OpenShift Container Platform 4.10

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: 2023-10-17

OpenShift Container Platform 4.10 リリースノート

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

法律上の通知

概要

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

目次

第1章 OPENSHIFT CONTAINER PLATFORM 4.10 リリースノート

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

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

1.1. このリリースについて

OpenShift Container Platform (RHSA-2022:0056) をご利用いただけるようになりました。本リリースでは、CRI-O ランタイムで Kubernetes 1.23 を使用します。以下では、OpenShift Container Platform 4.10 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。

Red Hat は OpenShift Container Platform 4.10.0 を GA バージョンとしてリリースせず、OpenShift Container Platform 4.10.3 を GA バージョンとしてリリースしています。

OpenShift Container Platform 4.10 クラスターは https://console.redhat.com/openshift でご利用いただけます。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 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することができます。

OpenShift Container Platform 4.10 は、Red Hat Enterprise Linux (RHEL) 8.4 および 8.7 ならびに Red Hat Enterprise Linux CoreOS (RHCOS) 4.10 でサポートされます。

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

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

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

1.3. 新機能および拡張機能

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. Documentation

1.3.1.1. OpenShift Container Platform のスタートガイド

OpenShift Container Platform 4.10 にはスタートガイドが追加されました。OpenShift Container Platform を使い始めることで、基本的な用語を定義し、開発者および管理者向けのロールベースの次のステップを提供します。

チュートリアルは、Web コンソールおよび OpenShift CLI (**oc**) インターフェイスを使用して新規ユーザーについて説明します。新規ユーザーは、スタートガイドを使用して以下のタスクを実行できます。

- プロジェクトを作成します。
- view パーミッションの付与
- Quay からのコンテナーイメージのデプロイ
- アプリケーションの検査およびスケーリング
- GitHub から Python アプリケーションのデプロイ
- Quay からデータベースへの接続
- シークレットの作成
- アプリケーションのロードと表示

詳細は、Getting Started with OpenShift Container Platform を参照してください。

1.3.2. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.2.1. ベアメタル RHCOS インストールのカスタマイズの強化

coreos-installer ユーティリティーには、ライブ ISO イメージおよび PXE イメージから RHCOS をベアメタルにインストールする際に、より柔軟なカスタマイズを可能にする **iso customize** および **pxe customize** サブコマンドが含まれるようになりました。

これには、カスタムの認証局または自己署名証明書を使用する HTTPS サーバーから Ignition 設定をフェッチするようにインストールをカスタマイズする機能が含まれます。

1.3.2.2. RHCOS が RHEL 8.4 を使用するように

RHCOS は、OpenShift Container Platform 4.10 で Red Hat Enterprise Linux (RHEL) 8.4 パッケージを使用するようになりました。これらのパッケージは、NetworkManager の機能など、最新の修正、機能、拡張、および最新のハードウェアサポートとドライバーの更新を提供します。

1.3.3. インストールおよびアップグレード

1.3.3.1. AWS インストールの新規デフォルトコンポーネントタイプ

OpenShift Container Platform 4.10 インストーラーは、AWS へのインストールに新規のデフォルトコンポーネントタイプを使用します。インストールプログラムはデフォルトで以下のコンポーネントを使用します。

- コントロールプレーンとコンピュートノードの両方用の AWS EC2 M6i インスタンス (利用可能な場合)
- AWS EBS gp3 ストレージ

1.3.3.2. install-config.yaml ファイルの API の機能強化

以前は、ユーザーがベアメタルインストーラーでプロビジョニングされたインフラストラクチャーに OpenShift Container Platform をインストールした場合、Ironic サーバーと通信するための静的 IP や vLAN などのカスタムネットワークインターフェイスを設定する場所がありませんでした。

ベアメタルのみで Day1 インストールを設定する場合、ユーザーは **install-config.yaml** ファイルの API を使用して、ネットワーク設定 (**networkConfig**) をカスタマイズできるようになりました。この設定は、インストールおよびプロビジョニングプロセス中に設定され、ホストごとの静的 IP の設定などの高度なオプションが含まれます。

1.3.3.3. ARM 上の OpenShift Container Platform

OpenShift Container Platform 4.10 は ARM ベースの AWS EC2 およびベアメタルプラットフォームでサポートされるようになりました。インスタンスの可用性およびインストールのドキュメントは、さまざまなプラットフォームのサポートされるインストール方法 を参照してください。

以下の機能は ARM の OpenShift Container Platform でサポートされます。

- OpenShift Cluster Monitoring
- RHEL 8 Application Streams
- OVNKube
- Elastic Block Store (EBS) for AWS
- AWS .NET アプリケーション
- ベアメタル上の NFS ストレージ

以下の Operator は ARM の OpenShift Container Platform でサポートされます。

- Node Tuning Operator
- Node Feature Discovery Operator
- Cluster Samples Operator
- Cluster Logging Operator
- Elasticsearch Operator
- Service Binding Operator

1.3.3.4. 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た IBM 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)

OpenShift Container Platform 4.10 では、テクノロジープレビューの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 IBM Cloud にクラスターをインストールするためのサポートが導入されました。

以下の制限は、IPI を使用する IBMCloud に適用されます。

- 既存のネットワークに IPI を使用して IBMCloud をデプロイすることはサポートされていません。
- Cloud Credential Operator (CCO) は、手動モードのみを使用できます。Mint モードまたは STS はサポートされていません。

- IBM Cloud DNS Services はサポートされていません。IBM Cloud Internet Services のインスタンスが必要です。
- プライベートデプロイまたは切断されたデプロイはサポートされていません。

詳細は、IBMCloud へのインストールの準備を参照してください。

1.3.3.5. VMware vSphere クラスターのインストールにおけるシンプロビジョニングのサポート

OpenShift Container Platform 4.10 では、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クラスターをインストールする場合は、シンプロビジョニングされたディスクのサポートが導入されました。ディスクは、**thin**、**thick**、または **eagerZeroedThick** としてプロビジョニングできます。VMware vSphere のディスクプロビジョニングモードについての詳細は、Installation configuration parameters を参照してください。

1.3.3.6. クラスターの Amazon Web Services GovCloud リージョンへのインストール

Red Hat Enterprise Linux CoreOS (RHCOS) Amazon Machine Images (AMI) が AWS GovCloud リージョンで利用可能になりました。これらの AMI の可用性は、クラスターをデプロイするためにカスタム RHCOS AMI をアップロードする必要がなくなるため、インストールプロセスが改善されます。

詳細は、AWS のクラスターの government リージョンへのインストール について参照してください。

1.3.3.7. インスタンスプロファイルのカスタム AWS IAM ロールの使用

OpenShift Container Platform 4.10 以降、クラスターを既存の IAM ロールで設定する場合、インストールプログラムはクラスターのデプロイ時に **shared** タグをロールに追加しなくなりました。今回の機能拡張により、カスタム IAM ロールを使用する組織のインストールプロセスが改善されましたが、セキュリティーポリシーにより **shared** タグが使用されなくなりました。

1.3.3.8. vSphere クラスターへの CSI ドライバーのインストール

vSphere で実行しているクラスターに CSI ドライバーをインストールするには、以下のコンポーネントがインストールされている必要があります。

- 仮想ハードウェアバージョン 15 以降
- vSphere バージョン 6.7 Update 3 以降
- VMware ESXi バージョン 6.7 Update 3 以降

上記よりも前のバージョンのコンポーネントは引き続きサポートされますが、非推奨です。これらのバージョンは引き続き完全にサポートされていますが、OpenShift Container Platform のバージョン 4.11 には、vSphere 仮想ハードウェアバージョン 15 以降が必要です。

注記

クラスターが vSphere にデプロイされている場合、前述のコンポーネントが上記のバージョンよりも低い場合は、vSphere での OpenShift Container Platform 4.9 から 4.10 へのアップグレードはサポートされますが、vSphere CSI ドライバーはインストールされません。4.10 へのバグ修正およびその他のアップグレードは引き続きサポートされますが、4.11 へのアップグレードは利用できなくなります。

1.3.3.9. 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)

OpenShift Container Platform 4.10 では、テクノロジープレビューとして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 Alibaba Cloud にクラスターをインストールする機能が導入されました。このタイプのインストールでは、インストールプログラムを使用して、インストールプログラムがプロビジョニングし、クラスターが管理するインフラストラクチャーにクラスターをデプロイできます。

1.3.3.10. 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た Microsoft Azure Stack Hub へのクラスターのインストール

OpenShift Container Platform 4.10 では、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た Azure Stack Hub へのクラスターのインストールのサポートが導入されました。このタイプのインストールでは、インストールプログラムを使用して、インストールプログラムがプロビジョニングし、クラスターが管理するインフラストラクチャーにクラスターをデプロイできます。

注記

OpenShift Container Platform 4.10.14 以降、**premium_LRS**、**standardSSD_LRS**、または **standard_LRS** ディスクタイプを使用して、コントロールプレーンおよびコンピュートノードをデプロイできます。デフォルトでは、インストールプログラムは **premium_LRS** ディスクタイプでコントロールプレーンとコンピュートノードをデプロイします。以前の 4.10 リリースでは、**standard_LRS** ディスクタイプのみがサポートされていました。

詳細は、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た Azure Stack Hub へのクラスターのインストール について参照してください。

1.3.3.11. 条件の更新

OpenShift Container Platform 4.10 は、OpenShift Update Service によって提供される条件付き更新パスの使用をサポートするようになりました。条件更新パスは、識別されたリスクと、これらのリスクがクラスターに適用される条件を伝えます。Web コンソールの Administrator パースペクティブは、クラスターが既知のリスクと一致しない推奨されるアップグレードパスのみを提供します。ただし、OpenShift CLI (**oc**) 4.10 以降を使用して、OpenShift Container Platform 4.10 クラスターの追加のアップグレードパスを表示できます。ドキュメントの参照など、関連するリスク情報がパスに表示されます。管理者は参照資料を確認し、サポートの実行を選択できますが、推奨されなくなったアップグレードは推奨されません。

詳細は、Conditional updates および Updating along a conditional upgrade path を参照してください。

1.3.3.12. oc-mirror CLI プラグインを使用したミラーリングの切断 (テクノロジープレビュー)

本リリースでは、oc-mirror OpenShift CLI (**oc**) プラグインがテクノロジープレビューとして導入されています。oc-mirror プラグインを使用して、非接続環境のイメージをミラーリングできます。

詳細は、Mirroring images for a disconnected installation using the oc-mirror plug-in を参照してください。

1.3.3.13. OVS-DPDK を使用する RHOSP へのクラスターのインストール

これで、Data Plane Development Kit (OVS-DPDK) ネットワークを使用して Open vSwitch でコンピュートマシンを実行する Red Hat OpenStack Platform (RHOSP) にクラスターをインストールできま

す。これらのマシンで実行されるワークロードは、OVS-DPDK のパフォーマンスとレイテンシーの改善から利点を得ることができます。

詳細は、Installing a cluster on RHOSP that supports DPDK-connected compute machines を参照してください。

1.3.3.14. RHOSP へのインストール中にコンピューティングマシンのアフィニティーを設定する

RHOSP にクラスターをインストールするときに、コンピューティングマシンアフィニティーを選択できるようになりました。デフォルトでは、コンピュートマシンは **soft-anti-affinity** サーバーポリシーでデプロイされますが、**anti-affinity** または **soft-affinity** ポリシーを選択することも可能です。

1.3.4. Web コンソール

1.3.4.1. Developer パースペクティブ

- この更新により、バインディング接続を確立するときに、**Topology** ビューでサービスバインディングコネクターの名前を指定できます。
- この更新により、パイプラインワークフローの作成が強化されました。
  - **Import from Git** パイプラインワークフローからアプリケーションをインポートするときに、ドロップダウンリストからユーザー定義のパイプラインを選択できるようになりました。
  - **Import from Git**ワークフローを使用して作成されたパイプラインにデフォルトの Webhook が追加され、**トポロジー**ビューで選択したリソースのサイドパネルに URL が表示されます。
  - **Tekton Config** カスタムリソースでパラメーター **enable-devconsole-integration** を **false** に設定することにより、デフォルトの Tekton Hub 統合をオプトアウトできるようになりました。

    Tekton Hub 統合をオプトアウトする Tekton Config CR の例

    ```
    ...
    hub:
      params:
        - name: enable-devconsole-integration
          value: 'false'
    ...
    ```

  - **パイプラインビルダー**には、クラスターでサポートされている Tekton Hub タスクが含まれており、サポートされていない他のすべてのタスクはリストから除外されます。
- この更新により、アプリケーションのエクスポートワークフローで、エクスポートの進行中にログのエクスポートダイアログまたはアラートが表示されるようになりました。ダイアログを使用して、エクスポートプロセスをキャンセルまたは再開できます。
- この更新により、カスタムリソースを作成することにより、新しい Helm Chart リポジトリーを**開発者カタログ**に追加できます。新しい**Project Helm Chart Repository**を追加するには、**開発者**パースペクティブのクイックスタートガイドを参照してください。

- この更新により、**Developer Catalog** を使用して community devfiles samples にアクセスできるようになりました。

1.3.4.2. 動的プラグイン (テクノロジープレビュー)

OpenShift Container Platform 4.10 以降、OpenShift コンソールの動的プラグインを作成する機能がテクノロジープレビュー機能として利用可能になりました。この機能を使用して、以下のような複数の方法でランタイム時にインターフェイスをカスタマイズできます。

- カスタムページの追加
- パースペクティブの追加およびナビゲーションアイテムの更新
- タブおよびアクションのリソースページへの追加

動的プラグインの詳細は、動的プラグインの OpenShift Container Platform Web コンソールへの追加 を参照してください。

1.3.4.3. デバッグモードでの Pod の実行

今回の更新により、Web コンソールでデバッグターミナルを表示できるようになりました。Pod に **CrashLoopBackOff** 状態にあるコンテナーがある場合、デバッグ Pod を起動できます。端末インターフェイスが表示され、クラッシュループコンテナーのデバッグに使用できます。

- この機能は、Pod のステータスのポップアップウィンドウからアクセスでき、Pod のステータスをクリックし、Pod 内のクラッシュループするコンテナーごとにデバッグターミナルへのリンクを提供します。
- また、Pod の詳細ページの **Logs** タブでこの機能にアクセスすることもできます。クラッシュループコンテナーを選択すると、デバッグターミナルのリンクがログウィンドウの上に表示されます。

さらに、Pod ステータスのポップアップウィンドウに、Pod 詳細ページの **Logs** タブおよび **Events** タブへのリンクが表示されるようになりました。

1.3.4.4. カスタマイズされたワークロード通知

今回の更新により、**ユーザー設定** ページでワークロード通知をカスタマイズできるようになりました。**通知** タブの**ユーザーワークロード通知** を使用すると、**Cluster Overview** ページまたはドロワーに表示されるユーザーワークロード通知を非表示にすることができます。

1.3.4.5. クォータの可視性の向上

今回の更新により、管理者以外のユーザーが **Project Overview**、**ResourceQuotas**、および **API Explorer** ページの **AppliedClusterResourceQuota** の使用を表示し、利用可能なクラスタースコープのクォータを判別できるようになりました。さらに、**AppliedClusterResourceQuota** の詳細は **Search** ページで確認できます。

1.3.4.6. クラスターのサポートレベル

OpenShift Container Platform では、**Overview → Details** カードの **Cluster Settings** で、クラスターについてのサポートレベル情報を **About** モーダルで表示でき、クラスターがサポートされていない場合に通知を通知ドロワーに追加できるようになりました。**概要** ページから、**サービスレベルアグリーメント (SLA)** でサブスクリプション設定を管理できます。

1.3.5. IBM Z および LinuxONE

本リリースでは、IBM Z および LinuxONE は OpenShift Container Platform 4.10 と互換性があります。インストールは z/VM または RHEL KVM で実行できます。インストール手順については、以下のドキュメントを参照してください。

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

主な機能拡張
以下の新機能は、OpenShift Container Platform 4.10 の IBM Z および LinuxONE でサポートされます。

- Horizontal Pod Autoscaling
- 以下の Multus CNI プラグインがサポートされます。
  - ブリッジ
  - host-device
  - IPAM
  - IPVLAN
- コンプライアンス Operator 0.1.49
- NMState Operator
- OVN-Kubernetes IPsec 暗号化
- Vertical Pod Autoscaler Operator

サポートされる機能
以下の機能が IBM Z および LinuxONE でもサポートされるようになりました。

- 現時点で、以下の Operator がサポートされています。
  - Cluster Logging Operator
  - コンプライアンス Operator 0.1.49
  - Local Storage Operator
  - NFD Operator
  - NMState Operator
  - OpenShift Elasticsearch Operator
  - Service Binding Operator

    - Vertical Pod Autoscaler Operator
- etcd に保存されるデータの暗号化
- Helm
- マルチパス化
- iSCSI を使用した永続ストレージ
- ローカルボリュームを使用した永続ストレージ (Local Storage Operator)
- hostPath を使用した永続ストレージ
- ファイバーチャネルを使用した永続ストレージ
- Raw Block を使用した永続ストレージ
- OVN-Kubernetes
- 複数ネットワークインターフェイスのサポート
- 3 ノードクラスターのサポート
- SCSI ディスク上の z/VM Emulated FBA デバイス
- 4k FCP ブロックデバイス

これらの機能は、4.10 について IBM Z および LinuxONE の OpenShift Container Platform にのみ利用できます。

- IBM Z および LinuxONE で有効にされている HyperPAV (FICON 接続の ECKD ストレージの仮想マシン用)。

制約
以下の制限は、IBM Z および LinuxONE の OpenShift Container Platform に影響します。

- 以下の OpenShift Container Platform のテクノロジープレビュー機能はサポートされていません。
    - Precision Time Protocol (PTP) ハードウェア
- 以下の OpenShift Container Platform 機能はサポートされていません。
    - 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
    - CodeReady Containers (CRC)
    - 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
    - CSI ボリュームのクローン作成
    - CSI ボリュームスナップショット
    - FIPS 暗号
    - NVMe

    - OpenShift Metering
    - OpenShift Virtualization
    - OpenShift Container Platform のデプロイメント時の Tang モードのディスク暗号化
- ワーカーノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続的な共有ストレージは、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
- 共有されていない永続ストレージは、iSCSI、FC、DASD、FCP または EDEV/FBA と共に LSO を使用するなど、ローカルストレージを使用してプロビジョニングする必要があります。

1.3.6. IBM Power

本リリースでは、IBM Power は OpenShift Container Platform 4.10 と互換性があります。インストール手順については、以下のドキュメントを参照してください。

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

主な機能拡張
以下の新機能は、OpenShift Container Platform 4.10 の IBM Power でサポートされます。

- Horizontal Pod Autoscaling
- 以下の Multus CNI プラグインがサポートされます。
    - ブリッジ
    - host-device
    - IPAM
    - IPVLAN
- コンプライアンス Operator 0.1.49
- NMState Operator
- OVN-Kubernetes IPsec 暗号化
- Vertical Pod Autoscaler Operator

サポートされる機能
以下の機能は、IBM Power でもサポートされています。

- 現時点で、以下の Operator がサポートされています。
    - Cluster Logging Operator
    - コンプライアンス Operator 0.1.49
    - Local Storage Operator
    - NFD Operator

    - NMState Operator
    - OpenShift Elasticsearch Operator
    - SR-IOV Network Operator
    - Service Binding Operator
    - Vertical Pod Autoscaler Operator
- etcd に保存されるデータの暗号化
- Helm
- マルチパス化
- Multus SR-IOV
- NVMe
- OVN-Kubernetes
- iSCSI を使用した永続ストレージ
- ローカルボリュームを使用した永続ストレージ (Local Storage Operator)
- hostPath を使用した永続ストレージ
- ファイバーチャネルを使用した永続ストレージ
- Raw Block を使用した永続ストレージ
- 複数ネットワークインターフェイスのサポート
- Power10 のサポート
- 3 ノードクラスターのサポート
- 4K ディスクのサポート

制約
以下の制限は、OpenShift Container Platform が IBM Power に影響を与えます。

- 以下の OpenShift Container Platform のテクノロジープレビュー機能はサポートされていません。
    - Precision Time Protocol (PTP) ハードウェア
- 以下の OpenShift Container Platform 機能はサポートされていません。
    - 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
    - CodeReady Containers (CRC)
    - 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
    - FIPS 暗号

    - OpenShift Metering
    - OpenShift Virtualization
    - OpenShift Container Platform のデプロイメント時の Tang モードのディスク暗号化
- ワーカーノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続ストレージは、ローカルボリュームを使用するファイルシステムタイプ、OpenShift Data Foundation、ネットワークファイルシステム (NFS)、またはコンテナーストレージインターフェイス (CSI) である必要があります。

1.3.7. セキュリティーおよびコンプライアンス

セキュリティーおよびコンプライアンスコンポーネントの新機能、拡張機能、およびバグ修正に関する情報は、Compliance Operator および File Integrity Operator のリリースノートに記載されています。

セキュリティーおよびコンプライアンスについての詳細は、OpenShift Container Platform セキュリティーおよびコンプライアンスを参照してください。

1.3.8. ネットワーク

1.3.8.1. デュアルスタックサービスでは、ipFamilyPolicy を指定する必要があります。

複数の IP アドレスファミリーを使用するサービスを作成する場合、Service オブジェクト定義で **ipFamilyPolicy: PreferDualStack** または **ipFamilyPolicy: RequireDualStack** を明示的に指定する必要があります。この変更により、OpenShift Container Platform の以前のリリースとの後方互換性が失われます。

詳細は、BZ#2045576 を参照してください。

1.3.8.2. クラスターのインストール後のクラスターネットワーク MTU の変更

クラスターのインストール後に、OpenShift SDN クラスターネットワークプロバイダーまたは OVN-Kubernetes クラスターネットワークプロバイダーを使用している場合、ハードウェア MTU およびクラスターネットワーク MTU 値を変更できます。クラスター全体で MTU を変更すると、混乱が生じ、各ノードが数回再起動される必要があります。詳細は、クラスターネットワーク MTU の変更を参照してください。

1.3.8.3. ゲートウェイ設定の OVN-Kubernetes サポート

OVN-Kubernetes CNI ネットワークプロバイダーは、egress トラフィックがノードゲートウェイに送信される方法の設定についてサポートを追加します。デフォルトでは、egress トラフィックは OVN で処理され、クラスターを終了するために処理され、トラフィックはカーネルルーティングテーブルの特殊なルートによる影響を受けません。

今回の機能拡張により、**gatewayConfig.routingViaHost** フィールドが追加されました。今回の更新により、このフィールドをインストール後のアクティビティーとしてランタイム時に設定でき、これが **true** に設定される場合、egress トラフィックは Pod からホストネットワークスタックに送信されます。今回の更新では、カーネルルーティングテーブルで手動で設定されたルートに依存する非常に特殊なインストールおよびアプリケーションが得られます。

今回の機能拡張により、Open vSwitch ハードウェアオフロード機能との対話が可能になりました。今回の更新により、**gatewayConfig.routingViaHost** フィールドが **true** に設定されている場合、egress トラフィックがホストネットワークスタックによって処理されるため、オフロードのパフォーマンス上

の利点は受けられなくなりました。

重要

Egress トラフィックを設定するには、**gatewayConfig.routingViaHost** を使用し、**gateway-mode-config** config map を **openshift-network-operator** namespace で設定している場合は削除します。**Gateway-mode-config** ソリューションと OpenShift Container Platform 4.10 以降での OVN-Kubernetes ゲートウェイモードの設定の詳細は、ソリューション を参照してください。

設定についての詳細は、OVN-Kubernetes CNI クラスターネットワークプロバイダーの設定 を 参照してください。

1.3.8.4. ネットワークメトリックの強化

以下のメトリックがクラスターで利用可能になりました。**sdn_controller** で始まるメトリック名は OpenShift SDN CNI ネットワークプロバイダーに固有のものです。**ovn** で始まるメトリック名は OVN-Kubernetes CNI ネットワークプロバイダーに固有のものです。

- **network_attachment_definition_instances{networks="egress-router"}**
- **openshift_unidle_events_total**
- **ovn_controller_bfd_run**
- **ovn_controller_ct_zone_commit**
- **ovn_controller_flow_generation**
- **ovn_controller_flow_installation**
- **ovn_controller_if_status_mgr**
- **ovn_controller_if_status_mgr_run**
- **ovn_controller_if_status_mgr_update**
- **ovn_controller_integration_bridge_openflow_total**
- **ovn_controller_ofctrl_seqno_run**
- **ovn_controller_patch_run**
- **ovn_controller_pinctrl_run**
- **ovnkube_master_ipsec_enabled**
- **ovnkube_master_num_egress_firewall_rules**
- **ovnkube_master_num_egress_firewalls**
- **ovnkube_master_num_egress_ips**
- **ovnkube_master_pod_first_seen_lsp_created_duration_seconds**
- **ovnkube_master_pod_lsp_created_port_binding_duration_seconds**

- **ovnkube_master_pod_port_binding_chassis_port_binding_up_duration_seconds**
- **ovnkube_master_pod_port_binding_port_binding_chassis_duration_seconds**
- **sdn_controller_num_egress_firewall_rules**
- **sdn_controller_num_egress_firewalls**
- **sdn_controller_num_egress_ips**

ovnkube_master_resource_update_total メトリックは 4.10 リリースに対して削除されます。

1.3.8.5. YAML ビューと Web コンソールフォームの切り替え

- 以前のバージョンでは、Web コンソールで **YAML ビュー**と **フォームビュー** を切り替える際に変更は保持されませんでした。さらに、**YAML ビュー** に切り替えた後、**フォームビュー** に戻ることができませんでした。今回の更新により、変更を失うことなく、Web コンソールの **YAML ビュー** と **フォームビュー** を簡単に切り替えできるようになりました。

1.3.8.6. ネットワークポリシーでターゲットとする Pod のリスト表示

OpenShift Container Platform Web コンソールでネットワークポリシー機能を使用する場合、ポリシーの影響を受ける Pod がリスト表示されます。これらのポリシーセクションで組み合わせた namespace および Pod セレクターの変更時に、このリストが変更されます。

- ピア定義
- ルール定義
- Ingress
- Egress

影響を受ける Pod のリストには、ユーザーがアクセス可能な Pod のみが含まれます。

1.3.8.7. ネットワークトレースを単純化するための must-gather の拡張機能

oc adm must-gather コマンドは、ネットワークパケットのキャプチャーの収集を単純化する方法で強化されています。

以前のバージョンでは、**oc adm must-gather** は単一のデバッグ Pod のみを起動することができました。今回の機能拡張により、デバッグ Pod を同時に複数のノードで起動できるようになりました。

この機能拡張を使用すると、ネットワーク通信問題のトラブルシューティングを単純化するために、複数のノードでパケットキャプチャーを同時に実行できます。新しい **--node-selector** 引数は、パケットキャプチャーを収集するノードを特定する方法を提供します。

詳細は、Network trace methods および Collecting a host network trace を参照してください。

1.3.8.8. セカンダリーネットワークの Pod レベルボンディング

Pod レベルでのボンディングは、高可用性とスループットを必要とする Pod 内のワークロードを有効にするために不可欠です。Pod レベルのボンディングでは、カーネルモードインターフェイスで複数の Single Root I/O Virtualization (SR-IOV) 仮想機能インターフェイスからボンドインターフェイスを作成できます。SR-IOV Virtual Function は Pod に渡され、カーネルドライバーに割り当てられます。

Pod レベルのボンディングが必要なシナリオには、異なる Physical Function 上の複数の SR-IOV Virtual Function からのボンディングインターフェイスの作成が含まれます。ホストの 2 つの異なる Physical Function からボンディングインターフェイスを作成して、Pod レベルで高可用性を実現するために使用できます。

1.3.8.9. パブリッククラウドにインストールされているクラスターの egress IP アドレスのサポート

クラスター管理者は、1 つ以上の egress IP アドレスを namespace に関連付けることができます。egress IP アドレスにより、一貫性のあるソース IP アドレスが、クラスターから出る特定の namespace からのトラフィックに関連付けられます。

OVN-Kubernetes および OpenShift SDN クラスターネットワークプロバイダーの場合、以下のパブリッククラウドプロバイダーで egress IP アドレスを設定できます。

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

詳細は、クラスターネットワークプロバイダーについての該当するドキュメントを参照してください。

1.3.8.10. egress ポリシーおよび ipBlock except の OpenShift SDN クラスターネットワークプロバイダーネットワークポリシーのサポート

OpenShift SDN クラスターネットワークプロバイダーを使用する場合、**ipBlock** および **ipBlock.except** を使用して、ネットワークポリシーで egress ルールを使用できるようになりました。**NetworkPolicy** オブジェクトの **egress** 配列で egress ポリシーを定義します。

詳細は、ネットワークポリシーについて を参照してください。

1.3.8.11. Ingress コントローラーのルーター圧縮

今回の機能拡張により、特定の MIME タイプについて HAProxy Ingress コントローラーでグローバル HTTP トラフィック圧縮を設定する機能が追加されました。今回の更新により、大量の圧縮ルーティングされたトラフィックが大量にある場合に、ingress ワークロードの gzip 圧縮が可能になりました。

詳細は、Using router compression を参照してください。

1.3.8.12. CoreDNS のカスタマイズのサポート

クラスター管理者は、デフォルトドメインの設定済みのサーバーを使用した DNS 名前解決を許可するように DNS サーバーを設定できるようになりました。DNS 転送設定には、**/etc/resolv.conf** ファイルおよびアップストリーム DNS サーバーで指定されたデフォルトのサーバーの両方を設定できます。

詳細は、DNS 転送の使用 を参照してください。

1.3.8.13. CoreDNS ログレベルと Operator ログレベルのサポート

この機能拡張により、Operator のログレベルを個別にまたはクラスター全体で手動で変更する機能が追加されます。

詳細は、Setting the CoreDNS log level を参照してください。

1.3.8.14. Ingress コントローラーでの syslog メッセージの最大長の設定のサポート

Ingress コントローラーの syslog メッセージの最大長を 480 から 4096 バイト間の任意の値に設定できるようになりました。

詳細は、Ingress Controller configuration parameters を参照してください。

1.3.8.15. CoreDNS 転送ポリシーの設定

DNS Operator を使用して CoreDNS 転送ポリシーを設定できるようになりました。デフォルト値は **Random** で、値を **RoundRobin** または **Sequential** に設定できます。

詳細は、DNS 転送の使用 を参照してください。

1.3.8.16. SR-IOV に対する Open vSwitch ハードウェアオフロードのサポート

Open vSwitch ハードウェアオフロードを設定して、互換性のあるベアメタルノードでデータ処理のパフォーマンスを向上できるようになりました。ハードウェアオフロードは、CPU からデータ処理タスクを削除し、ネットワークインターフェイスコントローラーの専用のデータ処理ユニットに転送するデータを処理する方法です。この機能の利点として、データ処理の高速化、CPU ワークロードの軽減、コンピューティングコストの削減などがあります。

詳細は、ハードウェアオフロードの設定を参照してください。

1.3.8.17. Red Hat 外部 DNS オペレーターを使用した DNS レコードの作成 (テクノロジープレビュー)

AWS、Azure、および GCP などのクラウドプロバイダーの Red Hat 外部 DNS Operator を使用して DNS レコードを作成できるようになりました。OperatorHub を使用して外部 DNS Operator をインストールできます。パラメーターを使用して、必要に応じて **ExternalDNS** を設定できます。

詳細は、Understanding the External DNS Operator を参照してください。

1.3.8.18. Mutable Ingress Controller エンドポイント公開戦略の強化

クラスター管理者は、OpenShift Container Platform の **Internal** と **Extrenal** の間でロードバランサースコープを変更するように Ingress Controller エンドポイントパブリッシング戦略を設定できるようになりました。

詳細は、Ingress Controller エンドポイント公開戦略を参照してください。

1.3.8.19. RHOSP でのクラスターの OVS ハードウェアオフロード (テクノロジープレビュー)

Red Hat Open Stack Platform (RHOSP) で実行されるクラスターの場合、Open vSwitch (OVS) ハードウェアオフロードを有効にできます。

詳細は、OVS ハードウェアオフロードの有効化を参照してください。

1.3.8.20. Kuryr によって作成された RHOSP リソースの削減

RHOSP で実行されるクラスターの場合、Kuryr は、Pod ネットワーク上に少なくとも 1 つの Pod を持つ名前空間の Neutron ネットワークとサブネットのみを作成するようになりました。さらに、名前空間内のプールは、Pod ネットワーク上の少なくとも 1 つの Pod が名前空間内に作成された後に作成されます。

1.3.8.21. RHOSP DCN (テクノロジープレビュー) のサポート

これで、分散コンピュートノード (DCN) 設定を使用する Red Hat Open Stack Platform (RHOSP) デプロイメントにクラスターをデプロイできます。このデプロイメント設定には、いくつかの制限があります。

- RHOSP バージョン 16 のみがサポートされています。
- RHOSP 16.1.4 の場合、ハイパーコンバージドインフラストラクチャー (HCI) と Ceph テクノロジーのみがエッジでサポートされます。
- RHOSP 16.2 では、非 HCI および Ceph テクノロジーもサポートされています。
- ネットワークは、テナントネットワークまたはプロバイダーネットワークとして事前に作成する必要があります (独自のネットワークを持参)。これらのネットワークは、適切なアベイラビリティーゾーンでスケジュールする必要があります。

1.3.8.22. RHOSP (テクノロジープレビュー) でのクラスターの外部クラウドプロバイダーのサポート

RHOSP で実行されるクラスターは、Cloud Provider Open Stack を使用できるようになりました。この機能は、**TechPreviewNoUpgrade** 機能セットの一部として利用できます。

1.3.8.23. インストーラーでプロビジョニングされるクラスターでの NMState を使用したホストネットワークインターフェイスの設定

OpenShift Container Platform は、インストーラーでプロビジョニングされるクラスターの **networkConfig** 設定を提供するようになりました。インストーラーでプロビジョニングされるインストールでは、**networkConfig** 設定と NMState YAML 設定を **install-config.yaml** ファイルに追加します。さらに、Bare Metal Operator を使用する際に、**networkConfig** 設定および NMState YAML 設定をベアメタルホストリソースに追加できます。

networkConfig 設定で最もよく使われるユースケースは、インストール時またはクラスターを拡張する間にホストのネットワークインターフェイスに静的 IP アドレスを設定することです。

詳細は、install-config.yaml ファイルでのホストネットワークインターフェイスの設定について参照してください。

1.3.8.24. linuxptp サービスへの境界クロックおよび PTP 機能拡張

PtpConfig プロファイルで複数のネットワークインターフェイスを指定できるようになり、RAN vDU アプリケーションを実行しているノードが Precision Time Protocol Telecom Boundary Clock (PTP T-BC) として機能するノードに対応できるようになりました。境界クロックとして設定されるインターフェイスが PTP 高速イベントに対応するようになりました。

詳細は、Configuring linuxptp services as boundary clock を参照してください。

1.3.8.25. Intel 800-Series Columbiaville NIC のサポート

Intel 800-Series Columbiaville NIC が、境界クロックまたは通常のクロックとして設定されるインターフェイスに対して完全にサポートされるようになりました。Columbiaville NIC は、以下の設定でサポートされています。

- 通常のクロック
- Grandmaster クロックに同期した境界クロック

- 帯域クロックと、アップストリームのソースクロックから同期する 1 つのポート、および宛先クロックにダウンストリームのタイミングを提供する 3 つのポート。

詳細は、PTP デバイスの設定を参照してください。

1.3.8.26. Kubernetes NMState Operator は、ベアメタル、IBM Power、IBM Z、および LinuxONE インストール向けの GA です。

OpenShift Container Platform は、ベアメタル、IBM Power、IBM Z、および LinuxONE インストールの Kubernetes NMState Operator を提供するようになりました。Kubernetes NMState Operator は依然として、他のすべてのプラットフォームでのテクノロジープレビューです。詳細は、Kubernetes NMState 演算子についてをご覧ください。

1.3.8.27. Mellanox MT2892 カードの SR-IOV サポート

Mellanox MT2892 カード で SR-IOV サポートが利用できるようになりました。

1.3.8.28. ネットワークトラフィックフローを監視する Network Observability Operator

管理者は、Network Observability Operator をインストールして、コンソールで OpenShift Container Platform クラスターのネットワークトラフィックを監視できるようになりました。さまざまなグラフィック表現でネットワークトラフィックデータを表示および監視できます。Network Observability Operator は、eBPF テクノロジーを使用してネットワークフローを作成します。その後、ネットワークフローは OpenShift Container Platform 情報で強化され、Loki に保存されます。ネットワークトラフィック情報を使用して、詳細なトラブルシューティングと分析を行うことができます。

Network Observability Operator は、OpenShift Container Platform の 4.12 リリースで一般公開 (GA) ステータスとなり、OpenShift Container Platform 4.10 でもサポートされています。

詳細は、Network Observability を参照してください。

1.3.8.28.1. ネットワーク可観測性 Operator の更新

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

1.3.9. ハードウェア

1.3.9.1. MetalLB 負荷分散の機能拡張

MetalLB および MetalLB Operator の以下の拡張機能は、本リリースに含まれています。

- Border Gateway Protocol (BGP) のサポートが追加されました。
- BGP と組み合わせて双方向転送検出 (BFD) のサポートが追加されました。
- IPv6 およびデュアルスタックネットワークのサポートが追加されました。
- **speaker** Pod でノードセレクターを指定するサポートが追加されます。ロードバランサーサービスの IP アドレスのアドバタイズに使用されるノードを制御できるようになりました。今回の機能拡張は、レイヤー 2 モードおよび BGP モードに適用されます。

- Web フックの検証により、アドレスプールと BGP ピアカスタムリソースが有効であることを確認します。
- 4.9 リリースで導入された **AddressPool** および **MetalLB** カスタムリソース定義の **v1alpha1** API バージョンは非推奨になりました。どちらのカスタムリソースも **v1beta1** API バージョンに更新されます。
- MetalLB カスタムリソース定義のスピーカー Pod の容認のサポートが追加されました。

詳細は、About MetalLB and the MetalLB Operator を参照してください。

1.3.9.2. ホストファームウェア設定の変更のサポート

OpenShift Container Platform は **HostFirmwareSettings** および **FirmwareSchema** リソースをサポートします。ベアメタルホストに OpenShift Container Platform をデプロイする場合、プロビジョニングの前後にホストに変更を加える必要がある場合があります。これには、ホストのファームウェアおよび BIOS の詳細の検証が含まれます。Bare Metal Operator (BMO) で使用できる新しいリソースが 2 つあります。

- **HostFirmwareSettings**: **HostFirmwareSettings** リソースを使用して、ホストの BIOS 設定を取得および管理できます。リソースには、ベースボード管理コントローラー (BMC) から返される完全な BIOS 設定が含まれます。**BareMetalHost** リソースのファームウェアフィールドは、3 つのベンダーに依存しないフィールドを返しますが、通常 **HostFirmwareSettings** リソースはホストモデルごとにベンダー固有のフィールドの BIOS 設定を多数設定します。
- **FirmwareSchema**: ホストファームウェア設定を変更する際に、**FirmwareSchema** を使用してホストの変更可能な BIOS 値および制限を特定できます。

詳細は、ベアメタルの設定を参照してください。

1.3.10. ストレージ

1.3.10.1. ストレージメトリックインジケーター

- この更新により、ワークロードは、Shared Resource CSI ドライバーによって提供されるインラインの一時**csi**ボリュームを使用して、namespace で **Secrets** および **ConfigMap** オブジェクトを安全に共有できます。Container Storage Interface (CSI) ボリュームおよび Shared Resource CSI ドライバーはテクノロジープレビュー機能です。(BUILD-293)

1.3.10.2. コンソールストレージプラグインの拡張機能

- スクリーンリーダーのインストールフロー全体で Aria ラベルを追加する Console Storage プラグインに新しい機能が追加されました。これにより、スクリーンリーダーを使用してコンソールにアクセスするユーザーに、アクセス性が向上します。
- Persistent Volume Claim (永続ボリューム要求、PVC) に使用されるボリュームで使用される領域の量を示すメトリックを提供する新機能が追加されました。この情報は PVC リストに表示され、PVC の詳細の **Used** 列に表示されます。(BZ#1985965)

1.3.10.3. Alibaba AliCloud Disk CSI ドライバー Operator を使用した永続ストレージ

OpenShift Container Platform は、AliCloud Disk の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。このドライバーを管理する AliCloud Disk Driver Operator は一般に利用可能であり、OpenShift Container Platform 4.10 ではデフォルトで有効になっています。

詳細は、AliCloud Disk CSI Driver Operator を参照してください。

1.3.10.4. Microsoft Azure File CSI ドライバー Operator を使用した永続ストレージ (テクノロジープレビュー)

OpenShift Container Platform は、Azure ファイルの Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。このドライバーを管理する Azure File Driver Operator はテクノロジープレビュー機能です。

詳細は、Azure File CSI Driver Operator を参照してください。

1.3.10.5. IBM VPC Block CSI Driver Operator を使用した永続ストレージ

OpenShift Container Platform は、Red Hat Virtualization (RHV) の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。このドライバーを管理する IBM VPC Block Driver Operator は一般に利用可能であり、OpenShift Container Platform 4.10 ではデフォルトで有効になっています。

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

1.3.10.6. VMware vSphere CSI Driver Operator を使用した永続ストレージが一般に利用可能になる

OpenShift Container Platform は、vSphere の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。この機能は以前は OpenShift Container Platform 4.8 のテクノロジープレビュー機能として導入されましたが、OpenShift Container Platform 4.10 では一般に利用可能となり、デフォルトで有効にされます。

詳細は、vSphere CSI Driver Operator を参照してください。

vSphere CSI ドライバー Operator のインストールには以下が必要です。

- 特定の最小コンポーネントバージョンがインストールされている。vSphere クラスターへの CSI ドライバーのインストールを参照してください。
- Red Hat vSphere CSI ドライバー (Red Hat vSphere CSI Operator ドライバーの削除) の削除
- **thin-csi** という名前のストレージクラスの削除

前述の条件が満たされなくても、クラスターはアップグレードされますが、サポートされる vSphere CSI Operator ドライバーを使用するにはこれらの条件を満たすことが推奨されます。

1.3.10.7. Microsoft Azure Disk CSI Driver Operator を使用した永続ストレージが一般に利用可能になる

OpenShift Container Platform は、Azure ディスクの Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。この機能は以前は OpenShift Container Platform 4.8 のテクノロジープレビュー機能として導入されましたが、OpenShift Container Platform 4.10 では一般に利用可能となり、デフォルトで有効にされます。

詳細は、Azure Disk CSI Driver Operator を参照してください。

1.3.10.8. AWS Elastic File Storage CSI ドライバー Operator を使用した永続ストレージが一般に利用可能になる

OpenShift Container Platform は、AWS Elastic File Storage (EFS) の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。この機能は以前は OpenShift Container Platform 4.9 のテクノロジープレビュー機能として導入されましたが、OpenShift Container Platform 4.10 では一般に利用可能となりました。

詳細は、AWS EFS CSI Driver Operator を参照してください。

1.3.10.9. CSI の自動移行による Microsoft Azure ファイルのサポート (テクノロジープレビュー)

OpenShift Container Platform 4.8 以降、インツリーボリュームプラグインの同等の Container Storage Interface (CSI) ドライバーへの自動移行がテクノロジープレビュー機能として利用可能になりました。この機能は、Azure File in-tree プラグインの Azure File CSI ドライバーへの自動移行をサポートするようになりました。

詳細は、CSI 自動移行を参照してください。

1.3.10.10. CSI の自動移行による VMware vSphere のサポート (テクノロジープレビュー)

OpenShift Container Platform 4.8 以降、インツリーボリュームプラグインの同等の Container Storage Interface (CSI) ドライバーへの自動移行がテクノロジープレビュー機能として利用可能になりました。この機能は、vSphere in-tree プラグインの vSphere CSI ドライバーへの自動移行をサポートするようになりました。

詳細は、CSI 自動移行を参照してください。

1.3.10.11. fsGroup を使用した Pod タイムアウトの削減

ストレージボリュームに多数のファイル (およそ 100 万以上) が含まれる場合には、Pod のタイムアウトが生じる可能性があります。

OpenShift Container Platform 4.10 では、**fsGroup** および **fsGroupChangePolicy** を使用して、ストレージボリュームの再帰的なパーミッションの変更をスキップする機能が導入されているため、Pod タイムアウトの問題を回避できます。

詳細は、fsGroup を使用した Pod タイムアウトの削減を参照してください。

1.3.11. レジストリー

1.3.12. Operator ライフサイクル

1.3.12.1. 大規模なクラスターをサポートするためにコピーされた CSV の無効化

Operator が Operator Lifecycle Manager (OLM) によってインストールされると、そのクラスターサービスバージョン (CSV) の簡単なコピーが Operator が監視するすべての namespace に作成されます。これらの CSV は、コピーされる CSV として知られ、それらは特定の namespace でリソースイベントをアクティブに調整しているコントローラーを特定します。

大規模なクラスターでは、namespace およびインストールされた Operator が数百または数千の場合に、コピーされた CSV は OLM のメモリー使用量、クラスター etcd 制限、およびネットワーク帯域幅などのリソースを有効にしない量を消費する可能性があります。これらの大規模なクラスターをサポートするために、クラスター管理者は、**AllNamespaces** モードでインストールされる Operator のコピーされた CSV を無効にできます。

詳細は、Operator Lifecycle Manager 機能の設定を参照してください。

1.3.12.2. 依存関係に対する汎用的および複雑な制約

特定の依存関係要件を持つ Operator は、複雑な制約または要件式を使用できるようになりました。新しい **olm.constraint** バンドルプロパティーは、依存関係制約情報を保持します。message フィールドにより、Operator の作成者は特定の制約が使用される理由についてハイレベルな詳細情報を伝えることができます。

詳細は、Operator Lifecycle Manager の依存関係の解決を参照してください。

1.3.12.3. Hypershift の Operator Lifecycle Manager のサポート

Operator カタログを含む Operator Lifecycle Manager (OLM) コンポーネントは、Hypershift 管理のコントロールプレーンで完全に実行できるようになりました。この機能により、ワーカーノードのテナントにコストがかかりません。

1.3.12.4. ARM の Operator Lifecycle Manager のサポート

以前のバージョンでは、デフォルトの Operator カタログは ARM をサポートしませんでした。今回の機能拡張により、Operator Lifecycle Manager (OLM) がデフォルトの Operator カタログを ARM クラスターに追加するようになりました。その結果、OperatorHub には ARM をサポートする Operator がデフォルトでコンテンツが含まれるようになりました。(BZ#1996928)

1.3.13. Operator の開発

1.3.13.1. ハイブリッド Helm Operator (テクノロジープレビュー)

Operator SDK における標準の Helm ベースの Operator サポートは、Operator の Operator 成熟度モデル で Auto Pilot 機能 (レベル V) に達した Go ベースおよび Ansible ベースの Operator サポートよりも機能が限定されています。

OpenShift Container Platform 4.10 以降、Operator SDK にはハイブリッド Helm Operator が含まれており、Go API 経由で既存の Helm ベースのサポートを強化します。Operator の作成者は Helm チャートで始まる Operator プロジェクトを生成し、Go 言語の Helm リコンサイラーに高度なイベントベースのロジックを追加できます。作成者は Go を使用して、同じプロジェクトに新規 API およびカスタムリソース定義 (CRD) の追加を継続できます。

詳細は、ハイブリッド Helm Operator の Operator SDK チュートリアル を参照してください。

1.3.13.2. Ansible ベースの Operator のカスタムメトリック

Operator の作成者は Operator SDK で Ansible ベースの Operator サポートを使用し、カスタムメトリックの公開、Kubernetes イベントの送信、および優れたロギングの提供が可能になりました。

詳細は、Ansible ベースの Operator のカスタムメトリックの公開を参照してください。

1.3.13.3. Go ベースの演算子のオブジェクトプルーニング

operator-lib プルーニングユーティリティーを使用すると、Go ベースのオペレーターは、クラスター内にとどまり、リソースを使用できるジョブや Pod などのオブジェクトをクリーンアップできます。このユーティリティーには、囲碁ベースのオペレーター向けの一般的な剪定戦略が含まれています。Operator の作成者は、ユーティリティーを使用してカスタムフックと戦略を作成することもできます。

プルーニングユーティリティーの詳細は、Go ベースの演算子のオブジェクトプルーニングユーティリティーを参照してください。

1.3.13.4. 切断された環境向けのダイジェストベースのバンドル

この機能拡張により、Operator SDK は、Operator Lifecycle Manager (OLM) を使用して切断された環境で機能するバンドルに Operator プロジェクトをパッケージ化できるようになりました。オペレーターの作成者は、**make bundle**コマンドを実行し、**USE_IMAGE_DIGESTS** を **true** に設定して、オペレーターのイメージ参照をタグではなくダイジェストに自動的に更新できます。このコマンドを使用するには、環境変数を使用して、ハードコードされた関連するイメージ参照を置き換える必要があります。

切断された環境用の Operator の開発の詳細には、制限されたネットワーク環境での Operator の有効化を参照してください。

1.3.14. ビルド

- 今回の更新により、OpenShift ビルドで CSI ボリュームを使用できるようになりました。これはテクノロジープレビュー機能です。この機能は、新たに導入された Shared Resource CSI ドライバーおよび Insights Operator に依存して、RHEL Simple Content Access (SCA) 証明書をインポートします。たとえば、この機能を使用すると、**SharedSecret** オブジェクトでエンタイトルメントが適用されたビルドを実行し、RHEL サブスクリプション認証情報および証明書をビルドの namespace にコピーするのではなく、ビルド時にエンタイトルメントのある RPM パッケージをインストールできます。(BUILD-274)

重要

SharedSecret オブジェクトおよび OpenShift Shared Resources 機能は、**TechPreviewNoUpgrade** 機能セットを有効にする場合にのみ利用できます。これらのテクノロジープレビュー機能は、デフォルトの機能の一部ではありません。この機能セットを有効にすると元に戻すことができなくなり、アップグレードできなくなります。この機能セットは、実稼働クラスターでは推奨されません。FeatureGate の使用によるテクノロジープレビュー機能の有効化を参照してください。

- この更新により、ワークロードは、Shared Resource CSI ドライバーによって提供されるインラインの一時**csi**ボリュームを使用して、namespace で **Secrets** および **ConfigMap** オブジェクトを安全に共有できます。Container Storage Interface (CSI) ボリュームおよび Shared Resource CSI ドライバーはテクノロジープレビュー機能です。(BUILD-293)

1.3.15. Jenkins

- 今回の更新により、Jenkins エージェントをサイドカーコンテナーとして実行できるようになりました。この機能を使用して、適切に設定された Pod テンプレートと Jenkins ファイルを持つ Jenkins パイプライン内のコンテナーイメージを実行できます。コードをコンパイルするために、**java-build** と **nodejs-builder** という名前の 2 つの新規 Pod テンプレートを Jenkins を使用してサイドカーコンテナーとして実行できるようになりました。これらの 2 つの Pod テンプレートは、**openshift** namespace の **java** および **nodejs** イメージストリームで提供される最新の Java および NodeJS バージョンを使用します。以前の non-sidecar **maven** および **nodejs** Pod テンプレートが非推奨になりました。(JKNS-132)

1.3.16. マシン API

1.3.16.1. Azure Ephemeral OS ディスクのサポート

今回の機能拡張により、マシンを Azure Ephemeral OS ディスクにデプロイする Azure で実行されるマシンセットを作成できるようになりました。Azure Ephemeral OS ディスクは、リモートの Azure Storage ではなく、ローカルの VM 容量を使用します。

詳細は、マシンを Ephemeral OS ディスクにデプロイするマシンセット ついて参照してください。

1.3.16.2. Azure Accelerated Networking のサポート

このリリースでは、Machine API を使用して、Microsoft Azure VM の高速ネットワークを有効にできます。アクセラレートネットワークでは、Single Root I/O Virtualization (SR-IOV) を使用して、仮想マシンのスイッチへの直接パスを提供します。

詳細は、Accelerated Networking for Microsoft Azure VMs を参照してください。

1.3.16.3. グローバル Azure 可用性セットのサポート

今回のリリースにより、高可用性を確保するために、複数のアベイラビリティーゾーンを持たないグローバル Azure リージョンで可用性セットを使用できるようになりました。

1.3.16.4. Google Cloud Platform での GPU サポート

Google Cloud Platform (GCP) Compute Engine を使用すると、ユーザーは仮想マシンインスタンスに GPU を追加できます。GPU リソースにアクセスできるワークロードは、この機能を有効にしてコンピュートマシンでより優れたパフォーマンスが得られます。今回のリリースにより、Machine API を使用して、インスタンスに使用するサポートされる GPU を定義できるようになりました。

詳細は、マシンセットの GPU サポートの有効化 について参照してください。

1.3.16.5. Cluster Autoscaler ノード使用率のしきい値

今回の機能拡張により、**ClusterAutoscaler** リソース定義にノード使用率のしきい値を指定できるようになりました。このしきい値は、不要なノードが削除の対象となっているノードの使用率レベルを表します。

詳細は、Cluster Autoscaler について を参照してください。

1.3.17. Machine Config Operator

1.3.17.1. 設定ドリフト検出の強化

今回の機能拡張により、Machine Config Daemon (MCD) は、ノード起動に加えて、マシン設定で指定されたファイルについてファイルシステム書き込みイベントが発生する場合、またはノードの起動に加えて新規のマシン設定が適用される前に、ノードの設定ドリフトをチェックするようになりました。以前のバージョンでは、MCD はノードの起動時にのみ設定のドリフトの有無を確認していました。この変更は、管理者が問題を修正するまで設定ドリフトによって生じる問題を回避するためにノードの再起動が頻繁に行われないために加えられました。

設定ドリフトは、ノードのディスク上の状態がマシン設定で設定される内容と異なる場合に発生します。Machine Config Operator (MCO) は MCD を使用して設定ドリフトの有無を確認し、検出される場合はノードおよびマシン設定プール (MCP) のパフォーマンスが **低下** します。

設定ドリフトの詳細は、Understanding configuration drift detection を参照してください。

1.3.18. ノード

1.3.18.1. Linux コントロールグループのバージョン 2(開発者プレビュー)

クラスター内の特定ノードで Linux control groups version 2 (cgroups v2) を有効化できるようになりました。cgroups v2 を有効にする OpenShift Container Platform プロセスにより、cgroups バージョン 1 コントローラーおよび階層がすべて無効になります。OpenShift Container Platform cgroups バージョン 2 機能は Developer プレビューとして提供されており、現時点では Red Hat ではサポートされていません。詳細は、Enabling Linux control groups version 2 (cgroups v2) を参照してください。

1.3.18.2. ノードでのスワップメモリー使用のサポート (テクノロジープレビュー)

ノードごとに OpenShift Container Platform ワークロードの swap メモリー使用量を有効にすることができます。詳細は、ノードでの swap メモリー使用の有効化を参照してください。

1.3.18.3. Node Maintenance Operator を使用したノードのメンテナンスモードへの配置

Node Maintenance Operator (NMO) は、クラスターの残りの部分からノードを切り離し、ノードからすべての Pod をドレイン (解放) します。ノードをメンテナンス状態にすることで、マシンの問題を調査したり、基礎となるマシンで操作を実行したり、ノードに障害が発生する可能性があります。これは NMO のスタンドアロンバージョンです。OpenShift Virtualization をインストールしている場合、バンドルされる NMO を使用する必要があります。

1.3.18.4. ノードヘルスチェックオペレーターの機能強化 (テクノロジープレビュー)

Node Health Check Operator は、これらの新たな拡張機能を提供します。

- 非接続モードでの実行サポート
- マシンヘルスチェックとの競合を防ぐことができます。詳細は、ノードのヘルスチェックによるマシンヘルスチェックの競合を参照してください。

1.3.18.5. Poison Pill Operator の拡張機能

Poison Pill Operator は **NodeDeletion** をデフォルトの修復ストラテジーとして使用します。**NodeDeletion** 修復ストラテジーは **node** オブジェクトを削除します。

OpenShift Container Platform 4.10 では、Poison Pill Operator は **ResourceDeletion** という新規の修復ストラテジーを導入しています。**ResourceDeletion** 修復ストラテジーは、**node** オブジェクトではなくノードでの Pod および関連付けられたボリュームの割り当てを削除します。このストラテジーは、ワークロードをより迅速に復元するのに役立ちます。

1.3.18.6. RHOSP でのコントロールプレーンノードの移行

これで、サービスを中断することなく、コントロールプレーンノードをある RHOSP ホストから別のホストに移行できます。

1.3.19. Red Hat OpenShift Logging

OpenShift Container Platform 4.7 では、**Cluster Logging** は **Red Hat OpenShift Logging** になりました。詳細は、Release notes for Red Hat OpenShift Logging を参照してください。

1.3.20. モニタリング

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

1.3.20.1. モニタリングスタックコンポーネントおよび依存関係

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バージョンの更新には、以下が含まれます。

- Alertmanager to 0.23.0
- Grafana to 8.3.4
- kube-state-metrics to 2.3.0
- node-exporter to 1.3.1
- prom-label-proxy to 0.4.0
- Prometheus to 2.32.1
- Prometheus adapter to 0.9.1
- Prometheus operator to 0.53.1
- Thanos to 0.23.1

1.3.20.2. OpenShift Container Platform Web コンソールでのメトリックターゲットの新規ページ

OpenShift Container Platform Web コンソールの新規 **Metrics Targets** ページには、デフォルトの OpenShift Container Platform プロジェクトおよびユーザー定義プロジェクトのターゲットが表示されます。このページを使用すると、現在収集の対象となっているエンドポイントを表示、検索、およびフィルタリングできます。これにより、問題を特定してトラブルシューティングしやすくなります。

1.3.20.3. メトリクス収集に TLS 認証を使用するように更新されたモニタリングコンポーネント

今回のリリースにより、すべてのモニタリングコンポーネントが、メトリクス収集にベアラートークンの静的認証ではなく、相互 TLS 認証を使用するように設定されるようになりました。TLS 認証は、Kubernetes API の停止に対してより回復力が高く、Kubernetes API の負荷が軽減されます。

1.3.20.4. Cluster Monitoring Operator がグローバル TLS セキュリティープロファイルを使用するように更新

今回のリリースにより、Cluster Monitoring Operator コンポーネントはグローバルな OpenShift Container Platform **tlsSecurityProfile** 設定を有効にするようになりました。以下のコンポーネントおよびサービスは、TLS セキュリティープロファイルを使用するようになりました。

- Alertmanager Pod (ポート 9092 および 9097)
- kube-state-metrics Pod (ポート 8443 および 9443)
- openshift-state-metrics Pod (ポート 8443 および 9443)
- node-exporter pods (ポート 9100)
- Grafana pod (ポート 3002)
- prometheus-adapter pods (ポート 6443)

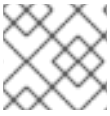
- prometheus-k8s pods (ポート 9092 および 10902)
- Thanos クエリー pods (ポート 9092、9093 および 9094)
- Prometheus Operator (ポート 8080 および 8443)
- Telemeter-client Pod (ポート 8443)

ユーザー定義モニタリングを有効にしている場合、以下の Pod がプロファイルを使用するようになりました。

- prometheus-user-workload Pod (ポート 9091 および 10902)
- prometheus-operator Pod (ポート 8080 および 8443)

1.3.20.5. アラートルールの変更

- New
  - すべての Thanos アラートルールに **namespace** ラベルを追加しました。
  - すべてのプラットフォームアラートに **openshift_io_alert_source="platform"** ラベルが追加されました。
- **変更済み**
  - **AggregatedAPIDown** の名前を **KubeAggregatedAPIDown** に変更します。
  - **AggregatedAPIErrors** の名前を **KubeAggregatedAPIErrors** に変更します。
  - **HighlyAvailableWorkloadIncorrectlySpread** アラートが削除されました。
  - **KubeMemoryOvercommit** アラートの説明が改善されました。
  - **NodeFilesystemSpaceFillingUp** アラートが強化され、Kubernetes ガベージコレクションのしきい値と一致しました。
  - **KubePersistentVolumeFillingUp** アラートから除外される **ReadOnlyMany** ボリューム。
  - 拡張 **PrometheusOperator** アラートが **openshift-user-workload-monitoring** namespace で実行されている Prometheus Operator を組み込むように拡張されました。
  - **ThanosSidecarPrometheusDown** および **ThanosSidecarUnhealthy** のアラートを **ThanosSidecarNoConnectionToStartedPrometheus** に変更しました。
  - **KubeletTooManyPods** の重大度を **warning** から **info** に変更しました。
  - **alerts.k8s.io/KubePersistentVolumeFillingUp: disabled** ラベルを永続ボリュームリソースに追加して、**KubePersistentVolumeFillingUp** アラートから特定の永続ボリュームの除外が有効にされています。



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。

1.3.20.6. メトリックの変更

- スライスレベルで利用可能な Pod 中心の cAdvisor メトリックがドロップされました。
- 以下のメトリックが公開されました。
  - **kube_poddisruptionbudget_labels**
  - **kube_persistentvolumeclaim_labels**
  - **kube_persistentvolume_labels**
- 名前が **kube_*annotation** のメトリックは **kube-state-metrics** から削除されました。

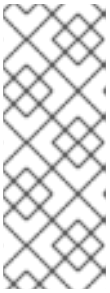
注記

Red Hat は、メトリックの後方互換性を保証しません。

1.3.20.7. 特定のコンポーネントのハード非アフィニティールールおよび Pod の Disruption Budget (停止状態の予算) を追加

今回のリリースにより、ハード非アフィニティールールおよび Pod の Disruption Budget (停止状態の予算) がモニタリングするコンポーネントで、パッチのアップグレード時にダウンタイムを短縮できるようになりました。

- Alertmanager



注記

この変更の一環として、Alertmanager レプリカの数が 3 から 2 に削減されました。ただし、削除された 3 番目のレプリカの Persistent Volume Claim (永続ボリューム要求、PVC) は、アップグレードプロセスの一環として自動的に削除されません。Alertmanager の永続ストレージを設定している場合、この PVC を Cluster Monitoring Operator から手動で削除できます。詳細は、既知の問題のセクションを参照してください。

- Prometheus アダプター
- Prometheus
- Thanos Querier

ユーザー定義のモニタリングを有効にしている場合、以下のコンポーネントはそれらのルールおよび予算も使用します。

- Prometheus
- Thanos Ruler

1.3.20.8. ユーザー定義プロジェクトのアラートルーティング (テクノロジープレビュー)

本リリースでは、管理者がユーザー定義プロジェクトのモニタリングのアラートルーティングを有効にできるテクノロジープレビュー機能が導入されました。ユーザーは、ユーザー定義プロジェクトのアラートルーティングを追加し、設定できます。

1.3.20.9. Alertmanager

OpenShift Container Platform ルートからサードパーティーの Alertmanager Web ユーザーインターフェイスへのアクセスが削除されました。

1.3.20.10. Prometheus

- OpenShift Container Platform クラスター管理者は、Prometheus のクエリーロギングを設定できるようになりました。
- サードパーティーの Prometheus Web ユーザーインターフェイスへのアクセスは非推奨となり、今後の OpenShift Container Platform リリースで削除されます。

1.3.20.11. Prometheus アダプター

- Prometheus アダプターは、Prometheus API ではなく Thanos Querier API を使用するようになりました。
- OpenShift Container Platform クラスター管理者は、Prometheus アダプターの監査ログを設定できるようになりました。

1.3.20.12. Thanos Querier

- OpenShift Container Platform ルートからサードパーティーの Thanos Querier Web ユーザーインターフェイスへのアクセスが削除されました。
- Thanos Querier テナントポートの **/api/v1/labels**、**/api/v1/label/*/values** および **/api/v1/series** エンドポイントが公開されるようになりました。
- OpenShift Container Platform クラスター管理者はクエリーロギングを設定できるようになりました。
- ユーザーワークロードモニタリングが有効にされている場合、OpenShift Container Platform ルートからサードパーティーの Thanos Ruler Web ユーザーインターフェイスへのアクセスが削除されます。

1.3.20.13. Grafana

サードパーティーの Grafana Web ユーザーインターフェイスへのアクセスは非推奨となり、今後の OpenShift Container Platform リリースで削除されます。

1.3.21. スケーラビリティーおよびパフォーマンス

1.3.21.1. 新しい Special Resource Operator メトリック

Special Resource Operator (SRO) は、SRO カスタムリソースおよびオブジェクトの正常性を監視するためのメトリックを公開するようになりました。詳細は、Prometheus Special Resource Operator metrics を参照してください。

1.3.21.2. 特別な Resource Operator カスタムリソース定義フィールド

Special Resource Operator (SRO) に **oc explain** を使用すると、SRO カスタムリソース定義 (CRD) のオンラインドキュメントが提供されるようになりました。今回の機能拡張により、CRD フィールドの詳細が改善されました。(BZ#2031875)

1.3.21.3. 新たな Node Tuning Operator メトリックが Telemetry に追加される

Node Tuning Operator (NTO) メトリックが Telemetry に追加されました。Telemetry によって収集されるデータの表示についての手順に従い、Telemetry によって 収集されるすべてのメトリックを表示します。

1.3.21.4. NFD Topology Updater が利用可能になりました。

Node Feature Discovery (NFD) Topology Updater は、ワーカーノードに割り当てられたリソースを調べるデーモンです。これは、ゾーンごとに新規 Pod に割り当てることができるリソースに対応し、ゾーンを Non-Uniform Memory Access (NUMA) ノードにすることができます。詳細は、NFD Topology Updater の使用を参照してください。

1.3.21.5. 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)

OpenShift Container Platform の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は追加のチューニングなしに利用できるようになりました。クラスター管理者は、必要に応じてこの機能を有効にできます。ハイパースレッドは、ハードウェアによって論理プロセッサーとして抽象化されます。ハイパースレッディングにより、単一の物理プロセッサーが同時に 2 つの負荷スレッド (プロセス) を実行し、プロセッサーリソースを動的に共有できます。

1.3.21.6. NUMA Resources Operator による NUMA 対応スケジューリング (テクノロジープレビュー)

デフォルトの OpenShift Container Platform スケジューラーは、コンピュートノード内の個々の Non-Uniform Memory Access (NUMA) ゾーンを認識しません。これにより、レイテンシーの影響を受けやすいワークロードのスケジューリングが最適化されない可能性があります。NUMA 対応のセカンダリースケジューラーをデプロイする新しい NUMA Resources Operator が利用可能です。NUMA 対応のセカンダリースケジューラーは、クラスター内で使用可能な NUMA ゾーンの全体像に基づいて、ワークロードのスケジューリングを決定します。これにより、レイテンシーの影響を受けやすいワークロードが単一の NUMA ゾーンで処理され、効率とパフォーマンスが最大化されます。

詳細は、About NUMA-aware scheduling を参照してください。

1.3.21.7. SiteConfig フィルターを使用して ZTP スポーククラスターのインストール中にカスタムリソースをフィルター処理する

フィルターを使用して **SiteConfig** CR をカスタマイズし、ゼロタッチプロビジョニング (ZTP) GitOps パイプラインのインストールフェーズで使用する他の CR を含めたり除外したりできるようになりました。詳細は、Filtering custom resources using SiteConfig filters を参照してください。

1.3.21.8. vDU ユースケースの PolicyGenTemplate CR で chronyd を無効にする

RAN vDU アプリケーションを実行しているノードでは、以前のバージョンから OpenShift Container Platform 4.10 に更新する場合に、**chronyd** を無効にする必要があります。**chronyd** を無効にするには、**TunedPerformancePatch.yaml** ファイルの **.spec.profile.data** の下の **[service]** セクションに以下の行を追加します。**TunedPerformancePatch.yaml** ファイルは、グループ **PolicyGenTemplate** CR で参照されます。

```
[service]
service.chronyd=stop,disable
```

詳細は、vDU アプリケーションを実行するための推奨クラスター設定 を参照してください。

1.3.22. バックアップと復元

1.3.23. 開発者エクスペリエンス

1.3.23.1. デプロイメントレプリカセットのプルーニング (テクノロジープレビュー)

本リリースでは、テクノロジープレビューフラグ **--replica-sets** が **oc adm prune deployments** コマンドに追加されました。デフォルトで、レプリケーションコントローラーのみが **oc adm prune deployments** コマンドでプルーニングされます。**--replica-sets** を **true** に設定すると、レプリカセットもプルーニングプロセスに含まれます。

詳細は、デプロイメントリソースのプルーニングを参照してください。

1.3.24. Insights Operator

1.3.24.1. シンプルなコンテンツアクセス証明書のインポート

OpenShift Container Platform 4.10 では、Insights Operator はデフォルトで Red Hat OpenShift Cluster Manager から単純なコンテンツアクセス証明書をインポートするようになりました。

詳細は、Importing simple content access certificates with Insights Operator を参照してください。

1.3.24.2. Insights Operator のデータ収集機能の拡張

Red Hat に送信されるデータ量を減らすために、Insights Operator は特定の条件が満たされる場合にのみ情報を収集します。たとえば、Insights Operator は、Alertmanager がアラート通知の送信に失敗する場合にのみ Alertmanager ログを収集します。

OpenShift Container Platform 4.10 では、Insights Operator は以下の追加情報を収集します。

- (条件)**KubePodCrashlooping** および **KubePodNotReady** アラートが実行される Pod からのログ
- (条件)**AlertmanagerClusterFailedToSendAlerts** または **AlertmanagerFailedToSendAlerts** アラートの実行時に Alertmanager ログ。
- Alertmanager からの無音アラート
- ジャーナルユニット (kubelet) からのノードログ
- **costmanagement-metrics-operator** がインストールされているクラスターの **CostManagementMetricsConfig**
- モニタリングスタック Prometheus インスタンスからの時系列データベースのステータス
- OpenShift Container Platform スケジューラーに関する追加情報

この追加情報により、Red Hat は OpenShift Container Platform 機能を強化し、Insights Advisor の推奨事項を強化します。

1.3.25. 認証および認可

1.3.25.1. OpenID Connect アイデンティティープロバイダーからのグループメンバーシップの同期

本リリースでは、ユーザーのログイン時に、OpenID Connect プロバイダーから OpenShift Container

Platform にグループメンバーシップを同期するサポートが導入されました。これを有効にするには、OpenShift Container Platform OpenID Connect アイデンティティープロバイダー設定で **groups** 要求を設定します。

詳細は、Sample OpenID Connect CRs を参照してください。

1.3.25.2. サポートされる追加の OIDC プロバイダー

Okta および Ping Identity OpenID Connect (OIDC) プロバイダーは、OpenShift Container Platform でテストされ、サポートされるようになりました。

OIDC プロバイダーの完全リストは、サポートされている OIDC プロバイダーを参照してください。

1.3.25.3. oc コマンドが Podman 設定の場所から認証情報を取得できるようになりました。

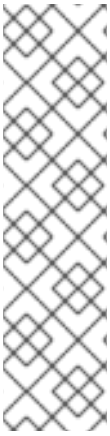
以前のバージョンでは、レジストリー設定 (**oc login** または **oc image** など) を使用する **oc** コマンドは、Docker 設定の場所から認証情報を取得していました。OpenShift Container Platform 4.10 では、レジストリーエントリーがデフォルトの Docker 設定の場所で見つからない場合、**oc** コマンドは Podman 設定の場所から認証情報を取得します。場所の優先順位付けのために **REGISTRY_AUTH_PREFERENCE** 環境変数を使用して **docker** または **podman** のいずれかの設定を設定できます。

また、ユーザーは **REGISTRY_AUTH_FILE** 環境変数を使用するオプションもあります。これは、既存の **--registry-config** CLI フラグの代わりに機能します。**REGISTRY_AUTH_FILE** 環境変数も **podman** と互換性があります。

1.3.25.4. Google Cloud Platform Workload Identity のサポート

Cloud Credential Operator (CCO) ユーティリティー **ccoctl** を使用して、Google Cloud Platform Workload Identity を使用するように CCO を設定できるようになりました。CCO が GCP Workload Identity を使用するように設定されている場合、クラスター内のコンポーネントは、短期的で制限付き権限のセキュリティー認証情報を使用して IAM サービスアカウントになりすますことができます。

詳細は、Using manual mode with GCP Workload Identity を参照してください。



注記

OpenShift Container Platform 4.10.8 では、イメージレジストリーへの悪影響が発見されたため、GCP ワークロード ID を使用するためのイメージレジストリーサポートが削除されました。ワークロード ID を使用する OpenShift Container Platform 4.10.8 クラスターでイメージレジストリーを使用するには、代わりに長期間有効なクレデンシャルを使用するようにイメージレジストリーを設定する必要があります。

OpenShift Container Platform 4.10.21 では、イメージレジストリーで GCP Workload Identity を使用するためのサポートが復活しました。OpenShift Container Platform 4.10.8 から 4.10.20 までのこの機能のステータスに関する詳細は、関連する ナレッジベースの記事 を参照してください。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.10 では、以下に示す顕著な技術的な変更点が加えられています。

TLS X.509 証明書にはサブジェクト代替名が必要です。
X.509 証明書には、Subject Alternative Name フィールドを適切に設定する必要があります。これなしにクラスターを更新すると、クラスターを破損したり、アクセスできなくなるリスクがあります。

以前のバージョンの OpenShift Container Platform では、X.509 証明書は Subject Alternative Name なしで機能していました。そのため、Common Name フィールドが設定されている限り、X.509 証明書は Subject Alternative Name なしで動作していました。この動作は OpenShift Container Platform 4.6 で削除されました。

Subject Alternative Name のない証明書は、OpenShift Container Platform 4.6、4.7、4.8、および 4.9 で引き続き機能します。これは Kubernetes 1.23 を使用するため、OpenShift Container Platform 4.10 はいずれの場合でもこれを許可しません。

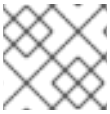
追加のクラウドプロバイダー向けのクラウドコントローラーマネージャー
Kubernetes コミュニティーは、クラウドコントローラーマネージャーを使用して基礎となるクラウドプラットフォームと対話することを優先し、Kubernetes コントローラーマネージャーの使用を計画しています。その結果、新しいクラウドプラットフォームの Kubernetes コントローラーマネージャーサポートを追加する計画はありません。このリリースの OpenShift Container Platform に追加された実装は、Google Cloud Platform (GCP)、VMware vSphere、IBM Cloud、Alibaba Cloud のクラウドコントローラーマネージャーをTechnology Preview として使用することをサポートしています。

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

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

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

Operator SDK v1.16.0
OpenShift Container Platform 4.10 は Operator SDK v1.16.0 をサポートします。この最新バージョンのインストール、または最新バージョンへの更新については、Operator SDK CLI のインストール を参照してください。



注記

Operator SDK v1.16.0 は Kubernetes 1.22 をサポートします。

非推奨の **v1beta1** API の多くは、**sigs.k8s.io/controller-runtime v0.10.0** および **controller-gen v0.7** を含む Kubernetes 1.22 で削除されました。これは、カスタムリソース定義 (CRD) または Webhook の **v1beta1** API をスキャフォールディングする必要がある場合には、重大な変更になります。

Kubernetes 1.22 で導入された変更の詳細は、OpenShift Container Platform 4.9 リリースノートの Validating bundle manifests for APIs removed from Kubernetes 1.22 と Beta APIs removed from Kubernetes 1.22 を参照してください。

以前に Operator SDK v1.10.1 で作成または保守された Operator プロジェクトがある場合は、Upgrading projects for newer Operator SDK versionsを参照してプロジェクトをアップグレードし、Operator SDK v1.16.0 との互換性が維持されていることを確認してください。

Cluster Autoscaler アラートの重大度の変更
以前のバージョンでは、**ClusterAutoscalerUnschedulablePods** アラートは重大度 (warning) を **warning** し、開発者の介入が必要であることを提案しました。このアラートは情報提供であり、介入を必要とする問題のある状態については説明しません。今回のリリースにより、**ClusterAutoscalerUnschedulablePods** アラートの重大度が **warning** から **info** に短縮されるようになりました。(BZ#2025230)

ネットワークフローを監視するための Network Observability Operator

Network Observability Operator は、OpenShift Container Platform の 4.12 リリースで一般公開 (GA) ステータスとなり、OpenShift Container Platform 4.10 でもサポートされています。

詳細は、Network Observability を参照してください。

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 4.10 で非推奨となり、削除された主な機能の最新のリストについては、以下の表を参照してください。非推奨になったか、削除された機能の詳細情報は、表の後に記載されています。

以下の表では、機能は以下のステータスでマークされています。

- **GA**: **一般公開機能**
- **DEP**: **非推奨機能**
- **REM**: **削除された機能**

表1.1 非推奨および削除機能のトラッカー

機能	OCP 4.8	OCP 4.9	OCP 4.10
Package Manifest Format (Operator Framework)	REM	REM	REM
Operator カタログの SQLite データベース形式	GA	DEP	DEP
oc adm catalog build	REM	REM	REM
oc adm catalog mirror の **--filter-by-os** フラグ	REM	REM	REM
v1beta1 CRD	DEP	REM	REM
Docker Registry v1 API	DEP	REM	REM
メータリング Operator	DEP	REM	REM
スケジューラーポリシー	DEP	DEP	REM
Cluster Samples Operator の **ImageChangesInProgress** 状態	DEP	DEP	DEP
Cluster Samples Operator の **MigrationInProgress** 状態	DEP	DEP	DEP
OpenShift Container Platform リソースの **apiVersion** でグループなしで **v1** の使用	DEP	REM	REM

機能	OCP 4.8	OCP 4.9	OCP 4.10
RHCOS での **dhclient** の使用	DEP	REM	REM
クラスターローダー	DEP	DEP	REM
独自の RHEL 7 コンピュートマシンの持ち込み	DEP	DEP	REM
ビルドの **BuildConfig** 仕様の **lastTriggeredImageID** フィールド	DEP	REM	REM
Jenkins Operator	DEP	DEP	REM
Prometheus に基づく HPA カスタムメトリックアダプター	REM	REM	REM
vSphere 6.7 Update 2 以前	GA	DEP	DEP
仮想ハードウェアバージョン 13	GA	DEP	DEP
VMware ESXi 6.7 Update 3 以前	GA	DEP	DEP
Microsoft Azure クラスターのクレデンシャルの作成	GA	GA	REM
FlexVolume を使用した永続ストレージ			DEP
Jenkins の非 sidecar pod テンプレート			DEP
マルチクラスターコンソール (テクノロジープレビュー)			REM

1.5.1. 非推奨の機能

1.5.1.1. IBM POWER8、IBM z13 のすべてのモデル、LinuxONE Emperor、LinuxONE Rockhopper、および x86_64 v1 アーキテクチャーは非推奨になりました。

IBM POWER8 の RHCOS 機能、IBM z13 のすべてのモデル、LinuxONE Emperor、LinuxONE Rockhopper、および AMD64 (x86_64) v1 CP アーキテクチャーは今後のリリースで非推奨となりました。これらのアーキテクチャーのサポートを停止する場合の追加情報は、今後のリリースで発表されます。

注記

AMD および Intel 64 ビットアーキテクチャー (x86-64-v2) は引き続きサポートされます。

1.5.1.2. デフォルトの Docker 設定の場所が非推奨になる

以前のバージョンでは、レジストリー設定を使用する **oc** コマンドは、Docker 設定の場所 (デフォルトは ~/**.docker/config.json**) から認証情報を取得していました。これは非推奨となっており、OpenShift Container Platform の今後のバージョンでは Podman 設定の場所に置き換えられます。

1.5.1.3. oc registry login で空のファイルおよび stdout のサポートが非推奨になる

oc registry login で **--registry-config** および **--to** フラグを使用する空のファイルのサポートが非推奨になりました。**oc registry login** の使用時に、**-**(標準出力) のサポートも引数として非推奨となりました。これらは OpenShift Container Platform の今後のバージョンで削除されます。

1.5.1.4. Jenkins の非 sidecar Pod テンプレート (非推奨)

OpenShift Container Platform 4.10 では、Jenkins の非 sidecar **maven** および **nodejs** Pod テンプレートが非推奨になりました。これらの Pod テンプレートは、今後のリリースで削除される予定です。バグ修正やサポートは、ライフサイクルの終了までに提供されますが、新しい機能拡張は加えられません。その代わりに、今回の更新で、Jenkins エージェントをサイドカーコンテナーとして実行できるようになりました。(JKNS-257)

1.5.1.5. サードパーティーのモニタリングコンポーネントのユーザーインターフェイスが非推奨に

以下のモニタリングスタックコンポーネントの場合、サードパーティーの Web ユーザーインターフェイス (UI) へのアクセスは非推奨となり、今後の OpenShift Container Platform リリースで削除される予定です。

- Grafana
- Prometheus

または、OpenShift Container Platform Web コンソールの **Observe** セクションに移動し、ダッシュボードおよびプラットフォームコンポーネントの他の UI にアクセスすることもできます。

1.5.1.6. FlexVolume を使用した永続ストレージ

OpenShift Container Platform 4.10 では、FlexVolume を使用した永続ストレージが非推奨になりました。この機能は完全にサポートされていますが、重要なバグのみが修正される予定です。ただし、今後の OpenShift Container Platform リリースで削除される可能性があります。OpenShift Container Platform でボリュームドライバーを作成するには、out-of-tree Container Storage Interface (CSI) ドライバーが推奨されます。FlexVolume ドライバーのメンテナーは、CSI ドライバーを実装し、FlexVolume のユーザーを CSI に移行する必要があります。FlexVolume のユーザーは、ワークロードを CSI ドライバーに移行する必要があります。

1.5.1.7. OpenShift CLI (oc) の RHEL 7 サポートは非推奨

OpenShift CLI (**oc**) での Red Hat Enterprise Linux (RHEL) 7 の使用に対するサポートは非推奨となり、今後の OpenShift Container Platform リリースでは削除される予定です。

1.5.2. 削除された機能

OpenShift Container Platform 4.10 は、OpenShift Container Platform Web コンソールインターフェイスの **OperatorHub** ページから、テクノロジープレビュー機能である Jenkins Operator を削除します。バグ修正やサポートは利用できなくなりました。

その代わりに、Samples Operator によって提供されるテンプレートを使用して、引き続き OpenShift Container Platform に Jenkins をデプロイすることができます。または、Web コンソールの Developer

パースペクティブの Helm ページを使用して、**Developer** Catalog から Jenkins **Helm** Chart をインストールできます。

1.5.2.1. OpenShift CLI (oc) コマンドが削除される

以下の OpenShift CLI (**oc**) コマンドは本リリースで削除されました。

- **oc adm completion**
- **oc adm config**
- **oc adm options**

1.5.2.2. スケジューラーポリシーの削除

スケジューラーポリシーの設定のサポートは本リリースで削除されました。代わりに スケジューラープロファイル を使用して、Pod をノードにスケジュールする方法を制御します。

1.5.2.3. コンピュートマシンの RHEL 7 サポートが削除される

OpenShift Container Platform で Red Hat Enterprise Linux (RHEL) 7 コンピュートマシンを実行するサポートが削除されました。RHEL コンピュートマシンを使用する場合は、RHEL 8 で実行する必要があります。

RHEL 7 コンピュートマシンを RHEL 8 にアップグレードすることはできません。新しい RHEL 8 ホストをデプロイする必要があり、古い RHEL 7 ホストを削除する必要があります。

1.5.2.4. サードパーティーのモニタリングコンポーネントのユーザーインターフェイスアクセスが削除される

今回のリリースにより、以下のモニタリングスタックコンポーネントのサードパーティーの Web ユーザーインターフェイス (UI) にアクセスできなくなりました。

- Alertmanager
- Thanos Querier
- Thanos Ruler (ユーザーワークロードの監視が有効になっている場合)

その代わりに、OpenShift Container Platform Web コンソールの **Observe** セクションに移動し、プラットフォームコンポーネントのメトリック、アラート、およびメトリックターゲット UI にアクセスできます。

1.5.2.5. Microsoft Azure のクレデンシャルの作成のサポートが削除されました

Microsoft Azure クラスターでミントモードで Cloud Credential Operator (CCO) を使用するためのサポートが削除されました。この変更は、2022 年 6 月 30 日に Microsoft が Azure AD Graph API を廃止する予定であるためであり、z-stream 更新でサポートされているすべてのバージョンの OpenShift Container Platform にバックポートされます。

ミントモードを使用する以前にインストールされた Azure クラスターの場合、CCO は既存のシークレットを更新しようとします。シークレットに以前に作成されたアプリ登録サービスプリンシパルのクレデンシャルが含まれている場合、そのシークレットは **kube-system/azure-credentials** のシークレットの内容で更新されます。この動作は、パススルーモードに似ています。

クレデンシャルモードがデフォルト値の **""** に設定されているクラスターの場合、更新された CCO は、ミントモードでの動作からパススルーモードでの動作に自動的に変更されます。クラスターでクレデンシャルモードが明示的にミントモード (**"Mint"**) に設定されている場合は、値を **""** または **"Passthrough"** に変更する必要があります。

注記

ミントモードで必要な **Contributor** のロールに加えて、変更されたアプリ登録サービスプリンシパルには、パススルーモードで使用される **User Access Administrator** のロールが必要になりました。

Azure AD Graph API は引き続き利用可能ですが、OpenShift Container Platform のアップグレードバージョンの CCO は、以前に作成されたアプリ登録サービスプリンシパルをクリーンアップしようとします。Azure AD Graph API を廃止する前にクラスターをアップグレードすると、リソースを手動でクリーンアップする必要がなくなる場合があります。

Azure AD Graph API が廃止された後、クラスターがミントモードをサポートしなくなったバージョンの OpenShift Container Platform にアップグレードされた場合、CCO は関連する **credentialsrequest** に **OrphanedCloudResource** 条件を設定しますが、エラーを致命的なものとして扱いません。この条件には、**unable to clean up App Registration / Service Principal: <app_registration_name>** と類似したメッセージが含まれます。Azure AD Graph API が廃止された後のクリーンアップでは、Azure CLI ツールまたは Azure Web コンソールを使用して手動で介入し、残りのアプリ登録サービスプリンシパルを削除する必要があります。

リソースを手動でクリーンアップするには、影響を受けるリソースを見つけて削除する必要があります。

1. Azure CLI ツールを使用して、次のコマンドを実行し、 **OrphanedCloudResource** 条件メッセージから **<app_registration_name>** を使用するアプリ登録サービスプリンシパルをフィルター処理します。

```
$ az ad app list --filter "displayname eq '<app_registration_name>'" --query '[].objectId'
```

出力例

```
[
  "038c2538-7c40-49f5-abe5-f59c59c29244"
]
```

2. 次のコマンドを実行して、アプリ登録サービスプリンシパルを削除します。

```
$ az ad app delete --id 038c2538-7c40-49f5-abe5-f59c59c29244
```

注記

リソースを手動でクリーンアップした後、CCO はリソースがクリーンアップされたことを確認できないため、**OrphanedCloudResource** 状態が持続します。

1.6. バグ修正

ベアメタルハードウェアのプロビジョニング

- 以前は、プロビジョニングネットワークを **disable** から **Managed** に切り替えるときに、MAC

アドレスを使用してプロビジョニングネットワークインターフェイスを設定することはサポートされていませんでした。今回の更新により、**provisioningMacAddresses** フィールドが **provisioning.metal3.io** CRD に追加されました。このフィールドを使用して、名前ではなく MAC アドレスを使用してプロビジョニングネットワークインターフェイスを特定します。(BZ#2000081)

- 以前のリリースでは、これらのモデルは CD ベースの仮想メディア用に **UsbCd** などの標準デバイス文字列を想定するため、Ironic は SuperMicro X11/X12 サーバーのプロビジョニングのために仮想メディアイメージを割り当てることができませんでした。今回の更新により、プロビジョニングが CD ベースの仮想メディアでプロビジョニングされる SuperMicro マシンで **UsbCd** を上書きするようになりました。(BZ#2009555)

- 以前のリリースでは、これらのマシンの BMC で制限が厳しい URI 検証により、SuperMicro X11/X12 サーバーでの仮想メディアイメージのアタッチに失敗していました。今回の更新で、仮想メディアイメージがローカルファイルでサポートされている場合に、**filename** パラメーターを URL から削除されました。その結果、イメージがオブジェクトストアでサポートされている場合には、パラメーターがパスし続けます。(BZ#2011626)

- 以前のバージョンでは、マシンポーサーイメージによって使用される **curl** ユーティリティーは、**no_proxy** でクラスレスのドメイン間ルーティング (CIDR) をサポートしていませんでした。その結果、Red Hat Enterprise Linux CoreOS (RHCOS) イメージのダウンロード時に 'noProxy' の CIDR が無視されました。今回の更新により、適切な場合に **curl** を呼び出す前に、プロキシーが環境から削除されるようになりました。その結果、マシンイメージをダウンロードする際に、**no_proxy** の CIDR は無視されなくなりました。(BZ#1990556)

- 以前のバージョンでは、OpenShift Container Platform の仮想メディアベースのデプロイメントは、iDRAC ハードウェアタイプで断続的に失敗することが確認されました。これは、未処理のライフサイクルコントローラーが仮想メディアの設定要求と競合する場合に生じました。今回の更新により、デプロイメント前に iDRAC ハードウェアの登録中に、ライフサイクルコントローラージョブをパージすることで、仮想メディアのデプロイメントの失敗が修正されました。(BZ#1988879)

- 以前は、インストール設定ファイルに IPv6 アドレスの長い形式を入力する必要がありました (例: **2001:0db8:85a3:0000:0000:8a2e:0370:7334**)。Ironic はこの IP アドレスに一致するインターフェイスを見つけることができませんでした。これにより、インストールが失敗しました。今回の更新で、ユーザーが提供した IPv6 アドレスは、短い形式アドレス (例: **2001:db8:85a3::8a2e:370:7334**) に変換されるようになりました。その結果、インストールが正常に実行されるようになりました。(BZ#2010698)

- 今回の更新の前は、Redfish システムが設定 URI を備えている場合、Ironic プロビジョニングサービスは常にこの URI を使用して、ブート関連の BIOS 設定を変更しようとしまていました。ただし、ベースボード管理コントローラー (BMC) が設定 URI を備えていても、この設定 URI を使用した特定の BIOS 設定の変更をサポートしていない場合、ベアメタルプロビジョニングは失敗します。OpenShift Container Platform 4.10 以降では、システムに設定 URI がある場合には、Ironic は続行する前に設定 URI を使用して特定の BIOS 設定を変更できることを確認します。それ以外の場合、Ironic はシステム URI を使用して変更を実装します。この追加のロジックにより、Ironic がブート関連の BIOS 設定の変更を適用でき、ベアメタルプロビジョニングが成功することが保証されます。(OCPBUGS-6886)

ビルド

- 今回の更新以前は、OpenShift Container Platform 4.7.x 以前でイメージ変更トリガーを含むビルド設定を作成している場合、イメージ変更トリガーはビルドを継続的にトリガーする可能性があります。
この問題は、ビルドの **BuildConfig** 仕様から **lastTriggeredImageID** フィールドは非推奨となり、ビルドをインスタンス化する前にイメージ変更トリガーコントローラーがそのフィールドをチェックしなくなったために生じました。OpenShift Container Platform 4.8 では、イメージ

変更トリガーコントローラーがチェックするために必要なステータスの新規フィールドが導入されましたが、これは実行しませんでした。

今回の更新により、イメージ変更トリガーコントローラーは、仕様の正しいフィールドと最後にトリガーされたイメージ ID のステータスを継続的にチェックするようになりました。今回のリリースより、必要な場合にのみビルドがトリガーされるようになりました。(BZ#2004203)

- 今回の更新以前は、Red Hat レジストリー名を明示的に指定するために必要となる Builds のイメージ参照です。今回の更新により、イメージ参照にレジストリーが含まれていない場合には、Build は Red Hat レジストリーおよびその他の既知のレジストリーを検索してイメージを見つけるようになりました。(BZ#2011293)

Jenkins

- 今回の更新以前は、OpenShift Jenkins 同期プラグインのバージョン 1.0.48 では、OpenShift Jenkins Pipeline ビルドストラテジーのビルド設定と関連付けられていない新規ジョブのプラグインに通知すると、**NullPointerException** エラーが導入されました。最終的にこのエラーは、受信 Jenkins ジョブに関連付ける **BuildConfig** オブジェクトがないために無害でした。コア Jenkins は、プラグイン内の例外を無視し、次のリスナーに移されました。ただし、長いスタックトレースは、ユーザーを引き継ぐ Jenkins ログに表示されました。今回の更新で、このプラグインは、このエラーと後続のスタックトレースを回避するために適切なチェックを行うことで問題を解決します。(BZ#2030692)

- 今回の更新以前は、OpenShift 同期 Jenkins プラグインのバージョン 1.0.48 におけるパフォーマンスの向上により、Jenkins Kubernetes プラグイン Pod テンプレートにマップされる **ConfigMap** および **ImageStream** オブジェクトに受け入れられるラベルが誤って指定されていました。その結果、プラグインは **jenkins-agent** ラベルの付いた **ConfigMap** および **ImageStream** オブジェクトから Pod テンプレートをインポートしなくなりました。
今回の更新により、受け入れ可能なラベル仕様が修正され、プラグインが **jenkins-agent** ラベルを持つ **ConfigMap** および **ImageStream** オブジェクトから Pod テンプレートをインポートするようになりました。(2034839)

クラウドコンピュート

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) でマシン仕様を編集すると、OpenShift Container Platform はマシンの削除および再作成を試行します。その結果、ホストされていたノードの回復不能な損失が発生していました。今回の修正により、作成後にマシン仕様に追加された編集が無視されるようになりました。(**BZ#1962066**)

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) で実行されるクラスターでは、Floating IP アドレスはマシンオブジェクトについて報告されませんでした。その結果、kubelet によって作成された証明書署名要求 (CSR) は受け入れられず、ノードがクラスターに参加できなくなりました。すべての IP アドレスがマシンオブジェクトについて報告されるようになりました。(**BZ#2022627**)

- 以前のバージョンでは、再度キューに入れる前に AWS マシンが更新されていないことを確認します。そのため、AWS マシンの仮想マシンが削除されても、そのオブジェクトが引き続き利用可能であった場合に問題が生じました。これが生じると、AWS マシンは無限ループで再度キューに入れられ、削除したり更新したりできませんでした。今回の更新により、AWS マシンが再度キューに入れる前に更新されないように使用されたチェックが復元されます。その結果、マシンが更新されても再度キューに置かれなくなりました。(**BZ#2007802**)

- 以前のバージョンでは、セレクターを変更すると、マシンセットが観察されるマシンのリストを変更しました。その結果、マシンセットがすでに作成されているマシンの追跡を失ったためにリークが発生する可能性がありました。今回の更新により、セレクターの作成後、セレクターがイミュータブルになります。その結果、マシンセットが正しいマシンをリスト表示するようになりました。(**BZ#2005052**)

- 以前のバージョンでは、仮想マシンテンプレートにスナップショットがある場合、**LinkedClone** 操作の正しくない使用により、誤ったディスクサイズが選択されていました。今回の更新で、すべての状況で、デフォルトのクローン操作が **fullClone** に変更されるようになりました。**linkedClone** はユーザーが指定するようにする必要があります。(BZ#2001008)

- 以前のバージョンでは、カスタムリソース定義 (CRD) スキーマの要件は数値を許可しませんでした。そのため、アップグレード中にエラーをマーシャルしました。今回の更新により、スキーマの要件が修正され、文字列と数値の両方が許可されます。その結果、マーシャルエラーは API サーバー変換によって報告されなくなりました。(BZ#1999425)

- 以前のバージョンでは、Machine API Operator を移動するか、Pod が名前変更の結果としてデプロイされた場合、**MachineNotYetDeleted** メトリクスはモニターされるマシンごとにリセットされました。今回の更新により、メトリッククエリーがソース Pod ラベルを無視するよう変更されました。その結果、**MachineNotYetDeleted** メトリックは、Machine API Operator Pod の名前が変更されたシナリオで適切にアラートされるようになりました。(BZ#1986237)

- 以前のバージョンでは、vSphere の egress IP は kubelet 内の vSphere クラウドプロバイダーによって選択されました。これらは証明書署名要求 (CSR) 承認者によって予期しないものでした。そのため、egress IP を持つノードには CSR 更新が承認されませんでした。今回の更新により、CSR 承認者は egress IP について考慮できるようになりました。その結果、vSphere SDN クラスターで egress IP が設定されたノードが引き続き機能し、有効な CSR 更新が含まれるようになりました。(BZ#1860774)

- 以前のバージョンでは、ワーカーノードは起動に失敗し、ディスクイメージの破損パスのデフォルトおよび Google Cloud Platform (GCP) SDK の互換性のない変更により、インストールプログラムは URL イメージの生成に失敗しました。その結果、マシンコントローラーはマシンを作成できませんでした。今回の修正により、GCP SDK のベースパスを変更して URL イメージを修復できるようになりました。(BZ#2009111)

- 以前のバージョンでは、vCenter の **powerOff** タスクのラグが原因で、削除プロセス中にマシンがフリーズしていました。VMware はマシンの電源がオフの状態に表示されましたが、OpenShift Container Platform はこれを電源がオンと報告し、削除プロセスでマシンがフリーズしました。今回の更新により、データベースから削除するタスクが作成される前に、vSphere の **powerOff** タスク処理が改善され、削除プロセス時にマシンがフリーズしなくなりました。(BZ#2011668)

- OpenShift Container Platform のインストールまたは更新後に、メトリックの値には、最後の CSR が調整された後に保留中の CSR が 1 つ表示されました。これにより、保留中の CSR がない場合、メトリックが保留中の CSR を 1 つ報告しました。今回の修正により、各調整ループの終了時にメトリックを更新して、保留中の CSR 数が常に有効な後に有効になりました。(BZ#2013528)

- 以前のバージョンでは、AWS は **cloud-provider** フラグが空の文字列に設定されている場合に認証情報の有無を確認していました。認証情報は、AWS 以外のプラットフォームでもメタデータサービスへの呼び出しを実行して確認されました。これにより、ECR プロバイダーの起動および AWS 認証情報エラー (AWS 以外のなど) がすべてのプラットフォームに記録されるレイテンシーが生じました。今回の修正により、認証情報チェックがメタデータサービスに要求を実行しなくなり、認証情報エラーがログに記録されなくなりました。(BZ#2015515)

- 以前のバージョンでは、マシン API は、AWS が API 全体で仮想マシンの作成と通信する前に、マシンを調整することがありました。その結果、AWS は仮想マシンが存在しないことを報告し、マシン API がこれが失敗したと判断しました。今回のリリースにより、Machine API は AWS API が同期してからマシンをプロビジョニング済みとしてマークしようとするまで待機します。(BZ#2025767)

- 以前のバージョンでは、UPI クラスター上に同時に作成される多数のノードにより、多数の

CSR が生成される可能性がありました。その結果、承認者は保留中の証明書要求が 100 を超える場合に証明書の承認を停止するため、証明書の更新は自動化されませんでした。今回のリリースにより、承認のカットオフおよび UPI クラスターを計算する際に、既存ノードが大規模な更新要求であっても、自動化された証明書の更新を活用できるようになりました。(BZ#2028019)

- 以前のバージョンでは、マシン API コントローラーに埋め込まれたインスタンスタイプのリストが古くなっていました。これらのインスタンスタイプの一部は不明なため、scale-from-zero 要件にはアノテーションが付けられませんでした。今回のリリースにより、生成されたリストが更新され、新しいインスタンスタイプのサポートが含まれるようになりました。(BZ#2040376)

- 以前のバージョンでは、AWS Machine API コントローラーは IO1 タイプ以外のブロックデバイスの IOPS 値を設定していなかったため、GP3 ブロックデバイスの IOPS フィールドは無視されていました。今回のリリースにより、IOPS が対応しているすべてのブロックデバイスタイプに設定され、ユーザーはマシンに接続されているブロックデバイスの IOPS を設定できるようになりました。(BZ#2040504)

Cloud Credential Operator

- 以前のバージョンでは、Azure クラスターで Cloud Credential Operator を手動モードで使用する場合は、**Upgradeable** ステータス が **False** に設定されませんでした。この動作は、他のプラットフォームで異なります。今回のリリースにより、手動モードで Cloud Credential Operator を使用する Azure クラスターの **Upgradeable** ステータスが **False** に設定されるようになりました。(BZ#1976674)

- 以前のバージョンでは、Cloud Credential Operator によって作成される不要な **controller-manager-service** サービスリソースは依然として存在していました。今回のリリースにより、Cluster Version Operator がこれをクリーンアップできるようになりました。(BZ#1977319)

- 以前のバージョンでは、**CredentialsRequest** カスタムリソースの Cloud Credential Operator のログレベル設定への変更は無視されました。今回のリリースにより、**CredentialsRequest** カスタムリソースを編集して、ロギングの詳細度を制御できます。(BZ#1991770)

- 以前のバージョンでは、AWS が Red Hat OpenStack Platform (RHOSP) のデフォルトシークレットとなる場合に、Cloud Credential Operator (CCO) Pod が継続的なエラーで再起動していました。この更新により、CCO Pod のデフォルト設定が修正され、CCO Pod が失敗するのを防ぎます。(BZ#1996624)

Cluster Version Operator

- 以前のバージョンでは、Pod はマニフェストの一部ではない無効なマウント要求により起動に失敗する可能性がありました。今回の更新により、Cluster Version Operator (CVO) は、マニフェストに含まれていないクラスター内のリソースからボリュームおよびボリュームマウントを削除するようになりました。これにより、Pod が正常に起動できます。(BZ#2002834)

- 以前のバージョンでは、モニタリング証明書がローテーションされる際に、Cluster Version Operator (CVO) はエラーをログに記録し、CVO Pod を手動で再起動するまでモニタリングがメトリクスをクエリーできませんでした。今回の更新により、CVO は証明書ファイルを監視し、証明書ファイルが変更されるたびにメトリック接続を自動的に再作成するようになりました。(BZ#2027342)

コンソールストレージプラグイン

- 以前のバージョンでは、永続ボリューム (PV) がプロビジョニングされ、容量が **0** TiB であった間にロードプロンプトが表示されませんでした。これにより、混乱を生じさせるシナリオが作成されました。今回の更新により、ロード状態用にローダーが追加され、PV がプロビジョニン

グされているか、容量が決定される場合にユーザーに詳細情報を提供するようになりました。また、プロセス内のエラーについてユーザーに通知します。(BZ#1928285)

- 以前のバージョンでは、特定の場所で文法は修正されず、トランスレーターがコンテキストを解釈できないインスタンスがありました。これにより、読みやすさに悪影響を及ぼしていました。今回の更新で、さまざまな場所の文法が修正され、トランスレーターのストレージクラスが項目化され、全体の読みやすさが改善されました。(BZ#1961391)

- 以前は、ブロックプールページ内でプールを押すと、削除後に最終的な **Ready** フェーズが永続化されていました。その結果、プールは削除後でも **Ready** 状態にありました。この更新により、ユーザーは **Pools** ページにリダイレクトされ、破棄後にプールが更新されます。(BZ#1981396)

DNS (Domain Name System)

- 以前のバージョンでは、DNS Operator は **spec.servers** を使用して設定されたアップストリームリゾルバーからの応答をキャッシュしませんでした。今回の更新により、DNS Operator はすべてのアップストリームサーバーからの応答をキャッシュするようになりました。(BZ#2006803)

- 以前のバージョンでは、DNS Operator はカスタムアップストリームリゾルバーのサーバーブロックで **prometheus** プラグインを有効にしませんでした。そのため、CoreDNS はアップストリームリゾルバーのメトリックや、デフォルトサーバーブロックのメトリックのみを報告しませんでした。今回の更新により、DNS Operator はすべてのサーバーブロックで **prometheus** プラグインを有効にするために変更されました。CoreDNS は、カスタムアップストリームリゾルバーの Prometheus メトリックを報告するようになりました。(BZ#2020489)

- 以前のバージョンでは、応答が 512 文字を超えるアップストリーム DNS により、アプリケーションが失敗しました。これは、DNS が解決できなかったために GitHub からリポジトリーをクローンできないために生じました。今回の更新により、GitHub からの名前解決を回避するために、KNI CoreDNS の **bufsize** が 521 に設定されるようになりました。(BZ#1991067)

- DNS Operator がオペランドを調整すると、Operator はクラスター DNS サービスオブジェクトを API から取得し、Operator がサービスを作成または更新する必要があるかどうかを判別します。サービスがすでに存在する場合、Operator はこれを Operator が取得する必要のある内容と比較して、更新が必要であるかどうかを判別します。OpenShift Container Platform 4.9 をベースとする Kubernetes 1.22 では、サービスに新規の **spec.internalTrafficPolicy** API フィールドが導入されました。Operator はサービスの作成時にこのフィールドを空のままにしますが、API はこのフィールドのデフォルト値を設定します。Operator はこのデフォルト値を確認し、フィールドを空の値に更新しようと試みました。これにより、Operator の更新ロジックがサービスの内部トラフィックポリシーに対して API セットのデフォルト値を継続的に元に戻すことができませんでした。今回の修正により、サービスを比較して更新が必要であるかどうかを判別する場合、Operator は **spec.internalTrafficPolicy** の空の値とデフォルト値を処理するようになりました。その結果、API がサービスの **spec.internalTrafficPolicy** フィールドのデフォルト値を設定する場合、Operator はクラスターの DNS サービスの更新を誤って試行しなくなりました。(BZ#2002461)

- 以前のバージョンでは、DNS Operator は、**dnses.operator.openshift.io/default** オブジェクトの **spec.servers** フィールドのエントリーに対応する CoreDNS **Corefile** 設定マップのサーバーブロックの cache プラグインを有効にしませんでした。そのため、CoreDNS は **spec.servers** を使用して設定されたアップストリームリゾルバーからの応答をキャッシュしませんでした。今回のバグ修正により、DNS Operator は、Operator がすでにデフォルトのサーバーブロックに設定されたのと同じパラメーターを使用して、すべてのサーバーブロックの cache プラグインを有効にするように変更されました。CoreDNS は、すべてのアップストリームリゾルバーからの応答をキャッシュするようになりました。(BZ#2006803)

Image Registry

- 以前のバージョンでは、レジストリーは内部的に **\docker.io** 参照を **\registry-1.docker.io** を参照し、これを認証情報を保存するために使用していました。その結果、**\docker.io** イメージの認証情報が配置されませんでした。今回の更新により、認証情報の検索時に **\registry-1.docker.io** のホスト名が **\docker.io** に戻されました。その結果、レジストリーは **\docker.io images** の認証情報を正しく検索できます。(BZ#2024859)

- 以前のバージョンでは、イメージプルーナージョブは失敗時に再試行されませんでした。その結果、単一の失敗により、次回の実行時にイメージレジストリー Operator が低下する可能性がありました。今回の修正により、プルーナーに関連する一時的な問題はイメージレジストリー Operator の低下が生じなくなりました。(BZ#2051692)

- 以前のバージョンでは、イメージレジストリー Operator はインフォーマーからオブジェクトを変更していました。その結果、これらのオブジェクトは通知者によって同時に変更され、競合状態が発生する可能性があります。今回の修正により、コントローラーおよびインフォーマーはオブジェクトのコピーが異なるため、競合状態が設定されなくなりました。(BZ#2028030)

- 以前のバージョンでは、Image Registry Operator の設定オブジェクトの場所に問題があるため、**TestAWSFinalizerDeleteS3Bucket** は失敗しました。今回の更新により、設定オブジェクトが適切な場所に保存されるようになりました。その結果、Image Registry Operator は **TestAWSFinalizerDeleteS3Bucket** の実行時にパニックしなくなりました。(BZ#2048443)

- 以前のバージョンでは、エラー処理により、**access denied** エラーが **authentication required** として出力されました。このバグにより、誤ったエラーログが生じました。Docker ディストリビューションエラー処理により、エラー出力が **authentication required** するために **access denied** から変更されました。**access denied** エラーにより、より正確なエラーログが表示されるようになりました。(BZ#1902456)

- 以前のバージョンでは、レジストリーはシャットダウン要求で即座に終了していました。その結果、ルーターはレジストリー Pod が削除され、要求を送信することを検出するための時間がありませんでした。今回の修正により、Pod が削除されると、他のコンポーネントが削除を検出するための追加の秒数についてアクティブな状態を維持するようになりました。今回のリリースより、ルーターはアップグレード時に存在しない Pod に要求を送信しないため、中断が生じなくなりました。(BZ#1972827)

- 以前のバージョンでは、レジストリーは最初に利用可能なミラーリングされたレジストリーからの応答をプロキシーしていました。ミラーレジストリーが利用可能であるものの、要求されたデータがない場合、プルスルーは必要なデータが含まれる場合でも他のミラーの使用を試行しませんでした。今回の修正により、最初のミラーが **Not Found** で応答した場合、プルスルーは他のミラーレジストリーを試行します。プルスルーはミラーレジストリーに存在する場合にデータを検出できるようになりました。(BZ#2008539)

イメージストリーム

- 以前のバージョンでは、イメージポリシーの受付プラグインはデプロイメント設定を認識せず、ステートフルセットを更新する可能性がありました。そのため、**resolve-names** アノテーションが使用されると、イメージストリームの参照はデプロイメント設定で解決されないままでした。このプラグインが更新され、デプロイメント設定およびステートフルセットのアノテーションを解決するようになりました。その結果、イメージストリームタグは作成/編集されたデプロイメント設定で解決されます。(BZ#2000216)

- 以前のバージョンでは、グローバルプルシークレットが更新されると、既存の API サーバー Pod プルシークレットが更新されませんでした。これで、プルシークレットのマウントポイントが **/var/lib/kubelet/config.json** ファイルから **/var/lib/kubelet** ディレクトリーに変更されるようになりました。その結果、更新されたプルシークレットが既存の API サーバー Pod に表示されるようになりました。(BZ#1984592)

- 以前のバージョンでは、イメージの受付プラグインはデプロイメント設定テンプレート内のア

ノテーションを確認しませんでした。そのため、デプロイメント設定テンプレート内のアノテーションはレプリカコントローラーで処理できず、無視されました。イメージの受付プラグインはデプロイメント設定のテンプレートを分析するようになりました。今回の修正により、イメージの受付プラグインはデプロイメント設定およびテンプレートでアノテーションを認識するようになりました。(BZ#2032589)

Installer

- Open Shift Container Platform Baremetal IPI インストーラーは、以前は、**master** ロールを持つホストをフィルタリングするのではなく、**install-config** のホストで定義された最初のノードをコントロールプレーンノードとして使用していました。**master** ノードと **worker** ノードのロールは、定義時に認識されるようになりました。(BZ#2003113)

- 今回の更新以前は、プロビジョニングネットワーク CIDR でホストビットを設定することができました。これにより、プロビジョニング IP が予想されたものと異なるため、プロビジョニングネットワークの他の IP アドレスとの競合が生じる可能性がありました。今回の更新により、検証により、プロビジョニングネットワーク CIDR にホストビットが含まれません。プロビジョニングネットワーク CIDR にホストビットが含まれる場合、インストールプログラムは停止し、エラーメッセージをログに記録します。(BZ#2006291)

- 以前のリリースでは、プリフライトチェックは Red Hat OpenStack Platform (RHOSP) リソースの使用状況を考慮しませんでした。その結果、クォータではなく使用率が正しくない場合に、これらのチェックは正しくないエラーメッセージを出して失敗し、インストールが妨げられていました。プリフライトチェックが RHOSP のクォータと使用状況の両方を処理するようになりました。クォータは十分ですが、リソースがない場合、チェックは正しいエラーメッセージを出して失敗します。(BZ#2001317)

- 今回の更新以前は、設定ファイルから PVC を作成する際に、oVirt Driver は ReadOnlyMany (ROX) および ReadWriteMany (RWX) アクセスモードを指定できました。これにより、ドライバーは共有ディスクをサポートしないため、これらのアクセスモードに対応できませんでした。今回の更新により、アクセスモードは単一ノードアクセスに制限されるようになりました。システムは、PVC の作成時に ROX または RWX を指定し、エラーメッセージをログに記録できないようにします。(BZ#1882983)

- 以前のバージョンでは、Terraform プロバイダーでのディスクアップロードが適切に処理されませんでした。その結果、OpenShift Container Platform インストールプログラムは失敗しました。今回の更新により、ディスクのアップロード処理が修正され、ディスクのアップロードに成功するようになりました。(BZ#1917893)

- 以前のバージョンでは、特殊サイズで Microsoft Azure 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は、仮想 CPU(vCPU) の合計数がクラスターをデプロイするために最小リソース要件を満たすかどうかを確認する必要がありました。そのため、これによりインストールエラーが発生する可能性がありました。今回の更新で、インストールプログラムにより、利用可能な仮想 CPU の合計数から仮想 CPU の数に変更が加えられました。その結果、仮想マシンのサイズが最小リソース要件を満たしていないことを Operator に認識できるようにする簡潔なエラーメッセージが出されます。(BZ#2025788)

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) の RAM 検証では、誤ったユニットを使用して値がないかを確認していました。そのため、検証では、最小 RAM 要件を満たしていないフレーバーを受け入れていました。今回の修正により、RAM 検証で RAM が不足していたフレーバーを拒否するようになりました。(BZ#2009699)

- 以前は、Open Shift Container Platform コントロールプレーンノードは、Red Hat Open Stack Platform (RHOSP) でスケジュール可能でデプロイされたときに、Ingress セキュリティーグループルールがありませんでした。その結果、RHOSP での OpenShift Container Platform デプロイメントは、専用のワーカーを持たないコンパクトなクラスターについて失敗していました。この修正により、コントロールプレーンノードがスケジュール可能である場合に、Red

Hat Open Stack Platform (RHOSP) に Ingress セキュリティーグループルールが追加されます。コンパクトな 3 ノードクラスターを RHOSP にデプロイできるようになりました。(BZ#1955544)

- 以前のバージョンでは、無効な AWS リージョンを指定した場合、インストールプログラムはアベイラビリティーゾーンの試行と検証を続行しました。これにより、タイムアウトする前にインストールプログラムが 60 分間応答しなくなりました。インストールプログラムは、アベイラビリティーゾーンの前に AWS リージョンおよびサービスエンドポイントを検証するようになりました。これにより、インストーラープログラムがエラーを報告するのにかかる時間が短縮されました。(BZ#2019977)

- 以前は、vCenter のホスト名が数字で始まっている場合、VMwarev Sphere にクラスターをインストールできませんでした。インストールプログラムが更新され、このタイプのホスト名が無効として扱われなくなりました。これで、vCenter のホスト名が数字で始まる場合、クラスターは正常にデプロイされます。(BZ#2021607)

- 以前のバージョンでは、クラスターを Microsoft Azure にデプロイする際にカスタムディスクインスタンスタイプを指定した場合、クラスターはデプロイされない可能性がありました。これは、インストールプログラムが最小リソース要件を満たすことを誤って判断したために生じました。インストールプログラムが更新され、選択したリージョンのインスタンスタイプで利用可能な vcpus の数が最小リソース要件を満たさない場合にエラーを報告するようになりました。(BZ#2025788)

- 以前のバージョンでは、AWS クラスターのデプロイ時にカスタム IAM ロールを定義した場合、クラスターのアンインストール後にブートストラップインスタンスのプロファイルを手動で削除する必要がある場合があります。断続的に、インストールプログラムはブートストラップインスタンスプロファイルを削除しませんでした。インストールプログラムが更新され、クラスターのアンインストール時にすべてのマシンインスタンスプロファイルが削除されます。(BZ#2028695)

- 以前のバージョンでは、デフォルトのプロビジョニング IP 値は、ホストビットがプロビジョニングネットワーク CIDR に設定されている場合に変わりませんでした。これにより、プロビジョニング IP の値が想定とは異なる値になりました。この違いにより、プロビジョニングネットワークの他の IP アドレスと競合していました。今回の修正により、ProvisioningNetworkCIDR にホストビットが設定されていないことを確認する検証が追加されました。その結果、ProvisioningNetworkCIDR にホストビットが設定されている場合、インストールプログラムは停止し、検証エラーを報告します。(BZ#2006291)

- 以前のリリースでは、BMC ドライバー IPMI はセキュアな UEFI ブートでサポートされませんでした。これにより、起動に失敗していました。今回の修正により、**UEFISecureBoot** モードがベアメタルドライバーで使用されていないことを確認する検証チェックが追加されました。これにより、セキュアな UEFI ブートは成功します。(BZ#2011893)

- 今回の更新により、4.8 UPI テンプレートは、Ignition バージョンに一致するようにバージョン 3.1.0 から 3.2.0 に更新されました。(BZ#1949672)

- 以前は、ベースレジストリーのコンテンツをミラーリングするように求められた場合、Open Shift Container Platform インストールプログラムは、 **image Content Sources** の誤った **install-config** ファイル値を引用して、検証エラーで終了していました。この更新により、インストールプログラムは **imageContentSources** の値をベースレジストリー名を指定することを許可し、ベースレジストリー名を指定するとインストールプログラムが終了しなくなりました。(BZ#1960378)

- 以前のバージョンでは、UPI ARM テンプレートは、作成した仮想マシン (VM) インスタンスに SSH キーを割り当てていました。その結果、ユーザーが提供した SSH キーが **ed25519** タイプになると、仮想マシンの作成に失敗します。今回の更新で、ユーザーが提供した SSH キーのタイプに関係なく、仮想マシンの作成が成功するようになりました。(BZ#1968364)

- **aws_vpc_dhcp_options_association** リソースを正常に作成した後も、AWS がリソースが存在しないことを依然として報告する可能性があります。そのため、AWS Terraform プロバイダーがインストールに失敗します。今回の更新により、AWS がリソースが存在すると報告されるまで、作成後の期間、**aws_vpc_dhcp_options_association** リソースのクエリーを再試行できるようになりました。そのため、AWS が **aws_vpc_dhcp_options_association** リソースが存在しないことを AWS が報告する場合でも、インストールは成功します。(BZ#2032521)

- 以前のバージョンでは、ローカルゾーンを有効にして AWS に OpenShift Container Platform をインストールする際に、インストールプログラムはアベイラビリティーゾーンではなく、ローカルゾーンにいくつかのリソースを作成できました。これにより、ロードバランサーがローカルゾーンでは実行できないため、インストールプログラムが失敗しました。今回の修正により、インストールプログラムはローカルゾーンを無視し、クラスターコンポーネントをインストールする際にアベイラビリティーゾーンのみを考慮しました。(BZ#1997059)

- 以前のバージョンでは、terraform は設定ファイルの作成の終了前にブートストラップ Ignition 設定ファイルの Azure へのアップロードを試行する可能性がありました。ローカルファイルの作成前にアップロードが開始されると、インストールは失敗します。今回の修正により、terraform は、最初にローカルコピーを作成するのではなく、Ignition 設定ファイルを Azure に直接アップロードできるようになりました。(BZ#2004313)

- 以前のバージョンでは、**cluster-bootstrap** および Cluster Version Operator コンポーネントが、同じリソースのマニフェストを同時に Kubernetes API に書き込みしようとすると競合状態が発生する可能性がありました。これにより、**Authentication** リソースがデフォルトのコピーによって上書きされ、そのリソースに対して行われたカスタマイズが削除される可能性がありました。今回の修正により、Cluster Version Operator はインストールプログラムに含まれるマニフェストを上書きすることがブロックされました。これにより、**Authentication** リソースにユーザー指定のカスタマイズが上書きされないようにします。(BZ#2008119)

- 以前のバージョンでは、OpenShift Container Platform を AWS にインストールする際に、インストールプログラムは **m5.large** インスタンスタイプを使用してブートストラップマシンを作成していました。これにより、インスタンスタイプが使用できないリージョンでインストールが失敗していました。今回の修正により、ブートストラップマシンはコントロールプレーンマシンと同じインスタンスタイプを使用するようになりました。(BZ#2016955)

- 以前は、AWS に OpenShift Container Platform をインストールするときに、インストールプログラムが EC2G および Intel Virtualization Technology (VT) インスタンスを認識せず、デフォルトで X インスタンスに設定されていました。これにより、これらのインスタンスに誤ったインスタンスクォータが適用されていました。この修正により、インストールプログラムは EC2 G インスタンスおよび VT インスタンスを認識し、正しいインスタンスクォータを適用するようになりました。(BZ#2017874)

Kubernetes API サーバー
Kubernetes Scheduler

- 今回の更新以前は、現行リリースへのアップグレードは、**TaintandToleration**、**NodeAffinity**、および **InterPodAffinity** パラメーターの正しい重みを設定しませんでした。今回の更新により問題が解決され、**TaintandToleration** の重みが **3**、**NodeAffinity** が **2** に、および **InterPodAffinity** が **2** に設定されるようになりました。(BZ#2039414)

- OpenShift Container Platform 4.10 では、非セキュアなメトリックを提供するコードは **kube-scheduler** コードベースから削除されます。今回のリリースより、メトリックはセキュアなサーバー経由でのみ提供されるようになりました。バグ修正とサポートは、今後のライフサイクルの終了により提供されます。その後は、新たな拡張機能は行われません。(BZ#1889488)

Machine Config Operator

- 以前のバージョンでは、Machine Config Operator (MCO) がディスクに保存される保留中の設定の変更がオペレーティングシステム (OS) の変更が適用される前に適用されました。その結果、電源の損失などの状況では、MCO は OS の変更が再起動時にすでに適用されていると仮定し、**kargs** や **kernel-rt** などの変更で検証が省略されていました。今回の更新で、OS の変更が適用された後にディスクへの設定変更が保存されるようになりました。設定アプリケーション中に電源が失われた場合、MCO は再起動時に設定アプリケーションを再度試行する必要があることを認識するようになりました。(BZ#1916169)

- 以前のバージョンでは、**baremetal-runtimecfg** プロジェクトの Kubernetes クライアントライブラリーの以前のバージョンにより、VIP フェイルオーバー後にクライアント接続を適時に閉じることができませんでした。これにより、API に依存するモニターコンテナーが長い時間がかかる可能性がありました。今回の更新により、VIP フェイルオーバー後にクライアント接続をタイムリーにクローズできるようになりました。(BZ#1995021)

- 以前のバージョンでは、SSH キーを更新する際に、Machine Config Operator (MCO) は **authorized_keys** ファイルの所有者とグループを **root** に変更しました。この更新により、MCO は **authorized_keys** ファイルの更新時に **core** を所有者およびグループとして保持するようになりました。(BZ#1956739)

- 以前は、**clone_slave_connection** 関数により送信される警告メッセージが誤って **new_uuid** 変数に保存されていたため、接続の UUID のみを保存することが意図されていました。そのため、誤った値が **new_uuid** 変数に保存されるため、**new_uuid** 変数を含む **nmcli** コマンドが失敗しました。今回の修正により、**clone_slave_connection** 関数の警告メッセージが **stderr** にリダイレクトされるようになりました。**new_uuid** 変数を参照する **nmcli** コマンドは失敗しなくなりました。(BZ#2022646)

- 以前のバージョンでは、古いバージョンの Kubernetes クライアントライブラリーが **baremetal-runtimecfg** プロジェクトに存在していました。仮想 IP(VIP) が失敗すると、クライアント接続がタイムリーに閉じられない可能性があります。これにより、API との通信に依存するモニターコンテナーが長い時間がかかる可能性がありました。今回の修正により、クライアントライブラリーが更新されました。今回のリリースより、接続は VIP フェイルオーバーで予想通りに閉じられ、モニターコンテナーは長時間ハングしなくなりました。(BZ#1995021)

- 今回の更新以前は、Machine Config Operator (MCO) がディスクに保存される保留中の設定変更は、それらを Red Hat Enterprise Linux CoreOS (RHCOS) に適用する前にディスクに適用していました。設定の適用から MCO の電源が失われた場合、これは設定の適用に応じて処理され、変更を検証しませんでした。この設定に無効な変更が含まれる場合、適用は失敗します。今回の更新により、MCO は適用後にのみ設定をディスクに保存します。これにより、MCO が設定を適用する際に電源が失われた場合、再起動後に設定が再適用されます。(BZ#1916169)

- 今回の更新以前は、Machine Config Operator (MCO) を使用して SSH キーを作成または更新すると、**authorized_keys** ファイルの所有者およびグループを **root** に設定します。今回の更新で問題が解決されました。MCO が **authorized_keys** ファイルを作成または更新すると、ファイルの所有者およびグループとして **core** を正しく設定または保持されます。(BZ#1956739)

- 以前のバージョンでは、Stateless Address AutoConfiguration (SLAAC) を使用するクラスターでは、Ironic **addr-gen-mode** パラメーターが OVNKubernetes ブリッジに永続化されませんでした。その結果、ブリッジの作成時に IPv6 アドレスが変更される可能性がありました。ノード IP の変更はサポートされていないため、これによりクラスターが中断します。この修正では、ブリッジの作成時に **addr-gen-mode** パラメーターが永続化されるようになりました。IP アドレスは、デプロイメントプロセス全体で一貫性を保つようになりました。(BZ#1990625)

- 以前のバージョンでは、マシン設定に **spec.config.storage.files.contents.compression** パラメーターが **gzip** に設定されている圧縮ファイルが含まれる場合、Machine Config Daemon (MCD) は圧縮ファイルを抽出せずにディスクに誤って書き込みました。今回の修正により、圧縮パラメーターが **gzip** に設定されている場合、MCD は圧縮ファイルを抽出するようになりました。(BZ#1970218)

- 以前のバージョンでは、**systemd** ユニットは完全に削除された場合にのみクリーンアップされました。そのため、**systemd** ユニットが完全に削除されていない限り、マスクが削除されないため、**systemd** ユニットはマシン設定を使用してマスクを解除できませんでした。今回の修正により、マシン設定で **systemd** ユニットを **mask: true** として設定すると、既存のマスクが削除されるようになりました。これにより、**systemd** ユニットをマスク解除できるようになりました。(BZ#1966445)

管理コンソール

- 以前のバージョンでは、OperatorHub カテゴリーおよびカードリンクに有効な **href** 属性が含まれていませんでした。そのため、OperatorHub カテゴリーおよびカードリンクを新規タブで開くことができませんでした。今回の更新により、OperatorHub カテゴリーおよびカードリンクに有効な **href** 属性が追加されました。その結果、OperatorHub およびそのカードリンクを新規タブで開くことができます。(BZ#2013127)

- 以前のバージョンでは、Operand Details ページで、**status.conditions** プロパティーの条件テーブルが他のすべてのテーブルの前に常にレンダリングされる特別なケースが作成されました。そのため、**status.conditions** テーブルは記述子の順序ルールに従いなかったため、ユーザーがテーブルの順序を変更しようとすると予期しない動作が生じました。今回の更新により **status.conditions** の特別なケースが削除され、そのプロパティーに記述子が定義されていない場合のみ最初にレンダリングするのはデフォルトになります。その結果、記述子がプロパティーで定義されると、**status.condition** のテーブルは記述子の順序ルールに基づいてレンダリングされます。(BZ#2014488)

- 以前のバージョンでは、**Resource Details** ページの metrics タブはクラススコープの Thanos エンドポイントを超えていました。そのため、このエンドポイントの承認のないユーザーは、すべてのクエリーについての **401** 応答を受け取ります。今回の更新により、Thanos テナンシーエンドポイントが更新され、冗長な namespace クエリー引数が削除されるようになりました。その結果、正しいロールベースアクセス制御 (RBAC) パーミッションを持つユーザーは、**Resource Details** ページの metrics タブでデータを確認できるようになりました。(BZ#2015806)

- 以前のバージョンでは、Operator が API を既存の API グループに追加する際に、API 検出がトリガーされませんでした。そのため、ページが更新されるまで、フロントエンドには新規 API が表示されませんでした。今回の更新により、ページの更新なしにフロントエンドで表示される Operator によって API が追加されます。(BZ#1815189)

- 以前は、Red Hat OpenStack Platform (RHOSP) の Red Hat OpenShift Cluster Manager では、コントロールプレーンは簡体字中国語に変換されていませんでした。そのため、命名は OpenShift Container Platform ドキュメントとは異なります。この更新により、Red Hat OpenShift Cluster Manager の翻訳の問題が修正されます。(BZ#1982063)

- 以前は、Red Hat OpenShift Cluster Manager での仮想テーブルのフィルタリングが機能していませんでした。そのため、利用可能なすべての **nodes** が検索後に表示されませんでした。この更新には、Red Hat OpenShift Cluster Manager のフィルタリングの問題を修正する新しい仮想テーブルロジックが含まれています。(BZ#1990255)

モニタリング

- 以前のバージョンでは、OpenShift Container Platform のアップグレード時に、2 つの Prometheus Pod が同じノードにあるか、Pod が同じ間隔で再起動されるために Prometheus サービスが利用できなくなる可能性がありました。この状態は、Prometheus Pod にはノードの配置に関するソフト非アフィニティールールがあり、**PodDisruptionBudget** リソースがプロビジョニングされていないために生じました。そのため、メトリックは収集されず、ルールが一定期間評価されませんでした。
  この問題を修正するために、Cluster Monitoring Operator(CMO) は 2 つの Prometheus Pod が異なるノードにスケジュールされるようにハード非アフィニティールールを設定するようにな

りました。CMO は **PodDisruptionBudget** リソースもプロビジョニングし、1 つ以上の Prometheus Pod が常に実行されていることを確認します。その結果、アップグレード時に、ノードは 1 つ以上の Prometheus Pod が常に実行されるように順番に再起動するようになりました。(BZ#1933847)

- 以前のバージョンでは、2 つの Thanos Ruler Pod が含まれるノードが停止した場合に、Thanos Ruler サービスが利用不可能になりました。この状況は、Thanos Ruler Pod にはノードの配置に関するソフト非アフィニティールールのみがあるために発生しました。そのため、ユーザー定義のルールは、ノードがオンラインに戻るまで評価されませんでした。
  今回のリリースにより、Cluster Monitoring Operator (CMO) はハード非アフィニティールールを設定し、2 つの Thanos Ruler Pod が異なるノードにスケジュールされるようになりました。その結果、単一ノードの停止により、ユーザー定義のルール評価にギャップが発生しなくなりました。(BZ#1955490)

- 以前のバージョンでは、2 つの Prometheus Pod が同じノードにあり、ノードが停止すると Prometheus サービスが利用できませんでした。この状態は、Prometheus Pod にはノードの配置に関するソフト非アフィニティールールのみがあるために発生しました。そのため、メトリックは収集されず、ノードがオンラインに戻るまでルールは評価されませんでした。
  今回のリリースにより、Cluster Monitoring Operator はハード非アフィニティールールを設定して、2 つの Prometheus Pod が異なるノードにスケジュールされるようになりました。その結果、Prometheus Pod は異なるノードにスケジュールされ、単一ノードの停止により、モニタリングにギャップが生じることはなくなりました (BZ#1949262)。

- 以前のバージョンでは、OpenShift Container Platform のパッチのアップグレード時に、3 つの Alertmanager Pod が同じノードにあるか、Alertmanager Pod を実行しているノードが同時に再起動されるため、Alertmanager サービスが利用できなくなる可能性がありました。この状態は、Alertmanager Pod にはノードの配置に関するソフト非アフィニティールールがあり、**PodDisruptionBudget** がプロビジョニングされていないために失敗しました。本リリースでは、ハード非アフィニティールールおよび **PodDisruptionBudget** リソースが有効になり、Alertmanager およびその他のモニタリングコンポーネントのパッチアップグレード時のダウンタイムがなくなりました。(BZ#1955489)

- 以前のバージョンでは、多くの Docker イメージでファイルシステム領域が占有されると、誤検出 **NodeFilesystemSpaceFillingUp** アラートはトリガーされていました。このリリースでは、**NodeFilesystemSpaceFillingUp** 警告アラートを発生させるしきい値が 40% ではなく 20% の空きスペースに減少し、誤検知アラートの発生を停止します。(BZ#1987263)

- 以前のバージョンでは、ユーザー定義のモニタリングが有効にされている場合に、Prometheus Operator コンポーネントのアラートは **openshift-user-workload-monitoring** namespace を実行する Prometheus Operator には適用されませんでした。そのため、**openshift-user-workload-monitoring** namespace を管理する Prometheus Operator で問題が発生した場合にアラートが発生しませんでした。
  今回のリリースにより、アラートが変更され、**openshift-monitoring** および **openshift-user-workload-monitoring** namespace の両方をモニターできるようになりました。その結果、クラスター管理者は、ユーザー定義のモニタリングを管理する Prometheus Operator で問題が発生した場合にアラート通知を受信するようになりました。(BZ#2001566)

- 以前のバージョンでは、**node-exporter** エージェントの DaemonSet Pod の数がクラスター内のノード数と等しくない場合、Cluster Monitoring Operator (CMO) は動作が **degraded** 状態を報告していました。この問題は、ノードのいずれかが **ready** 状態にない場合に発生しました。本リリースでは、**node-exporter** エージェントの DaemonSet Pod の数が、クラスター内の準備状態にあるノード数よりも少なくないことを検証するようになりました。このプロセスでは、**node-exporter** Pod がすべてのアクティブなノードで実行されるようにします。その結果、ノードのいずれかが Ready 状態にない場合に CMO は degraded 状態を報告しません。(BZ#2004051)

- 本リリースでは、TLS 証明書関連のリソースが存在する前にモニタリングスタックの一部の Pod が起動し、失敗し、再起動する問題が修正されました。(BZ#2016352)

- 以前のバージョンでは、設定されたサンプル制限に達するとメトリックの報告に失敗すると、メトリックターゲットはメトリックが見つからない場合でも、Web コンソール UI のステータスで **Up** が表示されました。今回のリリースにより、Prometheus はレポートメトリックのサンプル制限設定をバイパスし、サンプル制限の設定に関係なくメトリックが表示されるようになりました。(BZ#2034192)

ネットワーク

- 4.8 よりも前の OpenShift Container Platform バージョンで OVN-Kubernetes ネットワークプロバイダーを使用する場合、ノードのルーティングテーブルはルーティングの決定に使用されていました。OpenShift Container Platform のより新しいバージョンでは、ホストルーティングテーブルはバイパスされます。本リリースでは、トラフィックルーティングの決定にホストカーネルネットワークスタックを使用するか、またはバイパスするかを指定できるようになりました。(BZ#1996108)

- 以前のバージョンでは、Kuryr がプロキシーと共に制限されたインストールで使用されると、クラスターネットワーク Operator は Red Hat OpenStack Platform (RHOSP) API との通信を許可するようにプロキシーの使用を強制しませんでした。そのため、クラスターのインストールは進行中ではありませんでした。今回の更新により、Cluster Network Operator はプロキシー経由で RHOSP API と通信できるようになりました。その結果、インストールが正常に実行されるようになりました。(BZ#1985486)

- 今回の更新以前は、SRIOV Webhook は Red Hat OpenStack Platform (RHOSP) 環境での OpenShift Container Platform でのネットワークポリシーの作成をブロックしました。今回の更新により、SRIOV Webhook は RHOSP メタデータを読み取り、検証し、ネットワークポリシーの作成に使用できるようになりました。(BZ#2016334)

- 以前のバージョンでは、SRIOV Operator は **MachineConfig** プールオブジェクトを一時停止しないため、**MachineConfig** オブジェクトは更新されませんでした。この更新により、SRIOV オペレーターは、再起動が必要な設定を実行する前に、関連するマシン設定プールを一時停止します。(BZ#2021151)

- 以前のバージョンでは、**keepalived** のタイミングの問題があり、これが実行中の場合に終了しました。今回の更新で、複数の **keepalived** コマンドが短期間送信されなくなりました。その結果、タイミングの問題は問題なくなり、**keepalive** は継続的に実行されます。(BZ#2022050)

- 以前は、Kuryr がプロキシーを使用した制限付きインストールで使用された場合、Cluster Networking Operator は、Red Hat Open Stack Platform (RHOSP) API との通信を許可するためにプロキシーの使用を強制していませんでした。そのため、クラスターのインストールは進行中ではありませんでした。今回の更新により、Cluster Network Operator はプロキシー経由で RHOSP API と通信できるようになりました。その結果、インストールが正常に実行されるようになりました。(BZ#1985486)

- 以前のバージョンでは、IP アドレスが使い切られるため、Whereabouts Container Network Interface (CNI) プラグインによって提供される IP アドレスを持つセカンダリーインターフェイスを使用する Pod は **ContainerCreating** 状態のままになる可能性がありました。現在、以前に追跡されていなかった再起動などのクラスターイベントからのリリースされた IP アドレスについて、Wabouts が適切にアカウントされるようになりました。(BZ#1914053)

- 以前のバージョンでは、OpenShift SDN クラスターネットワークプロバイダーを使用する場合、アイドル状態のサービスはアイドル状態のサービスに対して CPU の量を増やしていました。本リリースでは、kube-proxy のアイドリングコードは、サービスのアイドリングに使用する CPU を減らすために最適化されています。(BZ#1966521)

- 以前のバージョンでは、OVN-Kubernetes クラスターネットワークプロバイダーを使用する場合、内部設定マップに不明なフィールドが存在すると、OVN-Kubernetes Pod がクラスターのアップグレード時に起動できなくなる可能性がありました。unknown フィールドが存在すると、失敗ではなく警告が出されるようになりました。その結果、OVN-Kubernetes Pod はクラスターのアップグレード時に正常に起動できるようになりました。(BZ#1988440)

- 以前のバージョンでは、SR-IOV Network Operator の Webhook は、OpenStack での OpenShift インストールのネットワークポリシーをブロックしていました。ユーザーは SR-IOV ネットワークポリシーを作成できませんでした。今回の更新により、webhook が修正されました。OpenStack へのインストール用に SR-IOV ネットワークポリシーを作成できるようになりました。(BZ#2016334)

- 以前のバージョンでは、CRI-O ランタイムエンジンは **K8S_POD_UID** 変数を使用して Pod UID を渡していました。ただし、Pod が削除された Pod サンドボックスのネットワークのセットアップと同時に削除および再作成される場合、このメソッドは追加のメタデータと不要な処理を行いました。今回の更新により、Multus は Pod UID を処理し、不要なメタデータ処理が回避されます。(BZ#2017882)

- 以前のバージョンでは、単一ノードでの OpenShift のデプロイメントでは、SR-IOV Network Operator のデフォルト設定により、ユーザーがノードに特定の変更を加えることができませんでした。デフォルトでは、設定の変更が適用された後に、影響を受けるノードがドレイン (解放) されてから新規設定で再起動します。この動作は、ノードが 1 つしかない場合は機能しません。今回の更新により、単一ノードデプロイメントで SR-IOV ネットワーク Operator をインストールする際に、Operator はその設定を変更して **.spec.disableDrain** フィールドが **true** に設定されるようになりました。ユーザーは、単一ノードデプロイメントで設定の変更を正常に適用できるようになりました。(BZ#2021151)

- クライアント go バージョン 1.20 以前には、Kubernetes API へのリクエストを再試行する方法が十分にありませんでした。そのため、Kubernetes API への再試行では不十分でした。今回の更新で、client-go 1.22 を導入して問題を修正しています。(BZ#2052062)

ノード

- 以前のバージョンでは、CRI-O によって管理されるネットワーク、IPC、および UTS namespace リソースは、Kubelet が停止した Pod を削除した場合にのみ解放されていました。今回の更新により、Pod の停止時に Kubelet がこれらのリソースを解放するようになりました。(BZ#2003193)

- 以前のバージョンでは、ワーカーノードにログインする際に、**systemd-coredump** サービスの失敗を示すメッセージが表示される可能性がありました。これは、コンテナーの **system-systemd** namespace が不必要であるために生じました。フィルターにより、この namespace がワークフローに影響を与えなくなりました。(BZ#1978528)

- 以前のバージョンでは、クラスターが再起動すると、終了した Pod のステータスが **Running** にリセットされている可能性があり、これによりエラーが生じました。これは修正され、終了したすべての Pod が終了し、アクティブな Pod に正しいステータスが反映されるようになりました。(BZ#1997478)

- 以前のバージョンでは、特定の stop シグナルが OpenShift Container Platform で無視され、コンテナーのサービスが実行を継続していました。シグナル解析ライブラリーが更新されると、すべての stop シグナルが認識されるようになりました。(BZ#2000877)

- 以前のバージョンでは、ネットワーク、IPC、および UTS などの CRI-O によって管理される Pod namespace は Pod の削除時にアンマウントされませんでした。その結果、Open vSwitch CPU が 100% になりました。これにより、Pod のレイテンシーやその他のパフォーマンスに影響が出ました。これは解決され、Pod namespace は削除時にアンマウントされます。(BZ#2003193)

OpenShift CLI (oc)

- 以前のバージョンでは、クラスターにインストールされているカスタムリソース定義 (CRD) の数が増えるために、API 検出に到達する要求はクライアントコードの制限によって制限されました。今回のリリースより、制限番号と QPS の両方が拡張され、クライアント側のスロットリング頻度は低くなりました。(BZ#2042059)

- 以前のバージョンでは、一部のマイナー要求でユーザーエージェントの文字列が正しく設定されていなかったため、**oc** の代わりにデフォルトの Go ユーザーエージェント文字列が使用されていました。ユーザーエージェント文字列はすべてのミラー要求に対して適切に設定され、予想される **oc** ユーザーエージェントの文字列がレジストリーに送信されるようになりました。(BZ#1987257)

- 以前のバージョンでは、**oc debug** は、Bash シェルの実行を試みて Linux ベースのコンテナーを常にターゲットとしていました。また、Bash がコンテナーに存在しない場合は、Windows コンテナーとしてデバッグを試みていました。**oc debug** コマンドは Pod セレクターを使用してコンテナーのオペレーティングシステムを判別し、Linux および Windows ベースのコンテナーの両方で適切に機能するようになりました。(BZ#1990014)

- 以前のバージョンでは、**--dry-run** フラグは複数の **oc set** サブコマンドで適切に機能しませんでした。そのため、**--dry-run=server** はドライランを実行するのではなく、リソースへの更新を実行していました。**--dry-run** フラグは、**oc set** サブコマンドでドライランを実行するために適切に機能するようになりました。(BZ#2035393)

OpenShift コンテナー

- 以前のバージョンでは、SELinux を使用するコンテナーは **/var/log/containers** ログファイルを読み取ることができませんでした。今回の更新で、シンボリックリンク経由でアクセスされるものを含め、**/var/log** のすべてのログファイルにアクセスできるようになりました。(BZ#2005997)

OpenShift Controller Manager

- 以前のバージョンでは、**openshift_apps_deploymentconfigs_last_failed_rollout_time** メトリックは **namespace** ラベルを **exported_namespace** ラベルの値として誤って設定していました。**openshift_apps_deploymentconfigs_last_failed_rollout_time** メトリックに正しい **namespace** ラベルが設定されるようになりました。(BZ#2012770)

Operator Lifecycle Manager (OLM)

- この更新前は、**marketplace-operator** のデフォルトのカタログソースはテイントされたノードを許容せず、**CatalogSource** Pod には許容度、**nodeSelector**、および **priorityClassName** のデフォルト設定のみがありました。今回の更新により、**CatalogSource** 仕様には、Pod の tolerations、**nodeSelector**、および **priorityClassName** を上書きできるオプションの **spec.grpcPodConfig** フィールドが含まれるようになりました。(BZ#1927478)

- 今回の更新以前は、OLM Operator の再起動時に **csv_suceeded** メトリックが失われました。今回の更新により、**csv_succeed** メトリックは OLM Operator の起動ロジックの開始時に出力されるようになりました。(BZ#1927478)

- 今回の更新以前は、**oc adm catalog mirror** コマンドは **--max-icsp-size** フラグの最小および最大値を設定しませんでした。そのため、フィールドが 0 未満または大きすぎる値が許可されます。今回の更新により、値は 0 よりも大きく、250001 未満のサイズに制限されるようになりました。この範囲外の値では検証に失敗します。(BZ#1972962)

- 今回の更新以前は、バンドルされたイメージにはファイルベースのカタログでの Operator デプロイメントに必要な関連イメージが含まれていませんでした。そのため、ClusterServiceVersion (CSV) の **relatedImages** フィールドに指定されない限り、イメージは非

接続クラスターにミラーリングされませんでした。今回の更新により、**opm render** コマンドは、ファイルベースのカタログバンドルイメージのレンダリング時 に CSV Operator イメージを **relatedImages** ファイルに追加するようになりました。Operator デプロイメントに必要なイメージは、CSV の **relatedImages** フィールドにリスト表示されていない場合でも、非接続クラスターにミラーリングされるようになりました。(BZ#2002075)

- 今回の更新以前は、Operator が **skipRange** の更新を実行するまで最長 15 分かかる可能性がありました。これは、クラスター管理者が **openshift-operator-lifecycle-manager** namespace の **catalog-operator** Pod を削除した場合に解決できる既知の問題でした。これにより、Pod が自動的に再作成され、**skipRange** のアップグレードがトリガーされました。今回の更新により、Operator Lifecycle Manager (OLM) で廃止された API 呼び出しが修正され、**skipRange** 更新がすぐにトリガーされるようになりました。(BZ#2002276)

- クラスターの更新イベントは、Operator Lifecycle Manager (OLM) がリストャーキャッシュからオブジェクトを変更する際に生じます。これにより、同時マップ書き込みが発生しました。今回の修正により OLM が更新され、リストャーキャッシュから取得したオブジェクトが変更されなくなりました。その代わりに、OLM は該当する場合にオブジェクトのコピーを変更します。その結果、OLM では同時マップ書き込みが発生しなくなりました。(BZ#2003164)

- 以前のバージョンでは、Operator Lifecycle Manager (OLM) は、プロキシー経由でのみ到達可能なカタログソース Pod への gRPC 接続を確立できませんでした。カタログソース Pod がプロキシーの背後にある場合、OLM はプロキシーに接続できず、ホストされる Operator コンテンツはインストールで利用できませんでした。今回のバグ修正により、OLM が gRPC カタログソースへの接続を確立するために使用するプロキシーを定義する **GRPC_PROXY** 環境変数が導入されました。その結果、OLM は gRPC カタログソースへの接続時にプロキシーを使用するように設定できます。(BZ#2011927)

- 以前のバージョンでは、スキップされたバンドルが同じパッケージのメンバーであるかどうかは検証されませんでした。バンドルはパッケージ全体でスキップされ、アップグレードチェーンを妨げる可能性があります。今回のバグ修正により、スキップされたバンドルが同じパッケージに配置されるように検証が追加されました。その結果、バンドルを別のパッケージでバンドルを省略できなくなり、アップグレードグラフはパッケージ間で破損しなくなりました。(BZ#2017327)

- **CatalogSource** オブジェクトでは、**RegistryServiceStatus** フィールドは、Operator Lifecycle Manager (OLM) が関連付けられた Pod との接続を確立するために依存するアドレスを生成するために使用されるサービス情報を保存します。**RegistryServiceStatus** フィールドが nil で、そのサービスの namespace、名前、およびポート情報がない場合、OLM は関連付けられた Pod に無効なイメージまたは仕様が含まれるまで回復できません。今回のバグ修正により、カタログソースを調整する際に、OLM は **CatalogSource** オブジェクトの **RegistryServiceStatus** フィールドが有効になり、その変更を反映するようにそのステータスを更新するようになりました。さらに、このアドレスは **status.GRPCConnectionState.Address** フィールドのカタログソースのステータスに保存されます。アドレスが変更されると、OLM はこのフィールドを更新して新規アドレスを反映します。その結果、カタログソースの **.status.connectionState.address** フィールドは nil にならなくなりました。(BZ#2026343)

OpenShift API サーバー
OpenShift Update Service
Red Hat Enterprise Linux CoreOS (RHCOS)

- 以前のバージョンでは、RHCOS ライブ ISO が独自の UEFI ブートエントリーを追加する場合、既存の UEFI ブートエントリー ID が連続すると仮定するため、非コンセンティブブートエントリー IDS のシステムでブートする際にライブ ISO が UEFI ファームウェアで失敗しました。今回の修正により、RHCOS ライブ ISO は、それ自体の UEFI ブートエントリーを追加しなくなり、ISO が正常に起動されるようになりました。(BZ#2006690)

- ユーザーによって提供されるイメージがすでに起動されているかどうかを判別するために、マシンが Ignition でプロビジョニングされたタイミングやユーザーの Ignition 設定が指定されているかどうかを記述するターミナルコンソールに情報が追加されています。これにより、Ignition が予想される際に実行されたことを確認できます。(BZ#2016004)

- 以前のバージョンでは、プロビジョニング時に既存の静的キーの LUKS ボリュームを再利用する際に、暗号化キーはディスクに正しく書き込まれず、Ignition は永続化されたキーファイルエラーを出して失敗しました。今回の修正により、Ignition は再利用された LUKS ボリュームのキーを正しく書き込み、プロビジョニング時に既存の静的に鍵を再利用できるようになりました。(BZ#2043296)

- 以前のバージョンでは、**ostree-finalize-staged.service** は、Red Hat Enterprise Linux CoreOS (RHCOS) ノードの 4.6.17 へのアップグレード時に失敗していました。これを修正するために、sysroot コードは、**/etc** 内の非通常ファイルまたは非シンボリックリンクファイルを無視するようになりました。(BZ#1945274)

- 以前のバージョンでは、割り当てられた SCSI デバイスの by-id シンボリックリンクの udev ルールが **initramfs** ファイルに欠落していました。そのため、これらのシンボリックリンクを参照する Ignition 設定ファイルにより、インストールされたシステムの起動が失敗しました。今回の更新で、SCSI ルールの **63-scsi-sg3_symlink.rules** が dracut に追加されました。(BZ#1990506)

- 以前のバージョンでは、ベアメタルマシンで、**system-rfkill.service** と **ostree-remount.service** の間で競合状態が発生していました。そのため、ブートプロセス中に **ostree-remount** サービスが失敗し、ノードのオペレーティングシステムがフリーズしていました。今回の更新で、**/sysroot/** ディレクトリーが読み取り専用になりました。その結果、この問題は発生しなくなりました。(BZ#1992618)

- 以前のバージョンでは、Red Hat Enterprise Linux CoreOS (RHCOS) ライブ ISO ブートは UEFI ブートエントリーを追加し、TPM のあるシステムでの再起動を求めるプロンプトが出されました。この更新により、RHCOS ライブ ISO は UEFI ブートエントリーを追加しなくなり、ISO は初回起動後に再起動を開始しなくなりました。(BZ#2004449)

Performance Addon Operator

- **spec.cpu.isolated** が **PerformanceProfile** で定義された唯一のパラメーターである場合、spec.cpu.reserved' フラグはデフォルトで適切に設定されない可能性があります。**PerformanceProfile** で **spec.cpu.reserved** と **spec.cpu.isolated** の両方の設定を設定する必要があります。セットは重複してはならず、上記のすべての CPU の合計は、ターゲットプール内のワーカーが想定する CPU をすべてカバーする必要があります。(BZ#1986681)

- 以前のバージョンでは、**oc adm must-gather** ツールは、**gather-sysinfo** バイナリーがイメージにない場合、ノードデータの収集に失敗していました。これは、Dockerfile に **COPY** ステートメントがないために生じました。この問題を回避するには、必要な **COPY** ステートメントを Dockerfile に追加し、バイナリーを生成およびコピーする必要があります。(BZ#2021036)

- 以前のバージョンでは、Performance Addon Operator は CRI-O キャッシュで利用可能なかどうかを確認せずに、イメージをレジストリーからダウンロードしました。そのため、Performance Addon Operator はレジストリーに到達できない場合や、ダウンロードがタイムアウトした場合の開始に失敗しました。今回の更新により、Operator は CRI-O キャッシュからイメージをプルできない場合のみ、イメージをレジストリーからダウンロードするようになりました。(BZ#2021202)

- OpenShift Container Platform をバージョン 4.10 にアップグレードする際に、行頭で開始しない tuned プロファイルのコメント (**#comment**) により、解析エラーが発生します。Performance Addon Operator の問題は、Open Shift Container Platform と同じレベル (4.10)

にアップグレードすることで解決できます。コメント関連のエラーは、1行にコメントをすべて配置し、行頭に # 文字を付けることで回避できます。(BZ#2059934)

Routing

- 以前のバージョンでは、クラスター管理者が最後の行の改行文字のないデフォルトの Ingress 証明書を指定した場合、OpenShift Container Platform ルーターは HAProxy 用に破損した PEM ファイルを書き込みました。入力に改行文字がない場合でも、有効な PEM ファイルへの書き込みが行われるようになりました。(BZ#1894431)

- 以前のバージョンでは、DNS セグメントに組み合わせた名前および namespace の組み合わせが 63 文字を超える場合に作成されたルートは拒否されました。この想定される動作により、OpenShift Container Platform のアップグレードされたバージョンとの統合で問題が発生する可能性があります。アノテーションは、適合しない DNS ホスト名を許可するようになりました。**AllowNonDNSCompliantHostAnnotation** を **true** に設定すると、conformant DNS ホスト名または 63 文字を超える 1 文字を使用できます。(BZ#1964112)

- 以前のバージョンでは、クラスターの **ControlPlaneTopology** が **External** に設定されている場合に、Cluster Ingress Operator は Ingress コントローラーのワイルドカード DNS レコードを作成しませんでした。**ControlPlaneTopology** が **External** に設定され、プラットフォームが AWS であった Hypershift クラスターでは、Cluster Ingress Operator は利用できなくなります。今回の更新により、**ControlPlaneTopology** が **External** で、プラットフォームが IBM Cloud の場合、DNS 更新の無効化が制限されます。その結果、AWS で実行される Hypershift クラスター用にワイルドカード DNS エントリーが作成されます。(BZ#2011972)

- 以前のバージョンでは、Ingress Operator は Azure Stack Hub IPI でクラスター Ingress ルーターのワイルドカード DNS レコードを設定できないため、クラスターの Ingress ルーターは機能しなくなっていました。今回の修正により、Ingress Operator は設定された ARM エンドポイントを使用して Azure Stack Hub IPI で DNS を設定するようになりました。その結果、クラスターの Ingress ルーターが適切に機能するようになりました。(BZ#2032566)

- 以前のバージョンでは、クラスター全体のプロキシー設定は **noProxy** 設定の IPv6 アドレスを許可できませんでした。そのため、IPv6 アドレスで **noProxy** があるクラスターをインストールできませんでした。今回の更新により、Cluster Network Operator はクラスター全体のプロキシーリソースの **noProxy** 設定の IPv6 アドレスを解析できるようになりました。その結果、**noProxy** 設定の IPv6 アドレスを除外できるようになりました。(BZ#1939435)

- OpenShift Container Platform 4.8 より前のバージョンでは、IngressController API には **status.endpointPublishingStrategy.hostNetwork** および **status.endpointPublishingStrategy.nodePort** フィールドにサブフィールドがありませんでした。これらのフィールドは、**spec.endpointPublishingStrategy.type** が **HostNetwork** または **NodePortService** に設定されている場合でも null になります。OpenShift Container Platform 4.8 では、**status.endpointPublishingStrategy.hostNetwork.protocol** および **status.endpointPublishingStrategy.nodePort.protocol** サブフィールドが追加され、Ingress Operator は HostNetwork または NodePortService ストラテジータイプを指定する IngressController が付与される際にこれらのサブフィールドのデフォルト値を設定します。ただし、このバグにより、Operator はこれらの仕様フィールドに対する更新を無視し、**spec.endpointPublishingStrategy.hostNetwork.protocol** または **spec.endpointPublishingStrategy.nodePort.protocol** から **PROXY** に更新され、既存の IngressController でプロキシープロトコルを有効にしませんでした。この問題を回避するには、PROXY プロトコルを有効にするために IngressController を削除し、再作成する必要がありました。今回の更新により、Ingress Operator は **status.endpointPublishingStrategy.hostNetwork** および **status.endpointPublishingStrategy.nodePort** が null であり、IngressController 仕様フィールドが **HostNetwork** または **NodePortService** エンドポイント公開ストラテジータイプでプロキシープロトコルを指定する場合に、ステータスフィールドを正しく更新するように変更されま

した。その結果、**spec.endpointPublishingStrategy.hostNetwork.protocol** または **spec.endpointPublishingStrategy.nodePort.protocol** を **PROXY** に設定することにより、アップグレードされたクラスターで適切に有効にされるようになりました。(BZ#1997226)

サンプル

- 今回の更新以前は、Cluster Samples Operator が **APIServerConflictError** エラーが発生した場合に、復元するまで **sample-operator** が **Degraded status** であると報告していました。アップグレード時にこのタイプの異常なエラーはありませんでしたが、管理者が Operator のステータスを監視する際に不注意なエラーが発生していました。今回の更新により、Operator が異常なエラーが生じると、**openshift-samples** が **Degraded status** で示されなくなり、API サーバーへの接続を再度試行するようになりました。異常な移行が **Degraded status** に切り替わりなくなりました。(BZ#1993840)

- 今回の更新以前は、クラスターイメージ設定の各種の許可およびブロックされたレジストリー設定オプションにより、Cluster Samples Operator がイメージストリームを作成できなくなる可能性があります。その結果、Samples Operator は、一般的な OpenShift Container Platform インストールおよびアップグレードのステータスに影響を与えるために、それ自体を degraded とマークする可能性があります。
  各種の状況では、Cluster Samples Operator の管理状態は **Removed** に移行することができます。今回の更新により、イメージコントローラー設定パラメーターがデフォルトのイメージレジストリーまたは **samplesRegistry** 設定で指定されたイメージレジストリーを使用してイメージストリームを作成できない場合にこれらの状況が含まれるようになりました。Operator のステータスには、クラスターイメージ設定がサンプルイメージストリームの作成を妨げていることも示されるようになりました。(BZ#2002368)

ストレージ

- 以前のバージョンでは、10 秒の遅延の発生により、Local Storage Operator (LSO) は孤立した永続ボリューム (PV) を削除するのに長い時間がかかりました。今回の更新により、LSO は 10 秒の遅延を使用せず、PV はすぐに削除され、ローカルディスクが新規の Persistent Volume Claim (永続ボリューム要求、PVC) についてすぐに利用可能になるようになりました。(BZ#2001605)

- 以前のバージョンでは、Manila のエラー処理により Manila Operator およびクラスターのパフォーマンスが低下しました。エラーは致命的ではないものとして処理されるようになり、Manila Operator はクラスターを低下させるのではなく無効にできるようになりました。(BZ#2001620)

- Cinder を使用する場合など、低速なクラウド環境では、クラスターがパフォーマンスが低下する可能性があります。OpenShift Container Platform は低速な環境に対応するようになり、クラスターのパフォーマンスが低下することはなくなりました。(BZ#2027685)

Telco Edge

- 生成されたポリシーに **mustonlyhave** の complianceType がある場合、Operator Lifecycle Manager (OLM) メタデータへの Operator Lifecycle Manager(OLM) の更新は、ポリシーエンジンとして CR の expected 状態を復元します。その結果、OLM およびポリシーエンジンは競合時に CR のメタデータを継続的に上書きします。これにより、CPU の使用率が高くなります。今回の更新により、OLM およびポリシーエンジンが競合しなくなり、CPU の使用率が軽減されるようになりました。(BZ#2009233)

- 以前のバージョンでは、フィールドがベースソース CR に存在しない場合に、**PolicyGenTemplate** オーバーレイのユーザーが提供するフィールドは、生成されたマニフェストにコピーされませんでした。その結果、一部のユーザーコンテンツが失われました。**policyGen** ツールが更新され、ユーザー指定の全フィールドがサポートされるようになりました。(BZ#2028881)

- 以前のバージョンでは、DNS ルックアップの失敗により、サポートされていないプラットフォームにインストールする際に Cluster Baremetal Operator が継続的に失敗する可能性がありました。今回の更新により、Operator はサポート対象外のプラットフォームにインストールすると無効にされたままになります。(**BZ#2025458**)

Web コンソール (Administrator パースペクティブ)
Web コンソール (開発者パースペクティブ)

- 今回の更新以前は、Web コンソールの **Developer** パースペクティブにあるリソースには、そのリソースの詳細への無効なリンクがありました。今回の更新で問題が解決されました。ユーザーがリソースの詳細にアクセスできるように有効なリンクを作成します。(BZ#2000651)

- 今回の更新以前は、名前ではなく、ラベルで **SinkBinding** フォームでサブジェクトのみを指定できました。今回の更新により、ドロップダウンリストを使用して、名前またはラベルでサブジェクトを指定するかどうかを選択できるようになりました。(BZ#2002266)

- 今回の更新以前は、Web 端末アイコンは、**openShift-operators** namespace に Web 端末 Operator をインストールした場合にのみ、Web コンソールのバナーヘッドで利用可能でした。今回の更新により、Web 端末 Operator をインストールする namespace に関係なく、ターミナルアイコンを利用できます。(2006329)

- 今回の更新以前は、**kind** プロパティーで **ServiceBinding** カスタムリソース (CR) を定義するのではなく、**resource** プロパティーを使用してサービスバインディングコネクターがトポロジーに表示されませんでした。今回の更新では、CR の **resource** プロパティーを読み取り、トポロジーでコネクターを表示することで問題が解決されます。(BZ#2013545)

- 今回の更新以前は、名前入力フィールドは、複雑な再帰的な正規表現を使用してユーザー入力を検証していました。この正規表現により、名前の検出が非常に遅くなり、エラーが発生することがよくあります。今回の更新で、正規表現を最適化し、再帰一致を回避することで、問題が解決されています。今回のリリースより、名前の検出は高速になり、エラーが生じなくなりました。(BZ#2014497)

- 今回の更新以前は、knative プラグインで提供される一部の拡張機能に機能フラグが欠落していました。この問題は表示される内容には影響しませんでしたが、これらのエクステンションはサーバーレス Operator がインストールされていなくても不必要に実行されました。今回の更新では、見つからないエクステンションに feature フラグを指定して問題が解決されます。今回のリリースより、エクステンションは不必要に実行されなくなりました。(BZ#2016438)

- この更新の前に、カスタムリソース定義や Pod などのリソースの詳細を取得するためにリンクを繰り返しクリックし、アプリケーションで複数のコード参照エラーが発生した場合は、失敗して、**t is not a function** エラーが表示されました。今回の更新で問題が解決されました。エラーが発生すると、アプリケーションはコード参照を解決し、解決状態を保存し、追加のエラーを適切に処理できるようにします。コード参照エラーが発生したときにアプリケーションが失敗することはなくなりました。(BZ#2017130)

- 今回の更新以前は、アクセスが制限されたユーザーは共有 namespace の設定マップにアクセスして、クラスター上でユーザー設定を保存し、それらを別のブラウザーまたはマシンで読み込むことができませんでした。その結果、固定されたナビゲーションアイテムなどのユーザー設定は、ローカルのブラウザーストレージにのみ保存され、複数のブラウザー間で共有されませんでした。今回の更新により問題が解決されています。Web コンソール Operator は RBAC ルールを自動的に作成し、各ユーザーがこれらの設定を共有 namespace に設定マップに保存し、ブラウザー間でより簡単に切り替えられるようになりました。(BZ#2018234)

- 今回の更新以前は、**Topology** ビューで仮想マシン (VM) 間の接続を作成しようとすると、Error creating connection というメッセージで失敗していました。この問題は、このアクションがカスタムリソース定義 (CRD) をサポートしないメソッドに依存するために生じました。今回

の更新により、CRD のサポートを追加して問題が解決されます。仮想マシン間の接続を作成できるようになりました。(BZ#2020904)

- 今回の更新以前は、**PipelineRun の詳細** のタスクのツールチップに誤解を招く情報が表示されていました。タスクの実行時間ではなく、タスクの実行から経過した時間が表示されました。たとえば、5 日間前に実行したタスクについて 122 時間が表示されました。今回の更新により、ツールチップにタスクの期間が表示されるようになりました。(BZ#2011368)

1.7. テクノロジープレビューの機能

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

テクノロジープレビュー機能のサポート範囲

以下の表では、機能は以下のステータスでマークされています。

- **TP**: **テクノロジープレビュー機能**
- **GA**: **一般公開機能**
- **-**: **利用不可の機能**
- **DEP**: **非推奨機能**

表1.2 テクノロジープレビュートラッカー

機能	OCP 4.8	OCP 4.9	OCP 4.10
通常のクロックとして設定された Precision Time Protocol (PTP) ハードウェア	TP	GA	GA
境界クロックとして設定された PTP シングル NIC ハードウェア	-	-	TP
通常のクロックでの PTP イベント	-	TP	GA
oc CLI プラグイン	GA	GA	GA
OpenShift ビルドの CSI ボリューム	-	-	TP
サービスバインディング	TP	TP	GA
Cinder での raw ブロック	GA	GA	GA
CSI ボリューム拡張	TP	TP	TP
CSI AliCloud Disk Driver Operator	-	-	GA
CSI Azure Disk Driver Operator	TP	TP	GA

機能	OCP 4.8	OCP 4.9	OCP 4.10
CSI Azure File Driver Operator	-	-	TP
CSI Azure Stack Hub Driver Operator	-	GA	GA
CSI GCP PD Driver Operator	GA	GA	GA
CSI IBM VPC Block Driver Operator	-	-	GA
CSI OpenStack Cinder Driver Operator	GA	GA	GA
CSI AWS EBS ドライバー Operator	TP	GA	GA
CSI AWS EFS Driver Operator	-	TP	GA
CSI の自動移行	TP	TP	TP
CSI インラインの一時ボリューム	TP	TP	TP
CSI vSphere Driver Operator	TP	TP	GA
Shared Resource CSI Driver	-	-	TP
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	TP	TP	TP
OpenShift Pipeline	GA	GA	GA
OpenShift GitOps	GA	GA	GA
OpenShift サンドボックスコンテナー	TP	TP	GA
Vertical Pod Autoscaler	GA	GA	GA
Cron ジョブ	GA	GA	GA
PodDisruptionBudget	GA	GA	GA
kvc を使用したノードへのカーネルモジュールの追加	TP	TP	TP
egress ルーター CNI プラグイン	GA	GA	GA
スケジューラーのプロファイル	TP	GA	GA
プリエンプションを実行しない優先順位クラス	TP	TP	TP

機能	OCP 4.8	OCP 4.9	OCP 4.10
Kubernetes NMState Operator	TP	TP	GA
アシステッドインストーラー	TP	TP	GA
AWS Security Token Service (STS)	GA	GA	GA
Kdump	TP	TP	TP
OpenShift Serverless	GA	GA	GA
ARM プラットフォームでの Open Shift	-	-	GA
Serverless functions	TP	TP	TP
Data Plane Development Kit (DPDK) サポート。	TP	GA	GA
Memory Manager	-	GA	GA
CNI VRF プラグイン	TP	GA	GA
クラスタークラウドコントローラーマネジャ Operator	-	GA	GA
Alibaba Cloud のクラウドコントローラーマネージャー	-	-	TP
Amazon Web Services のクラウドコントローラーマネージャー	-	TP	TP
Google Cloud Platform のクラウドコントローラーマネージャー	-	-	TP
IBM Cloud 向けクラウドコントローラーマネージャー	-	-	TP
Microsoft Azure のクラウドコントローラーマネージャー	-	TP	TP
Microsoft Azure Stack Hub のクラウドコントローラーマネージャー	-	GA	GA
Red Hat OpenStack Platform (RHOSP) のクラウドコントローラーマネージャー	-	TP	TP
VMware vSphere のクラウドコントローラーマネージャー	-	-	TP
ドライバーツールキット	TP	TP	TP
Special Resource Operator(SRO)	-	TP	TP

機能	OCP 4.8	OCP 4.9	OCP 4.10
Simple Content Access	-	TP	GA
Node Health Check Operator	-	TP	TP
ネットワークバウンドディスク暗号化 (Clevis、Tang が必要)	-	GA	GA
Metal LB オペレーター	-	GA	GA
CPU マネージャー	GA	GA	GA
セカンダリーネットワークの Pod レベルボンディング	-	-	GA
IPv6 デュアルスタック	-	GA	GA
選択可能なクラスターインベントリー	-	-	TP
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	-	-	TP
動的プラグイン	-	-	TP
ハイブリッド Helm Operator	-	-	TP
ユーザー定義プロジェクトのモニタリングのアラートルーティング	-	-	TP
oc-mirror CLI プラグインを使用した非接続ミラーリング	-	-	TP
RHEL の BuildConfigs で共有資格をマウントする	-	-	TP
RHOSP DCN のサポート	-	-	TP
RHOSP 上のクラスターの外部クラウドプロバイダーのサポート	-	-	TP
RHOSP 上のクラスターの OVS ハードウェアオフロード	-	-	TP
外部 DNS Operator	-	-	TP
Web 端末 Operator	TP	TP	GA
Topology Aware Lifecycle Manager	-	-	TP
NUMA Resources Operator による NUMA 対応のスケジューリング	-	-	TP

1.8. 既知の問題

- OpenShift Container Platform 4.1 では、匿名ユーザーは検出エンドポイントにアクセスできました。後のリリースでは、一部の検出エンドポイントは集約された API サーバーに転送されるため、このアクセスを無効にして、セキュリティーの脆弱性の可能性を減らすことができます。ただし、既存のユースケースに支障がで出ないように、認証されていないアクセスはアップグレードされたクラスターで保持されます。
  OpenShift Container Platform 4.1 から 4.10 にアップグレードされたクラスターのクラスター管理者の場合、認証されていないアクセスを無効にするか、これを引き続き許可することができます。特定の必要がなければ、認証されていないアクセスを無効にすることが推奨されます。認証されていないアクセスを引き続き許可する場合は、それに伴ってリスクが増大することに注意してください。

  警告

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

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

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

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

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

  (BZ#1821771)

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

- 現在、コンテナーは、空でない継承可能な Linux プロセス機能で開始します。この問題を回避するには、**capsh (1)** などのユーティリティーを使用してコンテナーのエントリーポイントを変更し、プライマリープロセスが開始する前に継承可能な機能を削除します。(BZ#2076265)

- OpenShift Container Platform 4.10 にアップグレードする場合、Cluster Version Operator は、前提条件チェックに失敗している間、アップグレードを約 5 分間ブロックします。**It may not be safe to apply this update** エラーテキストは、誤解を招く可能性があります。このエラーは、1 つまたは複数の前提条件チェックが失敗した場合に発生します。状況によっては、これらの前提条件チェックは、etcd バックアップ中など、短期間しか失敗しない場合があります。このような状況では、Cluster Version Operator と対応する Operator は、設計上、失敗した前提条件チェックを自動的に解決し、CVO はアップグレードを正常に開始します。
ユーザーは、クラスターオペレーターのステータスと条件を確認する必要があります。Cluster Version Operator により **It may not be safe to apply this update** エラーが表示される場合は、これらのステータスと条件により、メッセージの重大度に関する詳細情報が提供されます。詳細については、BZ#1999777、BZ#2061444、BZ#2006611 を参照してください。

- EgressIP 機能を持つコントロールプレーンノードへの egress IP アドレスの割り当ては、Amazon Web Services (AWS) でプロビジョニングされるクラスターではサポートされません。(BZ#2039656)

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) 認証情報シークレットの作成と **kube-controller-manager** の起動には競合状態がありました。その結果、Red Hat OpenStack Platform(RHOSP) クラウドプロバイダーは RHOSP の認証情報で設定されず、**LoadBalancer** サービスの Octavia ロードバランサーの作成時にサポートが破損していました。これを回避するには、マニフェストから Pod を手動で削除して **kube-controller-manager** Pod を再起動する必要があります。回避策を使用する場合、**kube-controller-manager** Pod が再起動され、RHOSP 認証情報が適切に設定されます。(BZ#2004542)

- **delete all operands** オプションを使用して Web コンソールからオペランドを削除する機能は現在無効にされています。これは OpenShift Container Platform の今後のバージョンで再度有効になります。詳細は、BZ#2012120 および BZ#2012971 を参照してください。

- 本リリースには、Jenkins の既知の問題が含まれています。OpenShift OAuth ルートのホスト名および証明書をカスタマイズする場合、Jenkins は OAuth サーバーエンドポイントを信頼しなくなりました。そのため、ユーザーは、アイデンティティーおよびアクセスを管理する OpenShift OAuth 統合に依存する場合に、Jenkins コンソールにログインできません。
回避策: Red Hat ナレッジベースソリューション Deploy Jenkins on OpenShift with Custom OAuth Server URL を参照してください。(BZ#1991448)

- 本リリースには、Jenkins の既知の問題が含まれています。XML ファイルの検証またはクエリーに必要な **xmlstarlet** コマンドラインツールキットは、この RHEL ベースのイメージに含まれていません。この問題は、認証に OpenShift OAuth を使用しないデプロイメントに影響します。OpenShift OAuth はデフォルトで有効になっていますが、ユーザーは無効にすることができます。
回避策: 認証に OpenShift OAuth を使用します。(BZ#2055653)

- インスタンスグループ名が 64 文字を超えると、Google Cloud Platform (GCP) UPI のインストールに失敗します。"-instance-group" 接尾辞を追加した後に、命名プロセスで制限されています。接尾辞を -ig に短縮し、文字数を減らします。(BZ#1921627)

- RHOSP で実行され、Kuryr を使用するクラスターの場合、Octavia の OVN プロバイダードライバーのバグにより、ロードバランサーリスナーが **PENDING_UPDATE** 状態でスタックし、接続されているロードバランサーが **active** 状態のままになる可能性があります。その結

果、**kuryr-controller** Pod がクラッシュする可能性があります。この問題を解決するには、RHOSP をバージョン 16.1.9 (BZ#2019980) またはバージョン 16.2.4 (BZ#2045088) に更新します。

- 正しくないネットワークが vSphere **install-config.yaml** ファイルに指定されている場合、Terraform からのエラーメッセージはしばらく後に生成されます。マニフェストの作成時にチェックを追加して、ネットワークが無効な場合にユーザーに通知します。(BZ#1956776)

- Special Resource Operator (SRO) は、ソフトウェア定義ネットワークポリシーにより、Google Cloud Platform へのインストールに失敗する可能性があります。その結果、simple-kmod Pod は作成されません。(BZ#1996916)

- 現時点で、ステートフルセットにマップされるサービスに対して **oc idle** を実行すると、ステートフルセットのアイドリングはサポートされていません。現時点では、既知の回避策はありません。(BZ#1976894)

- Alibaba Cloud International Portal アカウントの中国 (南京) および UAE (Dubai) の地域は、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 (IPI) のインストールをサポートしません。Alibaba Cloud International Portal アカウントを使用している場合、中国 (広州) および中国 (ウランチャブ) の地域は Server Load Balancer (SLB) をサポートしません。(BZ#2048062)

- Alibaba Cloud の韓国 (ソウル) **ap-northeast-2** リージョンは、インストーラープロビジョニングインフラストラクチャー (IPI) のインストールをサポートしていません。韓国 (ソウル) リージョンは Server Load Balancer (SLB) をサポートしていないため、IPI インストールもサポートしていません。このリージョンで OpenShift Container Platform を使用する場合は、Alibaba Cloud にお問い合わせください。(BZ#2062525)

- 現時点で、**Knative Serving: Revision CPU、Memory、および Network usage**および **Knative Serving: Revision Queue proxy Metrics** ダッシュボードは、Knative サービスを持たないものを含め、すべての namespace に表示されます。(BZ#2056682)

- 現在、**Developer** パースペクティブでは、**Observe** ダッシュボードが **Topology** ビューで選択したワークロードではなく、最近表示されるワークロードに対して開きます。この問題は、セッションが URL のクエリーパラメーターではなく Redux ストアを使用するために発生します。(BZ#2052953)

- 現時点で、**ProjectHelmChartRepository** カスタムリソース (CR) は、この CR の API スキーマがクラスターで初期化されていないため、クラスターには表示されません。(BZ#2054197)

- 現在、大量のパイプラインログを実行している間、自動スクロール機能は機能せず、古いメッセージを表示するログが停止します。この問題は、大量のパイプラインログを実行して **scrollIntoView** メソッドへの多数の呼び出しを生成するために発生します。(BZ#2014161)

- 現在、**Git** からインポートフォームを使用してプライベート Git リポジトリーをインポートすると、正しいインポートタイプとビルダーイメージが識別されません。この問題は、プライベートリポジトリーの詳細をフェッチするシークレットがデコードされないために発生します。(BZ#2053501)

- モニタリングスタックのアップグレード中、Prometheus および Alertmanager が一時的に利用できない可能性があります。短時間が経過するとコンポーネントが利用可能になるため、回避策は必要ありません。ユーザーの介入は必要ありません。(BZ#203059)

- 本リリースでは、モニタリングスタックコンポーネントが、メトリクス収集に TLS 認証を使用するように更新されています。ただし、Prometheus は、新規認証情報が提供された後にも、期限切れの TLS 認証情報を使用してメトリックターゲットへの HTTP 接続を開放しようとする

ことがあります。その後、認証エラーが発生し、一部のメトリックターゲットが利用できなくなります。この問題が発生すると、**TargetDown** アラートが実行されます。この問題を回避するには、down として報告される Pod を再起動します。(BZ#2033575)

- 本リリースでは、モニタリングスタックの Alertmanager レプリカの数が 3 から 2 に削減されました。ただし、削除された 3 番目のレプリカの Persistent Volume Claim (永続ボリューム要求、PVC) は、アップグレードプロセスの一環として自動的に削除されません。アップグレード後に、管理者は Cluster Monitoring Operator からこの PVC を手動で削除できます。(BZ#2040131)

- 以前のバージョンでは、**oc adm must-gather** ツールは、複数の **--image** 引数が指定される場合にパフォーマンス固有のデータを収集しませんでした。操作の完了時に、ノードおよびパフォーマンス関連のファイルを含むファイルは欠落していました。この問題は、4.7 から 4.10 までの OpenShift Container Platform バージョンに影響します。この問題は、イメージごとに **oc adm must-gather** 操作を 2 回実行して解決できます。その結果、予想されるファイルをすべて収集できます。(BZ#2018159)

- Technology Preview oc-mirror CLI プラグインを使用する場合、更新されたイメージセットをミラーレジストリーにミラーリングした後にクラスターを更新するときに発生する可能性がある既知の問題があります。以前のバージョンの Operator を削除してから新しいバージョンに置き換えることにより、新しいバージョンの Operator がチャネルに公開された場合は、oc-mirror プラグインから生成された **Catalog Source** ファイルを適用するときにエラーが発生する可能性があります。これはカタログは無効と見なされるためです。回避策として、ミラーレジストリーから以前のカタログイメージを削除し、新しい差分イメージセットを生成して公開してから、**Catalog Source** ファイルをクラスターに適用します。この問題が解決されるまで、新しい差分イメージセットを公開するたびに、この回避策に従う必要があります。(BZ#2060837)

- GitOps ZTP フロー中の **StoragePVC** カスタムリソースの処理では、ユーザーがその値を含めない場合は、**volume.beta.kubernetes.io/storage-class** アノテーションが除外されません。このアノテーションにより、**spec.storageClassName** フィールドは無視されます。これを回避するには、**StoragePVC**カスタムリソースを使用するときに、**PolicyGenTemplate** 内の **volume.beta.kubernetes.io/storage-class** アノテーションで目的の **StorageClass** 名を設定します。(BZ#2060554)

- ボーダーゲートウェイプロトコル (BGP) ピアリソースで有効になっている双方向フォワーディング検出 (BFD) カスタムプロファイルを削除しても、BFD は無効になりません。代わりに、BGP ピアはデフォルトの BFD プロファイルの使用を開始します。BGP ピアリソースから BFD をディセーブルにするには、BGP ピア設定を削除し、BFD プロファイルなしで再作成します。(BZ#2050824)

- RHOSP で実行され、シングルルート I/O 仮想化設定 (SR-IOV) の一部として Mellanox NIC を使用するクラスターの場合は、pod を起動してから SR-IOV デバイスプラグインを再起動して pod を停止すると、Pod を作成できない場合があります。この問題の回避策はありません。

- OpenShift Container Platform は、DHCP サーバーなしでインストーラーがプロビジョニングしたクラスターのデプロイをサポートします。ただし、DHCP サーバーがないと、ブートストラップ VM は **baremetal** ネットワークの外部 IP アドレスを受け取りません。i ブートストラップ VM に IP アドレスを割り当てるには、Assigning a bootstrap VM an IP address on the baremetal network without a DHCP server を参照してください。(BZ#2048600)

- OpenShift Container Platform は、DHCP サーバーのない環境の**baremetal** ネットワーク上で、静的 IP アドレスを使用してインストーラーでプロビジョニングされたクラスターのデプロイをサポートします。DHCP サーバーが存在する場合、ノードは再起動時に DHCP サーバーから IP アドレスを取得する可能性があります。DHCP が再起動時にノードに IP アドレスを割り当てないようにするには、Preventing DHCP from assigning an IP address on node reboot を参照してください。(BZ#2036677)

- RHCOS カーネルは、Netfilter モジュールのバグによりソフトロックアップを起こし、最終的にパニックに陥ります。この問題は、OpenShift Container Platform の今後の z-stream リリースで修正され、解決される予定です。(BZ#2061445)

- 一部のイメージインデックスに古いイメージが含まれているため、**oc adm catalog mirror** および **oc image mirror** を実行すると、**error: unable to retrieve source image** エラーが発生する場合があります。一時的な回避策として、**--skip-missing** オプションを使用してエラーを回避し、イメージインデックスのダウンロードを続行できます。詳細は、Service Mesh Operator mirroring failed を参照してください。

- 仮想機能 (VF) がすでに存在する場合、Physical Fundtion (PF) で macvlan を作成することはできません。この問題は、Intel E810 NIC に影響します。(BZ#2120585)

- ZTP 経由でデプロイされたクラスターに準拠していないポリシーがあり、**ClusterGroupUpdates** オブジェクトが存在しない場合は、TALM Pod を再起動する必要があります。TALM を再起動すると、適切な **ClusterGroupUpdates** オブジェクトが作成され、ポリシーへの準拠が強制されます。(OCPBUGS-4065)

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

1.9. エラータの非同期更新

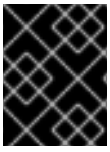
OpenShift Container Platform 4.10 のセキュリティー、バグ修正、拡張機能の更新は、Red Hat Network 経由で非同期エラータとして発表されます。OpenShift Container Platform 4.10 のすべてのエラータは Red Hat カスタマーポータルから入手できます。非同期エラータについては、OpenShift Container Platform ライフサイクル を参照してください。

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

注記

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

以下のセクションは、これからも継続して更新され、今後の OpenShift Container Platform 4.10 バージョンの非同期エラータリリースで発表される拡張機能およびバグ修正に関する情報を追加していきます。たとえば、OpenShift Container Platform 4.10.z などのバージョン付けされた非同期リリースについてはサブセクションで説明します。さらに、エラータの本文がアドバイザリーで指定されたスペースに収まらないリリースの詳細は、その後のサブセクションで説明します。



重要

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

1.9.1. RHSA-2022:0056 - OpenShift Container Platform 4.10.3 イメージのリリース、バグ修正およびセキュリティー更新アドバイザリー

発行日: 2022-03-10

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.3 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHSA-2022:0056 アドバイザリーにまとめられています。バグ修正の 2 番目のセットは、RHEA-2022:0748 アドバイザリーにあります。この更新に含まれる RPM パッケージは RHSA-2022:0055 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.3 --pullspecs
```

1.9.1.1. バグ修正

- 以前は、OVN-Kubernetes を備えた OpenShift Container Platform は、ExternalIP を介したサービスへの ingress アクセスを管理していました。4.10.2 から 4.10.3 にアップグレードすると、**ExternalIP** へのアクセスが "No Route to Host" などの問題で動作しなくなります。この更新により、管理者は externalIP からクラスターにトラフィックを転送しなければならなくなります。ガイダンスについては、(KCS*) および (**Kubernetes External IPs**) (**BZ#2076662**) を参照してください。

1.9.2. RHBA-2022:0811 - OpenShift Container Platform 4.10.4 バグ修正およびセキュリティー更新

発行日: 2022-03-15

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.4 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHBA-2022:0811 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは RHSA-2022:0810 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.4 --pullspecs
```

1.9.2.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.3. RHBA-2022:0928 - OpenShift Container Platform 4.10.5 バグ修正およびセキュリティー更新

発行日: 2022-03-21

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.5 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHBA-2022:0928 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは RHSA-2022:0927 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.5 --pullspecs
```

1.9.3.1. 既知の問題

- **ztp** * という名前のゼロタッチプロビジョニング (ZTP) を介してクラスターを追加する際に問題が発生します。クラスターの名前として **ztp** を追加すると、ACM がクラスターの namespace

にコピーするポリシーを削除するという **ArgoCD** の状況が発生します。**ztp** を使用してクラスターに名前を付けると、調整ループが発生し、ポリシーは準拠しなくなります。回避策として、名前の先頭に **ztp** を付けてクラスターに名前を付けないでください。クラスターの名前を変更することにより、競合により調整ループが停止し、ポリシーが準拠します。(BZ#2049154)

1.9.3.2. バグ修正

- 以前は、**Developer** コンソールの**Topology** ビューからの **Observer** ダッシュボードは、選択したワークロードではなく、最後に表示されたワークロードに対して開かれていました。この更新により、**Developer** コンソールの **Observe** ダッシュボードは、**Topology** ビューから選択したワークロードに対して常に開きます。(BZ#2059805)

1.9.3.3. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.4. RHBA-2022:1026 - OpenShift Container Platform 4.10.6 バグ修正およびセキュリティー更新

発行日 2022-03-28

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.6 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHBA-2022:1026 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは RHSA-2022:1025 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.6 --pullspecs
```

1.9.4.1. 機能

1.9.4.2. Kubernetes 1.23.5 からの更新

この更新には、Kubernetes1.23.3 から 1.23.5 までの変更が含まれています。より詳しい情報は、1.23.4、1.23.5 のチェンジログをご覧ください。

1.9.4.3. バグ修正

- 以前は、Red Hat OpenStack Platform (RHOSP)-16 で利用可能な Cisco ACI の neutron 実装でのサブネットのクエリーは、特定のネットワークに対して予期しない結果を返していました。その結果、RHOSP **cluster-api-provider** は、同じサブネット上に重複したポートを持つインスタンスをプロビジョニングしようとする可能性があり、プロビジョニングの失敗を引き起こしました。この更新により、RHOSP **cluster-api-provider** に追加のフィルターが付加され、サブネットごとに 1 つのポートのみが存在するようになります。その結果、CiscoACI を使用して RHOSP-16 に OpenShift Container Platform をデプロイできるようになりました。(BZ#2050064)

- 以前は、特定のイメージを実行できなかった場合、**oc adm must gather** は **oc adm inspect** コマンドにフォールバックする必要がありました。その結果、フォールバックが発生したときにログから情報を解釈することは困難でした。この更新により、ログが改善され、フォールバック検査が実行されたときに明確になります。その結果、**oc adm must gather** の出力はより容易に理解できます。(BZ#2049427)

- 以前は、**oc debug node** コマンドでアイドル時にタイムアウトが指定されていませんでした。その結果、ユーザーがクラスターからログアウトすることはありませんでした。この更新では、非アクティブタイムアウトを無効にするために、デバッグ Pod の**TMOUT** 環境変数が追加されました。その結果、**TMOUT** が非アクティブになると、セッションは自動的に終了します。(BZ#2060888)

- 以前は、Ingress Operator は Ingress カナリアルートに対して可用性チェックを実行していました。可用性チェックが完了すると、**keepalive** パケットが接続で有効になっているため、Ingress Operator は **LoadBalancer** への TCP 接続を閉じませんでした。次の可用性チェックの実行中に、既存の接続を使用する代わりに、**LoadBalancer** への新しい接続が確立されました。その結果、これにより接続が **LoadBalancer** に蓄積されました。時間の経過とともに、これにより **LoadBalancer** の接続数が使い果たされました。この更新では、Ingress カナリアルートに接続するときにキープアライブが無効になります。その結果、カナリアプローブが実行されるたびに、新しい接続が確立され、閉じられます。キープアライブが無効になっている間、確立された接続の蓄積はなくなります。(BZ#2063283)

- 以前は、**Topology** UI の**Trigger/Subscription** モーダルのイベントソースのシンクには、スタンドアロンとして作成されたか、バック KSVC、ブローカー、または KameletBinding に含まれ、基礎となるリソースとして作成されたかに関係なく、すべてのリソースが表示されていました。その結果、ユーザーは、シンクドロップダウンメニューに表示されたときに、基礎になるアドレス指定可能なリソースにシンクする可能性があります。この更新により、スタンドアロンのリソースシンクイベントのみを表示するリソースフィルターが追加されました。(BZ#2059807)

1.9.4.4. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.5. RHSA-2022:1162 - OpenShift Container Platform 4.10.8 バグ修正およびセキュリティー更新

発行日: 2022-04-07

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.8 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHSA-2022:1162 アドバイザリーにリスト表示されます。この更新に含まれる RPM パッケージは RHBA-2022:1161 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.8 --pullspecs
```

1.9.5.1. 削除された機能

OpenShift Container Platform 4.10.8 以降、イメージレジストリーの OpenShift Container Platform 4.10 から GoogleCloudPlatform ワークロード ID のサポートが削除されました。この変更は、イメージレジストリーへの悪影響が発見されたためです。

OpenShift Container Platform 4.10.21 では、イメージレジストリーで GCP Workload Identity を使用するためのサポートが復活しました。OpenShift Container Platform 4.10.8 から 4.10.20 までのこの機能のステータスに関する詳細は、関連する ナレッジベースの記事 を参照してください。

1.9.5.2. 既知の問題

- 現時点では、Web コンソールには、カスタム namespace にデプロイされた仮想マシンテンプレートが表示されません。デフォルトの namespace にデプロイされたテンプレートのみが Web コンソールに表示されます。回避策として、カスタム namespace にテンプレートをデプロイすることは避けてください。(BZ#2054650)

1.9.5.3. バグ修正

- 以前は、URL の **filename** パラメーターに疑問符や等号などの特殊文字が使用された場合にベアメタルコントローラー (BMC) によって作成された検証エラーのため、Infrastructure Operator は X11 ベースおよび X12 ベースのシステムをプロビジョニングできませんでした。今回の更新で、仮想メディアイメージがローカルファイルでサポートされている場合に、**filename** パラメーターを URL から削除されます。(BZ#2011626)

- 以前は、テンプレートから仮想マシンのクローンを作成するときに、ブートディスクが編集され、ストレージクラスが変更された場合、ダイアログボックスを閉じた後、オペレーターが行った変更が元に戻りました。この更新により、ストレージクラスに加えられた変更は、ダイアログボックスを閉じた後も設定されたままになります。(BZ#2049762)

- 以前は、**startupProbe** フィールドがコンテナーの定義に追加されていました。その結果、**startupProbe** はデバッグ Pod の作成時に問題を引き起こします。この更新により、**startupProbe** は、**Expose --keep-startup flag** パラメーターによってデバッグ Pod からデフォルトで削除されます。このパラメーターは、デフォルトで false に設定されています。(BZ#2068474)

- 以前は、Local Storage Operator (LSO) が作成した永続ボリューム (PV) に**OwnerReference** オブジェクトを追加していました。これにより、PV の削除要求により、Pod に接続されたまま PV が **terminating** 状態のままになることがあるという問題が発生することがありました。この更新により、LSO は**OwnerReference** オブジェクトを作成しなくなり、クラスター管理者は、ノードがクラスターから削除された後、未使用の PV を手動で削除できるようになりました。(BZ#2065714)

- この更新以前は、プライベート Git リポジトリーにシークレットが提供された場合、インポートストラテジーの検出は行われませんでした。その結果、シークレット値は使用される前にデコードされませんでした。この更新により、シークレット値は使用前にデコードされるようになりました。(BZ#2057507)

1.9.5.4. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.6. RHBA-2022:1241 - OpenShift Container Platform 4.10.9 バグ修正の更新

発行日: 2022-04-12

OpenShift Container Platform リリース 4.10.9 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:1241 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 RHBA-2022:1240 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.9 --pullspecs
```

1.9.6.1. 既知の問題

- OpenShift Container Platform 4.10.9 に更新すると、etcd Pod の起動に失敗し、etcd Operator が **degraded** 状態になります。この問題は、OpenShift Container Platform の今後のバージョンで解決される予定です。詳細は、etcd pod is failing to start after updating OpenShift Container Platform 4.9.28 or 4.10.9 および Potential etcd data inconsistency issue in OCP 4.9 and 4.10 を参照してください。

1.9.6.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.7. RHSA-2022:1357 - OpenShift Container Platform 4.10.10 バグ修正およびセキュリティー更新

発行日: 2022-04-20

OpenShift Container Platform リリース 4.10.10 が公開されました。この更新に含まれるバグ修正は、RHSA-2022:1357 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 RHBA-2022:1355 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.10 --pullspecs
```

1.9.7.1. バグ修正

- 以前は、Amazon Web Services (AWS) のクラスターストレージ Operator 認証情報リクエストに KMS ステートメントが含まれていませんでした。その結果、キーを提供できないため、永続ボリューム (PV) をデプロイできませんでした。この更新により、AWS のデフォルトの認証情報リクエストで、KMS のお客様が管理するキーを使用して暗号化されたボリュームをマウントできるようになりました。Cloud Credential Operator (CCO) を使用して手動モードで認証情報リクエストを作成する管理者は、それらの変更を手動で適用する必要があります。他の管理者は、この変更によって影響を受けることはありません。(**BZ#2072191**)

1.9.7.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.8. RHBA-2022:1431 - OpenShift Container Platform 4.10.11 バグ修正の更新

発行日: 2022-04-25

OpenShift Container Platform リリース 4.10.11 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:1431 アドバイザリーに記載されています。本リリース用の RPM パッケージはありません。

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 4.10.11 --pullspecs
```

1.9.8.1. バグ修正

- 以前は、テンプレートから仮想マシンのクローンを作成するときに、ブートディスクが編集され、ストレージクラスが変更された場合、ダイアログボックスを閉じた後、オペレーターが行った変更が元に戻りました。この更新により、ストレージクラスに加えられた変更は、ダイアログボックスを閉じた後も設定されたままになります。(BZ#2049762)

1.9.8.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.9. RHBA-2022:1601 - OpenShift Container Platform 4.10.12 バグ修正およびセキュリティー更新

発行日: 2022-05-02

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.12 が利用可能になりました。この更新に含まれるバグ修正は、RHBA-2022:1601 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-2022:1600 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.12 --pullspecs
```

1.9.9.1. バグ修正

- 以前は、インフラストラクチャー Operator は X11 ベースおよび X12 ベースのシステムをプロビジョニングできませんでした。これは、URL の **filename** パラメーターに疑問符や等号などの特殊文字が使用されたときにベアメタルコントローラー (BMC) によって作成された検証エラーが原因でした。今回の更新で、仮想メディアイメージがローカルファイルでサポートされている場合に、**filename** パラメーターを URL から削除されます。(BZ#2011626)

1.9.9.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.10. RHBA-2022:1690 - OpenShift Container Platform 4.10.13 バグ修正の更新

発行日: 2022-05-11

OpenShift Container Platform リリース 4.10.13 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:1690 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 RHBA-2022:1689 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.13 --pullspecs
```

1.9.10.1. バグ修正

- 以前は、OpenShift Container Platform 4.8 で Ingress オブジェクトを作成する場合、API の制限により、ユーザーはホスト名を使用してルートを定義したり、数値クラスターをインストールしたりできませんでした。この修正により、API の番号制限が削除され、ユーザーは番号を

使用してクラスターを作成し、ホスト名を使用してルートを定義できるようになりました。(BZ#2072739)

- 以前は、**JobTrackingWithFinalizers** 機能が原因で、ジョブに関連する Pod が OpenShift Container Platform 4.10 の終了状態でスタックしていました。この修正により、**JobTrackingWithFinalizers** 機能が無効になり、すべての Pod が意図したとおりに実行されるようになりました。(BZ2075831)

1.9.10.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.11. RHBA-2022:2178 - OpenShift Container Platform 4.10.14 バグ修正の更新

発行日: 2022-05-18

OpenShift Container Platform リリース 4.10.14 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:2178 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 RHBA-2022:2177 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.14 --pullspecs
```

1.9.11.1. 機能

1.9.11.1.1. 他のワーカーノードとは独立してコントロールプレーンを更新する

この更新により、**Update Cluster** モーダル内でクラスターの部分的な更新を実行できるようになりました。メンテナンスにかかる時間に対応するために、ワーカーノードまたはカスタムプールノードを更新することができます。各プールのプログレスバー内で一時停止および再開することもできます。1 つ以上のワーカープールまたはカスタムプールが一時停止されている場合、**Cluster Settings** ページの上部にアラートが表示されます。(BZ#2076777)

詳細は、Preparing to perform an EUS-to-EUS update および Updating a cluster using the web console を参照してください。

1.9.11.1.2. Web ターミナル Operator の一般提供

この更新により、**Web ターミナル Operator** が一般提供されるようになりました。

1.9.11.1.3. AWS premium_LRS および standardSSD_LRS ディスクタイプのサポート

今回の更新により、**premium_LRS**、**standardSSD_LRS**、または **standard_LRS** ディスクタイプを使用して、コントロールプレーンとコンピュートノードをデプロイできるようになりました。デフォルトでは、インストールプログラムは **premium_LRS** ディスクタイプでコントロールプレーンとコンピュートノードをデプロイします。以前の 4.10 リリースでは、**standard_LRS** ディスクタイプのみがサポートされていました。(BZ#2079589)

1.9.11.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.12. RHBA-2022:2258 - OpenShift Container Platform 4.10.15 バグ修正の更新

発行日: 2022-05-23

OpenShift Container Platform リリース 4.10.15 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:2258 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 RHBA-2022:2257 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.15 --pullspecs
```

1.9.12.1. バグ修正

- 以前は、Image Registry Operator は、IBM Cloud への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 (IPI) のインストールをブロックしていました。この更新により、認証情報を手動で作成するクラスターでは、管理者ロールが必要になります。(BZ#2083559)

1.9.12.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.13. RHBA-2022:4754 - OpenShift Container Platform 4.10.16 バグ修正の更新

発行日: 2022-05-31

OpenShift Container Platform リリース 4.10.16 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:4754 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 RHBA-2022:4753 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.16 --pullspecs
```

1.9.13.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.14. RHBA-2022:4882 - OpenShift Container Platform 4.10.17 バグ修正の更新

発行日: 2022-06-07

OpenShift Container Platform リリース 4.10.17 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:4882 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 RHBA-2022:4881 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.17 --pullspecs
```

1.9.14.1. バグ修正

- 以前は、ユーザー定義のメトリクスを格納する Prometheus のフェデレーションエンドポイントは公開されていませんでした。したがって、クラスター外のネットワークの場所からこれらのメトリクスをスクレイピングするためにアクセスすることはできませんでした。今回の更新により、フェデレーションエンドポイントを使用して、クラスター外のネットワークの場所からユーザー定義のメトリクスをスクレイピングできるようになりました。(BZ#2090602)

- 以前は、ユーザー定義プロジェクトの場合、Thanos Ruler 監視コンポーネントのデフォルトのデータ保持期間の値である 24 時間を変更できませんでした。今回の更新により、ユーザー定義プロジェクトの Thanos Ruler メトリクスデータを保持する期間を変更できるようになりました。(BZ#2090422)

1.9.14.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.15. RHBA-2022:4944 - OpenShift Container Platform 4.10.18 バグ修正およびセキュリティー更新

発行日: 2022-06-13

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.18 が利用可能になりました。この更新に含まれるバグ修正は、RHBA-2022:4944 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-2022:4943 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.18 --pullspecs
```

1.9.15.1. バグ修正

- 以前は、Alibaba Cloud は 20 GiB を超えるディスクボリュームでのみサポートされていました。その結果、20 GiB 未満の永続ボリューム要求 (PVC) に対して新しいボリュームを動的にプロビジョニングする試みは失敗していました。この更新により、OpenShift Container Platform は PVC のボリュームサイズを自動的に拡大し、少なくとも 20 GiB のサイズのボリュームをプロビジョニングするようになりました。(BZ#2076671)

- 以前は、Ingress Operator には、以前のバージョンの OpenShift Container Platform の **LoadBalancer-type** サービスのファイナライザーを削除するための不要なロジックがありました。この更新により、IngressOperator にはこのロジックが含まれなくなりました。(BZ#2082161)

1.9.15.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.16. RHBA-2022:5172 - OpenShift Container Platform 4.10.20 バグ修正の更新

発行日: 2022-06-28

OpenShift Container Platform リリース 4.10.20 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:5172 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 RHBA-2022:5171 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.20 --pullspecs
```

1.9.16.1. バグ修正

- 以前は、Bond Container Network Interface (CNI) バージョン 1.0 は、Multus Container Network Interface (CNI) プラグインと互換性がありませんでした。その結果、Bond-CNI IP アドレス管理 (IPAM) が **network-status** アノテーションを正しく入力していませんでした。この更新により、IPAM と Bond-CNI は Bond-CNI 1.0 をサポートするようになりました。(BZ#2084289)

- この更新の前は、使用されている実際のストレージクラスに関係なく、**Start Pipeline** ダイアログボックスに **gp2** がストレージクラスとして表示されていました。今回の更新により、**Start Pipeline** ダイアログボックスに実際のストレージクラス名が表示されるようになりました。

1.9.16.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.17. RHBA-2022:5428 - OpenShift Container Platform 4.10.21 バグ修正の更新

発行日: 2022-07-06

OpenShift Container Platform リリース 4.10.21 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:5428 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 RHBA-2022:5427 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.21 --pullspecs
```

1.9.17.1. 新機能

イメージレジストリーの Google Cloud Platform (GCP) Workload Identity のサポートを削除する OpenShift Container Platform 4.10.8 の機能変更は、OpenShift Container Platform 4.10.21 で解決されました。

1.9.17.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.18. RHBA-2022:5513 - OpenShift Container Platform 4.10.22 バグ修正の更新

発行日: 2022-07-11

OpenShift Container Platform リリース 4.10.22 が公開されました。この更新に含まれるバグ修正は、RHBA-2022:5513 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 RHBA-2022:5512 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.22 --pullspecs
```

1.9.18.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.19. RHBA-2022:5568 - OpenShift Container Platform 4.10.23 バグ修正の更新

発行日: 2022-07-20

OpenShift Container Platform リリース 4.10.23 が公開されました。更新に含まれるバグ修正は、RHBA-2022:5568 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、RHBA-2022:5567 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.23 --pullspecs
```

1.9.19.1. 機能

1.9.19.2. Topology Aware Lifecycle Manager (テクノロジープレビュー) を使用した管理対象クラスターの更新

Red Hat Advanced Cluster Management (RHACM) ポリシーを使用して、複数の単一ノード Openshift クラスターで更新を実行するためにアップストリームの Topology Aware Lifecycle Manager を使用できるようになりました。詳細は、About the Topology Aware Lifecycle Manager configuration を参照してください。

1.9.19.3. 低レイテンシー Redfish ハードウェアイベント配信 (テクノロジープレビュー)

OpenShift Container Platform は、ベアメタルクラスターで実行されているアプリケーションが、ハードウェアの変更や障害などの Redfish ハードウェアイベントにすぐに応答できるようにするハードウェアイベントプロキシーを提供するようになりました。

ハードウェアイベントプロキシーは、関連するアプリケーションが Redfish が検出するハードウェアイベントを消費できるようにするパブリッシュサブスクライブサービスをサポートします。プロキシーは Redfish v1.8 以降をサポートするハードウェアで実行する必要があります。Operator は **hw-event-proxy** コンテナーのライフサイクルを管理します。

REST API を使用すると、アプリケーションを開発して、温度のしきい値、ファン障害、ディスク損失、電源停止、メモリー障害などのイベントに消費および応答できます。永続的なストアのない信頼できるエンドツーエンドのメッセージングは、Advanced Message Queuing Protocol (AMQP) に基づいています。メッセージングサービスのレイテンシーは 10 ミリ秒の範囲にあります。

注記

この機能は、単一ノードの OpenShift クラスターでのみサポートされます。

1.9.19.4. ゼロタッチプロビジョニングの一般提供

ゼロタッチプロビジョニング (ZTP) を使用して、非接続環境で新しいエッジサイトに分散ユニットをプロビジョニングします。この機能は以前は OpenShift Container Platform 4.9 のテクノロジープレ

ビュー機能として導入されましたが、OpenShift Container Platform 4.11 では一般に利用可能となり、デフォルトで有効にされます。詳細は、ZTP 用のハブクラスターの準備 を参照してください。

1.9.19.5. ZTP の完了の表示

Red Hat Advanced Cluster Management (RHACM) 静的バリデーター通知ポリシーを使用して、ゼロタッチプロビジョニング (ZTP) インストールが完了したかどうかを確認するプロセスを簡素化する新しいツールが利用可能になりました。完了したインストールの条件を取得し、スポーククラスターの ZTP プロビジョニングが完了した場合にのみ準拠状態に移行することを検証することで、ZTP インストールの完了を示します。

このポリシーは、単一ノードクラスター、3 ノードクラスター、および標準クラスターのデプロイメントに使用できます。バリデーター通知ポリシーの詳細は、ZTP インストールの完了の表示 を参照してください。

1.9.19.6. ZTP の機能強化

OpenShift Container Platform 4.10 の場合、ハブクラスターの設定とソース CR の生成を容易にする多くの更新があります。スポーククラスター用の新しい PTP および UEFI セキュアブート機能も利用できます。これらの機能の概要は次のとおりです。

- **ztp-site-generate** コンテナー内の既存のソース CR を追加または変更するには、これを再構築し、通常はハブクラスターに関連付けられた切断されたレジストリーから、ハブクラスターで利用できるようにします。
- GitOps ゼロタッチプロビジョニング (ZTP) パイプラインを使用して、デプロイされた vRAN クラスターに PTP ファストイベントを設定することができます。
- GitOps ZTP パイプラインを使用してデプロイされた vRAN クラスターの UEFI セキュアブートを設定できます。
- Topology Aware Lifecycle Manager を使用して、設定 CR のハブクラスターへの適用をオーケストレーションすることができます。

1.9.19.7. マルチクラスターデプロイメントの ZTP サポート

ゼロタッチプロビジョニング (ZTP) は、単一ノードクラスター、3 ノードクラスター、および標準の OpenShift クラスターを含むマルチクラスターデプロイメントのサポートを提供します。これには、OpenShift のインストールと、分散ユニット (DU) の大規模なデプロイメントが含まれます。これにより、マスター、ワーカー、およびマスターとワーカーのロールを持つノードをデプロイできます。ZTP マルチノードサポートは、**SiteConfig** および **PolicyGenTemplate** カスタムリソース (CR) を使用して実装されます。全体の流れは単一ノードクラスターの ZTP サポートと同じですが、クラスターの種類によって設定に若干の違いがあります。

SiteConfig ファイル内:

- 単一ノードクラスターの場合、**nodes** セクションに 1 つのエントリーのみが必要になります。
- 3 ノードクラスターの場合、**nodes** セクションに 3 つのエントリーのみが定義されている必要があります。
- 標準 OpenShift クラスターの場合、**nodes** セクションに role: master を含むちょうど 3 つのエントリーと、role: worker を含む 1 つ以上の追加エントリーが必要です。

PolicyGenTemplate ファイルは、生成されたポリシーをどこに分類するかを Policy Generator に指示します。サンプル **PolicyGenTemplate** ファイルは、デプロイメントを簡素化するためのサンプルファイルを提供します。

- 一般的な **PolicyGenTemplate** ファイルの例は、すべてのタイプのクラスターで共通です。
- 単一ノード、3 ノード、および標準クラスターのグループ **PolicyGenTemplate** ファイルのサンプルが提供されます。
- 各サイトに固有のサイト固有の **PolicyGenTemplate** ファイルが提供されます。

マルチクラスターデプロイメントの詳細は、SiteConfig および ZTP を使用したマネージドクラスターのデプロイメント を参照してください。

1.9.19.8. Assisted Installer によるセキュアでない OS イメージのサポート

このリリースでは、IPI または ZTP の切断された環境でアシステッドインストーラーを使用して HTTPD サーバーの TLS を有効にする時のために、以下の警告が含まれています。これらの環境で HTTPD サーバーの TLS を有効にする場合、root 証明書がクライアントによって信頼された機関によって署名されていることを確認し、OpenShift Container Platform ハブおよびスポーククラスターと HTTPD サーバー間の信頼された証明書チェーンを検証する必要があります。信頼されていない証明書で設定されたサーバーを使用すると、イメージがイメージ作成サービスにダウンロードされなくなります。信頼されていない HTTPS サーバーの使用はサポートされていません。

1.9.19.9. 既知の問題

- Kubelet サービスモニターのスクレイプ間隔は現在、ハードコードされた値に設定されています。これは、ワークロードに使用できる CPU リソースが少ないことを意味します。(BZ#2035046)
- vRAN 分散ユニット用の単一ノード OpenShift クラスターのデプロイには、最大 4 時間かかる場合があります。(BZ#2035036)
- 現在、RHACM ポリシーがターゲットクラスターに適用された場合、その適用されたポリシーを含む **ClusterGroupUpgrade** CR を同じターゲットクラスターへの **managedPolicy** として再度作成できます。これはあり得ないはずです。(BZ#2044304)
- **ClusterGroupUpgrade** CR に **blockingCR** が指定されており、**blockingCR** がサイレントに失敗した場合 (クラスターのリストにタイプミスがある場合など)、クラスターに **blockingCR** が適用されていなくても、**ClusterGroupUpgrade** CR が適用されます。(BZ#2042601)
- 無効なスポーク名などの理由で **ClusterGroupUpgrade** CR 検証が失敗した場合、**ClusterGroupUpgrade** CR のステータスは、CR が無効であるかのように使用できません。(BZ#2040828)
- 現在、**ClusterGroupUpgrade** CR 状態の変更に使用できる条件タイプは **Ready** のみです。**Ready** 条件のステータスは、**True** または **False** のみです。これは、**ClusterGroupUpgrade** CR が取り得る状態の範囲を反映していません。(BZ#2042596)
- ベアメタルノードにマルチノードクラスターをデプロイする場合、マシン設定プール (MCP) は、コンテナーマウント namespace ドロップイン を回避する追加の CRI-O ドロップインを追加します。これにより、kubelet が非表示の namespace にあるのに対し、CRI-O は基本 namespace にあることになります。すべてのコンテナーは、シークレットやトークンなど、kubelet でマウントされたファイルシステムを取得できません。(BZ#2028590)

- カスタマイズされた namespace に RHACM 2.5.0 をインストールすると、十分な権限がないために **infrastructure-operator** Pod が失敗します。(BZ#2046554)

- OpenShift Container Platform は、オブジェクト名を 63 文字に制限します。**PolicyGenTemplate** CR で定義されたポリシー名がこの制限に近づくと、Topology Aware Lifecycle Manager は子ポリシーを作成できなくなります。これが発生すると、親ポリシーは **NonCompliant** 状態のままになります。(BZ#2057209)

- デフォルトの ZTP Argo CD 設定では、クラスター名は **ztp** で開始できません。ゼロタッチプロビジョニング (ZTP) でデプロイされるクラスター用に **ztp** で始まる名前を使用すると、プロビジョニングが完了しません。回避策として、クラスター名が **ztp** で起動しないか、クラスター名を除外し、ポリシー namespace に一致するパターンに Argo CD ポリシーアプリケーション namespace を調整するようにしてください。たとえば、クラスター名が **ztp** で開始する場合は、Argo CD ポリシーアプリ設定のパターンを **ztp-** などの異なるものに変更します。(BZ#2049154)

- スポーククラスターのアップグレード中に、1 つ以上の調整エラーがコンテナーログに記録されます。エラーの数は、子ポリシーの数に対応します。このエラーは、クラスターに目立った影響を与えません。以下は調整エラーの例です。

  ```
  2022-01-21T00:14:44.697Z	INFO	controllers.ClusterGroupUpgrade Upgrade is completed
  2022-01-21T00:14:44.892Z	ERROR	controller-runtime.manager.controller.clustergroupupgrade	Reconciler error	{"reconciler group": "ran.openshift.io", "reconciler kind": "ClusterGroupUpgrade", "name": "timeout", "namespace": "default", "error": "Operation cannot be fulfilled on clustergroupupgrades.ran.openshift.io \"timeout\": the object has been modified; please apply your changes to the latest version and try again"}
  sigs.k8s.io/controller-runtime/pkg/internal/controller.(*Controller).processNextWorkItem
  	/go/pkg/mod/sigs.k8s.io/controller-runtime@v0.9.2/pkg/internal/controller/controller.go:253
  sigs.k8s.io/controller-runtime/pkg/internal/controller.(*Controller).Start.func2.2
  	/go/pkg/mod/sigs.k8s.io/controller-runtime@v0.9.2/pkg/internal/controller/controller.go:214
  ```

  (BZ#2043301)

- 4.9 から 4.10 へのスポーククラスターのアップグレード中に、負荷の高いワークロードが実行されていると、**kube-apiserver** Pod の起動に予想以上の時間がかかる場合があります。その結果、アップグレードは完了せず、**kube-apiserver** は以前のバージョンにロールバックします。(BZ#2064024)

- AMQ Interconnect Operator をデプロイする場合、Pod は IPv4 ノードでのみ実行されます。AMQ Interconnect Operator は、IPv6 ノードではサポートされません。(ENTMQIC-3297)

1.9.19.10. バグ修正

- 以前は、Ingress Operator は Ingress Controller によって行われた変更を検出し、Ingress Operator の **Upgradeable** ステータス条件を **False** に設定していました。**False** ステータス条件により、アップグレードがブロックされていました。今回の更新により、Ingress Operator はアップグレードをブロックしなくなりました。(BZ#2097735)

1.9.19.11. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.20. RHSA-2022:5664 - OpenShift Container Platform 4.10.24 バグ修正およびセキュリティー更新

発行日: 2022-07-25

OpenShift Container Platform リリース 4.10.24 が公開されました。この更新に含まれるバグ修正の一覧は、RHSA-2022:5664 アドバイザリーにまとめられています。本リリース用の RPM パッケージはありません。

以下のコマンドを実行して、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 4.10.24 --pullspecs
```

1.9.20.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.21. RHSA-2022:5730 - OpenShift Container Platform 4.10.25 バグ修正およびセキュリティー更新

発行日: 2022-08-01

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.25 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2022:5730 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHSA-2022:5729 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.25 --pullspecs
```

1.9.21.1. バグ修正

- 以前は、クラスターに Security Context Constraint (SCC) があった場合、デフォルトの IngressController Deployment によって Pod の起動に失敗することがありました。これは、コンテナーの **securityContext** で、十分な権限を要求せずにデフォルトのコンテナー名 **router** が作成されたことが原因となっていました。今回の更新により、ルーター Pod は正しい SCC に許可され、エラーなしで作成されます。(BZ#2079034)

- 以前は、終了状態のルーターは **oc cp** コマンドを遅らせ、それが **must-gather** を遅らせていました。今回の更新で、各 **oc cp** コマンドのタイムアウトが設定され、**must-gathers** の遅延がなくなりました。(BZ#2106842)

1.9.21.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.22. RHSA-2022:5875 - OpenShift Container Platform 4.10.26 バグ修正およびセキュリティー更新

発行日: 2022-08-08

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.26 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2022:5875 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:5874 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.26 --pullspecs
```

1.9.22.1. バグ修正

- 以前のバージョンでは、新規リージョンは AWS SDK によって認識されず、マシンコントローラーはそれらを使用できませんでした。この問題は、AWS SDK がベンダーに渡された時点からしか、AWS SDK はリージョンを認識しないために発生していました。今回の更新により、管理者は **DescribeRegions** を使用してマシンに指定されたリージョンを確認し、SDK が認識していないリージョンに新しいマシンを作成できるようになりました。(BZ#2109124)

注記

これは新規の AWS パーミッションで、新規パーミッションで手動モードクラスターの認証情報を更新する必要があります。

1.9.22.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.23. RHBA-2022:6095 - OpenShift Container Platform 4.10.28 バグ修正およびセキュリティー更新

発行日: 2022-08-23

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.28 が利用可能になりました。更新に含まれるバグ修正は、RHBA-2022:6095 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-2022:6094 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.28 --pullspecs
```

1.9.23.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.24. RHSA-2022:6133 - OpenShift Container Platform 4.10.30 バグ修正およびセキュリティー更新

発行日: 2022-08-31

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.30 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2022:6133 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:6132 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.30 --pullspecs
```

1.9.24.1. 機能

1.9.24.1.1. セカンダリーネットワークの Pod レベルのボンディングの一般提供

今回の更新により、**Pod レベルのボンディングの使用** が一般提供されるようになりました。

1.9.24.2. バグ修正

- 以前は、Bond-CNI の機能はアクティブバックアップモードのみに制限されていました。今回の更新で、サポートされるボンディングモードは次のとおりです。
  - **balance-rr** -0
  - **active-backup** -1
  - **balance-xor** -2

  (BZ#2102047)

1.9.24.3. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.25. RHSA-2022:6258 - OpenShift Container Platform 4.10.31 バグ修正およびセキュリティー更新

発行日: 2022-09-07

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.31 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2022:6258 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:6257 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.31 --pullspecs
```

1.9.25.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.26. RHBA-2022:6372 - OpenShift Container Platform 4.10.32 バグ修正

発行日: 2022-09-13

OpenShift Container Platform リリース 4.10.32 が公開されました。更新に含まれるバグ修正は、RHBA-2022:6372 アドバイザリーに記載されています。本リリース用の RPM パッケージはありません。

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 4.10.32 --pullspecs
```

1.9.26.1. バグ修正

- 以前は、PROXY プロトコルを使用するデュアルスタッククラスターは、IPv4 ではなく IPv6 でのみ有効でした。今回の更新により、OpenShift Container Platform は、デュアルスタッククラスターで IPv6 と IPv4 の両方に対して PROXY プロトコルを有効にするようになりました。(BZ#2096362)

1.9.26.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.27. RHBA-2022:6532 - OpenShift Container Platform 4.10.33 バグ修正およびセキュリティー更新

発行日: 2022-09-20

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.33 が利用可能になりました。更新に含まれるバグ修正は、RHBA-2022:6532 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-2022:6531 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.33 --pullspecs
```

1.9.27.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.28. RHBA-2022:6663 - OpenShift Container Platform 4.10.34 バグ修正およびセキュリティー更新

発行日: 2022-09-27

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.34 が利用可能になりました。更新に含まれるバグ修正は、RHBA-2022:6663 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-2022:6661 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.34 --pullspecs
```

1.9.28.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.29. RHBA-2022:6728 - OpenShift Container Platform 4.10.35 バグ修正の更新

発行日: 2022-10-04

OpenShift Container Platform リリース 4.10.35 が公開されました。更新に含まれるバグ修正は、RHBA-2022:6728 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、RHBA-2022:6727 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.35 --pullspecs
```

1.9.29.1. バグ修正

- 以前は、Ingress Operator のロジックは、 **openshift-ingress** namespace の kubernetes サービスオブジェクトが、調整しようとしている Ingress コントローラーによって作成されたかどうかを検証しませんでした。その結果、Operator は、所有権に関係なく、同じ名前と namespace を持つ kubernetes サービスを変更または削除します。今回の更新により、Ingress Operator は、作成または削除しようとしている既存の kubernetes サービスの所有権を確認するようになりました。所有権が一致しない場合、Ingress Operator はエラーを提供します。(OCPBUGS-1623)

1.9.29.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.30. RHSA-2022:6805 - OpenShift Container Platform 4.10.36 バグ修正の更新

発行日: 2022-10-12

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.36 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2022:6805 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 RHBA-2022:6803 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.36 --pullspecs
```

1.9.30.1. バグ修正

- 以前のバージョンでは、ルータープロセスは初期化中に **SIGTERM** シャットダウンシグナルを無視していました。これにより、コンテナーのシャットダウン時間が 1 時間になりました。今回の更新により、ルーターは初期化中に **SIGTERM** シグナルに応答するようになりました。(BZ#2098230)

1.9.30.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.31. RHBA-2022:6901 - OpenShift Container Platform 4.10.37 バグ修正の更新

発行日: 2022-10-18

OpenShift Container Platform リリース 4.10.37 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2022:6901 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:6899 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.37 --pullspecs
```

1.9.31.1. バグ修正

- 以前は、IP アドレスを 1 つ以上のコントロールプレーンノードに追加すると、etcd クラスター Operator がノードの etcd サービス証明書を再生成できませんでした。今回の更新により、etcd クラスター Operator は、既存のノードへの変更に対してサービング証明書を再生成します。(**OCPBUGS-1758**)

1.9.31.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.32. RHBA-2022:7035 - OpenShift Container Platform 4.10.38 バグ修正の更新

発行日: 2022-10-25

OpenShift Container Platform release 4.10.38 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2022:7035 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:7033 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.38 --pullspecs
```

1.9.32.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.33. RHSA-2022:7211 - OpenShift Container Platform 4.10.39 バグ修正およびセキュリティー更新

発行日: 2022-11-01

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.39 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2022:7211 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 RHBA-2022:7210 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.39 --pullspecs
```

1.9.33.1. 主な技術上の変更点

- このリリースでは、サービスアカウント発行者がカスタム発行者に変更されたときに、既存のバインドされたサービストークンがすぐに無効になることはなくなりました。代わりに、サービスアカウントの発行者が変更されると、以前のサービスアカウントの発行者が 24 時間引き続き信頼されます。

詳細は、ボリュームプロジェクションを使用したバインドされたサービスアカウントトークンの設定 を参照してください。

1.9.33.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.34. RHBA-2022:7298 - OpenShift Container Platform 4.10.40 バグ修正の更新

発行日: 2022-11-09

OpenShift Container Platform リリース 4.10.40 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2022:7298 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:7297 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.40 --pullspecs
```

1.9.34.1. バグ修正

- この更新の前は、**noAllowedAddressPairs** 設定が同じネットワーク上のすべてのサブネットに適用されていました。今回の更新により、**noAllowedAddressPairs** 設定は、一致するサブネットにのみ適用されるようになりました。(**OCPBUGS-1951**)

1.9.34.2. 主な技術上の変更点

- Cloud Credential Operator ユーティリティー (**ccoctl**) は、AWS Security Token Service (AWS STS) のリージョンエンドポイントを使用するシークレットを作成するようになりました。このアプローチは、AWS の推奨のベストプラクティスに準拠しています。

1.9.34.3. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.35. RHBA-2022:7866 - OpenShift Container Platform 4.10.41 バグ修正およびセキュリティー更新

発行日: 2022-11-18

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.41 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHBA-2022:7866 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHSA-2022:7865 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.41 --pullspecs
```

1.9.35.1. 主な技術上の変更点

- 今回のリリースでは Cloud Credential Operator ユーティリティーを使用して GCP リソースを削除する ときに、コンポーネントの **CredentialsRequest** オブジェクトのファイルを含むディレクトリーを指定する必要があります。

1.9.35.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.36. RHBA-2022:8496 - OpenShift Container Platform 4.10.42 バグ修正の更新

発行日: 2022-11-22

OpenShift Container Platform リリース 4.10.42 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2022:8496 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:8495 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.42 --pullspecs
```

1.9.36.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.37. RHBA-2022:8623 - OpenShift Container Platform 4.10.43 バグ修正の更新

発行日: 2022-11-29

OpenShift Container Platform リリース 4.10.43 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2022:8623 アドバイザリーにまとめられています。この更新に含まれる RPM パッケージは、RHBA-2022:8622 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.43 --pullspecs
```

1.9.37.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.38. RHBA-2022:8882 - OpenShift Container Platform 4.10.45 バグ修正の更新

発行日: 2022-12-14

OpenShift Container Platform リリース 4.10.45 が公開されました。更新に含まれるバグ修正は RHBA-2022:8882 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-2022:8881 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.45 --pullspecs
```

1.9.38.1. バグ修正

- 以前は、一部のオブジェクトストレージインスタンスは、コンテンツが表示されていない場合に **204 No Content** で応答していました。OpenShift Container Platform で使用される Red Hat OpenStack Platform (RHOSP) SDK は、204 を正しく処理しませんでした。今回の更新により、インストールプログラムは、一覧表示する項目がない場合の問題を回避します。(OCPBUGS-4160)

1.9.38.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.39. RHBA-2022:9099 - OpenShift Container Platform 4.10.46 バグ修正およびセキュリティー更新

発行日: 2023-01-04

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.46 が利用可能になりました。更新に含まれるバグ修正は RHBA-2022:9099 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-2022:9098 アドバイザリーで提供されています。

以下のコマンドを実行して、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 4.10.46 --pullspecs
```

1.9.39.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.40. RHSA-2023:0032 - OpenShift Container Platform 4.10.47 バグ修正およびセキュリティー更新

発行日: 2023-01-04

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.47 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2023:0032 アドバイザリーに記載されています。更新に含まれる RPM パッケージは RHBA-2023:0031 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.47 --pullspecs
```

1.9.40.1. 機能強化

- SR-IOV CNI プラグインで、IPv6 未承認ネイバーアドバタイズメントと IPv4 Gratuitous アドレス解決プロトコルがデフォルトになりました。IP アドレス管理 CNI プラグインが IP を割り当てたシングルルート I/O 仮想化 (SR-IOV) CNI プラグインで作成された Pod は、IPv6 未承認ネイバーアドバタイズメントおよび/または IPv4 Gratuitous アドレス解決プロトコルをデフォルトでネットワークへ送信します。この機能強化により、特定の IP の新しい Pod の MAC アドレスがホストに通知され、正しい情報で ARP/NDP キャッシュが更新されます。詳細は、サポート対象のデバイス を参照してください。

1.9.40.2. バグ修正

- 以前は、CoreDNS v1.7.1 では、すべてのアップストリームキャッシュ更新で DNSSEC が使用されていました。アップストリームクエリーの bufsize は 2048 バイトにハードコードされていたため、ネットワークインフラストラクチャー内に UDP ペイロードの制限がある場合は、一部の DNS アップストリームクエリーが壊れていました。今回の更新により、OpenShift Container Platform はアップストリームのキャッシュ要求に常に bufsize 512 を使用します。これは Corefile で指定された bufsize です。アップストリーム DNS 要求に対して bufsize 2048 の不適切な機能に依存している場合は、お客様が影響を受ける可能性があります。(OCPBUGS-2902)

- 以前は、OpenShift Container Platform は **204 No Content** で応答したオブジェクトストレージインスタンスを処理しませんでした。これにより、Red Hat OpenStack Platform (RHOSP) SDK で問題が発生しました。今回の更新により、インストールプログラムは、Swift コンテナーに一覧表示するオブジェクトがない場合の問題を回避します。(OCPBUGS-5112)

1.9.40.3. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.41. RHSA-2023:0241 - OpenShift Container Platform 4.10.50 のバグ修正とセキュリティー更新

発行日: 2023-01-24

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.50 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:0241 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:0240 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.50 --pullspecs
```

1.9.41.1. バグ修正

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) 認証情報のローテーション時に、Cinder Container Storage Interface ドライバーはそのまま以前の認証情報を使用していました。以前の無効な認証情報を使用すると、すべてのボリューム操作に失敗します。今回の更新により、Red Hat OpenStack Platform (RHOSP) 認証情報が更新されると、Cinder Container Storage Interface ドライバーが自動的に更新されます。(OCPBUGS-4717)

- * 以前のリリースでは、Pod の障害によって証明書の有効期間が人為的に延長され、証明書が正しくローテーションされませんでした。今回の更新により、証明書の有効期間が正確に決定され、証明書が正しくローテーションされるようになりました。(BZ#2020484)

1.9.41.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.42. RHSA-2023:0561 - OpenShift Container Platform 4.10.51 のバグ修正とセキュリティー更新

発行日: 2023-02-08

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.51 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:0561 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:0560 アドバイザリーで提供されます。

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 4.10.51 --pullspecs
```

1.9.42.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.43. RHSA-2023:0698 - OpenShift Container Platform 4.10.52 のバグ修正とセキュリティー更新

発行日: 2023-02-15

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.52 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:0698 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:0697 アドバイザリーで提供されます。

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 4.10.52 --pullspecs
```

1.9.43.1. バグ修正

- 以前は、Redfish システムが設定 URI を備えている場合、Ironic プロビジョニングサービスは常にこの URI を使用して、ブート関連の BIOS 設定を変更しようとしていました。ただし、ベースボード管理コントローラー (BMC) が設定 URI を備えていても、この設定 URI を使用した特定の BIOS 設定の変更をサポートしていない場合、ベアメタルプロビジョニングは失敗します。OpenShift Container Platform 4.10 以降では、システムに設定 URI がある場合には、Ironic は続行する前に設定 URI を使用して特定の BIOS 設定を変更できることを確認します。それ以外の場合、Ironic はシステム URI を使用して変更を実装します。この追加のロジックにより、Ironic がブート関連の BIOS 設定の変更を適用でき、ベアメタルプロビジョニングが成功することが保証されます。(OCPBUGS-6886)

- 以前のリリースでは、**spec.provider** の定義が欠落していたため、**Operator details** ページで **ClusterServiceVersion** を表示しようとして失敗していました。今回の更新により、ユーザーインターフェイスは **spec.provider** なしで動作し、**Operator details** ページで問題が発生しなくなりました。(OCPBUGS-6690)

1.9.43.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.44. RHSA-2023:0698 - OpenShift Container Platform 4.10.53 のバグ修正とセキュリティー更新

発行日: 2023-03-01

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.53 が利用可能になりました。更新に含まれるバグ修正は RHSA-2023:0899 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:0898 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.53 --pullspecs
```

1.9.44.1. バグ修正

- Swift がインストールされていない OpenStack クラウドとの互換性を保つために、Cluster Image Registry Operator (CIRO) には、最初の起動時にストレージバックエンドを自動的に選択するメカニズムがあります。Swift が使用可能な場合は、Swift が使用されます。それ以外の場合は、永続ボリューム要求 (PVC) が発行され、ブロックストレージが使用されます。以前のリリースでは、Swift に到達できなかった場合、CIRO は PVC の使用にフォールバックしていました。特に、最初の起動時に接続が失われると、CIRO は PVC の使用にフォールバックします。今回の変更により、OpenStack API への到達の失敗、またはその他の偶発的な失敗が発生すると、CIRO はプローブを再試行します。PVC へのフォールバックは、OpenStack カタログが正しく検出され、そこにオブジェクトストレージが含まれていない場合、または現在のユーザーがコンテナーを一覧表示する権限を持っていない場合にのみ発生します。(**OCPBUGS-5974**)

- 以前のリリースでは、ユーザープロビジョニングインフラストラクチャー (UPI) はコンピュートマシンのサーバーグループを作成しませんでした。OpenShift Container Platform 4.10 は UPI スクリプトを更新し、スクリプトがコンピュートマシンのサーバーグループを作成するようにします。UPI スクリプトのインストール方法は、インストーラープロビジョニングインストール (IPI) 方法と同じになりました。(**OCPBUGS-2731**)

1.9.44.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.45. RHSA-2023:1154 - OpenShift Container Platform 4.10.54 のバグ修正とセキュリティー更新

発行日 2023-03-15

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.54 が利用可能になりました。更新に含まれるバグ修正は RHSA-2023:1154 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:1153 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.54 --pullspecs
```

1.9.45.1. バグ修正

- 以前は、OpenShift Container Platform コンソールでパイプラインを編集すると、**パイプラインビルダー** および **YAML ビュー** 設定オプションで正しいデータがレンダリングされず、**パイプラインビルダー** でパイプラインを編集できませんでした。今回の更新により、データが正しく解析され、ビルダーを使用してパイプラインを編集できるようになりました。(OCPBUGS-7657)

1.9.45.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.46. RHSA-2023:1392 - OpenShift Container Platform 4.10.55 のバグ修正とセキュリティー更新

発行日 2023 年 3 月 29 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.55 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:1392 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2023:1391 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.55 --pullspecs
```

1.9.46.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.47. RHSA-2023:1656 - OpenShift Container Platform 4.10.56 のバグ修正とセキュリティー更新

発行日: 2023-04-12

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.56 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:1656 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:1655 アドバイザリーで提供されます。

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 4.10.56 --pullspecs
```

1.9.47.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.48. RHBA-2023:1782 - OpenShift Container Platform 4.10.57 バグ修正の更新

発行日: 2023-04-19

OpenShift Container Platform リリース 4.10.57 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:1782 アドバイザリーに記載されています。この更新用の RPM パッケージはありません。

以下のコマンドを実行して、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 4.10.57 --pullspecs
```

1.9.48.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.49. RHBA-2023:1867 - OpenShift Container Platform 4.10.58 のバグ修正とセキュリティー更新

発行日: 2023-04-26

OpenShift Container Platform リリース 4.10.58 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:1867 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:1866 アドバイザリーで提供されます。

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 4.10.58 --pullspecs
```

1.9.49.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.50. RHBA-2023:2018 - OpenShift Container Platform 4.10.59 バグ修正の更新

発行日: 2023-05-03

OpenShift Container Platform リリース 4.10.59 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:2018 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:2017 アドバイザリーで提供されます。

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 4.10.59 --pullspecs
```

1.9.50.1. バグ修正

- 以前は、トポロジーサイドバーに更新された情報が表示されませんでした。トポロジーサイドバーからリソースを直接更新した場合、サイドバーを再度開いて変更を確認する必要がありました。今回の修正により、更新されたリソースが正しく表示されるようになりました。トポロジーサイドバーで、最新の変更を直接確認できます。(OCPBUGS-12438)

- 以前のリリースでは、**Secret** の作成時に、**Start Pipeline** モデルが無効な JSON 値を作成していました。その結果、**Secret** が使用できなくなり、**PipelineRun** が失敗する可能性がありまし

た。今回の修正により、**Start Pipeline** モデルがシークレットの有効な JSON 値を作成するようになりました。パイプラインの開始時に有効なシークレットを作成できるようになりました。(OCPBUGS-7961)

1.9.50.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.51. RHBA-2023:3217 - OpenShift Container Platform 4.10.60 のバグ修正とセキュリティー更新

発行日: 2023-05-24

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.60 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:3217 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:3216 アドバイザリーで提供されます。

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 4.10.60 --pullspecs
```

1.9.51.1. 機能

1.9.51.1.1. MetalLB ログの冗長性の制御

- このリリースでは、MetalLB ログの冗長性を制御できます。MetalLB カスタムリソース (CR) の **logLevel** 仕様に次の値を使用して、ログレベルを制御できます。
  - all
  - debug
  - info
  - warn
  - error
  - none

  たとえば、**debug** 値を指定して、トラブルシューティングに役立つ診断ログ情報を含めることができます。

  MetalLB のログレベルの詳細は、MetalLB ログレベルの設定 (OCPBUGS-11861) を参照してください。

1.9.51.2. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順は、CLI の使用によるマイナーバージョン間でのクラスターの更新 を参照してください。

1.9.52. RHSA-2023:3363 - OpenShift Container Platform 4.10.61 のバグ修正とセキュリティー更新

発行日 2023 年 6 月 7 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.61 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:3363 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:3362 アドバイザリーで提供されます。

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 4.10.61 --pullspecs
```

1.9.52.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.53. RHSA-2023:3626 - OpenShift Container Platform 4.10.62 のバグ修正とセキュリティー更新

発行日: 2023 年 6 月 23 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.62 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:3626 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:3625 アドバイザリーで提供されます。

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 4.10.62 --pullspecs
```

1.9.53.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.54. RHSA-2023:3911 - OpenShift Container Platform 4.10.63 のバグ修正とセキュリティー更新

発行日: 2023-07-06

セキュリティー更新を含む OpenShift Container Platform リリース 4.10.63 が利用可能になりました。この更新には、OpenShift Container Platform を FIPS モードで実行する顧客向けの Red Hat セキュリティー情報が含まれています。詳細は、RHSB-2023:001 を参照してください。

更新に含まれるバグ修正は、RHSA-2023:3911 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:3910 アドバイザリーで提供されます。

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 4.10.63 --pullspecs
```

1.9.54.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.55. RHBA-2023:4217 OpenShift Container Platform 4.10.64 バグ修正の更新

発行日: 2023-07-26

OpenShift Container Platform リリース 4.10.64 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:4217 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、 RHBA-2023:4219 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.64 --pullspecs
```

1.9.55.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.56. RHBA-2023:4445 - OpenShift Container Platform 4.10.65 バグ修正の更新

発行日: 2023 年 8 月 9 日

OpenShift Container Platform リリース 4.10.65 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:4445 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、 RHBA-2023:4447 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.65 --pullspecs
```

1.9.56.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

1.9.57. RHBA-2023:4667 OpenShift Container Platform 4.10.66 バグ修正の更新

発行日: 2023 年 8 月 23 日

OpenShift Container Platform リリース 4.10.66 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:4667 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、 RHBA-2023:4669 アドバイザリーによって提供されます。

以下のコマンドを実行して、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 4.10.66 --pullspecs
```

1.9.57.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。

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

発行日: 2023-10-10

セキュリティー更新を含む OpenShift Container Platform リリース 4.13.15 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:4667 アドバイザリーに記載されています。この更新に含まれる RPM パッケージは、RHSA-2023:3910 アドバイザリーで提供されます。

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 4.10.67 --pullspecs
```

1.9.58.1. 更新

既存の OpenShift Container Platform 4.10 クラスターをこの最新リリースに更新する手順については、Updating a cluster using the CLI を参照してください。