCを使用して、**spec.securityContext** または **spec.containers[*].securityContext** で指定された完全な SELinux ラベルがあります。
- ボリュームのアクセスモードは **ReadWriteOncePod** に設定されています。

1.3.11. Oracle® Cloud Infrastructure

1.3.11.1. Assisted installer を使用して OCI にクラスターをインストールする (テクノロジープレビュー)

専用、ハイブリッド、パブリックおよびマルチクラウド環境をサポートする Oracle® Cloud Infrastructure (OCI) インフラストラクチャー上でクラスターワークロードを実行できます。Red Hat と Oracle はどちらも、OCI 上の OpenShift Container Platform クラスターでの OCI の実行をテスト、検証、サポートしています。

OCI は、規制コンプライアンス、パフォーマンス、費用対効果のニーズを満たすサービスを提供します。OCI Resource Manager 設定にアクセスして、OCI リソースをプロビジョニングおよび設定できます。

詳細は、Assisted Installer を使用した OCI へのクラスターのインストール を参照してください。

1.3.11.2. エージェントベースのインストーラーを使用して OCI にクラスターをインストールする (テクノロジープレビュー)

エージェントベースのインストーラを使用して Oracle® Cloud Infrastructure (OCI) にクラスターをインストールすると、専用、ハイブリッド、パブリックおよびマルチクラウド環境をサポートするインフラストラクチャー上でクラスターのワークロードを実行できます。

エージェントベースのインストーラーは、Assisted Installation サービスを使いやすくするだけでなく、接続環境または非接続環境のいずれかにクラスターをインストールする機能を備えています。

OCI は、規制コンプライアンス、パフォーマンス、費用対効果のニーズを満たすサービスを提供します。OCI は、64 ビット **x86** インスタンスと 64 ビット ARM インスタンスをサポートします。

詳細は、エージェントベースのインストーラを使用した OCI へのクラスターのインストール を参照してください。

1.3.12. Operator ライフサイクル

1.3.12.1. Operator Lifecycle Manager (OLM) 1.0 (テクニカルプレビュー)

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。

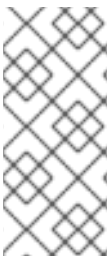
OpenShift Container Platform 4.15 の OLM 1.0 のテクノロジープレビューフェーズ中に、管理者はこのリリースに追加された以下の機能を試すことができます。

バージョン範囲のサポート

Operator またはエクステンションのカスタムリソース (CR) で比較文字列を使用して、バージョン範囲を指定できます。CR でバージョン範囲を指定すると、OLM 1.0 は、そのバージョン範囲内で解決できる Operator の最新バージョンをインストールまたは更新します。詳細は、Operator の更新 および バージョン範囲のサポート を参照してください。

Catalog API のパフォーマンスの向上

Catalog API は、HTTP サービスを使用してクラスター上でカタログコンテンツを提供するようになりました。以前は、カスタムリソース定義 (CRD) がこの目的に使用されていました。カタログコンテンツの提供に HTTP サービスを使用するように変更したことで、Kubernetes API サーバーの負荷が軽減されました。詳細は、カタログからインストールする Operator の検索 を参照してください。



注記

OpenShift Container Platform 4.15 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 (OLM) 1.0 について を参照してください。

1.3.12.2. Operator カタログの非推奨スキーマ

オプションの **olm.deprecations** スキーマは、ファイルベースのカタログ内の Operator パッケージ、バンドル、およびチャネルの非推奨情報を定義します。Operator の作成者は、**deprecations.yaml** ファイルでこのスキーマを使用して、サポートステータスや推奨されるアップグレードパスなど、Operator に関する関連メッセージをカタログからこれらの Operator を実行しているユーザーに提供できます。Operator がインストールされると、指定されたメッセージが、関連する **Subscription** オブジェクトのステータス状況として表示されます。

olm.deprecations スキーマの詳細は、 Operator Framework のパッケージ化形式 を参照してください。

1.3.13. Operator の開発

1.3.13.1. クラウドプロバイダー上の Operator のトークン認証: Azure AD Workload Identity

このリリースでは、Operator Lifecycle Manager (OLM) によって管理される Operator は、Azure AD Workload Identity 用に設定された Azure クラスター上で実行するときに、トークン認証をサポートできるようになります。Cloud Credential Operator (CCO) を更新すると、Operator の作成者が Operator による Azure AD Workload Identity のサポートを有効にしている場合に限り、特定の短期認証情報の半自動プロビジョニングが可能になります。

詳細は、Azure AD Workload Identity を使用した OLM 管理 Operator の CCO ベースのワークフロー を参照してください。

1.3.14. ビルド

1.3.15. Machine Config Operator

1.3.15.1. ノードごとの MCO 状態レポートの改善 (テクノロジープレビュー)

このリリースでは、テクノロジープレビューとして個々のノードの更新を監視できます。詳細は、マシン config ノードのステータスの確認 を参照してください。

1.3.16. マシン API

1.3.16.1. コントロールプレーンマシンセットの VMware vSphere 障害ドメインの定義 (テクノロジープレビュー)

vSphere 障害ドメインリソースを使用すると、コントロールプレーンマシンセットを使用して、プライマリー VMware vSphere インフラストラクチャーとは別のハードウェアにコントロールプレーンマシンをデプロイできます。コントロールプレーンマシンセットは、定義された障害ドメイン全体でコントロールプレーンマシンのバランスをとり、インフラストラクチャーにフォールトトレランス機能を提供する際に役立ちます。

詳細は、VMware vSphere 障害ドメイン設定のサンプル および 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。

1.3.17. ノード

1.3.17.1. /dev/fuse デバイスにより、特権のない Pod でのビルドの高速化が可能になる

/dev/fuse デバイスを使用して特権のない Pod を設定すると、より高速なビルドにアクセスできます。

詳細は、/dev/fuse を使用した高速ビルドへのアクセス を参照してください。

1.3.17.2. ログのリンクがデフォルトで有効化される

OpenShift Container Platform 4.15 以降、ログのリンクはデフォルトで有効化されています。ログのリンクにより、Pod のコンテナーログにアクセスできるようになります。

1.3.17.3. ICSP、IDMS、ITMS の互換性の確保

ImageContentSourcePolicy (ICSP)、**ImageDigestMirrorSet** (IDMS)、および **ImageTagMirrorSet**

(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。以前は、新しい IDMS または ITMS オブジェクトを使用するには、ICSP オブジェクトを削除する必要がありました。これで、クラスターのインストール後に 3 種類のオブジェクトのいずれかまたはすべてを使用して、リポジトリーミラーリングを設定できるようになります。詳細は、 Image Registry リポジトリーのミラーリングについて を参照してください。

重要

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

1.3.18. Monitoring

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

1.3.18.1. モニタリングスタックコンポーネントおよび依存関係の更新

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

- Alertmanager to 0.26.0
- kube-state-metrics to 2.10.1
- node-exporter to 1.7.0
- Prometheus to 2.48.0
- Prometheus Adapter to 0.11.2
- Prometheus Operator to 0.70.0
- Thanos Querier to 0.32.5

1.3.18.2. 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。

- Precision Time Protocol (PTP) が使用されている場合、**NodeClockNotSynchronising** および **NodeClockSkewDetected** アラートルールが無効になりました。

1.3.18.3. Metrics API にアクセスするための新しい Metrics Server コンポーネント (テクノロジープレビュー)

このリリースでは、Metrics Server コンポーネントをクラスター内モニタリングスタックに追加するためのテクノロジープレビューオプションが導入されています。**FeatureGate** カスタムリソースが **TechPreviewNoUpgrade** オプションで設定されている場合、テクノロジープレビュー機能として、Prometheus Adapter の代わりに Metrics Server が自動的にインストールされます。インストールされると、Metrics Server は、リソースメトリクスを収集して **metrics.k8s.io** Metrics API サービスで公開

し、他のツールや API で使用できるようにします。Prometheus Adapter の代わりに Metrics Server を使用すると、コアプラットフォームの Prometheus スタックがこの機能を処理しなくなります。詳細は、Cluster Monitoring Operator の config map API リファレンスの MetricsServerConfig および フィーチャーゲートを使用した機能の有効化 を参照してください。

1.3.18.4. ユーザー定義プロジェクトのリモート書き込みストレージにサンプルデータを送信する新機能

ユーザー定義プロジェクトは、リモート書き込みを使用して、Prometheus によって収集されたサンプルデータをリモートストレージに送信できるようになりました。この機能を使用するには、**RemoteWriteSpec** リソースの **sendExemplars** オプションを使用して、リモート書き込みを設定します。詳細は、Cluster Monitoring Operator の config map API リファレンスの RemoteWriteSpec を参照してください。

1.3.18.5. ユーザー定義プロジェクトのアラートクエリーの改善

ユーザー定義プロジェクトのアプリケーションは、Thanos Querier のルールテナンシーポートを介して、アプリケーション namespace のアラートをクエリーする API アクセスが可能となりました。HTTP 要求に **namespace** パラメーターが含まれている場合、Thanos Querier のポート 9093 経由で **/api/v1/alerts** エンドポイントにアクセスするクエリーを構築できるようになりました。以前のリリースでは、Thanos Querier のルールテナンシーポートは **/api/v1/alerts** エンドポイントへの API アクセスを提供しませんでした。

1.3.18.6. Prometheus が更新され、スクレイピング時のジッターを許容できるようになりました

モニタリングスタックのデフォルトの Prometheus 設定が更新され、スクレイピング時のジッターが許容されるようになりました。データストレージのチャンク圧縮が最適ではないモニタリングデプロイメントの場合、この更新はデータ圧縮の最適化に役立ち、その結果、これらのデプロイメントで時系列データベースによって使用されるディスク領域が削減されます。

1.3.18.7. kubelet サービスモニターの陳腐化処理の改善

アラートと時間集計が正確となるように、kubelet サービスモニターの陳腐化処理が改されました。この改善された機能はデフォルトでアクティブになり、専用のサービスモニター機能は廃止されます。その結果、専用サービスモニター機能が無効化され、現在は非推奨となっており、**DedicatedServiceMonitors** リソースを **enabled** に設定しても効果はありません。

1.3.18.8. 失敗したタスクのレポートのトラブルシューティング機能の向上

コンポーネントのモニタリングでタスクが失敗したときに提供される理由がより詳細に表示されるようになり、報告された障害の原因が **openshift-monitoring** namespace にデプロイされたコンポーネントにあるのか、**openshift-user-workload-monitoring** namespace にあるのかをより簡単に特定できるようになりました。Cluster Monitoring Operator (CMO) がタスクの失敗を報告した場合、失敗の原因を特定するために次の理由が追加されています。

- **PlatformTasksFailed** の理由は、**openshift-monitoring** namespace で発生したエラーを示します。
- **UserWorkloadTasksFailed** の理由は、**openshift-user-workload-monitoring** namespace で発生した障害を示します。

1.3.19. 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。

1.3.20. スケーラビリティーおよびパフォーマンス

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、システムがどの速度を使用するかを決定できるようになります。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。

1.3.20.1. PolicyGenTemplate CR のハブ側テンプレーティング

ハブテンプレートを使用して、マネージドクラスターに適用される生成されたポリシーにグループとサイトの値を入力することで、複数のクラスターの設定を管理できます。グループおよびサイトの **PolicyGenTemplate** (PGT) CR でハブテンプレートを使用すると、ハブクラスター上のポリシーの数を大幅に減らすことができます。詳細は、ハブテンプレートを使用して PolicyGenTemplate CR グループのグループとサイトの設定を指定する を参照してください。

1.3.20.2. Node Tuning Operator (NTO)

レイテンシーテスト用の Cloud-native Network Functions (CNF) テストイメージ (**cnf-tests**) が簡素化されました。新しいイメージには、レイテンシー測定のための 3 つのテストが含まれています。テストはデフォルトで実行され、クラスター上に設定されたパフォーマンスプロファイルが必要です。パフォーマンスプロファイルが設定されていない場合、テストは実行されません。

次の変数の使用は推奨されなくなりました。

- **ROLE_WORKER_CNF**
- **NODES_SELECTOR**
- **PERF_TEST_PROFILE**
- **FEATURES**
- **LATENCY_TEST_RUN**
- **DISCOVERY_MODE**

junit レポートを生成するには、**--ginkgo.junit-report** フラグを **--junit** に置き換えます。

詳細は、プラットフォーム検証のためのレイテンシーテストの実行 を参照してください。

1.3.20.3. Bare Metal Operator

OpenShift Container Platform 4.15 の場合、Bare Metal Operator がクラスターからホストを削除すると、ホストの電源もオフになります。この機能拡張により、ハードウェアのメンテナンスと管理が合理化されます。

1.3.21. Hosted Control Plane

1.3.21.1. 非ベアメタルエージェントマシンを使用した Hosted Control Plane クラスターの設定 (テクノロジープレビュー)

このリリースでは、非ベアメタルエージェントマシンを使用して、Hosted Control Plane クラスターをプロビジョニングできます。詳細は、非ベアメタルエージェントマシンを使用した Hosted Control Plane クラスターの設定 (テクノロジープレビュー) を参照してください。

1.3.21.2. OpenShift Container Platform コンソールを使用したホストされたクラスターの作成

このリリースでは、OpenShift Container Platform コンソールを使用して、ホストされたクラスターを KubeVirt プラットフォームで作成できるようになりました。Kubernetes Operator (MCE) のマルチクラスターエンジンにより、ホステッドクラスタービューが有効になります。詳細は、コンソールを使用したホステッドクラスターの作成 を参照してください。

1.3.21.3. 追加のネットワーク、Guaranteed CPU、およびノードプールの仮想マシンのスケジュールを設定する

このリリースでは、追加のネットワークの設定、仮想マシン用の Guaranteed CPU へのアクセス要求、およびノードプールの KubeVirt 仮想マシンのスケジュール管理を実行できるようになりました。詳細は、追加のネットワーク、Guaranteed CPU、およびノードプールの仮想マシンのスケジュールを設定する を参照してください。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.15 では、次の注目すべき技術的な変更が導入されています。

クラスターメトリクスポートの保護
このリリースでは、Cluster Machine Approver Operator と Cluster Cloud Controller Manager Operator のメトリクスを提供するポートは、セキュリティーを強化するために Transport Layer Security (TLS) プロトコルを使用します。(**OCPCLOUD-2272**、**OCPCLOUD-2271**)

Google Cloud Platform 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、Google Cloud Platform のクラウドコントローラーマネージャーの使用が一般公開されました。

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

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

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

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監査ログに警告として表示されますが、Pod は拒否されません。

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が実行されるタイミングを理解するには、Pod セキュリティーアドミッション同期について 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。

統合された OpenShift Image Registry が無効になっている場合はシークレットが自動的に生成されなくなる

ImageRegistry クラスター機能を無効にするか、Cluster Image Registry Operator の設定で統合された OpenShift Image Registry を無効にすると、サービスアカウントトークンシークレットとイメージプルシークレットは、サービスアカウントごとに生成されなくなります。

詳細は、自動生成されたシークレット を参照してください。

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

以前は、IP アドレス範囲 **168.254.0.0/16** が、Open Virtual Network Infrastructure Controller がトランジットスイッチサブネットに使用するデフォルトの IP アドレス範囲でした。この更新により、この Controller はデフォルトの 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-20178)

HAProxy no strict-limits の導入

HAProxy 2.6 への移行には、**strict-limits** 設定の強制が含まれており、その結果、**maxConnections** 要件が満たされない場合に回復不能なエラーが発生しました。**strict-limits** 設定はエンドユーザーによって設定できず、HAProxy テンプレートの制御下に残ります。

このリリースでは、移行に応じて **maxConnections** 問題への設定の調整が導入されています。これで、HAProxy 設定は **no strict-limits** を使用するように切り替わりました。その結果、**maxConnection** 設定が満たされない場合に、HAProxy が回復不能な形で終了することがなくなりました。代わりに、警告を発し、実行を継続します。**maxConnection** の制限が満たされない場合、次の例のような警告が返される場合があります。

- **[WARNING] (50) : [/usr/sbin/haproxy.main()] Cannot raise FD limit to 4000237, limit is 1048576.**
- **[ALERT] (50) : [/usr/sbin/haproxy.main()] FD limit (1048576) too low for maxconn=2000000/maxsock=4000237.Please raise 'ulimit-n' to 4000237 or more to avoid any trouble.**

これらの警告を解決するには、IngressController を調整するときに **maxConnections** フィールドに **-1** または **auto** を指定することを推奨します。この選択により、HAProxy は実行中のコンテナーで利用可能なリソースの制限に基づいて最大値を動的に計算できるようになり、これらの警告が表示されなくなります。(OCPBUGS-21803)

DeploymentConfig クラスター機能が無効になっている場合に、deployer サービスアカウントが作成されなくなる
DeploymentConfig クラスター機能を無効にすると、**deployer** サービスアカウントとそれに対応するシークレットは作成されなくなります。

詳細は、DeploymentConfig 機能 を参照してください。

must-gather ストレージ制限のデフォルト
oc adm must-gather コマンドによって収集されるデータには、コンテナーノードのストレージ容量の 30% というデフォルト制限が追加されました。必要に応じて、**--volume-percentage** フラグを使用して、デフォルトのストレージ制限を調整できます。

詳細は、must-gather ストレージ制限の変更 を参照してください。

エージェントベースのインストーラーの対話型ネットワーク設定がシリアルコンソールに表示される
この更新により、グラフィカルコンソールのないサーバーで Agent ISO が起動される場合、シリアルコンソールで対話型ネットワーク設定が可能になります。対話型ネットワーク設定がアクティブな間は、他のすべてのコンソールではステータス表示が一時停止されます。以前は、グラフィカルコンソールでのみ表示できました。(OCPBUGS-19688)

1.5. 非推奨および削除された機能

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

非推奨の機能は依然として OpenShift Container Platform に含まれており、引き続きサポートされますが、本製品の今後のリリースで削除されるため、新規デプロイメントでの使用は推奨されません。OpenShift Container Platform 4.15 内で非推奨化および削除された主な機能の最新のリストについては、以下の表を参照してください。非推奨となり、削除された機能の詳細は、表の後に記載されています。

次の表では、機能は次のステータスでマークされています。

- **一般公開 (GA)**
- **非推奨**
- **削除済み**

Operator のライフサイクルと開発の非推奨および削除された機能

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

機能	4.13	4.14	4.15
Operator カタログの SQLite データベース形式	非推奨	非推奨	非推奨

イメージの非推奨および削除された機能

表1.7 イメージは廃止され、トラッカーが削除されました

機能	4.13	4.14	4.15
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

非推奨および削除された機能の監視

表1.8 非推奨および削除されたトラッカーのモニタリング

機能	4.13	4.14	4.15
コアプラットフォームモニタリング用の専用サービスモニターを有効にする **dedicatedServiceMonitors** 設定	一般公開 (GA)	一般公開 (GA)	非推奨

インストールの非推奨および削除された機能

表1.9 インストールが非推奨になり、トラッカーが削除されました

機能	4.13	4.14	4.15
OpenShift SDN ネットワークプラグイン	一般公開 (GA)	非推奨	削除済み [1]
oc adm release extract の **--cloud** パラメーター	一般公開 (GA)	非推奨	非推奨
cluster.local ドメインの CoreDNS ワイルドカードクエリー	削除済み	削除済み	削除済み
RHOSP の **compute.platform.openstack.rootVolume.type**	一般公開 (GA)	非推奨	非推奨
RHOSP の **controlPlane.platform.openstack.rootVolume.type**	一般公開 (GA)	非推奨	非推奨
installer-provisioned infrastructure クラスターにおける **install-config.yaml** ファイル内の **ingressVIP** および **apiVIP** 設定	非推奨	非推奨	非推奨
Google Cloud Provider の **platform.gcp.licenses**	非推奨	削除済み	削除済み

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

ストレージの非推奨および削除された機能

表1.10 Storage の廃止と削除されたトラッカー

機能	4.13	4.14	4.15
FlexVolume を使用した永続ストレージ	非推奨	非推奨	非推奨

ネットワーキングの非推奨機能と削除された機能

表1.11 ネットワーキングの非推奨化と削除のトラッカー

機能	4.13	4.14	4.15
RHOSP 上の Kuryr	非推奨	非推奨	削除済み
OpenShift SDN ネットワークプラグイン	一般公開 (GA)	非推奨	非推奨

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

機能	4.13	4.14	4.15
Service Binding Operator	非推奨	非推奨	非推奨

ノードの非推奨および削除された機能

表1.13 ノードは廃止され、トラッカーが削除されました

機能	4.13	4.14	4.15
ImageContentSourcePolicy (ICSP) オブジェクト	非推奨	非推奨	非推奨
Kubernetes トポロジーラベル **failure-domain.beta.kubernetes.io/zone**	非推奨	非推奨	非推奨
Kubernetes トポロジーラベル **Failure-domain.beta.kubernetes.io/region**	非推奨	非推奨	非推奨

OpenShift CLI (oc) の非推奨および削除された機能

機能	4.13	4.14	4.15
oc-mirror の **--include-local-oci-catalogs** パラメーター	一般公開 (GA)	削除済み	削除済み
oc-mirror の **--use-oci-feature** パラメーター	非推奨	削除済み	削除済み

ワークロードの非推奨および削除された機能

表1.14 ワークロードの非推奨および削除されたトラッカー

機能	4.13	4.14	4.15
DeploymentConfig オブジェクト	一般公開 (GA)	非推奨	非推奨

ベアメタルの監視

表1.15 Bare Metal Event Relay Operator トラッカー

機能	4.13	4.14	4.15
Bare Metal Event Relay Operator	テクノロジープレビュー	テクノロジープレビュー	非推奨

1.5.1. 非推奨の機能

1.5.1.1. 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 4.15 以降の新規インストールでは、ネットワークプラグインというオプションはなくなりました。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、この機能は拡張されなくなります。OpenShift SDN CNI の代わりに、OVN Kubernetes CNI を使用できます。

1.5.1.2. Bare Metal Event Relay Operator

Bare Metal Event Relay Operator は非推奨になりました。Bare Metal Event Relay Operator を使用してベアメタルホストを監視する機能は、今後の OpenShift Container Platform リリースでは削除される予定です。

1.5.1.3. Service Binding Operator

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

1.5.1.4. コアプラットフォームモニタリングの専用サービスモニター

このリリースでは、コアプラットフォームモニタリングのための専用サービスモニター機能は非推奨になりました。**openshift-monitoring** namespaceの **cluster-monitoring-config** config map オブジェクトで **dedicatedServiceMonitors** を設定することで専用サービスモニターを有効にする機能は、今後の OpenShift Container Platform リリースでは削除される予定です。この機能に代わり、アラートと時間集計が正確となるように Prometheus 機能が改善されました。この改善された機能はデフォルトでアクティブになり、専用のサービスモニター機能は廃止されます。

1.5.1.5. oc registry info コマンドが非推奨に

このリリースでは、実験的な **oc registry info** コマンドは非推奨になりました。

統合された OpenShift Image Registry に関する情報を表示するには、**oc get imagestream -n openshift** を実行し、**IMAGE REPOSITORY** 列を確認します。

1.5.2. 削除された機能

1.5.2.1. OPENSHIFT_DEFAULT_REGISTRY の削除

OpenShift Container Platform 4.15 では、**OPENSHIFT_DEFAULT_REGISTRY** 変数のサポートが削除されました。この変数は主に、以前のセットアップの内部 Image Registry で下位互換性を有効にするために使用されました。**REGISTRY_OPENSHIFT_SERVER_ADDR** 変数を代わりに使用できます。

1.5.2.2. Kuryr を使用した Red Hat OpenStack Platform (RHOSP) へのクラスターインストールを削除

OpenShift Container Platform 4.15 の時点で、kuryr を使用した RHOSP へのクラスターインストールのサポートは削除されました。

1.5.3. 今後の Kubernetes API の削除

OpenShift Container Platform の次のマイナーリリースでは、Kubernetes 1.29 を使用する予定です。Kubernetes 1.29 では、非推奨 API が削除されました。

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

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

1.6. バグ修正

API サーバーと認証

- 以前は、アップストリームライブラリーの設定により、kube-apiserver ログフォルダー内の **termination.log** に無効なパーミッションがありました。このリリースでは、アップストリームライブラリーが更新され、**terminate.log** に予期されたパーミッションが与えられるようになりました。(OCPBUGS-11856)

- 以前は、アップグレード後に既存のマニフェストが機能アノテーションを取得した場合、Cluster Version Operator (CVO) によって機能が有効になりました。これにより、以前にコンソール機能を無効にしていたユーザーの場合、OpenShift Container Platform 4.14 にアップグレードした後にコンソールが有効化されます。このリリースでは、不要なコンソール機能が既存のマニフェストから削除され、コンソール機能は暗黙的に有効化されなくなりました。(OCPBUGS-20331)

- 以前は、**openshift-kube-controller-manager** namespace が削除されると、**failed to synchronize namespace** というエラーが繰り返しログに記録されていました。このリリースでは、**openshift-kube-controller-manager** namespace が削除される際に、エラーがログに記録されなくなりました。(OCPBUGS-17458)

ベアメタルハードウェアのプロビジョニング

- 以前は、デュアルスタック GitOps ZTP ハブから IPv6 専用ホストをデプロイすると、正しいコールバック URL がベースボード管理コントローラー (BMC) に渡されませんでした。その結

果、IPv4 URL が無条件に渡されました。この問題は解決され、URL の IP バージョンは BMC アドレスの IP バージョンに依存するようになりました。(OCPBUGS-23759)

- 以前は、Bare Metal Operator (BMO) コンテナーには **60000** として指定された **hostPort** がありましたが、その **hostPort** は仕様にもかかわらず実際には使用されていませんでした。その結果、他のサービスはポート 60000 を使用できなくなりました。この修正により、コンテナー設定から **hostPort** 仕様が削除されます。これで、ポート 60000 が他のサービスで使用できるようになりました。(OCPBUGS-18788)

- 以前は、Cluster Baremetal Operator (CBO) がインフラストラクチャーの **platformStatus** フィールドをチェックすると失敗し、**nil** を返しました。OpenShift Container Platform 4.15 では、CBO が更新され、**apiServerInternalIPs** が **nil** を返した場合に確認して空の値を返すようになり、この問題は解決されました。(OCPBUGS-17589)

- 以前は、**inspector.ipxe** 設定では **IRONIC_IP** 変数が使用されていましたが、IPv6 アドレスには括弧が含まれていたため、考慮されていませんでした。その結果、ユーザーが誤った **boot_mac_address** を指定すると、iPXE は **inspector.ipxe** 設定にフォールバックし、括弧が含まれていなかったため、不正な形式の IPv6 ホストヘッダーが提供されました。
  OpenShift Container Platform 4.15 では、**inspector.ipxe** 設定が **IRONIC_URL_HOST** 変数を使用するように更新されました。これにより、IPv6 アドレスが考慮され、この問題は解決されました。(OCPBUGS-27060)

- 以前は、Cisco UCS ハードウェアで RedFish 仮想メディアを使用して新しいベアメタルホストに OpenShift Container Platform をデプロイしようとするとバグがありました。このバグにより、Ironic が適切な仮想メディアデバイスを見つけることができなかったため、ベアメタルホストでの新しいプロビジョニングがブロックされました。今回の更新により、Ironic は利用可能なすべての仮想メディアデバイスでより多くのチェックを実行します。その結果、RedFish 仮想メディアを使用するときに Cisco UCS ハードウェアをプロビジョニングできるようになりました。(OCPBUGS-23105)

- 以前は、**secureBoot** フィールドが **disabled** に設定されているノードに、**bootMode** フィールドを **UEFISecureBoot** に設定して OpenShift Container Platform をインストールすると、インストールプログラムの起動に失敗していました。この更新により、Ironic が更新され、**secureBoot** を **enabled** に設定して、OpenShift Container Platform をインストールできるようになりました。(OCPBUGS-9303)

ビルド

- 以前は、コンテナー間でコンテンツをコピーするときにタイムスタンプが保持されませんでした。このリリースでは、タイムスタンプを保存できるように **-p** フラグが **cp** コマンドに追加されました。(OCPBUGS-22497)

クラウドコンピュート

- 以前は、**MachineSet** 仕様からのテイントの解析エラーにより、オートスケーラーは仕様に直接設定されたテイントを考慮できないことを意味していました。その結果、ゼロからスケーリングするために **MachineSet** テイントに依存する場合、仕様からのテイントが考慮されず、スケーリングの決定が正しく行われない可能性がありました。この更新により、ゼロからのスケールロジック内の解析の問題が解決されました。その結果、オートスケーラーは正しくスケールアップし、ワークロードのスケジュールを妨げるテインとを特定できるようになりました。(OCPBUGS-27750)

- 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-27486)

- 以前は、Hosted Control Plane (HCP) KubeVirt クラスターを **--node-selector** コマンドでデプロイするときに、ノードセレクターが HCP namespace 内の **kubevirt-cloud-controller-manager** Pod に適用されませんでした。その結果、HCP Pod 全体を特定のノードに固定できなくなりました。今回の更新により、この問題は修正されました。(OCPBUGS-27071)

- 以前は、Microsoft Azure ロードバランサーのデフォルトの仮想マシン (VM) タイプが **Standard** から **VMSS** に変更されました。その結果、サービスタイプのロードバランサーは標準仮想マシンをロードバランサーに接続できませんでした。この更新では、OpenShift Container Platform デプロイメントとの互換性を維持するために、これらの変更を以前の設定に戻します。その結果、ロードバランサーのアタッチメントの一貫性が向上しました。(OCPBUGS-26210)

- 以前は、**enable_port_security** フィールドが **false** に設定された追加ポートを持つ RHOSP ノード上のデプロイメントでは、**LoadBalancer** サービスを作成できませんでした。今回の更新で、この問題は解決されました。(OCPBUGS-22246)

- 以前は、ワーカーノードの初回起動時に Nova メタデータサービスが利用できなかった場合、Red Hat OpenStack Platform (RHOSP) 上のワーカーノードの名前には、ドメインコンポーネントが付けられていました。OpenShift Container Platform は、ノード名が Nova インスタンスと同じであることを想定します。名前の不一致により、ノードの証明書要求が拒否され、ノードはクラスターに参加できませんでした。この更新により、ワーカーノードは最初の起動時にメタデータサービスを待機して無期限に再試行し、ノードの名前が正しいことを確認します。(OCPBUGS-22200)

- 以前は、クラスターオートスケーラーは、Container Storage Interface (CSI) ストレージを持つノードで使用するとクラッシュしました。この問題は本リリースで解決されています。(OCPBUGS-23096)

- 以前は、特定のプロキシー環境では、Amazon Web Services (AWS) メタデータサービスが初回起動時に存在せず、起動直後にしか利用できない場合がありました。kubelet のホスト名の取得ではこの遅延が考慮されておらず、その結果、有効なホスト名がないためノードは起動に失敗します。この更新により、ホスト名取得スクリプトは失敗した場合にしばらく再試行されるようになります。その結果、メタデータサービスへのアクセス不能は短期間は許容されます。(OCPBUGS-20369)

- OpenShift Container Platform バージョン 4.14 以降では、Microsoft Azure Stack Hub のインストールが失敗する原因となる既知の問題があります。4.14 以降にアップグレードされた Microsoft Azure Stack Hub クラスターでは、ノードがスケールアップまたはスケールダウンするときにロードバランサーの設定の問題が発生する可能性があります。この問題が解決されるまで、Microsoft Azure Stack Hub 環境での 4.14 のインストールまたは 4.14 へのアップグレードは推奨されません。(OCPBUGS-20213)

- 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-18954)

- 以前は、コントロールノードが 2 番目の内部インスタンスグループに追加されたときに、Google Cloud Platform XPN 内部クラスターのインストールを実行しようとすると失敗していました。このバグは修正されています。(OCPBUGS-5755)

- 以前は、終了ハンドラーは、ノードに終了のマークを付ける前に途中で終了していました。この状況は、コントローラーが終了信号を受信したタイミングに基づいて発生しました。このリ

リースでは、追加の終了チェックを導入することで、早期終了の可能性が考慮されています。(OCPBUGS-2117)

Cloud Credential Operator

- 以前は、Cloud Credential Operator ユーティリティー (**ccoctl**) がクラスターレベルでカスタム GCP ロールを作成していたため、各クラスターが許可されるカスタムロール数の割り当て制限に影響していました。GCP 削除ポリシーにより、削除されたカスタムロールが削除後何日間も割り当て制限に影響を与え続けていました。このリリースでは、作成されるカスタムロールの総数を減らすために、カスタムロールがクラスターレベルではなくプロジェクトレベルで追加されます。さらに、**ccoctl** ユーティリティーがインストール中に作成する GCP リソースを削除するときに、カスタムロールをクリーンアップするオプションが利用できるようになりました。これらの変更により、許可されるカスタムロールの数がクォータ制限に達することを回避できます。(OCPBUGS-28850)

- 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して、**cco_credentials_mode** メトリクスを正確にレポートするようになりました。(OCPBUGS-26510)

- 以前は、Microsoft Azure バケットのデフォルト動作の変更により、**ccoctl azure create** コマンドを実行して作成されたバケットは、パブリック Blob アクセスを許可できませんでした。このリリースでは、**ccoctl azure create** コマンドを実行して作成されたバケットは、パブリック Blob アクセスを許可するように明示的に設定されています。(OCPBUGS-22369)

- 以前は、Azure Managed Identity ロールが Cloud Controller Manager サービスアカウントから省略されていました。その結果、Cloud Controller Manager は、プライベート公開方法を使用して既存の VNet にデプロイされた環境で、サービスタイプのロードバランサーを管理できませんでした。このリリースでは、欠落していたロールが Cloud Credential Operator ユーティリティー (**ccoctl**) に追加され、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-21745)

- 以前は、Cloud Credential Operator は、**kube-system** namespace に保存されているルートシークレット **vshpere-creds** 内の vCenter サーバー値の更新をサポートしていませんでした。その結果、この値を更新しようとすると、コンポーネントのシークレットが正しく同期されなかったため、古い値と新しい値の両方が存在することになりました。このリリースでは、Cloud Credential Operator が同期中にシークレットデータをリセットするため、vCenter サーバー値の更新がサポートされます。(OCPBUGS-20478)

- 以前は、中国リージョンの DNS 接尾辞 **.amazonaws.com.cn** が、他のリージョンで使用されている接尾辞 **.amazonaws.com** と異なるため、Cloud Credential Operator ユーティリティー (**ccoctl**) は中国リージョンで AWS Security Token Service (STS) リソースを作成できませんでした。このリリースでは、**ccoctl** は正しい DNS 接尾辞を検出し、それを使用して必要なリソースを作成できるようになりました。(OCPBUGS-13597)

Cluster Version Operator

- Cluster Version Operator (CVO) は、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ます。以前は、リスク評価に失敗すると、CVO が新しい更新推奨事項を取得できなくなりました。更新推奨サービスが適切に定義されていない更新リスクを処理したためにリスク評価が失敗した場合、この問題により、CVO が更新推奨サービスが改善されたリスク宣言を提供していることに気付かない可能性がありました。このリリースでは、CVO は、更新リスクが正常に評価されるかどうかに関係なく、更新推奨サービスのポーリングを継続します。(OCPBUGS-25949)

開発者コンソール

- 以前は、指定されたリソースの API バージョンが最近更新されたため、**BuildRun** ログは BuildRun の **Logs** タブに表示されませんでした。この更新により、**TaskRun** の Logs が、ビルド Operator の v1alpha1 バージョンと v1beta1 バージョンの両方の BuildRun の **Logs** タブに再度追加されました。(OCPBUGS-29283)

- 以前は、**ArtifactHub** から以前にインストールされた Pipeline Builder の **Task** が選択されると、コンソール UI が失敗し、エラーページが表示されました。この更新により、コンソール UI はオプションのデータを期待しなくなり、コンソール UI が失敗することもなくなりました。(OCPBUGS-24001)

- 以前は、Shipwright プラグインの **Actions** メニューの **Edit Build** と **BuildRun** オプションでは、YAML タブで編集できませんでした。今回の更新により、YAML タブで編集できるようになりました。(OCPBUGS-23164)

- 以前は、コンソールはリポジトリー内のファイル名 **Dockerfile** のみを検索して、Import Flows の **Container** ストラテジーに適したリポジトリーを特定していました。他のコンテナー化ツールが利用できるため、**Containerfile** ファイル名のサポートが **Container** ストラテジーに適したものになりました。(OCPBUGS-22976)

- 以前は、権限のないユーザーがパスとクエリーパラメーターを含むコンソールへのリンクを開き、ログインページにリダイレクトされた場合、ログインの成功後にクエリーパラメーターは復元されませんでした。その結果、ユーザーは検索を復元するか、コンソールへのリンクを再度クリックする必要がありました。今回の更新により、最新バージョンではパスと同様のクエリーパラメーターが保存および復元されます。(OCPBUGS-22199)

- 以前は、**Add** または **Topology** ビューから **Create Channel** ページに移動すると、デフォルト名として **Channel** が表示されましたが、**Create** ボタンは無効になり、名前フィールドの下に **Required** と表示されました。今回の更新により、デフォルトのチャンネル名が追加された場合、**Create** ボタンをクリックしたときに **Required** メッセージが表示されなくなります。(OCPBUGS-19783)

- 以前は、クイック検索機能を使用するときに同様のオプションを選択できました。この更新により、**Source-to-image** オプションは、**Topology** クイック検索の **Samples** オプションと区別されます。(OCPBUGS-18371)

- 以前は、{serverless-product-name} Operator がインストールされていて、Knative (Kn) サービングインスタンスが作成されていない場合、**Administration** → **Cluster Settings** から **Global configuration** ページに移動し、**Knative-serving** をクリックすると、**404 page not found** エラーが表示されていました。この更新により、**Knative-serving** を **Global configuration** に追加する前に、Knative サービングインスタンスが作成されたか判断するためのチェックが行われるようになりました。(OCPBUGS-18267)

- 以前は、**Edit Knative Service** フォームに問題があり、ユーザーは以前に作成した Knative サービスを編集できませんでした。この更新により、以前に作成された Knative サービスを編集できるようになりました。(OCPBUGS-6513)

etcd Cluster Operator

- 以前は、**cluster-backup.sh** スクリプトは **etcdctl** バイナリーをローカルマシンに無期限にキャッシュし、更新を不可能にしていました。この更新により、**cluster-backup.sh** スクリプトは実行されるたびに最新の **etcdctl** バイナリーをプルします。(OCPBUGS-19052)

Hosted Control Plane

- 以前は、ホストされたクラスターでカスタムの Container Network Interface (CNI) プラグイン

を使用する場合、ロールベースのアクセス制御 (RBAC) ルールは、**hostedcluster.spec.networking.networkType** フィールドを **Calico** に設定した場合にのみ、設定されていました。**hostedcluster.spec.networking.networkType** フィールドを **Other** に設定した場合、ロールベースのアクセス制御 (RBAC) ルールが設定されませんでした。このリリースでは、**hostedcluster.spec.networking.networkType** フィールドを **Other** に設定すると、RBAC ルールが適切に設定されます。(OCPBUGS-28235)

- 以前は、**kube-apiserver** リソースの **ipFamilyPolicy** フィールドが **SingleStack** に設定されていたため、ノードポートが適切に公開されませんでした。この更新により、**ipFamilyPolicy** が **PreferredDualStack** に設定されている場合、ノードポートは適切に公開されます。(OCPBUGS-23350)

- 以前は、ホストされたクラスターの Open Virtual Network (OVN) を設定した後、**cloud-network-config-controller**、**multus-admission-controller**、および `ovnkube-control-plane` リソースに **hypershift.openshift.io/hosted-control-plane:{hostedcluster resource namespace}-{cluster-name}** ラベルがありませんでした。この更新により、ホストされたクラスターの Open Virtual Network (OVN) を設定した後、**cloud-network-config-controller**、**multus-admission-controller**、および `ovnkube-control-plane` リソースに **hypershift.openshift.io/hosted-control-plane:{hostedcluster resource namespace}-{cluster-name}** ラベルが含まれるようになりました。(OCPBUGS-19370)

- 以前は、ホストされたクラスターを作成した後、config map を作成するために **user-ca-bundle** 以外の名前を使用すると、Control Plane Operator (CPO) のデプロイメントが失敗していました。この更新により、一意の名前を使用して config map を作成できるようになりました。CPO は正常にデプロイされるようになりました。(OCPBUGS-19419)

- 以前は、**.status.controlPlaneEndpoint.port: 443** を持つホストされたクラスターは、誤ってパブリックルーターとプライベートルーターにポート 6443 を公開していました。この更新により、**.status.controlPlaneEndpoint.port: 443** を持つホストされたクラスターは、ポート 443 のみを公開します。(OCPBUGS-20161)

- 以前は、Kube API サーバーが IPv4 および IPv6 を使用して公開され、IP アドレスが **HostedCluster** リソースに設定されている場合は、IPv6 環境は正しく動作しませんでした。この更新により、Kube API サーバーが IPv4 および IPv6 を使用して公開される場合、IPv6 環境が適切に動作するようになりました。(OCPBUGS-20246)

- 以前は、コンソール Operator と Ingress Pod が同じノード上にある場合、コンソール Operator は失敗し、コンソールクラスター Operator を使用不可としてマークしていました。このリリースでは、コンソール Operator と Ingress Pod が同じノード上に配置されている場合、コンソール Operator が失敗しなくなりました。(OCPBUGS-23300)

- 以前は、ホストされたクラスターのアンインストールがスタックした場合、Control Plane Operator (CPO) のステータスが誤って報告されていました。この更新により、CPO のステータスが正しく報告されるようになりました。(OCPBUGS-26412)

- 以前は、初期アップグレードの進行中に OpenShift Container Platform のバージョンをオーバーライドしようとすると、ホストされたクラスターのアップグレードが失敗していました。この更新により、現在のアップグレードを新しい OpenShift Container Platform バージョンでオーバーライドすると、アップグレードが正常に完了します。(OCPBUGS-18122)

- 以前は、Hosted Control Plane のプルシークレットを更新しても、ワーカーノードにすぐには反映されませんでした。この更新により、プルシークレットを変更すると、調整がトリガーされ、ワーカーノードが新しいプルシークレットですぐに更新されます。(OCPBUGS-19834)

- 以前は、Hypershift Operator は、存在しなくなったノードプールの時系列を報告していました。このリリースでは、Hypershift Operator はノードプールの時系列を正しく報告します。(OCPBUGS-20179)

- 以前は、**--enable-uwm-telemetry-remote-write** フラグがデフォルトで有効でした。この設定により、テレメトリー調整がブロックされました。この更新により、**--enable-uwm-telemetry-remote-write** フラグを無効にして、テレメトリー調整を可能にすることができます。(OCPBUGS-26410)

- 以前は、追加の許可プリンシパルとして IAM ロールパス ARN が指定された場合 (**arn:aws:iam::${ACCOUNT_ID}:role/${PATH}/name**)、Control Plane Operator (CPO) は VPC エンドポイントサービスの更新に失敗しました。この更新により、CPO は **arn:aws:iam::${ACCOUNT_ID}:role/${PATH}/name** が許可されたプリンシパルを使用して VPC エンドポイントサービスを正常に更新します。(OCPBUGS-23511)

- 以前は、OAuth テンプレートをカスタマイズするために **HostedCluster.spec.configuration.oauth** フィールドを設定した場合、この設定はホストされたクラスターに反映されませんでした。この更新により、ホストされたクラスターの **HostedCluster.spec.configuration.oauth** フィールドを正常に設定できるようになります。(OCPBUGS-15215)

- 以前は、デュアルスタックネットワークを使用してホストされたクラスターをデプロイする場合、デフォルトで、**clusterIP** フィールドが IPv4 ネットワークではなく IPv6 ネットワークに設定されていました。この更新により、デュアルスタックネットワークを使用してホストされたクラスターをデプロイする場合、**clusterIP** フィールドはデフォルトで IPv4 ネットワークに設定されます。(OCPBUGS-16189)

- 以前は、ホストされたクラスターをデプロイするときに、**HostedCluster** リソースの **advertiseAddress** フィールドを設定すると、ホストされたクラスター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、**HostedCluster** リソースの **advertiseAddress** フィールドを設定した後、ホストされたクラスターを正常にデプロイできます。(OCPBUGS-19746)

- 以前は、ホストされたクラスターで **hostedcluster.spec.networking.networkType** フィールドを **Calico** に設定すると、Cluster Network Operator には、 **network-node-identity** リソースをデプロイするための十分なロールベースのアクセス制御 (RBAC) 権限がありませんでした。この更新により、**network-node-identity** リソースが正常にデプロイされます。(OCPBUGS-23083)

- 以前は、ホストされたクラスターの監査ログのデフォルト設定を更新できませんでした。したがって、ホストされたクラスターのコンポーネントは監査ログを生成できませんでした。この更新により、デフォルト設定を更新することで、ホストされたクラスターのコンポーネントの監査ログを生成できるようになります。(OCPBUGS-13348)

Image Registry

- 以前は、Image Registry プルーナーは、OpenShift API サーバーによって管理されるクラスターロールに依存していました。これにより、アップグレード中にプルーナージョブが断続的に失敗する可能性があります。現在、Image Registry Operator はプルーナークラスターロールを作成するロールを担っており、これにより問題が解決されます。(OCPBUGS-18969)

- Image Registry Operator は、アクセスキーの取得の一環として、ストレージアカウントリストエンドポイントへの API 呼び出しを行います。複数の OpenShift Container Platform クラスターを含むプロジェクトでは、これにより API 制限に達する可能性があります。その結果、新しいクラスターを作成しようとすると **429** エラーが返されました。この更新により、呼び出し間の時間が 5 分から 20 分に延長され、API 制限に達しなくなります。(OCPBUGS-18469)

- 以前は、QPS とバーストのデフォルト設定が低いため、API サーバー要求が適切な時間内に返されなかった場合、Image Registry がゲートウェイタイムアウトエラーを返していました。この問題を解決するために、ユーザーは Image Registry を再起動する必要がありました。この更新により、QPS とバーストがデフォルトで高く設定され、この問題は発生しなくなります。(OCPBUGS-18999)

- 以前は、Cluster Image Registry Operator のデプロイメントリソースを作成するとき、エラー処理では最初に値が **nil** か確認せずにポインター変数が使用されていました。その結果、ポインター値が **nil** の場合、パニックがログに報告されました。この更新により、nil チェックが追加され、パニックがログに報告されなくなりました。(OCPBUGS-18103)

- 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。

注記

この修正は、Azure Stack Hub (ASH) では **機能しません**。4.14.14 以降にアップグレードする際に OCP バージョン 4.14.0 - 4.14.13 を使用していた ASH ユーザーは、手動手順を実行して Blob を正しいストレージパスに移動する必要があります。

(OCPBUGS-29525)

インストーラー

- 以前は、AWS へのクラスターのインストールが検証エラーにより失敗する場合がありました。この更新により、インストールプログラムは、マシン config Operator を満足させるために必要なクラウド設定オブジェクトを生成します。これにより、インストールは成功します。(OCPBUGS-12707)

- 以前は、認証のために仮想マシンにアタッチされたサービスアカウントを使用して GCP にクラスターをインストールすると、内部データ検証のバグが原因で失敗することがありました。このリリースでは、仮想マシンにアタッチされたサービスアカウントを使用する際に、認証パラメーターを正しく検証するようにインストールプログラムが更新されました。(OCPBUGS-19376)

- 以前は、vSphere 接続設定インターフェイスの "vCenter cluster" フィールドに、クラスター名の代わりにネットワーク名が表示されていました。この更新により、"vCenter cluster" フィールドが更新され、クラスター名が表示されるようになりました。(OCPBUGS-23347)

- 以前は、**credentialsMode** パラメーターが **Manual** に設定されていない状態で認証し、**gcloud cli** ツールを使用すると、インストールプログラムは **osServiceAccount.json** ファイルから Google Cloud Platform (GCP) 認証情報を取得していました。この操作は、GCP クラスターのインストールが失敗する原因となっていました。現在は、検証チェックによって **install-config.yaml** ファイルがスキャンされ、**credentialsMode** を **Manual** に設定しなかった場合はメッセージが表示されます。**Manual** モードでは、マニフェストを編集して認証情報を指定する必要があることに注意してください。(OCPBUGS-17757)

- 以前は、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を使用して OpenShift Container Platform を VMware vSphere にインストールしようとすると、リソースプールオブジェクトに二重バックスラッシュが含まれていました。この形式により、インストールプログラムはネットワークリソースへの誤ったパスを生成し、インストール操作が失敗する原因となりました。インストールプログラムがこのリソースプールオブジェクトを処理した後、プログラムは "network not found" というエラーメッセージを出力しました。インストー

ルプログラムは現在、InventoryPath とネットワーク名を結合する目的でクラスターオブジェクトを取得し、プログラムがリソースプールオブジェクトへの正しいパスを指定できるようにします。(OCPBUGS-23376)

- 以前は、Azure Red Hat OpenShift クラスターをインストールした後、一部のクラスター Operator が使用できなくなりました。これは、クラスターのロードバランサーの 1 つがインストールプロセスの一部として作成されなかったことが原因でした。この更新により、ロードバランサーが正しく作成されるようになりました。クラスターをインストールすると、すべてのクラスター Operator が使用可能になります。(OCPBUGS-24191)

- 以前は、VMware vSphere クラスターにオフラインの ESXi ホストが含まれている場合、"panic: runtime error: invalid memory address or nil pointer dereference" というメッセージが表示されてインストールが失敗していました。この更新により、ESXi ホストが利用できないというエラーメッセージが表示されます。(OCPBUGS-20350)

- 以前は、AWS にクラスターをインストールするときにデフォルトのマシン設定のみを使用して既存の AWS セキュリティーグループを指定した場合 (**platform.aws.defaultMachinePlatform.additonalSecurityGroupsIDs**)、セキュリティーグループはコントロールプレーンマシンに適用されませんでした。この更新により、既存の AWS セキュリティーグループがデフォルトのマシン設定を使用して指定される場合、コントロールプレーンに正しく適用されるようになりました。(OCPBUGS-20525)

- 以前は、指定されたマシンインスタンスタイプ (**platform.aws.type**) が、コントロールプレーンまたはコンピュートマシン (**controlPlane.architecture** および **compute.architecture**) に指定されたマシンアーキテクチャーをサポートしていない場合、AWS へのクラスターのインストールは失敗していました。今回の更新により、インストールプログラムは、マシンインスタンスタイプが指定されたアーキテクチャーをサポートしているか確認し、サポートしていない場合はエラーメッセージを表示するようになりました。(OCPBUGS-26051)

- 以前は、インストールプログラムはクラスターをインストールする前に一部の設定を検証しませんでした。この現象は、これらの設定がデフォルトのマシン設定 (**platform.azure.defaultMachinePlatform**) でのみ指定されている場合に発生しました。その結果、次の条件が満たされた場合でもインストールは成功します。

  - サポート対象外のマシンインスタンスタイプが指定された場合

  - 高速ネットワークや Azure Ultra ディスクの使用などの追加機能が、指定されたマシンインスタンスタイプでサポートされていない場合

  この修正により、インストールプログラムは、サポート対象外の設定を示すエラーメッセージを表示するようになりました。(OCPBUGS-20364)

- 以前は、AWS クラスターを Secret Commercial Cloud Services (SC2S) リージョンにインストールし、既存の AWS セキュリティーグループを指定すると、そのリージョンではこの機能を利用できないことを示すエラーが表示され、インストールが失敗していました。この修正により、インストールは成功します。(OCPBUGS-18830)

- 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-13664)

- 以前は、Oracle® Cloud Infrastructure (OCI) でのエージェントベースのインストールでは、インストールの進行状況をユーザーに表示するコンソールが表示されず、インストールの進行状況を追跡することがより困難でした。この更新により、OCI でのエージェントベースのインス

トールでは、インストールの進行状況がコンソールに表示されるようになりました。(OCPBUGS-19092)

- 以前は、静的ネットワークがエージェントベースのインストーラーの **install-config.yaml** または **agent-config.yaml** ファイルで定義されており、インターフェイス名の長さが 15 文字を超えている場合、ネットワークマネージャーはインターフェイスの起動を許可しませんでした。この更新により、15 文字を超えるインターフェイス名が切り捨てられ、インストールを続行できるようになりました。(OCPBUGS-18552)

- 以前は、ユーザーが **agent-config.yaml** ファイルで **rendezevousIP** フィールドを指定せず、ホストが静的ネットワーク設定と同じファイルで定義されていた場合、最初のホストはそのロールに関係なく、ランデブーノードとして指定されていました。これにより、インストールが失敗していました。この更新により、エージェントベースのインストーラーは、**master** ロールと静的 IP が定義されているホストを最初に検索することにより、ランデブーノードの検索に優先順位を付けます。何も見つからない場合は、ロールが定義されていないホストを通じて潜在的な候補が検索されます。**worker** ロールが明示的に設定されている静的なネットワーク設定を持つホストは無視されます。(OCPBUGS-5471)

- 以前は、すべてのエージェントベースのインストールの起動プロセス中にエージェントコンソールアプリケーションが表示され、インストールを続行する前にネットワークのカスタマイズが可能でした。クラウドのインストール中にネットワーク設定が必要なことはほとんどないため、これにより、Oracle® Cloud Infrastructure (OCI) でのインストールが不必要に遅くなっていました。
  今回の更新により、OCI でのエージェントベースのインストールではエージェントコンソールアプリケーションが表示されなくなり、より迅速にインストールできるようになりました。(OCPBUGS-19093)

- 以前は、プラットフォームが **external** と定義されていた場合、エージェントベースのインストーラーはデフォルトで外部 Cloud Controller Manager (CCM) を有効にしていました。これにより、ユーザーは、外部 CCM を必要としないクラウドプラットフォーム上でインストールを実行するときに、外部 CCM を無効化できませんでした。この更新により、ユーザーは、Oracle® Cloud Infrastructure (OCI) でエージェントベースのインストールを実行する場合にのみ、外部 CCM を有効にする必要があります。(OCPBUGS-18455)

- 以前は、**agent wait-for** コマンドは **.openshift_install.log** ファイルにログを記録できませんでした。この更新により、**agent wait-for** コマンドを使用すると、ログが **.openshift_install.log** ファイルに記録されます。(OCPBUGS-5728)

- 以前は、ブートストラップノードの再起動後にブートストラップマシン上の **assisted-service** が利用できなくなり、**assisted-installer-controller** からの通信が妨げられていました。これにより、**assisted-installer-controller** がワーカーノードから初期化されていないテイントを削除できなくなり、クラスターインストールがクラスター Operator の待機中にハングする原因となりました。
  この更新により、**assisted-service** が利用できなくなった場合でも、**assisted-installer-controller** は初期化されていないテインとを削除でき、インストールを続行できるようになります。(OCPBUGS-20049)

- 以前は、エージェントベースのインストーラーで使用される **AgentClusterInstall** クラスターマニフェストでは、プラットフォームタイプを誤って小文字にする必要がありました。この更新により、大文字と小文字が混在した値が必要になりますが、元の小文字の値が受け入れられ、正しく変換されるようになりました。(OCPBUGS-19444)

- 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-9331)

- 以前は、Assisted Installer によってすべての vSphere ノードの初期化されていないテイントが削除され、これにより、vSphere CCM はノードを適切に初期化できませんでした。これにより、ノードのプロバイダー ID が欠落し、最初のクラスターのインストール中に vSphere CSI Operator の機能が低下しました。このリリースでは、Assisted Installer は、vSphere 認証情報が **install-config.yaml** に提供されていたか確認します。認証情報が指定され、OpenShift バージョンが 4.15 以上で、エージェントインストーラーが使用された場合、Assisted-Installer および Assisted-Installer-Controller は初期化されていないテインとを削除しません。これは、ノードのプロバイダー ID と仮想マシンの UUID が適切に設定され、vSphere CSI Operator がインストールされていることを意味します。(OCPBUGS-29485)

Kubernetes コントローラーマネージャー

- 以前は、**maxSurge** フィールドがデーモンセットに設定され、容認値が更新されると、Pod のスケールダウンに失敗し、スケジューリングに別のノードセットが使用されるためにロールアウトが失敗していました。このリリースでは、スケジュールの制約が満たされない場合にノードが適切に除外され、ロールアウトは正常に完了できます。(OCPBUGS-19452)

Machine Config Operator

- 以前は、環境変数のスペルが間違っていると、スクリプトは **node.env** ファイルの存在を検出できませんでした。これにより、**node.env** ファイルの内容がブートのたびに上書きされ、kubelet ホスト名を変更できなくなりました。この更新により、環境変数のスペルが修正され、**node.env** ファイルへの編集内容が再起動後も保持されます。(OCPBUGS-27307)

- 以前は、Machine Config Operator により、新しいマシン config をトリガーすることなく、ユーザー指定の認証局の更新を行うことができました。これらの更新の新しい書き込みメソッドには改行文字が欠けていたため、ディスク上の CA ファイルの内容に対して検証エラーが発生し、Machine Config Daemon の機能が低下しました。このリリースでは、CA ファイルの内容が修正され、更新が想定どおりに行われます。(OCPBUGS-25424)

- 以前は、Machine Config Operator では、中断を防ぐために、マシン config を必要とせずに、ユーザー指定の認証局バンドルの変更をクラスターに適用できました。このため、**user-ca** バンドルはクラスター上で実行されているアプリケーションに伝播されず、変更の適用を確認するには再起動が必要でした。この更新により、MCO は **update-ca-trust** コマンドを実行し、CRI-O サービスを再起動して、新しい CA が適切に適用されるようになりました。(OCPBUGS-24035)

- 以前は、Machine Config Operator が Image Registry 証明書を処理するために使用する初期メカニズムは、既存の config map にパッチを適用するのではなく、削除して新しい config map を作成していました。これにより、MCO からの API 使用量が大幅に増加しました。今回の更新では、代わりに JSON パッチを使用するようにメカニズムが更新され、問題が解決されました。(OCPBUGS-18800)

- 以前は、Machine Config Operator は、**baremetalRuntimeCfgImage** コンテナーイメージを複数回プルしていました。1 回目はノードの詳細を取得するため、2 回目以降はイメージが利用可能であることを確認するためでした。これにより、ミラーサーバーまたは Quay が利用できない状況で証明書のローテーション中に問題が発生し、その後のイメージのプルが失敗していました。ただし、最初のイメージのプルによりイメージがすでにノード上にある場合は、それに関係なくノードは kubelet を開始する必要があります。この更新により、**baremetalRuntimeCfgImage** イメージが 1 回だけプルされるようになり、問題が解決されました。(OCPBUGS-18772)

- 以前は、一部のネットワーク環境での OpenShift Container Platform の更新中に、**nmstatectl** コマンドは正しい永続 MAC アドレスを取得できませんでした。これにより、インターフェイスの名前が変更され、更新中にノード上のボンディング接続が切断されました。このリリースでは、名前の変更を防ぐために **nmstate** パッケージと MCO にパッチが適用され、更新は期待どおりに行われます。(OCPBUGS-17877)

- 以前は、Machine Config Operator が Image Registry 証明書のデフォルトのプロバイダーとなり、**node-ca** デーモンは削除されました。これにより、HyperShift Operator で問題が発生しました。**node-ca** デーモンを削除すると、HyperShift が Ignition 設定を取得してブートストラッププロセスを開始するために使用する Machine Config Server (MCS) 内のイメージレジストリーパスも削除されたためです。この更新により、MCS イメージレジストリーデータを含むフラグが提供され、Ignition がブートストラッププロセス中に使用できるようになり、問題が解決されました。(OCPBUGS-17811)

- 以前の古い RHCOS ブートイメージには、ブート時にサービス間の競合状態が含まれており、これによりノードはイメージをプルする前に **rhcos-growpart** コマンドを実行できず、ノードの起動が阻止されていました。これにより、ディスクに空き領域が残っていないと判断され、古いブートイメージを使用するクラスターでノードのスケーリングが失敗することがありました。この更新では、ノードが正しく起動できるようにサービスの順序をより厳密にするためのプロセスが Machine Config Operator に追加されました。

  注記

  このような状況では、新しいブートイメージに更新すると、同様の問題の発生を防ぐことができます。

  (OCPBUGS-15087)

- 以前は、Machine Config Operator (MCO) は **oc image extract** コマンドを利用して更新中にイメージをプルしていましたが、**ImageContentSourcePolicy** (ICSP) オブジェクトはそれらのイメージのプル時に尊重されませんでした。今回の更新により、MCO は内部で **podman pull** コマンドを使用するようになり、ICSP で設定された場所からイメージがプルされるようになりました。(OCPBUGS-13044)

管理コンソール

- 以前は、**Expand PVC** モーダルは、既存の PVC にユニットを含む **spec.resources.requests.storage** 値があると想定していました。その結果、**Expand PVC** モーダルを使用して、ユニットなしで **request.storage** 値を持つ PVC を拡張すると、コンソールはモーダルに誤った値を表示していました。この更新により、ユニットの有無にかかわらず、ストレージ値を処理できるようにコンソールが更新されました。(OCPBUGS-27909)

- 以前は、ファイルがバイナリーか判断するコンソールチェックは十分に堅牢ではありませんでした。その結果、XML ファイルがバイナリーとして誤って認識され、コンソールに表示されませんでした。今回の更新により、ファイルがバイナリーかをより正確に確認するためのチェックが追加されました。(OCPBUGS-26591)

- 以前は、**spec.unhealthyConditions** のない **MachineHealthCheck** がクラスター上に存在する場合、**Node Overview** ページのレンダリングに失敗していました。この更新により、**Node Overview** ページが更新され、**spec.unhealthyConditions** なしで **MachineHealthCheck** ができるようになりました。今後は、**spec.unhealthyConditions** のない **MachineHealthCheck** がクラスター上に存在する場合でも、**Node Overview** ページがレンダリングされるようになりました。(OCPBUGS-25140)

- 以前は、コンソールはアラート通知レシーバーの最新のマッチャーキーを使用した最新状態ではなく、コンソールによって作成されたアラートマネージャーレシーバーは、古い一致キーを使用していました。この更新により、コンソールは代わりにマッチャーを使用し、既存のアラートマネージャーレシーバーを変更するときに既存の一致インスタンスをマッチャーに変換します。(OCPBUGS-23248)

- 以前は、偽装アクセスが誤って適用されていました。この更新により、コンソールは偽装アクセスを正しく適用します。(OCPBUGS-23125)

- 以前は、Advanced Cluster Management for Kubernetes (ACM) および Multicluster Engine for Kubernetes (MCE) Operators がインストールされ、それらのプラグインが有効になっている場合、YAML コード の Monaco Editorの読み込みに失敗していました。この更新では、リソース呼び出しの失敗を防ぐためにオプションのリソースチェーンが追加され、ACM Operator および MCE Operator がインストールされ、それらのプラグインが有効化されている場合に、YAML エディターは読み込みに失敗することがなくなりました。(OCPBUGS-22778)

Monitoring

- 以前は、クラスターで IPv6 が無効になっている場合、monitoring-plugin コンポーネントは起動しませんでした。このリリースでは、クラスター内で次のインターネットプロトコル設定 (IPv4 のみ、IPv6 のみ、および IPv4 と IPv6 の両方を同時に) をサポートするようにコンポーネントが更新されます。この変更により問題は解決され、クラスターが IPv6 のみをサポートするように設定されている場合に、monitoring-plugin コンポーネントが起動するようになりました。(OCPBUGS-21610)

- 以前は、コアプラットフォームモニタリングおよびユーザー定義プロジェクト用の Alertmanager のインスタンスが、アップグレード中に誤ってピアリングされる可能性がありました。この問題は、複数の Alertmanager インスタンスが同じクラスターにデプロイされている場合に発生する可能性があります。このリリースでは、クラスターを対象としていないトラフィックをブロックするのに役立つ **--cluster.label** フラグを Alertmanager に追加することで問題が修正されています。(OCPBUGS-18707)

- 以前は、Alertmanager 設定でテキストのみのメールテンプレートを使用してテキストのみのメールアラートを送信することはできませんでした。この更新により、メール受信者の **html** フィールドを空の文字列に設定することで、テキストのみのメールアラートを送信するように Alertmanager を設定できるようになりました。(OCPBUGS-11713)

ネットワーク

- 以前は、空の仕様で IngressController を作成すると、IngressController のステータスが **Invalid** と表示されていました。ただし、**route_controller_metrics_routes_per_shard** メトリクスは引き続き作成されます。無効な IngressController が削除された場合、**route_controller_metrics_routes_per_shard** メトリクスはクリアされず、そのメトリクスの情報が表示されます。今回の更新により、許可された IngressController に対してのみメトリクスが作成されるようになり、この問題は解決されました。(OCPBUGS-3541)

- 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-6959)

- 以前は、クラスターのシャットダウンまたはハイバーネート中に、外部ネイバーの MAC アドレスが変更される可能性がありました。Gratuitous Address Resolution Protocol (GARP) はこの変更について他のネイバーに通知する必要がありますが、クラスターは GARP を処理しません。これは、GARP が実行されていなかったためです。クラスターが再起動されると、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そのネイバーに到達できない可能性がありました。この更新により、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す。(OCPBUGS-11710)

- 以前は、IngressController が 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は、Ingress Operator は IngressController が削除対象としてマークされているかを確認せずに、ファイナライザーを追加しようとしていました。その結果、IngressController が 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

ザーを正常に削除しました。その後、ファイナライザーを追加し直すために IngressController を更新しようとして失敗を繰り返し、Operator のログにエラーメッセージが記録されていました。
この更新により、Ingress Operator は、削除対象としてマークされた IngressController に **clientca-configmap** ファイナライザーを追加しなくなります。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す。(OCPBUGS-14994)

- 以前は、スケジュールされた Pod の処理と、OVN-Kubernetes の開始時にノード上で完了した Pod の処理の間で、競合状態が発生していました。この状況は、ノードの再起動時によく発生していました。その結果、同じ IP が複数の Pod に誤って割り当てられました。この更新により競合状態が修正され、そのような状況で同じ IP が複数の Pod に割り当てられなくなりました。(OCPBUGS-16634)

- 以前は、ホスト要求の重複によりルートが拒否されるエラーがありました。これが発生すると、システムは最初に遭遇したルートを誤って選択しますが、それが常に競合するルートであるとは限りませんでした。この更新により、競合するホストのすべてのルートが最初に取得され、送信時間に基づいて並べ替えられます。これにより、システムは最新の競合ルートを正確に判断して選択することができます。(OCPBUGS-16707)

- 以前は、新しい **ipspec-host** Pod が開始されると、既存の **XFRM** 状態がクリアまたは削除されていました。その結果、既存の north-south トラフィックポリシーが削除されました。この問題は解決されています。(OCPBUGS-19817)

- 以前は、Kubevirt プロバイダーを使用する場合、**ovn-k8s-cni-overlay, topology:layer2** NetworkAttachmentDefinition がホストされた Pod で機能しませんでした。その結果、Pod は起動しませんでした。この問題は解決され、Pod は **ovn-k8s-cni-overlay** NetworkAttachmentDefinition で起動できるようになりました。(OCPBUGS-22869)

- 以前は、Azure アップストリーム DNS は、512 バイトを超えるペイロードを返したため、EDNS DNS 以外のクエリーに準拠していませんでした。CoreDNS 1.10.1 はアップストリームクエリーに EDNS を使用しなくなり、元のクライアントクエリーが EDNS を使用する場合にのみ EDNS を使用するため、この組み合わせにより、アップストリームが CoreDNS 1.10.1 を使用する EDNS 以外のクエリーに対して 512 バイトを超えるペイロードを返した場合、オーバーフロー **servfail** エラーが発生しました。その結果、OpenShift Container Platform 4.12 から 4.13 にアップグレードすると、以前は機能していた一部の DNS クエリーが失敗するようになりました。
このリリースでは、オーバーフロー **servfail** エラーを返す代わりに、CoreDNS が応答を切り詰め、クライアントが TCP で再試行できることを示すようになりました。その結果、準拠していないアップストリームを持つクラスターは、オーバーフローエラーが発生した場合に TCP を使用して再試行するようになりました。これにより、OpenShift Container Platform 4.12 と 4.13 の間での機能の中断が阻止されます。(OCPBUGS-27904)、(OCPBUGS-28205)

- 以前は、プライベート Microsoft Azure クラスターには、Egress IP アドレスとして指定されたセカンダリー IP アドレスにアウトバウンド接続がないという制限がありました。これは、これらの IP アドレスに関連付けられた Pod がインターネットにアクセスできないことを意味していました。ただし、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ました。これが、Egress IP アドレスの意図された使用例です。この更新により、Microsoft Azure クラスターの Egress IP アドレスが有効になり、アウトバウンドルールを通じてアウトバウンド接続を実現できるようになります。(OCPBUGS-5491)

- 以前は、複数の NICS を使用する場合、ラベル付けの有無かかわらず、Egress IP アドレスが正しい Egress ノードに正しく再割り当てらていませんでした。このバグは修正され、Egress IP アドレスが正しい Egress ノードに再割り当てされるようになりました。(OCPBUGS-18162)

- 以前は、Keepalived プロセスを実行する場所を決定するために導入された新しいロジックでは、Ingress VIP が考慮されていませんでした。その結果、Keepalived Pod が Ingress ノードで

実行されなかった可能性があり、クラスターが破損する可能性がありました。この修正により、ロジックに Ingress VIP が含まれるようになり、Keepalived Pod が常に利用可能になります。(OCPBUGS-18771)

- 以前の Hypershift クラスターでは、Pod が常に別のゾーンにスケジュールされているわけではありませんでした。この更新により、**multus-admission-controller** デプロイでは、Hypershift が適切なゾーンで動作するように **PodAntiAffinity** 仕様が使用されるようになりました。(OCPBUGS-15220)

- 以前は、Multus の実装には 10 分間存在した証明書が使用されていました。この更新により、ノードごとの証明書が Multus CNI プラグインに使用され、証明書の存続期間が 24 時間に延長されました。(OCPBUGS-19861)、(OCPBUGS-19859)

- 以前は、**spec.desiredState.ovn.bridge-mappings** API 設定により、各 Kubernetes ノードの Open vSwitch (OVS) ローカルテーブル内のすべての外部 ID が削除されました。その結果、OVN シャーシ設定が削除され、デフォルトのクラスターネットワークが切断されました。この修正により、OVS 設定に影響を与えることなく **ovn.bridge-mappings** 設定を使用できるようになります。(OCPBUGS-18869)

- 以前は、NMEA センテンスが E810 コントローラーに送信される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ませんでした。これらの条件がそろった場合、PTP Operator はエラーを報告しました。このリリースでは、NMEA 文字列が失われた場合に 'FREERUN' を報告する修正が実装されました。(OCPBUGS-20514)

- 以前は、Whereabouts CNI プラグインによって作成されたプールから IP が割り当てられた Pod は、ノードの強制再起動後も **ContainerCreating** 状態のままでした。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-18893)

- 以前は、Assisted Installer を使用すると、OVN-Kubernetes のブートストラップに長い時間がかかりました。この問題は、**ovnkube-control-plane** ノードが 3 つあったために発生しました。最初の 2 つは正常に起動しましたが、3 つ目はインストール時間が遅れました。この問題はタイムアウトが経過した後にのみ解決されます。その後、インストールが続行されます。この更新により、3 番目の **ovnkube-control-plane** ノードが削除されました。その結果、インストール時間が短縮されました。(OCPBUGS-29480)

ノード

- 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)

- 以前は、CRI-O は、**crun** が cgroups を作成する独自の方法を考慮して cgroup 階層を正しく設定していませんでした。その結果、PerformanceProfile を使用して CPU クォータを無効化できませんでした。この修正により、PerformanceProfile を使用して CPU クォータを無効にすることが期待どおりに機能します。(OCPBUGS-20492)

- 以前は、デフォルト設定 (**container_use_dri_devices, true**) のため、コンテナーは dri デバイスを使用できませんでした。この修正により、コンテナーは期待どおりに dri デバイスを使用できるようになります。(OCPBUGS-24042)

- 以前は、kubelet は **unconfined_service_t** SELinux タイプで実行されていました。その結果、Selinux の拒否により、すべてのプラグインがデプロイできませんでした。この修正により、kubelet は **kubelet_exec_t** SELinux タイプで実行されるようになりました。その結果、プラグインは期待どおりにデプロイされます。(OCPBUGS-20022)

- 以前は、**CRI-O** はアップグレード時にコンテナーイメージを自動的に削除していました。これにより、イメージの事前プルに問題が発生しました。このリリースでは、OpenShift Container Platform がマイナーアップグレードを実行するときに、コンテナーイメージは自動的に削除されず、代わりに、ディスク使用量に基づいてトリガーされる kubelet のイメージガベージコレクションの対象となります。(OCPBUGS-25228)

- 以前は、ansible Playbook を使用して既存のクラスターに RHCOS マシンを追加する場合、マシンには openvswitch バージョン 2.7 がインストールされていました。この更新により、ansible Playbook を使用して既存のクラスターに追加された RHCOS マシンには、openvswitch バージョン 3.1 がインストールされます。この openvswitch バージョンでは、ネットワークパフォーマンスが向上します。(OCPBUGS-18595)

Node Tuning Operator (NTO)

- 以前は、Tuned プロファイルは、PerformanceProfile の適用後に **Degraded** 状態を報告していました。生成された Tuned プロファイルは、**/etc/sysctl.d** ファイルを使用して同じ値がすでに設定されているときに、デフォルトの Receive Packet Steering (RPS) マスクの **sysctl** 値を設定しようとしていました。Tuned はそれについて警告し、Node Tuning Operator (NTO) は次のメッセージを表示してこれを機能低下として扱います。**The TuneD daemon issued one or more error message(s) when applying the profile profile.TuneD stderr: net.core.rps_default_mask**。今回の更新では、Tuned を使用してデフォルトの RPS マスクを設定しないことで重複が解決されました。**sysctl.d** ファイルは、起動時の早い段階で適用されるため、そのまま残されました。(OCPBUGS-25092)

- 以前は、Node Tuning Operator (NTO) は **UserAgent** を設定せず、デフォルトの UserAgent を使用していました。この更新により、NTO は **UserAgent** を適切に設定するようになり、クラスターのデバッグが容易になります。(OCPBUGS-19785)

- 以前は、クラスター内に多数の CSV が存在するときに Node Tuning Operator (NTO) Pod が再起動すると、NTO Pod は失敗し、**CrashBackLoop** 状態になりました。この更新により、CSV 要求のリストにページネーションが追加され、**CrashBackLoop** 状態を引き起こす **api-server** タイムアウトの問題が回避されました。(OCPBUGS-14241)

OpenShift CLI (oc)

- 以前は、チャネル別 (**mirror.operators.catalog.packages.channels** など) に Operator パッケージをフィルター処理するには、そのチャネルのパッケージを使用するつもりがない場合でも、パッケージのデフォルトチャネルを指定する必要がありました。この情報に基づいて、**imageSetConfig** にパッケージのデフォルトチャネルが含まれていない場合、結果として生成されるカタログは無効であると見なされます。
この更新では、**mirror.operators.catalog.packages** セクションに **defaultChannel** フィールドが導入されています。デフォルトのチャネルを選択できるようになりました。このアクションにより、**oc-mirror** は、**defaultChannel** フィールドで選択されたチャネルをパッケージのデフォルトとして定義する新しいカタログをビルドできるようになります。(OCPBUGS-385)

- 以前は、**oc-mirror** でのミラーリングに **eus-** チャネルを使用すると失敗していました。これは、偶数番号のリリースのみをミラーリングするという **eus-** チャネルの制限によるものでした。この更新により、**oc-mirror** はリリースのミラーリングに **eus-** チャネルを効果的に使用できるようになりました。(OCPBUGS-26065)

- 以前は、非表示フォルダーからローカル OCI Operator カタログをミラーリングするために **oc-mirror** を使用すると、エラー **error: ".hidden_folder/data/publish/latest/catalog-oci/manifest-list/kubebuilder/kube-rbac-proxy@sha256:<SHASUM>" is not a valid image reference: invalid reference format** が発生しました。この更新により、イメージ参照がローカル OCI カタログ内で調整され、ミラーリング中のエラーが阻止されます。(OCPBUGS-25077)

- 以前は、**must-gather** ツールの実行時に OpenShift Container Platform CLI (**oc**) バージョンが出力されませんでした。このリリースでは、**must-gather** の実行時に **oc** バージョンが概要セクションにリストされるようになりました。(OCPBUGS-24199)

- 以前は、ターミナルにアタッチせずに **oc debug** でコマンドを実行した場合 (**oc debug node/worker — sleep 5; exit 1** など)、コマンドの終了コードに関係なく、常に **0** 終了コードが返されました。このリリースでは、終了コードがコマンドから適切に返されるようになりました。(OCPBUGS-20342)

- 以前は、ミラーリング時に、認証トークンの期限切れが原因で **HTTP401** エラーが発生していました。これらのエラーは、カタログイントロスペクションフェーズまたはイメージミラーリングフェーズ中に発生しました。カタログイントロスペクションの場合、この問題は修正されました。さらに、Network Time Protocol (NTP) を修正すると、ミラーリングフェーズ中に発生した問題が解決されます。詳細は、イメージをミラーリングする際の "要求されたリソースへのアクセス" エラーに関する記事を参照してください。(OCPBUGS-7465)

Operator Lifecycle Manager (OLM)

- Operator をインストールした後、カタログが使用できなくなると、Operator のサブスクリプションは **ResolutionFailed** ステータス条件で更新されます。この更新前は、カタログが再び利用可能になったときに、**ResolutionFailed** ステータスがクリアされませんでした。今回の更新により、カタログが利用可能になった後、このステータスは想定どおりにサブスクリプションから消去されるようになりました。(OCPBUGS-29116)

- この更新により、OLM は、更新されたカスタムリソース定義 (CRD) をインストールするときに、既存のカスタムリソース (CR) が無効化されないことを確認するベストエフォート検証を実行します。(OCPBUGS-18948)

- この更新前は、Operator のインストールプランで、**clusterSeviceVersionNames** フィールドに重複した値が表示されていました。この更新により、重複した値が削除されます。(OCPBUGS-17408)

- この更新前は、以前の既存のクラスターロールと同じ名前で Operator グループを作成した場合、Operator Lifecycle Manager (OLM) によってクラスターロールが上書きされました。この修正により、OLM は次の構文を使用して、Operator グループごとに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>
  ```

  詳細は、Operator グループ を参照してください。(OCPBUGS-14698)

- 以前は、Operator のインストールまたはアップグレードに 10 分超の時間がかかると、次のエラーが発生して操作が失敗することがありました。

  ```
  Bundle unpacking failed. Reason: DeadlineExceeded, Message: Job was active longer than specified deadline
  ```

  この問題は、Operator Lifecycle Manager (OLM) に 600 秒のタイムアウトが設定されたバンドル解凍ジョブがあったために発生しました。バンドル解凍ジョブは、クラスター内のネットワークまたは設定の問題が原因で失敗する可能性があります。これらの問題は一時的なものであるか、ユーザーの介入によって解決される可能性があります。このバグ修正により、OLM は失敗した解凍ジョブの再作成をデフォルトで無期限に自動化します。

この更新により、Operator グループにオプションの **operatorframework.io/bundle-unpack-min-retry-interval** アノテーションが追加されました。このアノテーションは、失敗したジョブの再作成を試行する前に待機する最小間隔を設定します。(OCPBUGS-6771)

- Operator Lifecycle Manager (OLM) では、カタログ Operator が、Operator がインストールされていない namespace での **OperatorGroup** オブジェクトの欠落に関する多くのエラーをログに記録していました。この修正により、namespace に **Subscription** オブジェクトがない場合、OLM は **OperatorGroup** オブジェクトが namespace に存在するか確認しなくなります。(OCPBUGS-25330)

- Security Context Constraints (SCC) API を使用すると、ユーザーはクラスター上でワークロードをスケジュールするためのセキュリティーコンテキストを設定できます。コア OpenShift Container Platform コンポーネントの一部は、コントロールプレーンノード上でスケジュールされた Pod として実行されるため、これらのコアコンポーネントが **openshift-*** namespace で適切にスケジュールされることを妨げる SCC を作成する可能性があります。
このバグ修正により、**package-server-manager** コアコンポーネントの実行に使用される **openshift-operator-lifecycle-manager** サービスアカウントのロールベースのアクセス制御 (RBAC) スコープが縮小されます。この更新により、**package-server-manager** コンポーネントで予期しないスケジュールの問題を引き起こすクラスターに SCC が適用される可能性が大幅に低くなりました。

警告

SCC API は、OpenShift Container Platform クラスター上のスケジューリングにグローバルに影響を与える可能性があります。このような制約をクラスター上のワークロードに適用する場合は、SCC のドキュメントを注意深くお読みください。

(OCPBUGS-20347)

スケーラビリティーおよびパフォーマンス

- 以前は、**udev** イベントと物理デバイスに関連付けられた作成キューの間の競合状態により、一部のキューがゼロにリセットされる必要がある場合に、間違った Receive Packet Steering (RPS) マスクで設定されていました。これにより、物理デバイスのキューに RPS マスクが設定され、Receive Side Scaling (RSS) の代わりに RPS が使用されることになり、パフォーマンスに影響を与える可能性がありました。この修正により、イベントはデバイスの作成時ではなくキューの作成ごとにトリガーされるように変更されました。これにより、欠落するキューがないことが保証されます。すべての物理デバイスのキューが、空の正しい RPS マスクを使用してセットアップされるようになりました。(OCPBUGS-18662)

- 以前は、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ていました。このリリースでは、**PerformanceProfile** 要求を処理するときに、CRI-O は **crun** の違いを考慮し、パフォーマンスを確保するために CPU クォータを正しく設定します。(OCPBUGS-20492)

ストレージ

- 以前は、LVM Storage はオーバープロビジョニングの無効化をサポートしておらず、**LVMCluster** CR の **thinPoolConfig.overprovisionRatio** フィールドの最小値は 2 でした。このリリースでは、**thinPoolConfig.overprovisionRatio** フィールドの値を 1 に設定すること

で、オーバープロビジョニングを無効にできます。(OCPBUGS-24396)

- 以前は、**deviceSelector.optionalPaths** フィールドに無効なデバイスパスを指定して **LVMCluster** CR が作成された場合、**LVMCluster** CR は **Progressing** 状態にありました。このリリースでは、**deviceSelector.optionalPaths** フィールドに無効なデバイスパスが含まれている場合、LVM Storage は **LVMCluster** CR 状態を **Failed** に更新します。(OCPBUGS-23995)

- 以前は、クラスターが混雑しているときに LVM Storage リソース Pod がプリエンプトされていました。このリリースでは、OpenShift Container Platform の更新時に、クラスターが輻輳しているときに適切なスケジューリングとプリエンプション動作を確保するために、LVM Storage は **priorityClassName** パラメーターを設定します。(OCPBUGS-23375)

- 以前は、**LVMCluster** CR の作成時に、LVM Storage はボリュームグループのカウントをスキップしていました。その結果、ボリュームグループが有効であっても、**LVMCluster** CR が **Progressing** 状態に移行しました。このリリースでは、**LVMCluster** CR の作成時に、LVM Storage はすべてのボリュームグループをカウントし、ボリュームグループが有効であれば **LVMCluster** CR の状態を **Ready** に更新します。(OCPBUGS-23191)

- 以前は、選択したすべてのノードにデフォルトのデバイスクラスが存在しなかった場合、LVM Storage は **LVMCluster** CR をセットアップできませんでした。このリリースでは、デフォルトのデバイスクラスが選択したノードの 1 つにのみ存在する場合でも、LVM Storage はすべてのデフォルトのデバイスクラスを検出します。今回の更新により、選択したノードの 1 つでのみデフォルトのデバイスクラスを定義できるようになりました。(OCPBUGS-23181)

- 以前は、シングルノード OpenShift (SNO) およびワーカーノードトポロジーでワーカーノードを削除しても、**LVMCluster** CR には削除されたワーカーノードの設定が含まれていました。その結果、**LVMCluster** CR は **Progressing** 状態のままになりました。このリリースでは、SNO およびワーカーノードトポロジー内のワーカーノードを削除すると、LVM Storage は **LVMCluster** CR 内のワーカーノード設定を削除し、**LVMCluster** CR の状態を **Ready** に更新します。(OCPBUGS-13558)

- 以前は、AWS EFS CSI ドライバーコンテナーの CPU 制限により、AWS EFS CSI Driver Operator によって管理されるボリュームのパフォーマンスが低下する可能性がありました。このリリースでは、潜在的なパフォーマンスの低下を防ぐために、AWS EFS CSI Driver コンテナーの CPU 制限が削除されました。(OCPBUGS-28645)

- 以前は、Azure Disk CSI ドライバーで **performancePlus** パラメーターを使用し、512 GiB 以下のボリュームをプロビジョニングした場合、少なくとも 512 GiB のディスクサイズが必要であるというエラーがドライバーから返されていました。このリリースでは、**performancePlus** パラメーターを使用して 512 GiB 以下のボリュームをプロビジョニングすると、Azure Disk CSI ドライバーはボリュームのサイズを自動的に 513 GiB に変更します。(OCPBUGS-17542)

1.7. テクノロジープレビュー機能のステータス

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

テクノロジープレビュー機能のサポート範囲

次の表では、機能は次のステータスでマークされています。

- **テクノロジープレビュー**

- **一般公開 (GA)**

- **利用不可**
- **非推奨**

ネットワーキングテクノロジープレビュー機能

表1.16 ネットワーキングテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
Ingress Node Firewall Operator	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
特定の IP アドレスプールを使用した、ノードのサブセットから MetalLB サービスの L2 モードを使用したアドバタイズ	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
SR-IOV ネットワークのマルチネットワークポリシー	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	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
インターフェイス固有の安全な sysctls リストの更新	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Egress サービスのカスタムリソース	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
BGPPeer カスタムリソースの VRF 仕様	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
NodeNetworkConfigurationPolicy カスタムリソースの VRF 仕様	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
管理ネットワークポリシー (**AdminNetworkPolicy**)	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
IPsec 外部トラフィック (north-south)	利用不可	テクノロジープレビュー	一般公開 (GA)

機能	4.13	4.14	4.15
SR-IOV VF のホストネットワーク設定	利用不可	利用不可	テクノロジープレビュー

ストレージテクノロジープレビュー機能

表1.17 ストレージテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
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	一般公開 (GA)	一般公開 (GA)
IBM Power® Virtual Server Block CSI Driver Operator	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)
Read Write Once Pod アクセスモード	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
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	一般公開 (GA)	一般公開 (GA)
OpenShift ビルドの共有リソース CSI Driver	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Secrets Store CSI Driver Operator	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

インストールテクノロジープレビュー機能

表1.18 インストールテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
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	該当なし	開発者プレビュー	テクノロジープレビュー

機能	4.13	4.14	4.15
ベアメタル上の Oracle® Cloud Infrastructure (OCI) への OpenShift Container Platform のインストール	該当なし	開発者プレビュー	開発者プレビュー
kvc を使用したノードへのカーネルモジュールの追加	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Azure Tagging	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
SR-IOV デバイスの NIC パーティション設定の有効化	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
GCP Confidential 仮想マシン	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
Google Cloud Platform (GCP) のユーザー定義ラベルとタグ	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
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
OpenShift Container Platform on Oracle Cloud Infrastructure (OCI)	利用不可	開発者プレビュー	テクノロジープレビュー
選択可能なクラスターインベントリー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
vSphere を使用した静的 IP アドレス (IPI のみ)	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
RHCOS での iSCSI デバイスのサポート	利用不可	利用不可	テクノロジープレビュー

ノードテクノロジープレビュー機能

表1.19 ノードテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
Cron ジョブのタイムゾーン	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
MaxUnavailableStatefulSet featureSet	利用不可	テクノロジープレビュー	テクノロジープレビュー

マルチアーキテクチャーテクノロジーのプレビュー機能

表1.20 マルチアーキテクチャーテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
installer-provisioned infrastructure を使用する IBM Power® Virtual Server	テクノロジープレビュー	テクノロジープレビュー	一般公開 (GA)
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

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1.21 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	4.13	4.14	4.15
ドライバーツールキット	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
ハブアンドスポーククラスターのサポート	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)

Web コンソールのテクノロジープレビュー機能

表1.22 Web コンソールテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
マルチクラスターコンソール	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

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テクノロジープレビュートラッカー

機能	4.13	4.14	4.15
factory-precaching-cli ツール	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
ハイパースレッディング対応の CPU マネージャーポリシー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
PTP およびベアメタルイベントの AMQP を HTTP トランスポートに置き換え	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
マウント namespace のカプセル化	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
NUMA Resources Operator による NUMA 対応のスケジューリング	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
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
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	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
Topology Aware Lifecycle Manager (TALM)	一般公開 (GA)	一般公開 (GA)	一般公開 (GA)
etcd レイテンシー許容値の調整	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	4.13	4.14	4.15
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	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)

Operator のライフサイクルと開発テクノロジープレビュー機能

表1.24 Operator のライフサイクルと開発テクノロジープレビュートラッカー

機能	4.13	4.14	4.15
Operator Lifecycle Manager (OLM) v1	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
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
プラットフォーム 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

モニタリングテクノロジープレビュー機能

表1.25 モニタリングテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
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	一般公開 (GA)	一般公開 (GA)
メトリクス収集プロファイル	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Metrics Server	利用不可	利用不可	テクノロジープレビュー

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

表1.26 RHOSP テクノロジープレビュートラッカー

機能	4.13	4.14	4.15
installer-provisioned infrastructure での外部ロードバランサー	テクノロジープレビュー	一般公開 (GA)	一般公開 (GA)
installer-provisioned infrastructure でのデュアルスタックネットワーキング	利用不可	テクノロジープレビュー	一般公開 (GA)
ユーザーによってプロビジョニングされるインフラストラクチャーを備えたデュアルスタックネットワーキング	利用不可	利用不可	一般公開 (GA)
クラスター CAPI Operator への CAPO の統合 [1]	利用不可	利用不可	テクノロジープレビュー
ローカルディスク上の **rootVolumes** と **etcd** を備えたコントロールプレーン	利用不可	利用不可	テクノロジープレビュー

1. 詳細は、クラスター CAPI Operator への CAPO の統合 を参照してください。

アーキテクチャーテクノロジープレビューの機能

表1.27 アーキテクチャーテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
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	一般公開 (GA)	一般公開 (GA)
OpenShift Virtualization 上の OpenShift Container Platform の Hosted Control Plane	利用不可	一般公開 (GA)	一般公開 (GA)
非ベアメタルエージェントマシンを使用した OpenShift Container Platform の Hosted Control Plane	利用不可	利用不可	テクノロジープレビュー

マシン管理テクノロジープレビュー機能

表1.28 マシン管理テクノロジープレビュートラッカー

機能	4.13	4.14	4.15
Cluster API によるマシンの管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
コントロールプレーンマシンセットの vSphere 障害ドメインの定義	利用不可	利用不可	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	一般公開 (GA)	一般公開 (GA)
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	一般公開 (GA)
IBM Power® VS 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
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	一般公開 (GA)	一般公開 (GA)

認証と認可のテクノロジープレビュー機能

表1.29 認証と認可のテクノロジープレビュートラッカー

機能	4.13	4.14	4.15
Pod セキュリティーアドミッションの制限付き適用	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

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

表1.30 Machine Config Operator のテクノロジープレビュートラッカー

機能	4.13	4.14	4.15

機能	4.13	4.14	4.15
MCO 状態レポートの改善	利用不可	利用不可	テクノロジープレビュー

1.8. 既知の問題

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

- 静的 IP アドレス (テクノロジープレビュー) を使用して VMware vSphere にクラスターをインストールする場合、インストールプログラムがコントロールプレーンマシンセット (CPMS) に誤った設定を適用する可能性があります。これにより、静的 IP アドレスが定義されていないコントロールプレーンマシンが再作成される可能性があります。(OCPBUGS-28236)

- Azure クラスターをインストールする場合、標準の Ebdsv5 または Ebsv5 ファミリーマシンタイプインスタンスの指定はサポートされていません。この制限は、Azure terraform プロバイダーがこれらのマシンタイプをサポートしていないために発生します。(OCPBUGS-18690)

- FIPS を有効にしてクラスターを実行している場合、RHEL 9 システムで OpenShift CLI (**oc**) を実行すると、**FIPS mode is enabled, but the required OpenSSL backend is unavailable** というエラーが発生する場合があります。回避策として、OpenShift Container Platform クラスターで提供される **oc** バイナリーを使用します。(OCPBUGS-23386)

- Red Hat OpenStack Platform (RHOSP) 環境で IPv6 ネットワークが実行されている 4.15 では、**endpointPublishingStrategy.type=LoadBalancerService** YAML 属性で設定された **IngressController** オブジェクトが正しく機能しません。(BZ#2263550、BZ#2263552)

- Red Hat OpenStack Platform (RHOSP) 環境で IPv6 ネットワークが実行されている 4.15 では、IPv6 **ovn-octavia** ロードバランサーで作成されたヘルスモニターが正しく機能しません。(OCPBUGS-29603)

- Red Hat OpenStack Platform (RHOSP) 環境で IPv6 ネットワーキングが実行されている 4.15 では、IPv6 ロードバランサーをクラスターの内部として誤ってマークする問題のため、IPv6 ロードバランサーを複数のサービスと共有することはできません。(OCPBUGS-29605)

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

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

     a. マニフェストを作成します。

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

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

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

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

ip 設定については、次のように置き換えます。

1. **<static_ip>** は、ノードの静的 IP アドレスに置き換えます (例: **192.168.1.100**)
2. **<gateway>** は、ネットワークのゲートウェイの IP アドレスに置き換えます (例: **192.168.1.1**)
3. **<netmask>** は、ネットワークマスクに置き換えます (例: **255.255.255.0**)
4. **<hostname_1>** は、ノードのホスト名に置き換えます (例: **node1.example.com**)
5. **<interface>** は、ネットワークインターフェイスの名前に置き換えます (例: **eth0**)
6. **<fqdn>** は、ノードの完全修飾ドメイン名に置き換えます。
7. **<role>** は、ノードのロールを反映する **worker** または **master** に置き換えます。
8. **<bmc_ip>** は、必要に応じて BMC IP アドレス、BMC のプロトコルとパスに置き換えます。

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

d. クラスターを作成します。

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

```
$ curl https://api.openshift.com/api/assisted-install/v2/infra-
```

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

以前のネットワーク設定の場合は、次のように置き換えます。

1. **<static_ip>** は、ノードの静的 IP アドレスに置き換えます (例: **192.168.1.100**)
2. **<gateway>** は、ネットワークのゲートウェイの IP アドレスに置き換えます (例: **192.168.1.1**)
3. **<netmask>** は、ネットワークマスクに置き換えます (例: **255.255.255.0**)
4. **<hostname_1>** は、ノードのホスト名に置き換えます (例: **node1.example.com**)
5. **<interface>** は、ネットワークインターフェイスの名前に置き換えます (例: **eth0**)

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

(OCPBUGS-23119)

- OpenShift Container Platform 4.15 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)

- 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)

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

- 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、対応する割り込み要求 (IRQ) スレッドは更新をすぐには受け取りません。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)

- 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)

- 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、Kubernetes Operator (MCE) のマルチクラスターエンジンがインストールされている場合、Web コンソールの一部のページの **YAML** タブが一部のブラウザーで予期せず停止します。次のメッセージが表示されます: "Oh no!Something went wrong." (OCPBUGS-29812)

- クラスターで IPsec が有効になっており、クラスターと外部ノード間で IPsec 暗号化が設定されている場合、外部ノードで IPsec 接続を停止すると、外部ノードへの接続が失われます。接続の OpenShift Container Platform 側で IPsec トンネルのシャットダウンが認識されないため、このように接続できなくなります。(RHEL-24802)

- クラスターで IPsec が有効になっており、クラスターが OpenShift Container Platform クラスターの Hosted Control Plane である場合、Pod 間のトラフィックの IPsec トンネルを考慮した MTU 調整は自動的には行われません。(OCPBUGS-28757)

- クラスター上で IPsec が有効になっている場合、作成した外部ホストへの既存の IPsec トンネルを変更することはできません。既存の NMState Operator **NodeNetworkConfigurationPolicy** オブジェクトを変更して既存の IPsec 設定を調整し、外部ホストへのトラフィックを暗号化しても、OpenShift Container Platform では認識されません。(RHEL-22720)

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

- 現在、OpenShift Container Platform 4.15 とともにリリースされた **opm** CLI ツールのバージョンが RHEL 8 をサポートしないという既知の問題があります。回避策として、RHEL 8 ユーザーは OpenShift ミラーサイト に移動し、OpenShift Container Platform 4.14 でリリースされた tarball の最新バージョンをダウンロードできます。

- 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)

- 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、やはり CPU マネージャーはこの Pod のリソースを使用可能なプールに戻すことができなくなります。
  この問題は、CPU 負荷分散機能に影響を与えます。これは、これらの機能が 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するためです。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 は最後に許可された Pod となり、これによりリソースが使用可能なプールに正しく解放されます。(OCPBUGS-17792)

- ノードの再起動が発生すると、すべての Pod がランダムな順序で再起動されます。このシナリオでは、**tuned** Pod がワークロード Pod の後に開始された可能性があります。これは、ワークロード Pod が部分的なチューニングから開始されることを意味します。これは、パフォーマンスに影響を与えたり、ワークロードの失敗を引き起こしたりする可能性があります。(OCPBUGS-26400)

- パフォーマンスプロファイルが追加のマニフェストフォルダーに存在し、プライマリープールまたはワーカープールをターゲットにしている場合、OpenShift Container Platform のインストールが失敗することがあります。これは、デフォルトのプライマリーおよびワーカー **MachineConfigPool** が作成される前に、パフォーマンスプロファイルを処理する内部インストール順序によって発生します。この問題は、追加のマニフェストフォルダーにストックプライマリーまたはワーカー **MachineConfigPools** のコピーを含めることで回避できます。(OCPBUGS-27948) (OCPBUGS-18640)

- 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)

1.9. 非同期エラータの更新

OpenShift Container Platform 4.15 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 4.15 エラータは、Red Hat カスタマーポータルから入手できます。非同期エラータについては、OpenShift Container Platform ライフサイクル を参照してください。

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

注記

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

このセクションは、これからも継続して更新され、OpenShift Container Platform 4.15 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 4.15.z 形式などのバージョン管理された非同期リリースについては、サブセクションで詳しく説明します。さらに、エラータの本文がアドバイザリーで指定されたスペースに収まらないリリースの詳細は、その後のサブセクションで説明します。

重要

OpenShift Container Platform リリースでは、クラスターの更新 手順を必ず確認してください。

1.9.1. RHSA-2024:1770 - OpenShift Container Platform 4.15.9 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 16 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.9 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1770 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-2024:1773 アドバイザリーで提供されています。

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

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.15.9 --pullspecs
```

1.9.1.1. 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。

1.9.1.1.1. 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が 2 などの無効な値に設定されることがありました。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-30822)

1.9.1.2. バグ修正

- 以前は、Open Virtual Network (OVN) デプロイメントでは、kdump ログの SSH ターゲットへの保存に失敗していました。OVN が設定されている場合、kdump クラッシュログが SSH リモートに作成されませんでした。このリリースでは、OVS 設定が kdump の前に実行されなくなりました。(OCPBUGS-30884)

- 以前は、**coreos-installer** CLI ツールは、**openshift-install agent create image** コマンドで生成された ISO のカーネル引数の変更、リセット、表示を正しく行いませんでした。このリリースでは、**coreos-installer iso kargs modify <iso>**、**coreos-installer iso kargs reset**

<iso>、coreos-installer iso kargs show <iso> コマンドがすべて期待どおりに動作するようになりました。(OCPBUGS-30922)

- 以前は、サービスのセカンダリー IP ファミリーのテストが、デュアルスタッククラスターでは失敗していました。このリリースでは、30000:32767 のトラフィック範囲が有効になり、問題が解決しました。(OCPBUGS-31284)

1.9.1.3. 更新

既存の OpenShift Container Platform 4.15 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-2024:1668 - OpenShift Container Platform 4.15.8 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.8 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1668 アドバイザリーに記載されています。この更新用の RPM パッケージはありません。

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

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.15.8 --pullspecs
```

1.9.2.1. 更新

既存の OpenShift Container Platform 4.15 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-2024:1559 - OpenShift Container Platform 4.15.6 のバグ修正とセキュリティー更新

発行日: 2024 年 4 月 2 日

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

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

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.15.6 --pullspecs
```

1.9.3.1. 既知の問題

- このリリースには、Red Hat Enterprise Linux (RHEL) 8 システムで **oc-mirror** バイナリーが失敗するという既知の問題があります。回避策: Red Hat OpenShift Container Platform 4.15.5 **oc-mirror** バイナリーを使用するか、**oc-mirror.rhel8** を展開します。(OCPBUGS-31609)

1.9.3.2. 更新

既存の OpenShift Container Platform 4.15 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-2024:1449 - OpenShift Container Platform 4.15.5 のバグ修正とセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1449 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2024:1452 アドバイザリーで提供されています。

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

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.15.5 --pullspecs
```

1.9.4.1. バグ修正

- 以前は、Azure CLI で検証したときにインスタンスタイプが存在していても、割り当てられた時間内に OpenShift インストーラーが Microsoft Azure からインスタンスタイプ情報を取得できないことがありました。このリリースでは、Azure の応答を待機するためのタイムアウト時間が長くなりました。また、エラーメッセージに失敗の正確な理由が含まれるようになりました。(OCPBUGS-29964)

- 以前は、OpenShift インストーラーを使用する Hive プロビジョナーを使用して OpenShift Cluster Manager (OCM) によりクラスターを作成すると、クラスターの削除後にインストーラーが AWS IAM インスタンスプロファイルを削除できませんでした。この問題により、インスタンスプロファイルが蓄積されていました。このリリースでは、インストーラーがインスタンスプロファイルにタグを付け、適切にタグ付けされたプロファイルを削除します。(OCPBUGS-18986)

1.9.4.2. 更新

既存の OpenShift Container Platform 4.15 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-2024:1255 - OpenShift Container Platform 4.15.3 のバグ修正とセキュリティー更新

発行日: 2024-03-19

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.3 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1255 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-2024:1258 アドバイザリーで提供されています。

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

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.15.3 --pullspecs
```

1.9.5.1. バグ修正

- 以前は、mint モードの Google Cloud Platform (GCP)クラスターから root 認証情報が削除された場合、Cloud Credential Operator (CCO)は約 1 時間後に degraded 状態になりました。この問題は、CCO がコンポーネントの認証情報 root シークレットを管理できなかったことを意味します。今回の更新により、mint モードはカスタムロールをサポートするようになり、GCP クラスターから root 認証情報を削除しても CCO が degraded 状態にならなくなりました。(OCPBUGS-30412)

1.9.5.2. 更新

既存の OpenShift Container Platform 4.15 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-2024:1210 - OpenShift Container Platform 4.15.2 のバグ修正とセキュリティー更新

発行日: 2024 年 3 月 13 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.2 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:1210 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-2024:1213 アドバイザリーで提供されています。

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

以下のコマンドを実行して、本リリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.15.2 --pullspecs
```

1.9.6.1. 既知の問題

- OpenShift Container Platform 4.15.0 では、Day 0 で追加のマニフェストとしてパフォーマンスプロファイルを提供することは機能しませんでしたが、4.15.2 では次の制限付きで可能になりました。
  パフォーマンスプロファイルが追加のマニフェストフォルダーに存在し、プライマリープールまたはワーカープールをターゲットにしている場合、OpenShift Container Platform のインストールが失敗することがあります。これは、デフォルトのプライマリーおよびワーカー **MachineConfigPool** が作成される前に、パフォーマンスプロファイルを処理する内部インストール順序によって発生します。この問題は、追加のマニフェストフォルダーにストックプライマリーまたはワーカー **MachineConfigPools** のコピーを含めることで回避できます。(OCPBUGS-27948、OCPBUGS-29752)

1.9.6.2. バグ修正

- 以前は、OpenShift Container Platform 4.15 に更新すると、**CatalogSource** オブジェクトが更

新されず、オプションの Operator カタログの更新に失敗していました。このリリースでは、イメージプルポリシーが **Always** に変更され、オプションの Operator カタログが正しく更新されるようになりました。(OCPBUGS-30193)

- 以前は、**nodeStatusReportFrequency** 設定は、**nodeStatusUpdateFrequency** 設定にリンクされていました。このリリースでは、**nodeStatusReportFrequency** 設定は 5 分に設定されています。(OCPBUGS-29797)

- 以前は、特定の条件下で、インストーラーが失敗し、エラーメッセージ **unexpected end of JSON input** が表示されました。このリリースでは、エラーメッセージが明確になり、問題を解決するために **install-config.yaml** ファイルの **serviceAccount** フィールドを設定することをユーザーに提案します。(OCPBUGS-29495)

- 以前は、**HostedCluster** オブジェクトで提供された **oauthMetadata** プロパティーは、受け入れられませんでした。このリリースでは、**oauthMetadata** プロパティーが **HostedCluster** オブジェクトによって受け入れられます。(OCPBUGS-29025)

1.9.6.3. 更新

既存の OpenShift Container Platform 4.15 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。