OpenShift Container Platform 4.11

リリースノート

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

Last Updated: 2024-03-29

OpenShift Container Platform 4.11 リリースノート

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

法律上の通知

概要

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

目次

第1章 OPENSHIFT CONTAINER PLATFORM 4.11 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-2022:5069) 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 1.24 を使用します。以下では、OpenShift Container Platform 4.11 に関連する新機能、変更点および既知の問題について説明します。

OpenShift Container Platform 4.11 クラスターは https://console.redhat.com/openshift で入手できます。OpenShift Container Platform 向けの Red Hat OpenShift Cluster Manager アプリケーションを使用して、OpenShift 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 4.12 は、Red Hat Enterprise Linux (RHEL) 8.6 および Red Hat Enterprise Linux CoreOS (RHCOS) 4.12 でサポートされています。

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

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

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

1.3. 新機能および機能拡張

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

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. Fabric での NVMe サポートの改善

OpenShift Container Platform 4.11 では、NVMe デバイスを管理するためのインターフェイスを提供する **nvme-cli** パッケージが導入されました。

1.3.1.2. kdump で AMD64 マシンでのカーネルクラッシュの調査

RHCOS は、OpenShift Container Platform 4.11 の **x86_64** アーキテクチャーの **kdump** に対応するようになりました。他のアーキテクチャーでの **kdump** のサポートは依然としてテクノロジープレビューです。

1.3.1.3. kdump で ARM64 マシンでのカーネルクラッシュの調査 (テクノロジープレビュー)

RHCOS は、テクノロジープレビューとして OpenShift Container Platform 4.11 の **arm64** アーキテクチャーの **kdump** をサポートするようになりました。

1.3.1.4. RHCOS が RHEL 8.6 を使用するようになる

RHCOS は、OpenShift Container Platform 4.11 以降で Red Hat Enterprise Linux(RHEL)8.6 パッケージを使用するようになりました。これにより、最新の修正、機能、機能拡張、および最新のハードウェアサポートおよびドライバー更新を利用できます。

1.3.1.5. 更新された RHCOS レジストリー URL

RHCOS ブートイメージのダウンロード用のリ director ホスト名は **rhcos.mirror.openshift.com** になりました。ブートイメージへのアクセス権限を付与するようにファイアウォールを設定する必要があります。詳細は、Configuring your firewall for OpenShift Container Platform を参照してください。

1.3.2. インストールおよびアップグレード

1.3.2.1. OpenShift インストーラーの RHEL 9 サポート

OpenShift インストーラー (openshift-install) での Red Hat Enterprise Linux (RHEL) 9 の使用がサポートされるようになりました。

詳細は、お使いのプラットフォームのインストールドキュメントの "Obtaining the installation program" セクションを参照してください。

1.3.2.2. OpenShift Container Platform を単一ノードにインストールするための新規の最小要件

今回のリリースにより、OpenShift Container Platform を単一ノードにインストールするための最小要件が更新されました。OpenShift Container Platform を単一ノードにインストールする場合は、最低 16 GB の RAM を設定する必要があります。特定のワークロード要件では、追加の RAM が必要になる場合があります。サポート対象プラットフォームの完全なリストは、ベアメタル、vSphere、Red Hat OpenStack Platform (RHOSP)、および Red Hat Virtualization プラットフォームが含まれるように更新されました。いずれの場合も、**openshift-installer** バイナリーが single-node OpenShift のインストールに使用される際に、**install-config.yaml** 設定ファイルに **platform.none: {}** パラメーターを指定する必要があります。

1.3.2.3. ARM 上の OpenShift Container Platform

OpenShift Container Platform 4.11 は、ARM アーキテクチャーベースの AWS のユーザーによってプロビジョニングされるインフラストラクチャーおよびベアメタル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やインストールに関するドキュメントの詳細は、Supported installation methods for different platforms 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。

- 非接続インストールのサポート

- AWS 用の Elastic File System (EFS)
- ベアメタル上のローカルストレージ Operator
- ベアメタル用の Internet Small Computer Systems Interface (iSCSI)

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

- Special resource operator (SRO)

1.3.2.4. AWS へのインストール時におけるブートストラップ障害のトラブルシューティング

インストールプログラムは、AWS のブートストラップおよびコントロールプレーンホストから、シリアルコンソールログを収集するようになりました。このログデータは標準のブートストラップログバンドルに追加されます。

詳細は、インストールに関する問題のトラブルシューティング を参照してください。

1.3.2.5. Microsoft Hyper-V 生成バージョン 2 のサポート

デフォルトでは、インストールプログラムは、Hyper-V 生成バージョン 2 仮想マシン (VM) を使用して Microsoft Azure クラスターをデプロイするようになりました。仮想マシンに選択したインスタンスタイプがバージョン 2 に対応していないことをインストールプログラムが検出すると、デプロイメントにバージョン 1 が使用されます。

1.3.2.6. デフォルトの AWS および VMware vSphere コンピュートノードリソース

OpenShift Container Platform 4.11 以降、インストールプログラムは、4 vCPU および 16 GB の仮想 RAM を持つ AWS および VMware vSphere コンピュートノードをデプロイするようになりました。

1.3.2.7. AWS SC2S リージョンのサポート

OpenShift Container Platform 4.11 では、AWS Secret Commercial Cloud Services (SC2S) リージョンのサポートが追加されました。OpenShift Container Platform クラスターを **us-isob-east-1** SC2S リージョンにインストールし、更新できるようになりました。

詳細は、Installing a cluster on AWS into a Secret or Top Secret Region を参照してください。

1.3.2.8. 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 Nutanix へのクラスターのインストール

OpenShift Container Platform 4.11 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 Nutanix 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。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。

詳細は、Installing a cluster on Nutanix を参照してください。

1.3.2.9. Azure Ultra SSD を使用した OpenShift Container Platform のインストール

OpenShift Container Platform を Azure にインストールする際に、Ultra SSD ストレージを有効にできるようになりました。この機能には、OpenShift Container Platform をインストールする Azure リージョンとゾーンの両方が Ultra ストレージを提供する必要があります。

詳細は、Additional Azure configuration parameters を参照してください。

1.3.2.10. bootstrapExternalStaticIP および bootstrapExternalStaticGateway の設定に対するサポートの追加

インストーラーでプロビジョニングされる OpenShift Container Platform クラスターを静的 IP アドレスでベアメタルにデプロイし、**baremetal** ネットワークに DHCP サーバーがない場合、ブートストラップ仮想マシンの静的 IP アドレスとブートストラップ仮想マシンのゲートウェイの静的 IP アドレスを指定する必要があります。OpenShift Container Platform 4.11 は、**bootstrapExternalStaticIP** および **bootstrapExternalStaticGateway** 設定を提供します。これらは、デプロイ前に **install-config.yaml** ファイルで設定できます。これらの設定の導入により、回避手順が置き換えられます。OpenShift Container Platform4.10 リリースの DHCP サーバーを使用せずに、ベアメタルネットワークでブートストラップ VM に IP アドレスを割り当てます。

詳細は、Configuring the install-config.yaml file および Additional install-config parameters を参照してください。

1.3.2.11. Fujitsu ハードウェアの設定

OpenShift Container Platform 4.11 では、Fujitsu ハードウェアを使用して OpenShift Container Platform をベアメタルにインストールする際に、コントロールプレーンノードの BIOS および RAID アレイを設定するサポートが導入されました。OpenShift Container Platform 4.10 では、Fujitsu ハードウェアに BIOS および RAID アレイを設定するとワーカーノードに制限されます。

詳細は、Configuring the BIOS および Configuring the RAID を参照してください。

1.3.2.12. oc-mirror CLI プラグインを使用した非接続ミラーリングが一般利用可能に

oc-mirror OpenShift CLI (**oc**) プラグインを使用して、非接続環境でイメージをミラーリングできます。この機能は以前は OpenShift Container Platform 4.10 でテクノロジープレビューとして提供され、OpenShift Container Platform 4.11 で一般に利用可能になりました。

oc-mirror プラグインの今回のリリースには、以下の新機能が含まれます。

- ターゲットミラーレジストリーからのイメージのプルーニング
- Operator パッケージおよび OpenShift Container Platform リリースのバージョン範囲の指定
- OpenShift Update Service(OSUS) の使用でサポートされるアーティファクトの生成
- 初期イメージセット設定のテンプレートの取得

重要

OpenShift Container Platform 4.10 のテクノロジープレビューバージョンの oc-mirror プラグインを使用している場合、ミラーレジストリーを OpenShift Container Platform 4.11 に移行することはできません。新規の oc-mirror プラグインをダウンロードし、新規ストレージバックエンドを使用して、ターゲットミラーレジストリーで新しい最上位の namespace を使用する必要があります。

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

1.3.2.13. ユーザー管理の暗号化キーを使用した Azure へのクラスターのインストール

OpenShift Container Platform 4.11 では、ユーザー管理のディスク暗号化を使用して、Azure 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。

詳細は、Enabling user-managed encryption for Azure を参照してください。

1.3.2.14. Azure の Accelerated Networking がデフォルトで有効化

Azure 上の OpenShift Container Platform 4.11 は、コントロールプレーンとコンピュートノードに Accelerated Networking を提供します。Accelerated Networking は、インストーラーによってプロビジョニングされたインフラストラクチャーインストールでサポートされているインスタンスタイプに対して、デフォルトで有効になっています。

詳細は、Openshift 4 on Azure - accelerated networking を参照してください。

1.3.2.15. AWS VPC エンドポイントおよび制限されたインストール

制限された OpenShift Container Platform クラスターを AWS にインストールする際に AWS VPC エンドポイントを設定する必要がなくなりました。VPC エンドポイントの設定はオプションのままですが、VPC エンドポイントのないプロキシーを設定するか、VPC エンドポイントでプロキシーを設定することもできます。

詳細は、Requirements for using your VPC を参照してください。

1.3.2.16. OpenShift Container Platform のインストール時における追加のカスタマイズ

OpenShift Container Platform 4.11 では、**baremetal** および **marketplace** Operator のインストールを無効にすることができます。また、**openshift** namespace に保存される **openshift-samples** コンテンツも無効にすることができます。インストール前に **baselineCapabilitySet** および **additionalEnabledCapabilities** パラメーターを **install-config.yaml** 設定ファイルに追加してこれらの機能を無効にすることができます。インストール時にこれらの機能のいずれかを無効にする場合は、クラスターのインストール後にそれらの機能を有効にできます。機能を有効にしたら、再度無効にすることはできません。

詳細は、お使いのプラットフォームのインストールドキュメントのインストール設定パラメーターセクションを参照してください。

1.3.2.17. Azure Marketplace オファリング

OpenShift Container Platform が Azure Marketplace で利用できるようになりました。Azure Marketplace オファリングは、北米および EMEA で OpenShift Container Platform を入手されたお客様にご利用いただけます。

詳細は、Installing OpenShift using Azure Marketplace を参照してください。

1.3.2.18. AWS Marketplace オファリング

OpenShift Container Platform が AWS Marketplace で利用できるようになりました。AWS Marketplace オファリングは、北米で OpenShift Container Platform を入手されたお客様にご利用いただけます。

詳細は、Installing OpenShift using AWS Marketplace を参照してください。

1.3.2.19. 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 7.0 Update 2 以降、バージョン 8 まで。vSphere 8 はサポートされていません。
- VMware ESXi バージョン 7.0 Update 2 以降

上記よりも前のバージョンのコンポーネントは、非推奨になるか、削除されています。廃止されたバージョンも引き続き完全にサポートされていますが、Red Hat では、ESXi 7.0 Update 2 以降および vSphere 7.0 Update 2 まで (バージョン 8 を除く) を使用することを推奨します。vSphere 8 はサポートされていません。

詳細は、Deprecated and removed features を参照してください。

1.3.3. インストール後の設定

1.3.3.1. クラスター機能

クラスター管理者は、インストールまたはインストール後に、クラスター機能を有効にして 1 つ以上のオプションのコンポーネントを選択または選択解除できます。

詳細は、Cluster capabilities を参照してください。

1.3.3.2. マルチアーキテクチャーのコンピューティングマシンを備えた OpenShift Container Platform クラスター (テクノロジープレビュー)

OpenShift Container Platform 4.11 では、テクノロジープレビューの Azure インストーラーによってプロビジョニングされたインフラストラクチャーを使用して、マルチアーキテクチャーコンピューティングマシンをサポートするクラスターが導入されています。この機能は、2 日目の操作として、マルチアーキテクチャーのインストーラーバイナリーでプロビジョニングされたインストーラーである既存の **x86_64** Azure クラスターに **arm64** コンピュートノードを追加する機能を提供します。手動で生成された **arm64** ブートイメージを使用するカスタム Azure マシンセットを作成することで、クラスターに **arm64** コンピュートノードを追加できます。**arm64** アーキテクチャー上のコントロールプレーンは現在サポートされていません。詳細は、マルチアーキテクチャークラスターの設定 を参照してください。

注記

リリースの **image-pullsec** を使用して、クラスターを最新のマルチアーキテクチャーリリースイメージに手動でアップグレードできます。詳細は、マルチアーキテクチャーコンピュートマシンのアップグレード を参照してください。

1.3.4. Web コンソール

1.3.4.1. Developer パースペクティブ

- 今回の更新により、開発者の観点から、パイプラインを含む GitHub リポジトリーを OpenShift Container Platform クラスターに追加できるようになりました。プッシュやプルリクエストなどの関連する Git イベントが発生した際に、クラスター上の GitHub リポジトリーからパイプラインやタスクを実行することができるようになりました。
  - 管理者視点では、GitHub アプリケーションを OpenShift クラスターで設定し、パイプラインをコードとして使用することができます。この設定により、ビルドデプロイメントに必要な一連のタスクを実行することができます。

- 今回の更新により、独自のキュレーションタスクを使用して、カスタマイズしたパイプラインを作成することが可能になりました。デベロッパーコンソールから直接、タスクの検索、インストール、およびアップグレードが可能です。
- 今回の更新により、Web ターミナルでは、複数のタブを使用したり、bash 履歴を表示したりできるようになりました。また、Web ターミナルは、ブラウザーのウィンドウまたはタブを閉じるまで開いたままになります。
- 今回の更新により、開発者パースペクティブの **Add+** ページに、プロジェクトと Helm Chart リポジトリーを共有するための新しいメニューが追加され、プロジェクトにユーザーを追加または削除できるようになりました。

1.3.4.2. 動的プラグインの更新

今回の更新により、新しい **console.openshift.io/use-i18next** アノテーションを使用して、**ConsolePlugin** にローカリゼーションリソースが含まれているかどうかを判断できるようになりました。アノテーションを **"true"** に設定すると、ダイナミックプラグインにちなんだ i18n namespace からローカライズリソースがロードされます。アノテーションが他の値に設定されているか、**ConsolePlugin** リソースにない場合、ローカリゼーションリソースは読み込まれません。

詳細は、動的プラグインの概要 を参照してください。

1.3.4.3. ダークモードテーマのサポート

OpenShift Container Platform の Web コンソールがダークモードテーマをサポートするようになりました。**User Preferences** ページで、お好みのテーマを選択して Web コンソールを表示します。

1.3.4.4. Installed Operator ページでの全マネージド namespace のオペランドインスタンスの表示

今回の更新により、**Operator → Installed Operator** ページには、全 namespace の全 Operator が表示されます。プロジェクトセレクター内で選択した namespace のインスタンスのみを引き続き表示できます。オペランドインスタンスを表示する場合、新しい切り替えコントロールにより、すべての namespace または現在の namespace のみのすべてのオペランドインスタンスを表示できます。

1.3.4.5. 条件の更新

今回の更新では、条件付き更新が利用可能な場合、**Update cluster** モーダルの **Select new version** ドロップダウンで **Include supported but not recommended versions** を有効にして、ドロップダウンリストに条件付き更新を入力できます。**Supported but not recommended** バージョンを選択すると、ドロップダウンメニューの下に、バージョンの潜在的な問題が記載されたアラートが表示されます。

1.3.4.6. Pod の Disruption Budget (PDB: 停止状態の予算)

今回の更新により、Pod の Disruption Budget (PDB: 停止状態の予算) のサポートが OpenShift Container Platform Web コンソールに提供されます。**Workloads → PodDisruptionBudgets** から、Pod リソースの PDB を作成できます。可用性要件リストから **maxUnavailable** と **minAvailable** を選択し、実行中の Pod の値を設定できます。または、Pod の Disruption Budget (PDB: 停止状態の予算) は、**pod controller resources** リストおよび **詳細** ページから作成することもできます。たとえば、**Workloads → Deployments** から **Add PodDisruptionBudget** をクリックします。

詳細は、Pod preemption and other scheduler settings を参照してください。

1.3.5. OpenShift CLI (oc)

1.3.5.1. OpenShift CLI (oc) の RHEL 9 サポート

OpenShift CLI (**oc**) での Red Hat Enterprise Linux (RHEL) 9 の使用がサポートされるようになりました。

注記

OpenShift CLI (**oc**) を Red Hat Enterprise Linux (RHEL) 9 の RPM としてインストールすることはできません。バイナリーをダウンロードし、RHEL 9 の OpenShift CLI をインストールする必要があります。

詳細は、Installing the OpenShift CLI を参照してください。

1.3.6. IBM Z および LinuxONE

本リリースでは、IBM Z および LinuxONE は OpenShift Container Platform 4.11 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 4.11 の IBM Z および LinuxONE でサポートされます。

- 代替の認証プロバイダー
- ローカルストレージ Operator を使用した自動デバイス検出
- CSI ボリューム
  - クローン
  - 拡張
  - スナップショット
- File Integrity Operator
- ユーザー定義プロジェクトのモニタリング
- Operator API
- OC CLI プラグイン

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
    - Compliance Operator
    - Local Storage Operator
    - NFD Operator
    - NMState Operator
    - OpenShift Elasticsearch Operator
    - Service Binding Operator
    - Vertical Pod Autoscaler Operator
- 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
- etcd に保存されるデータの暗号化
- Helm
- Horizontal Pod Autoscaling
- 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
- IPsec 暗号化を含む 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、4.11 の IBM Z および LinuxONE の OpenShift Container Platform についてのみ利用できます。

- 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
  - Red Hat OpenShift Local
  - 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
  - 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
- コンピュートノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続共有ストレージは、Red Hat OpenShift Data Foundation またはその他のサポートされ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。

1.3.7. IBM Power

本リリースでは、IBM Power は OpenShift Container Platform 4.11 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 4.11 の IBM Power でサポートされます。

- 代替の認証プロバイダー
- CSI ボリューム
  - クローン
  - 拡張
  - スナップショット
- File Integrity Operator

- IPv6
- ユーザー定義プロジェクトのモニタリング
- Operator API
- OC CLI プラグイン

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
  - Compliance Operator
  - Local Storage Operator
  - NFD Operator
  - NMState Operator
  - OpenShift Elasticsearch Operator
  - SR-IOV Network Operator
  - Service Binding Operator
  - Vertical Pod Autoscaler Operator
- 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
- etcd に保存されるデータの暗号化
- Helm
- Horizontal Pod Autoscaling
- マルチパス化
- Multus SR-IOV
- IPsec 暗号化を含む 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
  - Red Hat OpenShift Local
  - 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
- コンピュートノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続ストレージは、ローカルボリューム、Red Hat OpenShift Data Foundation、Network File System (NFS)、または Container Storage Interface (CSI) を使用する Filesystem タイプである必要があります。

1.3.8. セキュリティーおよびコンプライアンス

1.3.8.1. 監査ログに OAuth サーバー監査イベントが含まれるようになる

ログインイベントでアノテーションされた OAuth サーバー監査イベントは、監査ログのメタデータレベルでログに記録されるようになりました。ログインイベントには、失敗したログイン試行が含まれます。

詳細は、About audit log policy profiles を参照してください。

1.3.9. ネットワーク

1.3.9.1. 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。

詳しくは、Configuring a bond interface from two SR-IOV interfaces を参照してください。

1.3.9.2. hostnetwork エンドポイントのある Ingress コントローラーの新規オプション

今回の更新により、**hostnetwork** エンドポイントストラテジーを持つ Ingress コントローラーの新規オプションが導入されました。**httpPort**、**httpsPort**、および **statsPort** バインディングポートを使用して、同じワーカーノードで複数の Ingress コントローラーをホストできるようになりました。

1.3.9.3. コントロールプレーンおよびワーカーノードの複数ノード設定

単一設定を同時に、クラスター内の複数のベアメタル、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ノードに適用できます。単一の設定を複数のノードに適用すると、シングルプロビジョニングプロセスによる設定ミスのリスクが軽減されます。

このメカニズムは、**install-config** ファイルを使用している場合のみ初期デプロイメントに利用できます。

1.3.9.4. AWS での Classic Load Balancer Timeout 設定へのサポート

Ingress コントローラーで AWS Classic Load Balancers (CLB) のアイドル接続タイムアウトを設定できるようになりました。

詳細は、Configuring Classic Load Balancer timeouts を参照してください。

1.3.9.5. HAProxy 2.2.24 への更新

OpenShift Container Platform が HAProxy 2.2.24 に更新されました。

1.3.9.6. HAProxy プロセスの最大接続数設定のサポート

Ingress コントローラーの HAProxy プロセスごとに確立できる同時接続の最大数を 2000 から 2,000,000 まで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。

1.3.9.7. Ingress Controller のヘルスチェック間隔の設定

今回の更新により、クラスター管理者はヘルスチェックの間隔を設定して、連続する 2 つのヘルスチェックの間にルーターが待機する時間を定義できるようになりました。この値は、すべてのルートのデフォルトとしてグローバルに適用されます。デフォルト値は 5 秒です。

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

1.3.9.8. インターフェイスレベルの安全なネットワーク sysctl 設定のサポート

新しい **tuning-cni** メタプラグインを使用して、特定のインターフェイスのみに適用されるインターフェイスレベルの安全なネットワーク sysctl を設定します。たとえば、**tuning-cni** プラグインを設定して、特定のネットワークインターフェイスの **accept_redirects** の動作を変更できます。設定可能なインターフェイス固有の安全な sysclt の完全リストは、ドキュメントを参照してください。

今回の機能拡張により、**net.ipv4.ping_group_range** および **net.ipv4.ip_unprivileged_port_start** をサポートするように設定できるシステム全体の安全な sysctl のセットが増えました。

tuning-cni プラグインの設定に関する詳細は、Setting interface level network sysctls を参照してください。

新たにサポートされるインターフェイスレベルのネットワーク安全な sysclt sysclts および更新の詳細は、Using sysctls in containers を参照してください。

1.3.9.9. TLS での CoreDNS 転送 DNS 要求のサポート

高度に規制された環境で作業する場合は、要求をアップストリームリゾルバーに転送する際にドメインネームシステム (DNS) トラフィックのセキュリティーを確保して、追加の DNS トラフィックおよびデータのプライバシーを確保できるようにする必要がある場合があります。クラスター管理者は、転送された DNS クエリーにトランスポート層セキュリティー (TLS) を設定できるようになりました。この機能は DNS Operator にのみ適用され、Machine Config Operator が管理する CoreDNS インスタンスには適用されません。

詳細は、DNS 転送の使用 を参照してください。

1.3.9.10. OVN-Kubernetes の内部トラフィックのサポート

クラスター管理者は、OVN-Kubernetes Container Network Interface (CNI) クラスターネットワークプロバイダーを使用する場合に、Kubernetes サービスオブジェクトで **internalTrafficPolicy=Local** を設定できます。この機能により、クラスター管理者はトラフィックの発信元の同じノードのエンドポイントにトラフィックをルーティングすることができます。ローカルノードのエンドポイントがない場合、トラフィックはドロップされます。

詳細は、Service Internal Traffic Policy を参照してください。

1.3.9.11. AWS Load Balancer Operator のサポート (テクノロジープレビュー)

クラスター管理者は、OpenShift Container Platform Web コンソールまたは CLI を使用して OperatorHub から AWS Load Balancer Operator をインストールできます。AWS Load Balancer Operator はテクノロジープレビュー機能です。

詳細は、Installing AWS Load Balancer Operator を参照してください。

1.3.9.12. ルート API の機能拡張

以前のバージョンでは、ルートのサブドメインを指定できず、**spec.host** フィールドはホスト名を設定する必要がありました。**spec.subdomain** フィールドを指定し、ルートの **spec.host** フィールドを省略できるようになりました。ルートを公開するルーターデプロイメントは **spec.subdomain** 値を使用してホスト名を判別します。

この拡張機能を使用して、ルートがルートを公開する各ルーターデプロイメントによって決定される複数の異なるホスト名を指定できるようにすることで、シャード化を簡素化できます。

1.3.9.13. 外部 DNS Operator

OpenShift Container Platform 4.11 では、外部 DNS Operator は AWS Route53、Azure DNS、GCP DNS、および Infoblox in General Availability (GA) ステータスで利用できます。外部 DNS Operator は、GovCloud の BlueCat および AWS Route53 のテクノロジープレビュー (TP) ステータスです。今回の更新により、外部 DNS Operator は以下の拡張機能を提供するようになりました。

- Infoblox の DNS ゾーンに DNS レコードを作成できます。
- デフォルトでは、外部 DNS Operator は namespace **external-dns-operator** にオペランドを作成します。インストール前にオペランドおよびロールベースアクセス制御 (RBAC) の namespace を手動で作成する必要はありません。
- ルートのステータスを使用して、DNS FQDN 名を取得できます。
- BlueCat DNS プロバイダーのプロキシーサポートが利用できるようになりました。
- BlueCat DNS プロバイダーを使用する際に自動 DNS 設定デプロイメントを有効にできます。

TP から GA に移行するようにしてください。OpenShift Container Platform 4.11 の **ExternalDNS** のアップストリームバージョンは **v0.12.0** で、TP の場合は **v0.10.2** です。詳細は、About the External DNS Operator を参照してください。

1.3.9.14. デュアル NIC 境界クロックの PTP サポート

各 NIC チャネルの **PtpConfig** プロファイルを使用して、デュアルネットワークインターフェイス (NIC) を境界クロックとして設定できるようになりました。

詳細は、Using PTP with dual NIC hardware を参照してください。

1.3.9.15. PTP イベントの拡張機能

新しい PTP イベント API エンドポイント **api/cloudNotifications/v1/publishers** が利用できるようになりました。このエンドポイントを使用して、クラスターノードの PTP **os-clock-sync-state**、**ptp-clock-class-change**、および **lock-state** の詳細を取得できます。

詳細は、Subscribing DU applications to PTP events REST API reference を参照してください。

1.3.9.16. Pensando DSC カードの SR-IOV サポート

SR-IOV のサポートが、Pensando DSC カード で利用できるようになりました。OpenShift SR-IOV はサポートされますが、SR-IOV を使用する際に SR-IOV CNI 設定ファイルを使用して静的な Virtual Function (VF) メディアアクセス制御 (MAC) アドレスを設定する必要があります。

1.3.9.17. 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。

1.3.9.18. ネットワーク用の OpenShift Container Platform CIDR 範囲

ネットワークの CIDR 範囲は、クラスターのインストール後に調整できないことに注意してください。Red Hat では、範囲を判断する際の直接ガイダンスを提供しません。作成された Pod 数について慎重に考慮する必要があるためです。

1.3.9.19. OVN-Kubernetes ネットワークプロバイダー: ランタイム時の IPsec の有効化

OVN-Kubernetes クラスターネットワークプロバイターを使用している場合、クラスターのインストール後に IPsec 暗号化を有効化できるようになりました。IPsec の有効化方法の詳細は、Configuring IPsec encryption を参照してください。

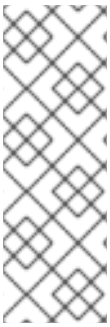
1.3.9.20. 追加の MetalLB CRD のサポートおよびロギングの詳細度の制御

より複雑な設定をサポートするために、追加の MetalLB カスタムリソース定義 (CRD) が追加されました。

以下の CRD が追加されました。

- **IPAddressPools**
- **L2Advertisement**
- **BGPAdvertisement**
- **コミュニティー**

これらの機能強化により、Operator を使用してより複雑な設定を使用できるようになりました。たとえば、機能拡張を使用して、ノードを分離したり、ネットワークをセグメント化したりできます。さらに、FRRouting (FRR) ロギングコンポーネントに追加された機能強化により、生成されたログの詳細を制御できます。



注記

About MetalLB and the MetalLB Operator で説明されているように、OpenShift Container Platform 4.10 および metalLB Operator 向けに文書化された CRD はサポートされますが、非推奨となっています。**AddressPool** 設定は非推奨になりました。

4.10 では、**AddressPool** を使用するレイヤー 2 および BGP IP アドレスは、異なるアドレスプールから割り当てられました。OpenShift Container Platform 4.11 では、レイヤー 2 および BGP IP アドレスを同じアドレスプールから割り当てることができます。

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

1.3.9.21. Ingress アノテーションで宛先 CA 証明書を使用してルートを作成する機能

route.openshift.io/destination-ca-certificate-secret アノテーションを Ingress オブジェクトで使用して、カスタム証明書 (CA) でルートを定義できるようになりました。

詳細は、Creating a route using the destination CA certificate in the Ingress annotation を参照してください。

1.3.9.22. ホストされているコントロールプレーン (テクノロジープレビュー)

OpenShift Container Platform のホスト型コントロールプレーンでは、クラスターを大規模にホストして管理コストの軽減、クラスターデプロイメント時間の最適化、および個別の管理およびワークロードに関する懸念点を実現します。Kubernetes Operator バージョン 2.0 のマルチクラスターエンジンをインストールする場合は、このデプロイメントモデルをテクノロジープレビュー機能として有効にできます。詳細は、Overview of hosted control planes (Technology Preview) を参照してください。

Open Virtual Network (OVN) は、コントロールプレーンとデータストアをクラスターのコントロールプレーンと共にホストするように再設計されました。ホスト型コントロールプレーンでは、OVN は分割されたコントロールプレーンをサポートします。

1.3.9.23. OVN-Kubernetes クラスターネットワークプロバイダーを使用した、ユーザーがプロビジョニングしたベアメタルインフラストラクチャーでの IPv6 シングルおよびデュアルスタックのサポート

ユーザーによってプロビジョニングされる ベアメタルインフラストラクチャー 上のクラスターの場合、OVN-Kubernetes クラスターネットワークプロバイダーは IPv4 アドレスと IPv6 アドレスファミリーの両方をサポートします。

1.3.9.24. RHOSP での OVS ハードウェアのオフロード

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が一般提供されるようになりました。

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。

1.3.9.25. RHOSP での NFV ユーザー エクスペリエンスの向上

RHOSP で実行されるクラスターの場合、ネットワーク機能の仮想化デプロイメントエクスペリエンスが向上しました。このリリースの変更点は次のとおりです。

- 設定ドライブではなく、メタデータサービス URL から取得するネットワークデータ
- 検出されたすべてのデバイスに対して IOMMU を使用しない自動 VFIO ロード
- DPDK vHost のユーザーポート

これらの変更は、簡素化されたインストール後およびネットワーク設定のドキュメントに反映されています。

1.3.9.26. Red Hat OpenStack Platform、VMware vSphere、または oVirt へのインストールで、ユニキャストをデフォルトとしてキープアライブが設定されるように

Red Hat OpenStack Platform (RHOSP)、VMware vSphere、または oVirt に OpenShift Container Platform インストーラーによってプロビジョニングされたインストールの場合には、keepalived は、デフォルトでマルチキャストではなくユニキャストとして設定されるようになりました。マルチキャストトラフィックを許可する必要はなくなりました。すべてのノードを同時に移行する必要があるため、クラスターのアップグレードが完了してから数分後にユニキャスト移行が行われます。keepalived はユニキャストとマルチキャストを完全に別のものとして扱うため、マルチキャストクラスターとユニキャストクラスターの両方を同時に使用しても問題は発生しません。

1.3.10. ストレージ

1.3.10.1. Microsoft Azure File CSI Driver Operator を使用した永続ストレージが一般で利用可能

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。この機能は以前は OpenShift Container Platform 4.10 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、Azure File CSI Driver Operator を参照してください。

1.3.10.2. OpenStack Cinder の自動 CSI の移行が一般で利用可能

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。Cinder のサポートは OpenShift Container Platform 4.8 のこの機能で提供され、OpenShift Container Platform 4.11 では Cinder の自動移行に対するサポートが一般で利用可能になりました。Cinder の CSI 移行はデフォルトで有効化され、管理者によるアクションは不要になりました。

この機能は in-tree オブジェクトを自動的に対応する CSI 表現に変換するため、ユーザーに対して完全に透過的である必要があります。変換されたオブジェクトはディスクに保存され、ユーザーデータは移行されません。

in-tree ストレージプラグインを参照するストレージクラスは引き続き機能しますが、デフォルトのストレージクラスを CSI ストレージクラスに切り替えることが推奨されます。

詳細は、CSI 自動移行を参照してください。

1.3.10.3. Microsoft Azure Disk の自動 CSI 移行が一般で利用可能

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。Azure Disk のサポートは OpenShift Container Platform 4.9 のこの機能で提供され、OpenShift Container Platform 4.11 では Azure Disk の自動移行に対するサポートが一般で利用可能になりました。Azure Disk の CSI 移行はデフォルトで有効化され、管理者によるアクションは不要になりました。

この機能は in-tree オブジェクトを自動的に対応する CSI 表現に変換するため、ユーザーに対して完全に透過的である必要があります。変換されたオブジェクトはディスクに保存され、ユーザーデータは移行されません。

in-tree ストレージプラグインを参照するストレージクラスは引き続き機能しますが、デフォルトのストレージクラスを CSI ストレージクラスに切り替えることが推奨されます。

詳細は、CSI 自動移行を参照してください。

1.3.10.4. CSI ボリュームの拡張が一般で利用可能

OpenShift Container Platform 4.3 以降で、作成済みの Container Storage Interface (CSI) ストレージボリュームの拡張がテクノロジープレビュー機能として利用可能になり、OpenShift Container Platform 4.11 で一般に利用可能になりました。

詳細は、Expanding CSI volumes を参照してください。

1.3.10.5. CSI 汎用一時ボリュームのサポートが一般で利用可能

OpenShift Container Platform 4.11 では、Container Storage Interface (CSI) の汎用一時ボリュームのサポートが一般で利用可能になりました。汎用一時ボリュームは、永続ボリュームおよび動的プロビジョニングもサポートするすべてのストレージドライバーが提供できる一時ボリュームの一種です。

詳細は、Generic ephemeral volumes を参照してください。

1.3.10.6. VMware vSphere がサイズ変更およびスナップショットをサポート

OpenShift Container Platform 4.11 は、以下の制限のある vSphere Container Storage Interface (CSI) Driver Operator のボリュームサイズ変更およびスナップショットをサポートします。

- スナップショット:

    - vSphere バージョン 7.0 Update 3 以降 (バージョン 8 を除く) が必要です。vSphere 8 は、vCenter Server と ESXi の両方でサポートされていません。
    - ファイル共有ボリュームはサポートされません。
- サイズ変更:
    - オフラインボリューム拡張: 必要な vSphere の最低バージョンは 6.7 Update 3 P06 です。
    - オンラインボリューム拡張: 必要な vSphere の最低バージョンは 7.0 Update 2 です。

詳細は、CSI drivers supported by OpenShift Container Platform を参照してください。

1.3.11. レジストリー

1.3.11.1. アベイラビリティーゾーン全体での Image Registry Operator のディストリビューション

Image Registry Operator のデフォルト設定は、イメージレジストリー Pod をトポロジーゾーン全体に分散させ、すべての Pod が影響を受ける完全なゾーン障害が発生した場合の復旧時間の遅延を防ぎます。

詳細は、アベイラビリティーゾーン全体での Image Registry Operator のディストリビューション を参照してください。

1.3.11.2. Red Hat OpenShift Data Foundation レジストリーストレージ

OpenShift Container Platform 4.11 でサポートされる Red Hat OpenShift Data Foundation レジストリーストレージ。

OpenShift Data Foundation は、以下のような内部イメージレジストリーで使用できる複数のストレージタイプを統合します。

- オンプレミスのオブジェクトストレージを備えた共有および分散ファイルシステムである Ceph
- Multicloud Object Gateway を提供する NooBaa

1.3.12. Operator ライフサイクル

1.3.12.1. ファイルベースのカタログ形式

ファイルベースのカタログ形式で OpenShift Container Platform 4.11 リリース用のデフォルトの Red Hat が提供する Operator カタログ。SQLite データベース形式でリリースされた OpenShift Container Platform 4.6 から 4.10。ファイルベースのカタログは、Operator Lifecycle Manager(OLM) のカタログ形式の最新の反復になります。JSON または YAML のプレーンテキストベースファイルであり、以前の SQLite データベース形式の宣言的設定の進化です。クラスター管理者およびユーザーには、新規カタログ形式でのインストールワークフローおよび Operator の消費への変更は表示されません。

詳細は、File-based catalogs を参照してください。

1.3.13. Operator の開発

1.3.13.1. Java ベースの Operator (テクノロジープレビュー)

OpenShift Container Platform 4.11 以降、Operator SDK には Java ベースの Operator を開発するためのツールおよびライブラリーが含まれます。Operator 開発者は、Operator SDK での Java プログラミング言語のサポートを利用して、Java ベースの Operator をビルドし、そのライフサイクルを管理できます。

詳細は、Getting started with Operator SDK for Java-based Operators を参照してください。

1.3.13.2. Operator SDK によるファイルベースカタログのサポート

OpenShift Container Platform 4.11 の時点で、Operator カタログに関して、**run bundle** コマンドはデフォルトでファイルベースのカタログ形式をサポートします。Operator カタログに関して、非推奨の SQLite データベース形式は引き続きサポートされますが、今後のリリースで削除される予定です。

詳細は、Working with bundle images を参照してください。

1.3.13.3. Operator バンドルの検証

Operator の作成者は、Operator SDK で **bundle validate** コマンドを実行して Operator バンドルのコンテンツおよび形式を検証できます。デフォルトのテストに加え、オプションのバリデーターを実行して、空の CRD 記述やサポートされていない Operator Lifecycle Manager (OLM) リソースなど、バンドル内の問題をテストできます。

詳細は、Validating Operator bundles を参照してください。以前のバージョンの OpenShift Container Platform では、Performance Addon Operator はアプリケーションの自動低レイテンシーパフォーマンスチューニングを提供していました。OpenShift Container Platform 4.11 では、これらの機能は Node Tuning Operator の一部です。Node Tuning Operator は、OpenShift Container Platform 4.11 の標準インストールの一部です。OpenShift Container Platform 4.11 にアップグレードする場合、Node Tuning Operator は起動時に Performance Addon Operator およびすべての関連アーティファクトを削除します。

詳細は、Node Tuning Operator を参照してください。

1.3.14. Jenkins

- この機能強化により、Jenkins の新しい環境変数 **JAVA_FIPS_OPTIONS** が追加され、FIPS ノードでの実行時に JVM がどのように動作するかを制御します。詳細は、OpenJDK support article (BZ#2066019) を参照してください。

1.3.15. マシン API

1.3.15.1. Amazon EC2 Instance Metadata Service (IMDS) のオプションの設定

マシンセットを使用して、Amazon EC2 Instance Metadata Service (IMDS) の特定バージョンを使用するコンピュートマシンを作成できるようになりました。マシンセットは、IMDSv1 と IMDSv2 の両方の使用を許可するコンピュートマシン、または IMDSv2 の使用を必要とするコンピュートマシンを作成することができます。

詳細は、Machine set options for the Amazon EC2 Instance Metadata Service を参照してください。

1.3.15.2. Azure Ultra ディスクのマシン API サポート

Ultra ディスクを使用してマシンをデプロイする 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。Ultra ディスクをデータディスクとして使用するか、ツリー内または Container Storage Interface (CSI) PVC を使用する永続ボリューム クレーム (PVC) を使用してマシンをデプロイできま

す。

詳細は、以下のトピックを参照してください。

- Machine sets that deploy machines with ultra disks as data disks
- Machine sets that deploy machines with ultra disks using CSI PVCs
- Machine sets that deploy machines with ultra disks using in-tree PVCs

1.3.15.3. Google Cloud Platform の永続ディスクタイプの設定オプション

Google Cloud Platform (GCP) Compute Engine の **pd-balanced** 永続ディスクタイプをサポートするようになりました。詳細は、Configuring persistent disk types by using machine sets を参照してください。

1.3.15.4. Nutanix クラスターの Machine API サポート

Nutanix クラスターの新しいプラットフォームのサポートには、Machine API マシンセットを使用してマシンを管理する機能が含まれています。詳細は、Creating a machine set on Nutanix を参照してください。

1.3.15.5. Cluster API によるマシンの管理 (テクノロジープレビュー)

OpenShift Container Platform 4.11 では、AWS および GCP クラスターのテクノロジープレビューとして、OpenShift Container Platform に統合されたアップストリームの Cluster API を使用してマシンを管理する機能が導入されています。この機能は、Machine API を使用してマシンを管理するための追加または代替の機能になります。詳細は、Managing machines with the Cluster API を参照してください。

1.3.16. Machine Config Operator

1.3.16.1. MCO がゾーンおよび経過時間でノードを更新へ

Machine Config Operator(MCO) は **topology.kubernetes.io/zone** ラベルに基づいて、ゾーンによってアルファベット順に影響を受けるノードを更新するようになりました。ゾーンに複数のノードがある場合、最も古いノードが最初に更新されます。ベアメタルデプロイメントなど、ゾーンを使用しないノードの場合、ノードは年齢別にアップグレードされ、最も古いノードが最初に更新されます。以前のバージョンでは、MCO はゾーンまたはノードの経過時間を考慮しませんでした。

詳細については、マシン設定の概要 を参照してください。

1.3.16.2. 証明書の更新時に一時停止された Machine Config Pool の通知の強化

MCO が一時停止する Machine Config Pool (MCP) で期限切れの **kube-apiserver-to-kubelet-signer** CA 証明書の更新を試行した場合に、OpenShift Container Platform Web コンソールのアラート UI でアラートを受信するようになりました。MCP が一時停止されると、MCO は新たにローテーションされた証明書をそれらのノードにプッシュできず、障害が発生する可能性があります。

詳細は、Pausing the machine config pools を参照してください。

1.3.17. ノード

1.3.17.1. Poison Pill Operator 代わる Self Node Remediation Operator

OpenShift Container Platform 4.11 では、Puison Pill Operator に代わる Self Node Remediation Operator が導入されました。

Self Node Remediation Operator は以下の拡張機能を提供します。

- 修復ストラテジーに基づいて個別の修復テンプレートを導入します。
- 修復に失敗した場合は、最後のエラーメッセージをキャプチャーします。
- パラメーターの最小値を指定して、Self Node Remediation Operator の設定パラメーターのメトリックを強化します。

詳細は、Remediating nodes with the Self Node Remediation Operator を参照してください。

1.3.17.2. シングルノード OpenShift クラスター用のワーカーノード

シングルノード OpenShift クラスターにワーカーノードを追加することができるようになりました。これは、リソースに制約のある環境でのデプロイメントや、クラスターに容量を追加する必要があるネットワークエッジでのデプロイメントに役立ちます。

詳細は、Worker nodes for single-node OpenShift clusters を参照してください。

1.3.17.3. Descheduler が Pod エビクションのシミュレーションにデフォルト設定されるようになる

デフォルトで、Descheduler は予測モードで実行されるようになりました。つまり、これは Pod エビクションのみをシミュレートします。Descheduler メトリックを確認し、エビクトされる Pod の詳細を表示できます。

エビクションをシミュレーションせずに Pod をエビクトするには、Descheduler モードを automatic に変更します。

詳細は、Evicting pods using the descheduler を参照してください。

1.3.17.4. 新しい Descheduler のカスタマイズ

本リリースでは、Descheduler について以下のカスタマイズが導入されました。

- 優先順位のしきい値のフィルタリング: 優先順位のしきい値は、クラス名 (**thresholdPriorityClassName**) または数値 (**thresholdPriority**) で、この値以上の優先順位を持つ Pod をエビクトしないように設定します。
- namespace フィルタリング: Descheduler 操作を含めるか、除外するように、ユーザーが作成した namespace の一覧を設定します。保護されている namespace (**openshift-***、**kube-system**、**hypershift**) は常に除外されることに注意してください。
- **LowNodeUtilization** ストラテジーのしきい値: **LowNodeUtilization** ストラテジーの使用率および高使用率について実験的なしきい値を設定します。

詳細は、Evicting pods using the descheduler を参照してください。

1.3.17.5. Node Maintenance Operator の機能強化

Node Maintenance Operator は、以下の拡張機能を提供します。

- **NodeMaintenance** CR タスクのステータスに関して、追加のフィードバック (**drainProgress** および **lastUpdate**) が提供されるようになりました。
- ベアメタルノードを持つクラスターの場合、ノードをメンテナンスモードにし、メンテナンスモードからノードを再開できる、より簡単な方法が Web コンソールで利用できるようになりました。

詳細は、Using the Node Maintenance Operator to place nodes in maintenance mode を参照してください。

1.3.18. ロギング

1.3.18.1. Red Hat OpenShift on RHV Logging (テクノロジープレビュー)

OpenShift Container Platform 4.11 では、RHV API の新しいコネクターが導入されました。これは、クラスター内のすべてのインストールおよび oVirt コンポーネントの自動ログメッセージを追加します。

1.3.19. 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。

1.3.19.1. モニタリングスタックコンポーネントおよび依存関係の更新

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 (0.24.0 へ)
- kube-state-metrics (2.5.0 へ)
- Prometheus (2.36.2 へ)
- Prometheus operator (0.57.0 へ)
- Thanos (0.26.0 へ)

1.3.19.2. アラートルールの変更

注記

Red Hat は、記録ルールまたはアラートルールの後方互換性を保証しません。

- New
  - **KubePersistentVolumeInodesFillingUp** アラートを追加しました。これは、既存の **KubePersistentVolumeFillingUp** アラートと同様の機能ですが、ボリュームスペースではなく inode に適用されます。
  - **PrometheusScrapeBodySizeLimitHit** アラートを追加し、ボディーサイズの制限に達したターゲットを検出できるようにしました。
  - **PrometheusScrapeSampleLimitHit** アラートを追加し、サンプルリミットに達したターゲットを検出できるようにしました。
- **変更済み**

- **KubeDaemonSetRolloutStuck** アラートが **kube-state-metrics** から更新されたメトリック **kube_daemonset_status_updated_number_scheduled** を使用するように修正されました。
- **KubeJobCompletion** アラートを **KubeJobNotCompleted** に置き換えました。新しい **KubeJobNotCompleted** アラートは、以前のジョブが失敗し、最新のジョブが成功した場合に誤検出を回避します。
- **NodeNetworkInterfaceFlapping** アラートを更新し、アラート式から **tunbr** インターフェイスを除外するようにしました。

1.3.19.3. ユーザーのワークロードモニタリング向けのアラートルーティングの有効化

クラスター管理者は、ユーザーワークロードモニタリングのアラートルーティングを有効にし、開発者やその他のユーザーが、ユーザー定義のプロジェクトにカスタムアラートとアラートルーティングを設定できるようになりました。

1.3.19.4. ユーザー定義のアラート向け専用 Alertmanager インスタンスの有効化

ユーザー定義のプロジェクトにのみアラートを送信する Alertmanager の独立したインスタンスを有効にするオプションが追加されました。この機能は、デフォルトプラットフォームの Alertmanager インスタンスの負荷を軽減し、ユーザー定義のアラートをデフォルトのプラットフォームアラートからより適切に分離する際に役立ちます。

1.3.19.5. リモート書き込み設定における追加の認証設定の使用

リモート書き込みエンドポイントにアクセスする際に、AWS Signature Version 4、カスタム Authorization ヘッダー、および OAuth 2.0 の認証方法を使用できるようになりました。このリリース以前は、TLS クライアントと Basic 認証しか使用できませんでした。

1.3.19.6. Web コンソールでのより簡単な PromQL クエリーの作成、閲覧、および管理

OpenShift Container Platform Web コンソールの **Observe → Metrics** ページにある Query Browser には、PromQL クエリーを作成、閲覧、および管理する機能を改善するためのさまざまな拡張機能が追加されています。たとえば、管理者は既存のクエリーを複製し、クエリーの作成および編集時に、オートコンプリートの提案を使用できるようになりました。

1.3.19.7. 単一ノードデプロイメントで ServiceMonitors のスクレープ間隔が 2 倍に

単一ノード OpenShift Container Platform デプロイメント上のすべての Cluster Monitoring Operator (CMO) 制御の ServiceMonitors に対して、スクレープ間隔が 2 倍になりました。最大間隔は 2 分になりました。

1.3.19.8. プラットフォームモニタリングメトリクスに基づいたアラートルールの作成 (テクノロジープレビュー)

このリリースでは、管理者が既存のプラットフォームモニタリングメトリクスに基づいて、アラートルールを作成することができるテクノロジープレビュー能が導入されています。この機能により、管理者はより迅速かつ容易に、それぞれの環境に特化した新しいアラートルールを作成することができます。

1.3.19.9. リモート書き込みストレージへのクラスター ID ラベルの追加

リモート書き込みストレージに送信されるメトリックに、クラスター ID ラベルを追加できるようになりました。次に、これらのラベルをクエリーし、メトリックのソースクラスターを特定し、そのデータを他のクラスターによって送信される同様のメトリックデータと区別することができます。

1.3.19.10. ユーザーのワークロードモニタリング向けのフェデレーションエンドポイントを使用したクエリーメトリックス

Prometheus /**federate** 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ロケーションからユーザー定義のメトリックをスクレイプできるようになりました。このリリース以前は、フェデレーションエンドポイントにアクセスして、デフォルトのプラットフォームモニタリングでメトリクスをスクレイプすることしかできませんでした。

1.3.19.11. デフォルトのプラットフォームモニタリングにおけるメトリクススクレイピングのボディサイズ制限の有効化

デフォルトのプラットフォームモニタリング用の **enforcedBodySizeLimit** config map オプションを設定して、メトリクススクレイピングでボディーサイズ制限を有効化できるようになりました。この設定は、少なくとも 1 つの Prometheus スクレイプターゲットが、設定された **enforcedBodySizeLimit** より大きいレスポンスボディーで応答したときに、新しい **PrometheusScrapeBodySizeLimitHit** アラートをトリガーします。この設定により、悪意のあるターゲットが Prometheus コンポーネントとクラスター全体の両方に与える影響を制限できます。

1.3.19.12. メトリックストレージの保持サイズの設定

デフォルトのプラットフォームモニタリングとユーザーワークロードモニタリングの両方で、保持されたメトリクスストレージ用に予約された最大ディスク容量を設定できるようになりました。このリリースより前は、これは設定できませんでした。

1.3.19.13. ユーザー定義プロジェクトにおける Thanos Ruler の保持期間の設定

ユーザー定義のプロジェクトで、Thanos Ruler データの保持期間を設定できるようになりました。このリリースより前は、デフォルト値の **24h** を変更できませんでした。

1.3.20. 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。

詳細は、Network Observability を参照してください。

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. Node Tuning Operator のワークロードヒント

OpenShift Container Platform 4.11 は、さまざまな業界環境の要求を満たすように **PerformanceProfile** を調整できる Node Tuning Operator のヒントメカニズムもサポートします。このリリースでは、ワークロードのヒントは、**highPowerConsumption** (消費電力が増加する代わりに非常に低いレイテンシーを実現) および **realtime** (最適なレイテンシーを優先) で利用できます。これらのヒントの true/false 設定の組み合わせを使用して、アプリケーション固有のワークロードプロファイルと要件を処理できます。

1.3.21.2. etcd クラスターのスケールアップ操作の強化

Raft アルゴリズムでは、新しい **learner** 状態を用いて etcd メンバーのスケーリングが可能です。その結果、クラスタークォーラムの維持、新しいメンバーの追加と削除、**learners** 昇格は、クラスターの運用を中断することなく行われます。

OpenShift Container Platform 4.11 では、**AgentServiceConfig** カスタムリソースの一部として **imageStorage** オプションが導入されています。このオプションは、ユーザーが Image サービスで使用するための Persistent Storage Claim (永続ボリューム要求、PVC) の詳細を指定できるようにすることで、アプリケーションのパフォーマンスが向上します。

ClusterImageSet カスタムリソースの **releaseImage** パラメーターは、オペレーティングシステムのイメージバージョン ID をサポートするようになりました。検出 ISO は、オペレーティングシステムイメージのバージョンを releaseImage として作成するか、指定したバージョンが利用できない場合は最新バージョンに基づいています。

AgentServiceConfig カスタムリソース (CR) の **openshiftVersion** パラメーターは、"x.y" (major.minor) または "x.y.z"(major.minor.patch) 形式のいずれかをサポートするようになりました。

1.3.21.3. Ingress コントローラー (ルーター) Liveness、Readiness、および Startup プローブの設定

OpenShift Container Platform 4.11 では、OpenShift Container Platform Ingress Operator によって管理されるルーターデプロイメントの kubelet の liveness、readiness、および startup プローブのタイムアウト値を設定する機能が導入されました。大きなタイムアウト値を設定する機能を使用すると、短いデフォルトのタイムアウトである 1 秒によって発生する不要な再起動のリスクが軽減されます。

詳細は、Configuring Ingress Controller (router) Liveness, Readiness, and Startup probes を参照してください。

1.3.21.4. 新たな省電力 CPU 機能

パフォーマンスプロファイルの **offlined** フィールドに CPU を指定して、Node Tuning Operator による電力消費を減らすことができます。詳細は、Reducing power consumption by taking CPUs offline を参照してください。

1.3.21.5. Node Observability Operator (テクノロジープレビュー)

OpenShift Container Platform 4.11 では、Node Observability Operator がテクノロジープレビューとして導入されます。

Node Observability Operator は以下の機能を提供します。

- ワーカーノードにノードの可観測性エージェントをデプロイします。
- CRIO-O および Kubelet プロファイリングをトリガーします。
- プロファイリングデータファイルを詳細な分析に使用できるようにします。

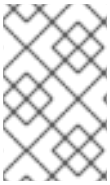
詳細は、Requesting CRI-O and Kubelet profiling data using the Node Observability Operator を参照してください。

1.3.21.6. Performance Addon Operator 関数が Node Tuning Operator に移動

以前のバージョンの OpenShift Container Platform では、Performance Addon Operator はアプリケーションの自動低レイテンシーパフォーマンスチューニングを提供していました。OpenShift Container

Platform 4.11 では、これらの機能は Node Tuning Operator の一部です。Node Tuning Operator は、OpenShift Container Platform 4.11 の標準インストールの一部です。OpenShift Container Platform 4.11 にアップグレードする場合、Node Tuning Operator は起動時に Performance Addon Operator およびすべての関連アーティファクトを削除します。

詳細は、Node Tuning Operator を参照してください。



注記

must-gather コマンドを Performance Profile Creator で実行する場合は、 **performance-addon-operator-must-gather** イメージを引き続き使用する必要があります。詳細は、Gathering data about your cluster using must-gather を参照してください。

1.3.21.7. 低レイテンシーチューニングドキュメントの更新

以前のバージョンの OpenShift Container Platform では、低レイテンシーのチューニングに関するドキュメントに Performance Addon Operator への参照が含まれていました。Node Tuning Operator が低レイテンシーチューニングを提供するようになったため、ドキュメントのタイトルが "Performance Addon Operator for low latency nodes" から "Low latency tuning" に変更され、それに応じてこのドキュメントへの複数の相互参照が更新されました。詳細は、Low latency tuning を参照してください。

1.3.21.8. ハブアンドスポーククラスターのサポート

スポーククラスターがツリー外ドライバーのサポートを必要とするハブアンドスポークデプロイメントの場合、ハブクラスターにデプロイされた Special Resource Operator (SRO) を使用して、必要なカーネルモジュールの 1 つ以上のマネージドクラスターへのデプロイメントを管理できます。これは Red Hat Advanced Cluster Management (RHACM) を使用し、Node Feature Discovery (NFD) を使用する必要がなくなりました。詳細は、Building and running the simple-kmod SpecialResource for a hub-and-spoke topology を参照してください。

1.3.21.9. 強化された SRO クラスターアップグレードのサポート

特別なリソースが管理されているクラスターをアップグレードする場合、アップグレード前のカスタムリソースを実行して、カーネルの更新をサポートする新しいドライバーコンテナーが存在することを確認できます。これにより、マネージドの特殊リソースが中断される可能性を回避できます。この機能のドキュメントは現在利用できず、後日リリースされる予定です。

1.3.21.10. SRO の強化されたデバッグとロギング

Special Resource Operator (SRO) には、トラブルシューティングのためのより詳細なメッセージを含む一貫したログ出力形式が含まれています。

1.3.21.11. 外部レジストリーのサポート

この更新の前は、SRO は切断された環境でのレジストリーへの接続をサポートしていませんでした。このリリースは、ドライバーコンテナーが OpenShift Container Platform クラスター外のレジストリーでホストされている切断された環境のサポートを提供します。

1.3.22. Insights Operator

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

OpenShift Container Platform 4.11 では、Insights Operator は以下の追加情報を収集します。

- **images.config.openshift.io** リソース定義
- **kube-controller-manager** コンテナーは、**"Internal error occurred: error resolving resource"** または **"syncing garbage collector with updated resources from discovery"** のエラーメッセージが存在する場合にログに記録します。
- **storageclusters.ocs.openshift.io/v1** resources

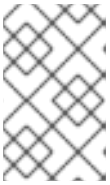
この追加情報により、Red Hat は OpenShift Container Platform 機能を強化し、Insights Advisor の推奨事項を強化します。

1.3.23. 認証および認可

1.3.23.1. サポートされる追加の OIDC プロバイダー

以下の 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。

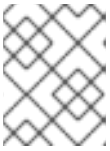
- Windows Server 向けの Active Directory Federation サービス



注記

現時点では、カスタムクレームが使用される場合に、Windows Server for Windows Server 向けの Active Directory Federation Services を OpenShift Container Platform で使用することはサポートされていません。

- Microsoft Identity Platform (Azure Active Directory v2.0)



注記

現時点で、グループ名の同期が必要な場合に Microsoft identity platform を使用することは サポートされていません。

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。

1.3.23.2. Pod セキュリティーアドミッション

Pod セキュリティーアドミッション が OpenShift Container Platform で有効になりました。

Pod アドミッションは、Pod セキュリティーとセキュリティーコンテキスト制約 (SCC) アドミッションの両方によって実施されます。Pod セキュリティーアドミッションは、**privileged** 適用と **restricted** 監査ログと API 警告により、グローバルに実行されます。

コントローラーは、ユーザーが作成した namespace 内のサービスアカウントの SCC 関連のパーミッション を監視し、これらの namespace に Pod セキュリティーアドミッション の **warn** および **audit** ラベルを自動的に付けます。

restricted Pod セキュリティープロファイルに従ってワークロード セキュリティーを向上させるために、このリリースでは、新しい Pod セキュリティーアドミッションコントロールに従って Pod セキュリティーを実施する SCC が導入されています。これらの SCC は次のとおりです。

- **restricted-v2**
- **hostnetwork-v2**

- **nonroot-v2**

これらは、同様の名前の古い SCC に対応していますが、以下のような拡張機能があります。

- **ALL** 機能がコンテナーから削除されます。以前は、**KILL**、**MKNOD**、**SETUID**、および **SETGID** 機能のみが削除されました。
- **NET_BIND_SERVICE** 機能を明示的に追加できるようになりました。
- 設定されていない場合、**seccompProfile** はデフォルトで **runtime/default** に設定されます。以前のリリースでは、このフィールドは空でなければなりませんでした。
- セキュリティーコンテキストでは、**allowPrivilegeEscalation** を設定解除するか、**false** に設定する必要があります。以前は、**true** の値が許可されていました。

OpenShift Container Platform 4.11 では、**restricted** SCC ではなく、**restricted-v2** SCC がデフォルトでユーザーに付与される SCC になりました。新規クラスターでは、**restricted-v2** SCC が **restricted** SCC の代わりに、認証済みのユーザーに使用されます。アクセスが明示的に付与されない限り、**restricted** SCC は新規クラスターのユーザーが利用できなくなります。OpenShift Container Platform 4.10 以前でインストールされたクラスターでは認証済みのユーザーはすべて、OpenShift Container Platform 4.11 のアップグレード時に **restricted** SCC を使用します。こうすることで、OpenShift Container Platform のデフォルトのセキュリティーパーミッションを secure-by-default のままにし、アップグレードされたクラスターのパーミッションを以前の状態に保つ一方で、アップストリームの Kubernetes プロジェクトからの Pod セキュリティー受付および Pod セキュリティー基準に合わせます。

ほとんどの namespace の同期を有効にし、すべての namespace の同期を無効にすることができます。

このリリースでは、**openshift-** が接頭辞として付けられた namespace には、制限付き実施はありません。このような namespace の制限付き実施は、今後のリリースに含まれる予定です。

詳細は、 Understanding and managing pod security admission を参照してください。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.11 では、主に以下のような技術的な変更点が加えられています。

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 4.11 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。

ルーター負荷分散アルゴリズムを設定するためのデフォルト値の更新
ルーター負荷分散アルゴリズムを設定する **haproxy.router.openshift.io/balance** 変数のデフォルトが **leastconn** ではなく **random** の値になりました。詳細は、ルート固有のアノテーション について参照してください。

LegacyServiceAccountTokenNoAutoGeneration がデフォルトでオン
以前のリリースでは、サービスアカウントの作成時に 2 つのサービスアカウントトークンシークレットが生成されました。

- 内部 OpenShift Container Platform レジストリーに対する認証のためのサービスアカウントトークンのシークレット
- Kubernetes API にアクセスするためのサービスアカウントトークンシークレット

OpenShift Container Platform 4.11 以降、Kubernetes API にアクセスするためのこの 2 番目のサービス

アカウントトークンシークレットは作成されなくなりました。これは、**LegacyServiceAccountTokenNoAutoGeneration** アップストリームの Kubernetes 機能ゲートが Kubernetes 1.24 で有効になっており、Kubernetes API にアクセスするためのシークレットベースのサービスアカウントトークンの自動生成が停止されるためです。OpenShift Container Platform 4.11 にアップグレードした後も、既存のサービスアカウントトークンシークレットは削除されず、引き続き機能します。

注記

これらの自動生成されたシークレットは、自分での使用に依存することがないようにしてください。これらは将来の OpenShift Container Platform リリースで削除される可能性があります。

バインドされたサービスアカウントトークンを取得するために、予測されたボリュームでワークロードが自動的に挿入されます。ワークロードに追加のサービスアカウントトークンが必要な場合は、ワークロードマニフェストに追加の予測ボリュームを追加します。詳細は、バインドされたサービスアカウントトークンの使用 を参照してください。

読み取り可能な API オブジェクト内の有効期限のないトークンのセキュリティー露出が許容される場合は、サービスアカウントトークンシークレットを手動で作成してトークンを取得することもできます。詳細は、サービスアカウントトークンシークレットの作成 を参照してください。

Operator SDK 1.22.2
OpenShift Container Platform 4.11 は Operator SDK 1.22.2 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、Installing the Operator SDK CLI を参照してください。

注記

Operator SDK 1.22.2 は Kubernetes 1.24 をサポートします。

以前に Operator SDK 1.16.0 で作成または管理されている Operator プロジェクトがある場合は、Operator SDK 1.22.2 との互換性を維持するためにプロジェクトを更新してください。

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

Cluster Operator はプラットフォーム Operator とは呼ばれなくなりました
OpenShift Container Platform のドキュメントでは、以前はクラスター Operator を別名プラットフォーム Operators と同じ意味で参照していました。この二重命名は、議論されている Operator のタイプについて混乱を招く可能性があるため、**ClusterOperator** API オブジェクトによって表されるクラスター Operator を参照するときに、プラットフォーム Operator という用語は使用されなくなりました。OpenShift Container Platform 4.11 以前のドキュメントセットが更新され、クラスター Operator という用語のみが使用されるようになりました。

たとえば、Cluster Operators リファレンス 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 4.11 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。非推奨となり、削除された機能の詳細は、表の後に記載されています。

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 4.9	OCP 4.10	OCP 4.11
Operator カタログの SQLite データベース形式	DEP	DEP	DEP
Cluster Samples Operator の **ImageChangesInProgress** 状態	DEP	DEP	DEP
Cluster Samples Operator の **MigrationInProgress** 状態	DEP	DEP	DEP
クラスターローダー	DEP	REM	REM
独自の RHEL 7 コンピュートマシンの持ち込み	DEP	REM	REM
Jenkins Operator	DEP	REM	REM
モニタリングスタックの Grafana コンポーネント	-	DEP	REM
モニタリングスタック内の Prometheus および Grafana UI へのアクセス		DEP	REM
vSphere 6.7 Update 2 以前	DEP	DEP	REM
vSphere 7.0 Update 1 以前	-	-	DEP
仮想ハードウェアバージョン 13	DEP	DEP	REM
VMware ESXi 6.7 Update 2 以前	DEP	DEP	REM
VMware ESXi 7.0 Update 1 以前	-	-	DEP
Snapshot.storage.k8s.io/v1beta1 API エンドポイント	DEP	DEP	REM
Microsoft Azure クラスターのクレデンシャルの作成	GA	REM	REM

機能	OCP 4.9	OCP 4.10	OCP 4.11
FlexVolume を使用した永続ストレージ	-	DEP	DEP
サービスアカウントトークンシークレットの自動生成	GA	GA	REM
インストールペイロードからの Jenkins イメージの削除	GA	GA	REM
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	REM

1.5.1. 非推奨の機能

1.5.1.1. トークンを要求する OpenShift CLI (oc) コマンドおよびフラグが非推奨に

トークンを要求するための以下の **oc** コマンドおよびフラグが非推奨になりました。

- **oc serviceaccounts create-kubeconfig** コマンド
- **oc serviceaccounts get-token** コマンド
- **oc serviceaccounts new-token** コマンド
- **oc registry login** コマンドの **--service-account/-z** フラグ

トークンを要求するには、代わりに **oc create token** コマンドを使用します。

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

Red Hat Virtualization (RHV) は、OpenShift Container Platform の今後のリリースで非推奨になります。RHV での OpenShift Container Platform のサポートは、今後の OpenShift Container Platform リリースから削除される予定です (現時点では OpenShift Container Platform 4.14 に削除予定)。

1.5.1.3. vSphere 7.0 Update 1 以前のサポートを非推奨化

OpenShift Container Platform 4.11 では、VMware vSphere 7.0 Update 1 以前のサポートが非推奨になりました。vSphere 7.0 Update 1 以前は引き続き完全にサポートされますが、Red Hat では、vSphere 7.0 Update 2 以降 (バージョン 8 を除く) までを使用することを推奨します。vSphere 8 はサポートされていません。

1.5.1.4. ESXi 7.0 Update 1 以前のサポートを非推奨化

OpenShift Container Platform 4.11 では、VMware ESXi 7.0 Update 1 以前のサポートが非推奨となりました。EXSi 7.0 Update 1 以前は完全にサポートされますが、Red Hat は ESXi 7.0 Update 2 以降の使用を推奨します。

1.5.1.5. pidsLimit および logSizeMax CRI-O パラメーターのサポートは非推奨になります

OpenShift Container Platform 4.11 では、**ContainerRuntimeConfig** CR の **pidsLimit** および

logSizeMax フィールドは非推奨になり、将来のリリースで削除されます。代わりに、**KubeletConfig** CR の **podPidsLimit** および **containerLogMaxSize** フィールドを使用してください。**podPidsLimit** フィールドのデフォルト値は **4096** です。

1.5.2. 削除された機能

1.5.2.1. OpenShift CLI (oc) の RHEL 7 サポートが削除される

OpenShift CLI (**oc**) で Red Hat Enterprise Linux (RHEL) 7 を使用するためのサポートが削除されました。RHEL で OpenShift CLI (**oc**) を使用する場合は、RHEL 8 以降を使用する必要があります。

1.5.2.2. 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 migrate etcd-ttl**
- **oc adm migrate image-references**
- **oc adm migrate legacy-hpa**
- **oc adm migrate storage**

1.5.2.3. モニタリング スタックから削除された Grafana コンポーネント

Grafana コンポーネントは、OpenShift Container Platform 4.11 モニタリングスタックの一部ではなくなりました。別の方法として、OpenShift Container Platform Web コンソールで **Observe** → **Dashboards** に移動して、モニタリングダッシュボードを表示します。

1.5.2.4. モニタリングスタックから削除された Prometheus および Grafana ユーザーインターフェイスアクセス

サードパーティーの Prometheus および Grafana ユーザーインターフェイスへのアクセスは、OpenShift Container Platform 4.11 モニタリングスタックから削除されました。別の方法として、OpenShift Container Platform Web コンソールで **Observe** をクリックして、モニタリングコンポーネントのアラート、メトリクス、ダッシュボード、およびメトリクスターゲットを表示します。

1.5.2.5. 仮想ハードウェアバージョン 13 のサポートを削除

OpenShift Container Platform 4.11 では、仮想ハードウェアバージョン 13 のサポートが削除されました。仮想ハードウェアバージョン 13 のサポートは OpenShift Container Platform 4.9 で非推奨になりました。Red Hat は、仮想ハードウェアのバージョン 15 以降の使用を推奨します。

1.5.2.6. vSphere 6.7 Update 2 以前のサポートを削除

OpenShift Container Platform 4.11 では、VMware vSphere 6.7 Update 2 以前のサポートが削除されました。vSphere 6.7 Update 2 以前のサポートは OpenShift Container Platform 4.9 で非推奨になりました。Red Hat では、vSphere 7.0 Update 2 以降 (バージョン 8 を除く) を使用することを推奨します。vSphere 8 はサポートされていません。

1.5.2.7. ESXi 6.7 Update 2 以前のサポートを削除

OpenShift Container Platform 4.11 では、VMware ESXi 6.7 Update 2 以前のサポートが削除されました。ESXi 6.7 Update 2 以前のサポートは OpenShift Container Platform 4.10 で非推奨となりました。Red Hat は、ESXi 7.0 Update 2 以降の使用を推奨します。

1.5.2.8. スナップショット v1beta1 API エンドポイントのサポートを削除

OpenShift Container Platform 4.11 では、**snapshot.storage.k8s.io/v1beta1** API エンドポイントのサポートが削除されました。**snapshot.storage.k8s.io/v1beta1** API エンドポイントのサポートは OpenShift Container Platform 4.7 で非推奨となりました。Red Hat は、**snapshot.storage.k8s.io/v1** の使用を推奨します。**v1beta1** として作成されたすべてのオブジェクトは、v1 エンドポイントで利用できます。

1.5.2.9. カスタムスケジューラーの手動デプロイのサポートが削除される

本リリースでは、カスタムスケジューラーを手動でデプロイするためのサポートが削除されました。代わりに Red Hat OpenShift の Secondary Scheduler Operator を使用して、OpenShift Container Platform にカスタムセカンダリースケジューラーをデプロイします。

1.5.2.10. OpenShiftSDN を使用した単一ノードの OpenShift のデプロイサポート

本リリースでは、OpenShiftSDN を使用した単一ノードの OpenShift クラスターのデプロイのサポートが削除されました。OVN-Kubernetes は、単一ノードの OpenShift デプロイメントのデフォルトのネットワークソリューションです。

1.5.2.11. インストールペイロードからの Jenkins イメージの削除

- OpenShift Container Platform 4.11 は、"OpenShift Jenkins" および "OpenShift Agent Base" イメージを **registry.redhat.io** の **ocp-tools-4** リポジトリーに移動し、Red Hat が OpenShift Container Platform のライフサイクル外でイメージを生成および更新できるようにします。以前は、これらのイメージは OpenShift Container Platform インストールペイロードと、**registry.redhat.io** の **openshift4** リポジトリーにありました。詳細は、OpenShift Jenkins を参照してください。

- OpenShift Container Platform 4.11 は、ペイロードから "OpenShift Jenkins Maven" および "NodeJS Agent" イメージを削除します。OpenShift Container Platform 4.10 は以前、これらのイメージを非推奨にしました。Red Hat はこれらのイメージを生成しなくなり、**registry.redhat.io** の **ocp-tools-4** リポジトリーから入手できなくなりました。
  ただし、OpenShift Container Platform 4.11 にアップグレードしても、"OpenShift Jenkins Maven" および "NodeJS Agent" イメージは、4.10 以前のリリースから削除されません。また、Red Hat は、OpenShift Container Platform ライフサイクル ポリシー に従って、4.10 リリースライフサイクルの終わりまで、これらのイメージのバグ修正とサポートを提供します。

  詳細は、OpenShift Jenkins を参照してください。

1.5.3. 今後の Kubernetes API の削除

OpenShift Container Platform の次のマイナーリリースは Kubernetes 1.25 を使用することが想定されます。現在、Kubernetes 1.25 は、いくつかの非推奨の **v1beta1** および **v2beta1** API を削除する予定です。

予定されている Kubernetes API の削除一覧については、アップストリームの Kubernetes ドキュメントの Deprecated API Migration Guide を参照してください。

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

1.6. バグ修正

ベアメタルハードウェアのプロビジョニング

- 以前は、RHCOS イメージを一部のディスクに書き込むときに、**qemu-img** がスパース領域を含むディスク全体にスペースを割り当てていました。これにより、一部のハードウェアで書き込みプロセスの時間が長くなりました。この更新により、イメージ作成で **qemu-img** スパースが無効になります。その結果、影響を受けるハードウェアでイメージの書き込みに時間がかからなくなりました。(BZ#2002009)

- 以前は、**rotation** フィールドが **RootDeviceHints** に設定されている場合、ホストがプロビジョニングに失敗する可能性がありました。今回の更新により、**RootDeviceHints** の **rotational** フィールドが適切にコピーされ、チェックされるようになりました。その結果、**rotational** フィールドを使用するとプロビジョニングが成功します。(BZ#2053721)

- 以前は、Ironic は仮想メディアを使用して Nokia OE 20 サーバーをプロビジョニングできませんでした。これは、**TransferProtocolType** 属性がオプションの属性であるにもかかわらず、BMC がこの属性を明示的にリクエストに設定することを要求したためです。さらに、ほとんどの BMC は **system** リソースのみを使用するのに対し、この BMC は専用の **RedFish** 設定リソースを使用してブート順序をオーバーライドする必要もありました。このエラーは、Nokia OE 20 が vMedia アタッチメントにオプションの **TransferProtocolType** 属性を厳密に必要とし、ブートシーケンスをオーバーライドするために **RedFish** 設定リソースを使用する必要があるために発生しました。その結果、Nokia OE 20 では仮想メディアベースのプロビジョニングが失敗します。この問題を回避する方法は 2 つあります。

  1. **TransferProtocolType** 属性が欠落していることを示すエラーで vMedia アタッチメントリクエストが失敗した場合は、リクエストを再試行し、この属性を明示的に指定します。

  2. システムに RedFish 設定リソースが存在することを確認します。存在する場合は、ブートシーケンスのオーバーライドに使用します。

  これらの回避策により、仮想メディアベースのプロビジョニングは Nokia OE 20 マシン上で成功します。(BZ#2059567)

- 以前は、Ironic API インスペクターイメージは、OpenShift Container Platform ベアメタル IPI デプロイメントを使用する場合、パッシブマルチパスセットアップの一部であるディスクをクリーンアップできませんでした。この更新プログラムは、アクティブまたはパッシブストレージアレイが使用されている場合の障害を修正します。その結果、お客様がアクティブまたはパッシブのマルチパスセットアップを使用したい場合に、OpenShift Container Platform ベアメタル IPI を使用できるようになりました。(BZ#2089309)

- 以前は、Ironic は **wwn** シリアル番号をマルチパス デバイスに一致させることができませんでした。そのため、デバイスマッパーデバイスの **wwn** シリアル番号は、**install-config.yaml** 設定ファイルの **rootDeviceHint** パラメーターで使用することができませんでした。今回の更新により、Ironic は **wwn** シリアル番号をマルチパスデバイスの一意の識別子として認識するようになりました。その結果、**install-config.yaml** ファイルのデバイスマッパーデバイスに **wwn** シリアル番号を使用できるようになりました。(BZ#2098392)

- 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 4.11 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-2052)

ビルド

- 以前は、**BuildConfig** インスタンスの **ImageLabel** 名にスラッシュ (/) を使用すると、エラーが発生していました。この修正は、検証に使用されるユーティリティーを変更することで問題を解決します。その結果、**BuildConfig** インスタンスの **ImageLabel** 名にフォワードスラッシュを使用できます。(BZ#2105167)

- 以前は、**$ oc new-app --search <image_stream_name>** コマンドを使用すると、**docker.io** イメージに関連する誤ったメッセージを受け取ることがありました。OpenShift Container Platform は **docker.io** を指すイメージストリームを使用しないため、ユーザーに混乱が生じました。この修正により、コードチェックが追加され、**docker.io** への参照が阻止されます。その結果、そのコマンドからの出力にはメッセージが含まれません。(BZ#2049889)

- 以前は、Shared Resource CSI Driver メトリックは Telemetry サービスにエクスポートされませんでした。その結果、Shared Resource CSI Driver の使用状況メトリックを分析できませんでした。今回の修正により、Shared Resource CSI Driver メトリックが Telemetry サービスに公開されます。その結果、Shared Resource CSI Driver の使用状況メトリックを収集して分析することができます。(BZ#2058225)

- デフォルトでは、Buildah は環境変数の内容を含むステップをログファイルに出力します。これには、ビルド入力シークレット が含まれる場合があります。**--quiet** ビルド引数を使用してこれらの環境変数の出力を抑制することができますが、source-to-image (S2I) ビルドストラテジーを使用する場合は、この引数は使用できません。現在のリリースではこの問題は修正されています。環境変数の出力を抑制するには、ビルド設定で **BUILDAH_QUIET** 環境変数を設定します。

```
sourceStrategy:
...
  env:
    - name: "BUILDAH_QUIET"
      value: "true"
```

- 今回の更新以前は、**$ oc new-app --search <image_stream_name>** コマンドを使用すると、コンテナーイメージ **"docker.io/library/<image_name>:<tag>"** にアクセスできない可能性がある警告が表示されていました。そのため、OpenShift Container Platform で **docker.io** を指すイメージストリームがあるという混乱が生じていました。今回の更新ではコードチェックを追加して問題を解決することで、'docker.io' を指すという混乱が解消されました。現在、そのコマンドからの出力に **docker.io** に関するメッセージは含まれていません (BZ#2049889)。

クラウドコンピュート

- **CertificateSigningRequest** (CSR) リソースの更新は、Kubernetes コントローラーマネージャーによって処理され、Cluster Machine Approver Operator によって適切に保留されたままになります。これにより、**mapi_current_pending_csr** メトリックの値が **1** に増加します。以前は、Kubernetes コントローラーマネージャーが CSR を承認すると、Operator はそれを無視し、メトリックを変更しませんでした。その結果、**mapi_current_pending_csr** メトリックは、Operator が次に調整するまで **1** のままでした。このリリースでは、他のコントローラーからの CSR 承認が常に調整されてメトリックが更新され、調整のたびに **mapi_current_pending_csr** メトリックの値が更新されます。(BZ#2047702)

- 以前は、AWS SDK 内の既知のリージョンのリストに含まれるリージョンのみが検証され、他のリージョンを指定するとエラーが発生しました。これは、新しいリージョンが追加されると、SDK が更新されて新しいリージョン情報が含まれるまで使用できないことを意味していました。今回のリリースでは、リージョンが認識されない場合にユーザーに警告を発するなど、よ

り厳密でない設定でリージョンが検証されるようになりました。その結果、新しいリージョンでは警告メッセージが表示される場合がありますが、すぐに使用することができます。(BZ#2065510)

- 以前は、Cluster Machine Approver Operator が **"Approved"** ステータス条件を条件リストに追加していました。その結果、Kubernetes API サーバーは、メッセージ **[SHOULD NOT HAPPEN] failed to update managedFields** を含むエラーをログに記録していました。このリリースでは、Operator が更新され、リストに追加する前にその条件をチェックし、必要な場合にのみ条件を更新します。その結果、**CertificateSigningRequest** リソースで条件が重複しなくなり、Kubernetes API サーバーは重複に関するエラーをログに記録しなくなりました。(BZ#1978303)

- 以前は、Red Hat OpenStack Platform (RHOSP) バージョン 16 に存在した Cisco ACI neutron 実装の欠陥が原因で、特定のネットワークに属するサブネットのクエリーが予期しない結果を返していました。その結果、RHOSP Cluster API プロバイダーは、同じサブネット上で重複するポートを使用してインスタンスをプロビジョニングしようとし、プロビジョニングが失敗する可能性がありました。このリリースでは、RHOSP Cluster API プロバイダーでの追加のフィルタリングにより、サブネットごとに複数のポートが存在しないことが保証され、Cisco ACI を使用して RHOSP バージョン 16 に OpenShift Container Platform をデプロイできるようになりました。(BZ#2033862)

- 以前は、Red Hat OpenStack Platform (RHOSP) Machine API プロバイダーがプロキシー環境変数ディレクティブを使用していなかったため、HTTP または HTTPS プロキシーの背後でのインストールが失敗していました。このリリースでは、プロバイダーはプロキシーディレクティブに従い、egress トラフィックがプロキシー経由でのみ許可される制限された環境で正しく機能します。(BZ#2046133)

- 以前は、OpenShift Container Platform 4.9 から 4.10 にアップグレードすると、複数のコントローラー間で不整合が発生し、誤ったバージョン番号になることがありました。その結果、バージョン番号に一貫性がありませんでした。このリリースでは、バージョン番号の一貫した読み取りが実行され、リリースバージョンはクラスター Operator ステータスで安定しています。(BZ#2059716)

- 以前は、AWS Machine API プロバイダーでロードバランサーターゲットのリークが発生する場合がありました。これは、コントロールプレーンマシンを交換するときに、IP ベースのロードバランサーアタッチメントがロードバランサーの登録内に残る可能性があるためです。このリリースでは、Amazon EC2 インスタンスが AWS から削除される前に、IP ベースのロードバランサーアタッチメントがロードバランサーから削除されます。その結果、リークが回避されます。(BZ#2065160)

- 以前は、アップグレード中に、Machine API を介して作成された新しいマシンが HW-13 にデフォルト設定され、クラスターの機能が低下していました。このリリースでは、テンプレートクローンからマシンを作成する際に、マシンコントローラーが仮想マシンのハードウェアバージョンをチェックします。テンプレートのハードウェアバージョンが 15 未満の場合、マシンは **failed** 状態になります。これは、OpenShift Container Platform 4.11 以降のバージョンでサポートされる最小のハードウェアバージョンです。(BZ#2059338)

- 以前は、Azure 可用性セットの手順名ジェネレーターは、最大 80 文字の制限を超えていました。これにより、Machine API は、複数の可用性セットを作成するのではなく、名前切り捨ての際に同じセットを再利用する可能性があります。このリリースでは、手順名ジェネレーターが更新され、名前が 80 文字を超えないようにし、クラスター名がセット名で重複しないようにします。その結果、Azure 可用性セットが予期しない方法で手順名ジェネレーターによって切り捨てられることがなくなりました。(BZ#2093044)

- Cluster Autoscaler Operator は、リーダー選択パラメーターを設定せずにクラスターオートスケーラーをデプロイしていたため、クラスターの再起動後に、クラスターオートスケーラーが予期せず失敗して再起動することがありました。今回の修正により、Cluster Autoscaler

Operator は、適切に定義されたリーダー選出フラグを使用して、クラスターオートスケーラーをデプロイするようになりました。その結果、クラスターオートスケーラーは再起動後に期待どおりに動作します。(BZ#2063194)"

- 以前は、証明書署名要求 (CSR) の更新は **kube-controller-manager** によって処理され、マシンの承認者によって適切に保留されていたため、**mapi_current_pending_csr** が **1** に増加していました。その後、**kube-controller-manager** は CSR を承認しましたが、マシンの承認者はそれを無視したため、メトリックは変更されませんでした。その結果、**mapi_current_pending_csr** は、別のマシン承認者が調整するまで **1** のままでした。今回の更新により、CSR の承認が他のコントローラーから調整され、メトリックが適切に更新されるようになります。その結果、**mapi_current_pending_csr** は、調整のたびに常に最新の状態になります。(BZ#2072195)

- 以前は、クラスターのインストール時に十分な数のワーカーノードが開始されなかった場合、他の Operator が機能低下を報告していても、Machine API Operator は機能低下を報告しませんでした。このリリースでは、Machine API Operator が機能低下として報告されるようになり、このシナリオではインストールログにエラーが記録されます。その結果、Machine API Operator が失敗した Operator のリストに表示されるので、ユーザーはワーカーノードが不十分な理由としてマシンの状態を調べることを理解するようになりました。(BZ#1994820)

- Machine API Operator がプロキシー環境変数ディレクティブを受け入れなかったため、HTTP または HTTPS プロキシーの背後でのインストールが失敗しました。今回の修正により、Machine API Operator の HTTP トランスポートロジックが、プロキシーディレクティブに従うようになりました。その結果、Machine API Operator は、egress トラフィックがプロキシー経由でのみ許可される制限された環境で動作するようになりました。(BZ#2082667)

- 以前は、数千のタグと重い API 負荷を持つクラスターの vShpere へのインストールは失敗していました。現在、マシンコントローラーは、特定の OpenShift Container Platform インストールに関連するタグのみをクエリーします。その結果、OpenShift Container Platform はこれらのクラスターの vSphere に正しくインストールされます。(BZ#2097153)

- kubelet はノードゾーンラベルを取得するために vCenter に接続する必要があるため、vCenter 認証情報がシークレットに保存されている場合、kube クライアントが時間どおりに作成されなかったため、kubelet を起動できませんでした。その結果、ノードを再起動すると、**cloud-provider-config** config map を編集するときに発生するように、ノードが起動しませんでした。今回の修正により、認証情報がシークレットに保存されている場合、kubelet はノード登録後にゾーンラベルを取得するようになりました。その結果、ノードは期待どおりに再起動します。(BZ#1902307)

- 以前は、**timeout** オプションがないためにコントローラーがブロックされ、vCenter がまったく応答しないか、応答が非常に遅くなることがありました。このリリースでは、vSphere マシン コントローラー内の vCenter クライアントの **timeout** オプションが追加されています。(BZ#2083237)

Cluster Version Operator

- 以前は、アップグレード中にエラーが発生した場合、Cluster Version Operator (CVO) は現在のリリースマニフェストの調整を停止していました。今回の更新では、リリースの読み込みは調整から分離されているため、調整が読み込みをブロックすることはありません。また、リリースの読み込みのステータスを明確にするために、新しい条件 **ReleaseAccepted** が追加されました。(BZ#1822752)

Console Metal3 プラグイン

- 以前は、**bootMode** ストラテジーを設定するためのオプションが UI にありませんでした。その結果、UI は常にデフォルト (UEFI) のブートストラテジーを使用し、これにより、ベアメタルデプロイメントの一部のタイプの起動で問題が発生していました。この更新により、適切な

ブートモードストラテジーを選択するための **Add Bare Metal** ホストフォームに新しいフィールドが公開されます。その結果、ベアメタルマシンが正常に起動します。(BZ#2091030)

- 以前は、ノードメンテナンス機能が新しいプロジェクトに移動されたため、API が変更されました。その結果、ノードのメンテナンスが機能しなくなりました。この更新により、新しい API で正しく動作するようにコードが修正されます。その結果、ノードのメンテナンスが再び機能します。(BZ#2090621)

- 以前は、支援インストーラーによって作成されたクラスターの day 2 ワーカーで、基礎となるベアメタルホストとマシンリソースが欠落している場合がありました。その結果、ワーカーノードの詳細を表示しようとすると、UI が失敗しました。今回の更新により、ベアメタルホストとマシンリソースがより適切に処理され、UI に利用可能なすべての詳細が表示されます。(BZ#2090993)

DNS (Domain Name System)

- Topology Aware Hint (トポロジーを意識したヒント) は、OpenShift Container Platform 4.11 の新機能で、**EndpointSlice** コントローラーが、サービスのエンドポイントにトラフィックをルーティングする方法について、Container Network Interface (CNI) にヒントを指定できるようにするものです。DNS Operator は、クラスター DNS サービスの Topology Aware Hint を有効にしていませんでした。その結果、CNI ネットワークプロバイダーは DNS トラフィックをゾーンまたはノードに対してローカルに保持しませんでした。この修正により、DNS Operator が更新され、クラスター DNS サービスで Topology Aware Hint が指定されるようになりました。(BZ#2095941)

- 以前は、kubelet は、ノードホストの **/etc/resolv.conf** に基づいて、Pod のデフォルトの **/etc/resolv.conf** を作成していました。その結果、不正な形式の **resolv.conf** ファイルにより、リゾルバーが **resolv.conf** の解析に失敗し、Pod での DNS 解決が中断される可能性がありました。今回の更新により、kubelet は **resolv.conf** ファイルを受け入れ、Pod は有効な **resolv.conf** ファイルを取得します。(BZ#2063414)

- 以前は、DNS Operator は DNS Pod に **cluster-autoscaler.kubernetes.io/enable-ds-eviction** アノテーションを設定していませんでした。そのため、クラスターオートスケーラーは、ノードを削除する前にノードから DNS Pod を削除しませんでした。今回の更新により、DNS Operator が変更され、**cluster-autoscaler.kubernetes.io/enable-ds-eviction** アノテーションが DNS Pod に追加されました。クラスターオートスケーラーによってノードを削除する前に、ノードから DNS Pod を削除できるようになりました。(BZ#2061244)

Image Registry

- 以前は、イメージレジストリーは、完全に一致する場合にのみ **ImageContentSourcePolicy** (ICSP) をソースとして使用していました。すべてのサブリポジトリーで、同じソースファイルがプルされると予想されていました。サブリポジトリーの ICSP 名とパスが一致しませんでした。その結果、イメージは使用されませんでした。現在は、ICSP がサブリポジトリーに正常に適用され、ミラーリングされたイメージを使用できるようになりました。(BZ#2014240)

- 以前は、プルーナーが失敗した場合、プルーナーが正常に実行されるまで、イメージレジストリー Operator は機能が低下していると報告されていました。今回の更新により、Operator はプルーナーの障害に対する回復力が向上しました。(BZ#1990125)

- これまでレジストリーは、**ImageContentSourcePolicy** (ICSP) を適用するときに完全な一致を使用していました。今回の更新で、ICSP がサブリポジトリーに適用され、ミラーが期待どおりに機能するようになりました。(BZ#2014240)

- これまで、Image Registry Operator は RHOSP 上の AWS S3 で機能しませんでした。今回の更新で、イメージレジストリー Operator はすべてのプラットフォームで AWS S3 を信頼するようになりました。(BZ#2007611)

- これまで、OpenShift Container Platform イメージレジストリーは Ceph Radosgw で機能しませんでした。今回の更新で、イメージレジストリーは Ceph Radosgw で機能するようになりました。(BZ#1976782)

- これまで、Image Registry Operator はアップストリームレジストリーからの **429** エラーメッセージを、あたかもデータが利用できないかのように解釈していました。Operator は、**429 Too many Requests** の代わりに **404 Not Found** メッセージを返しました。今回の更新により、適切な **429 Too many Requests** メッセージが返され、管理者はリクエストの再試行する必要があることを認識できるようになりました。(BZ#1923536)

- これまで、Image Registry Operator は CloudFront の設定に使用できませんでした。今回の更新により、Image Registry Operator が CloudFront を設定できるようになりました。(BZ#2065224)

- これまで、Image Registry Operator は KMS 暗号化が有効な場合にイメージをプッシュしましたが、プルしませんでした。今回の更新により、KMS 暗号化を有効にしてイメージをプッシュおよびプルできるようになりました。(BZ#2048214)

- これまで、Image Registry Operator は認証情報が提供されないためにパブリックイメージを匿名でプルできませんでした。今回の更新により、クライアントはパブリックイメージを匿名でプルできるようになりました。(BZ#2060605)

- これまで、Image Registry Operator は **ap-southeast-3** AWS リージョンを使用できませんでした。今回の更新により、レジストリーを **ap-southeast-3** に設定できるようになりました。(BZ#2065552)

インストーラー

- 以前は、ユーザーが OpenShift Container Platform クラスター名にピリオドを指定すると、インストールが失敗していました。今回の更新で、クラスター名にピリオドが含まれている場合にエラーを返す検証チェックがインストールプログラムに追加されました。(BZ#2084580)

- 以前は、インストールプログラムを使用して **install-config.yaml** ファイルを作成するときに、ユーザーは AWS **us-gov-east-1** リージョンを選択できました。インストールプログラムは、パブリック AWS リージョンの **install-config.yaml** ファイルの作成にしか使用できなかったため、デプロイが失敗しました。この更新により、パブリック AWS クラウドでサポートされていないすべての AWS リージョンがインストール プログラムから削除されます。(BZ#2048222)

- 以前は、インストールプログラムを使用して **install-config.yaml** ファイルを作成するときに、ユーザーは **ap-north-east-3** リージョンを選択できませんでした。この問題の原因となった AWS SDK が更新され、ユーザーは **ap-north-east-3** リージョンを選択できるようになりました。(BZ#1996544)

- 以前は、インストールプログラムが API 仮想 IP アドレスの DNS レコードを作成しなかったため、プライベート (内部) OpenShift Container Platform クラスターを Azure Stack Hub にインストールできませんでした。この更新により、この問題の原因となった無効なチェックが削除されます。インストールプログラムは、プライベートクラスターの DNS レコードを正しく作成するようになりました。(BZ#2061549)

- 以前は、IBM Cloud VPC クラスターをアンインストールすると、予期しない結果が生じる可能性がありました。ユーザーがクラスター (クラスター 1) をアンインストールすると、別のクラスター (クラスター 2) の DNS レコードが削除されました。これは、クラスター 1 の名前 (example) がクラスター 2 の名前 (myexample) のサブセットである場合、または両方のクラスターがベースドメインを共有している場合に削除されました。この更新では、この動作を修正しています。アンインストールされるクラスターに固有のリソースのみが削除されるようになりました。(BZ#2060617)

- 以前は、Azure Stack Hub は Standard_LRS 以外のディスクタイプをサポートしていませんでした。今回の更新により、ディスクタイプをカスタマイズする機能が追加されました。これにより、手動でカスタマイズしなくても、クラスターにデフォルトのディスクタイプを設定することができます。その結果、ディスクタイプをハードコーディングするのではなく、ユーザーからの入力を受け付け、Stack Hub API に対して検証する方法に切り替えられました。(BZ#2061544)

- 以前は、クラスターを破棄する際、DNS レコードがホストゾーンから削除されたときに、クラスターのプライベート route5 ホストゾーンの ID が誤って報告されていました。これにより、破棄する側のログに誤ったホストゾーン ID が報告されました。この更新では、ログで正しいホストゾーン ID が使用されます。その結果、ベースドメインのホストゾーンで DNS レコードを破棄すると、ログには正しいホストゾーン ID が表示されます。(BZ#1965969)

- 以前は、AWS カスタムサービスエンドポイントをリクエストするときに、システムプロキシー設定が考慮されませんでした。この更新により、AWS カスタムサービスエンドポイントの検証が設定され、AWS カスタムサービスエンドポイントへの **HEAD** リクエストと共にシステムプロキシー設定が考慮されます。その結果、ユーザーのマシンから AWS カスタムサービスエンドポイントにアクセスすることができます。(BZ#2048451)

- これまで、インストールプログラムは、インストーラーホスト上の **$PATH** で 任意の Terraform プロバイダーを使用していました。したがって、**$PATH** に Terraform プロバイダーがあり、インストールプログラムに組み込まれたプロバイダーではなく、誤ったバージョンまたはプロバイダーを使用していると、インストールは失敗しました。今回の更新により、インストールプログラムはプロバイダーを既知のディレクトリーに組み込み、既知のディレクトリーを使用するように Terraform を設定します。その結果、インストールプログラムは常に既知のディレクトリー内のプロバイダーを使用するため、インストールは成功します。(BZ#1932812)

- 以前は、新しいロードバランサーを更新するときに、AWS Terraform プロバイダーに結果整合性の問題がありました。したがって、新しいロードバランサーにアクセスしようとすると、インストールが失敗します。今回の修正により、インストールプログラムがアップストリームの Terraform プロバイダーに更新され、結果整合性が保証されるようになりました。その結果、インストールは失敗しなくなりました。(BZ#1898265)

- 以前は、インストールプログラムには、クォータとパーミッションをチェックする必要な API のリストがあり、そのリストには、ユーザーがパーミッションを提供しないと失敗する不要な API が含まれていました。今回の更新により、API のリストが **required** と **optional** に分割され、**optional** API にはアクセスできなくなりました。**optional** API については、警告メッセージが表示されます。(BZ#2084280)

- 以前は、特定のクラスター用に作成されたすべてのリソースを分離して削除するコードをデータベースから削除するためにインストールプログラムによって使用されるタグ **kubernetes.io_cluster<infraID>** が **.apps** エントリーにありませんでした。今回の更新により、作成時にクラスター Ingress Operator にタグが追加され、エントリーが削除可能になりました。(BZ#2055601)

- 以前は、内部公開ストラテジーを使用すると、**openshift-install** コマンドが失敗していました。今回の更新により、**openshift-install** コマンドが失敗しなくなりました。(BZ#2047670)

- 以前は、新しく作成された Virtual Private Cloud (VPC) に更新するときに、AWS Terraform プロバイダーに結果整合性の問題がありました。その結果、VPC にアクセスしようとすると、インストールプログラムが失敗していました。今回の更新により、インストールプログラムがアップストリームの Terraform プロバイダーに更新され、インストールが失敗しなくなりました。(BZ#2043080)

- 以前は、新しく作成されたネットワークインターフェイスに更新するときに、AWS Terraform プロバイダーに結果整合性の問題がありました。その結果、インストールはネットワークイン

ターフェイスにアクセスできませんでした。今回の更新により、結果整合性を受け入れるように Terraform プロバイダーが更新され、インストールが失敗しなくなりました。(BZ#2047741)

- 以前は、インストーラーによってプロビジョニングされたインフラストラクチャーを使用して VMware クラスターをインストールするときに、**corespersocket** の値が **numCores** の値よりも高くなることがありました。これにより、インストール中に予期しない結果が生じる可能性がありました。今回の更新により、ユーザーはクラスターが作成される前にこれらの値を修正するよう警告を受け取ります。(BZ#2034147)

- 以前は、まれなバグにより、AWS クラスターのインストール中に不整合が発生していました。このシナリオを回避するために、インストールプログラムが更新されました。(BZ#2046277)

- 以前は、サポートされているユーザー定義タグの数は 8 で、AWS リソース用に予約された OpenShift Container Platform タグは 2 でした。このリリースでは、サポートされるユーザー定義タグの数が 25 になり、AWS リソース用に予約された OpenShift Container Platform タグが 25 になりました。インストール時に最大 25 のユーザータグを追加できるようになりました。(CFE#592)

- 以前は、ブートストラップマシンは、インストーラーによってプロビジョニングされたインフラストラクチャーを使用して Azure にインストールするときに、デフォルトのサイズとインスタンスタイプを使用していました。今回の更新により、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のサイズとインスタンスタイプを使用します。インストール設定のコントロールプレーン設定を変更することで、ブートストラップマシンのサイズとインスタンスタイプを制御できるようになりました。(BZ#2026356)

- 以前は、インストールプログラムが Terraform にあいまいなネットワーク名を提供していました。これにより、Terraform が使用する正しいネットワークを決定できなくな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が Terraform に一意のネットワーク ID を提供するため、インストールが成功するようになります。(BZ#1918005)

- 以前は、AWS にクラスターをインストールするときに、依存する NAT ゲートウェイが作成される前にコントロールプレーンマシンが作成される可能性があり、インストールが失敗していました。今回の更新により、Terraform は、コントロールプレーンマシンが作成される前に、NAT ゲートウェイが作成されていることを確認します。これにより、インストールが成功することが保証されます。(BZ#2049108)

- 以前は、デフォルトの OSN ネットワークではなく OVN ネットワークを使用した場合、必要な最大時間よりも長くかかるため、スケールアップタスクが失敗していました。この更新により、タスクを完了できるように、スケールアップタスク中の再試行回数が 2 倍になります。(BZ#2090151)

- 以前は、データベースから複数のクラスターを並行して削除しようとすると、**vmware** ライブラリーおよび **govmomi** ライブラリーのバグが原因で削除プロセスが失敗していました。このバグにより、クラスターのタグの 1 つが削除され、削除プロセスでタグが見つからなかったときに 404 エラーが発生しました。この更新は、見つからないタグを無視し、エラーなしで終了するように削除プロセスを続行します。(BZ#2021041)

- 今回の更新により、Red Hat Virtualization (RHV) 上の OpenShift Container Platform は、コントロールプレーン用の事前割り当てディスクと、インストーラーによってプロビジョニングされたインフラストラクチャー用のワーカーノードをサポートします。高負荷環境では、事前に割り当てられたディスクにより、etcd やその他のコンポーネントのパフォーマンスが向上します。(BZ#2035334)

- これまで、複数のクラスターを並行して削除しようとすると、**vmware/govmomi** ライブラリーのバグが原因でプロセスが失敗していました。このバグにより、クラスタータグが削除され、削除プロセスでタグが見つからない場合に **404** エラーが発生していました。今回の更新で

は、見つからないタグが無視され、削除を継続してエラーなしで終了するようになりました。(BZ#2021041)

- 以前は、VMware vSphere のインストール方法には、設定ファイルの作成中にネットワークの存在を確認する検証が含まれていました。これにより、ユーザーがプロビジョニングしたインフラストラクチャーや、インフラストラクチャーのプロビジョニングの一部としてネットワークを作成できるその他のインストール方法で、エラーが発生しました。この場合、config ファイルの生成時にネットワークが存在しない可能性があります。この修正により、インストールプログラムが更新され、インストーラーによってプロビジョニングされたインフラストラクチャーインストールでのみ、ネットワーク検証が実行されます。その結果、ユーザーがプロビジョニングしたインフラストラクチャーやその他のインストール方法で、ネットワークの存在に関係なく設定ファイルを生成できます。(BZ#2050767)

- 以前は、**runc** は **libseccomp** 2.5 以降に対して反転した依存関係を持っていたため、オペレーティングシステムがバージョン 8.3 以降を使用してインストールされ、8.4 以降に完全に更新されていない場合に問題が発生していました。今回の更新により、RHEL ホストが正常にインストールされ、パッケージの初期バージョンの問題が回避されます。(BZ#2060147)

- 以前は、インストールプログラムは、terraform へのネットワークリソースを相対パスで指定していました。ネットワークリソースがフォルダーにネストされている場合、terraform プロバイダーはリソースを見つけることができませんでした。今回の更新により、ネットワークリソースが ID で指定されるようになり、インストールが成功するようになりました。(BZ#2063829)

- 以前は、vSphere RHCOS イメージに **/etc/resolv.conf** ファイルがありませんでした。これにより、デフォルトの **networkmanager** 設定で **/etc/resolv.conf** のエラーが表示されました。今回の更新では、**rc-manager=unmanaged** 値が設定され、**networkmanager** 設定は **/etc/resolv.conf** にダイレクトされなくなりました。(BZ#2029438)

- 以前は、Amazon Web Services (AWS) では必要ないため、インストールプログラムはクラウドプロバイダー設定を作成しませんでした。これにより、Kubernetes API サーバーでは、クラウドプロバイダーの設定なしでエラーが発生していました。今回の更新により、AWS 用の空のクラウドプロバイダー設定が作成され、Kubernetes API サーバーが正常に実行できるようになりました。(BZ#1926975)

Kubernetes API サーバー

- 以前は、ストリーミングに使用される実行時間の長いリクエストは、**KubeAPIErrorBudgetBurn** の計算で考慮されていました。その結果、**KubeAPIErrorBudgetBurn** からのアラートがトリガーされ、誤検出が発生していました。この更新により、長時間実行されるリクエストが **KubeAPIErrorBudgetBurn** の計算から除外されます。その結果、**KubeAPIErrorBudgetBurn** メトリックでの誤検出が減少するようになりました。(BZ#1982704)

Kubernetes Scheduler

- OpenShift Container Platform 4.11 では、ホストされたコントロールプレーンが有効になっているクラスターに descheduler がインストールされている場合、ホストされたコントロールプレーンの namespace はエビクションから除外されます。その結果、descheduler がインストールされている場合、Pod はホストされたコントロールプレーンの namespace から削除されなくなりました。(BZ#2000653)

- 以前は、リソースは、**kubedescheduler** カスタム リソース (CR) の所有者参照で API バージョンを誤って指定していました。その結果、所有者参照が無効になり、**kubedescheduler** CR の実行時に影響を受けるリソースが削除されませんでした。この更新では、すべての所有者参照で正しい API バージョンが指定されます。その結果、**kubedescheduler** CR への所有者参照を持つすべてのリソースは、CR が削除された後に削除されます。(BZ#1957012)

Machine Config Operator

- **keyFile** は RHEL ノード上の NetworkManager のデフォルトプラグインとして設定されていないため、再起動後に RHEL ノードが準備完了状態にならない場合があります。今回の修正により、**keyFile** はすべてのクラスターノードでデフォルトの NetworkManager プラグインとして設定されます。その結果、ノードは再起動後に正常に **準備完了** 状態になります。(BZ#2060133)

- vSphere UPI クラスターはインストール時に **PlatformStatus.VSphere** パラメーターを設定しないため、パラメーターは **nil** に設定されていました。これにより、MCO のログには、このパラメーターは値を **nil** にすることはできませんという不要なメッセージが繰り返し出力されるようになりました。この修正により、警告が削除されます。この警告は、別の問題を解決するために追加されたものでした。その結果、ログには vSphere UPI インストールに関するこのメッセージが表示されなくなりました。(BZ#2080267)

- 以前は、FIPS と **realTimeKernel** の両方でクラスターを作成しようとすると、コード内のマージロジックの問題により、Machine Config Operator (MCO) が低下しました。今回の更新により、FIPS と **realTimeKernel** の両方でクラスターを作成するときに MCO が低下しなくなりました。(BZ#2096496)

Compliance Operator

- 以前は、Compliance Operator がマシン設定データへの参照を保持していたため、メモリー使用量が大幅に増加していました。その結果、Compliance Operator は、OOM (Out-of-Memory) 例外のために **CrashLoopBackoffs** で失敗していました。回避策として、Compliance Operator の更新バージョンを使用する必要があります。たとえば、0.1.53 では、メモリー内の大規模なマシン設定データセットの処理が改善されています。その結果、Compliance Operator は、大規模なマシン設定データセットを処理する際に引き続き実行されます。(BZ#2094854)

管理コンソール

- 以前は、**InstallPlans** を承認するときに、Web コンソールはパーミッションを適切に認証していませんでした。その結果、処理されないエラーが発生する可能性がありました。今回の更新により、一貫性を保つためにパーミッションが変更され、エラーメッセージが Web コンソールに正しく表示されるようになりました。(BZ#2006067)

モニタリング

- 今回の更新前は、コンテナーラベルが高いカーディナリティーのために削除されていたため、**container_fs*** メトリックのコンテナーラベルを使用するクエリーを含む OpenShift Container Platform Web コンソールのダッシュボードは、データポイントを返しませんでした。この更新により問題が解決され、これらのダッシュボードに期待どおりにデータが表示されるようになりました。(BZ#2037513)

- この更新の前は、**prometheus-operator** コンポーネントは config map で **ScrapeTimeout** の任意の時間値を許可していました。**ScrapeTimeout** を **ScrapeInterval** 値よりも大きい値に設定すると、Prometheus は config map 設定のロードを停止し、その後のすべての設定変更の適用に失敗します。今回の更新により、指定された **ScrapeTimeout** 値が **ScrapeInterval** 値より大きい場合、システムは設定を無効としてログに記録しますが、他の config map 設定のロードを続行します。(BZ#2037762)

- 今回の更新前は、OpenShift Container Platform Web コンソールの **Kubernetes / Compute Resources / Cluster** ダッシュボードの **CPU 使用率** パネルで、ノードの CPU 使用率を計算するために使用される式が、無効な負の値を誤って表示することがありました。今回の更新により、式が更新され、**CPU 使用率** パネルに正しい値が表示されるようになりました。(BZ#2040635)

- この更新の前は、新しい Pod が使用可能になる前に、更新プロセスによって古い Pod が削除されたため、15 日ごとに発生する自動更新中に、**prometheus-adapter** コンポーネントのデータにアクセスできませんでした。このリリースでは、更新プロセス中に古い Pod のデータを引き続き使用できるように、新しい Pod がリクエストを処理できるようになった後、自動更新プロセスで古い Pod のみが削除されるようになりました。(BZ#2048333)

- この更新の前は、**kube-state-metrics** から、**kube_pod_container_status_terminated_reason**、**kube_pod_init_container_status_terminated_reason**、および **kube_pod_status_scheduled_time** のメトリックが誤って欠落していました。今回のリリースでは、**kube-state-metrics** がこれらのメトリックを正しく表示して使用できるようになりました。(BZ#2050120)

- この更新の前は、**prometheus-operator** コンポーネントに無効な書き込み再ラベル config map 設定が存在した場合、この設定は引き続きすべての後続の設定を読み込んでいました。このリリースでは、設定を読み込むときに、コンポーネントが有効な書き込み再ラベル設定をチェックします。無効な設定が存在する場合、エラーがログに記録され、設定の読み込みプロセスが停止します。(BZ#2051470)

- この更新の前は、Prometheus Pod の **init-config-reloader** コンテナーは、コンテナーに実際に必要なリソースが少ない場合でも、**100m** の CPU と **50Mi** のメモリーを要求していました。今回の更新により、コンテナーは **1m** の CPU と **10Mi** のメモリーを要求します。これらの設定は、**config-reloader** コンテナーの設定と一致しています。(BZ#2057025)

- この更新の前は、管理者がユーザーワークロードモニタリングを有効にした場合、**user-workload-monitoring-config** config map は自動的に作成されませんでした。**user-workload-monitoring-config-edit** ロールを持つ管理者以外のユーザーには、config map を手動で作成するパーミッションがなかったため、管理者が config map を作成する必要がありました。今回の更新により、管理者がユーザーワークロードモニタリングを有効にすると、**user-workload-monitoring-config** config map が自動的に作成され、適切なロールを持つユーザーが編集できるようになりました。(BZ#2065577)

- この更新の前は、デプロイメントを削除した後、Cluster Monitoring Operator (CMO) は削除が完了することを待たなかったため、調整エラーが発生していました。今回の更新により、CMO はデプロイメントが削除されるまで待機してから、デプロイを再作成するようになり、この問題が解決されました。(BZ#2069068)

- この更新の前は、ユーザーワークロードモニタリングに関しては、Prometheus でメトリクスの外部ラベルを設定した場合、CMO はこれらのラベルを Thanos Ruler に正しく伝播しませんでした。Prometheus のユーザーワークロードモニタリングインスタンスで提供されていないユーザー定義プロジェクトの外部メトリクスをクエリーした場合、Prometheus で外部ラベルを追加するように設定されていても、これらのメトリクスに外部ラベルが表示されないことがありました。今回の更新により、CMO は、Prometheus で設定した外部ラベルを Thanos Ruler に適切に伝播するようになり、外部メトリックをクエリーするときにラベルを表示できるようになりました。したがって、ユーザー定義のプロジェクトの場合、Prometheus のユーザーワークロードモニタリングインスタンスによって提供されない外部メトリクスをクエリーすると、外部ラベルを追加するように Prometheus を設定していても、これらのメトリクスの外部ラベルが表示されないことがあります。今回の更新により、CMO は、Prometheus で設定した外部ラベルを Thanos Ruler に適切に伝播するようになり、外部メトリックをクエリーするときにラベルを表示できるようになりました。(BZ#2073112)

- この更新の前は、**tunbr** インターフェイスが **NodeNetworkInterfaceFlapping** アラートを誤ってトリガーしていました。今回の更新により、アラートが無視するインターフェイスのリストに **tunbr** インターフェイスが含まれるようになり、アラートが誤ってトリガーされることはなくなりました。(BZ#2090838)

- 以前は、Prometheus Operator は無効な再ラベル設定を許可していました。今回の更新により、Prometheus Operator は再ラベル付けされた設定を検証します。(BZ#2051407)

ネットワーク

- 以前は、追加のネットワークアタッチメントにボンディング CNI プラグインを使用する場合、Multus と互換性がありませんでした。ボンディング CNI プラグインを Whereabouts IPAM プラグインと組み合わせてネットワークアタッチメント定義に使用すると、割り当てられた IP アドレスが正しく調整されませんでした。ボンディング CNI プラグインを使用するネットワークアタッチメント定義が、IP アドレスの割り当てに Whereabouts IPAM プラグインで正しく機能するようになりました。(BZ#2082360)

- 以前は、OVN-Kubernetes クラスターネットワークプロバイダーを複数のデフォルトゲートウェイで使用すると、間違ったゲートウェイが選択され、OVN-Kubernetes Pod が予期せずに停止していました。これらの Pod が失敗しないように、正しいデフォルトゲートウェイが選択されるようになりました。(BZ#2040933)

- OVN-Kubernetes クラスターネットワークプロバイダーを使用するクラスターの場合、以前は NetworkManager サービスがノードで再起動すると、そのノードのネットワーク接続が失われました。現在は、ネットワーク接続は NetworkManager サービスの再起動後も維持されます。(BZ#2048352)

- 以前は、キャッシュの更新を処理する **goroutine** が、**mutex** を保持している間、バッファリングされていないチャネルへの書き込みを停止させる可能性がありました。今回の更新で、これらの競合状態が解決されました。(BZ#2052398)

- 以前は、ovn-kubernetes の場合、ボンディングまたは チームインターフェイスを使用して起動時に **br-ex** をセットアップすると、**br-ex** とボンディングインターフェイスの間でメディアアクセス制御 (MAC) アドレスの不一致が発生していました。その結果、ベアメタルまたは一部の仮想プラットフォームでは、予期しない **br-ex** MAC アドレスが原因で、ネットワークインターフェイスコントローラー (NIC) ドライバーがトラフィックをドロップしたため、すべてのトラフィックがドロップされました。今回の更新により、**br-ex** とボンディングインターフェイスは、同じ MAC アドレスを使用するため、トラフィックがドロップされなくなりました。(BZ#2103080)

- 以前は、**cluster-reader** ロールを持つユーザーは、**NodeNetworkConfigurationPolicy** などのカスタムリソースを kubernetes-nmstate から読み取ることができませんでした。今回の更新により、**cluster-reader** ロールを持つユーザーは、kubernetes-nmstate カスタム リソースを読み取ることができるようになります。(BZ#2022745)

- 以前は、サービスエンドポイントが削除されたときに **LoadBalancer** IP の contrack エントリーが削除されず、接続が失敗していました。今回の更新により、contrack エントリーによって接続が失敗することはなくなりました。(BZ#2061002)

- 以前は、**jq package** がないことが原因で、ノードのデプロイメント時に RHEL ノードを含むクラスターのスケールアップが失敗していました。今回の更新により、デプロイ時に ` jq package` がインストールされ、RHEL ノードを含むクラスターのスケールアップが成功するようになります。(BZ#2052393)

- 以前は、サービスの設定変更で、OVN-Kubernetes は必要以上の時間を費やしていました。これにより、サービスの設定変更で著しいレイテンシーが発生していました。今回の更新により、OVN-Kubernetes は、サービスの設定変更のレイテンシーを低減するように最適化されました。(BZ#2070674)

- 以前は、Whereabouts IPAM CNI の IP 調整 CronJob が API 接続の問題により失敗し、CronJob が断続的に失敗していました。今回の更新により、Whereabouts IPAM CNI で起動された CronJob は、api-internal サーバーアドレスと延長された api タイムアウトを使用して、これらの接続の問題を回避しています。(BZ#2048575)

- 今回の更新により、Kubernetes-NMstate がインストールされた OpenShift Container Platform

クラスターは、` must-gathers` Kubernetes-NMstate リソースに含まれるようになりました。これにより、**must-gathers** に Kubernetes-NMstate のリソースを含めることで、問題の処理が改善されています。(BZ#2062355)

- 現在、ロードバランサーサービスがクラスタートラフィックポリシーで設定されている場合、ホストルートが無視されるという既知の問題があります。その結果、ロードバランサーサービスの egress トラフィックは、ホストルーティングテーブルに存在する最適なルートではなく、デフォルトゲートウェイに誘導されます。回避策として、ロードバランサータイプ Service を **Local** トラフィックポリシーに設定します。(BZ#2060159)

- 以前は、**PodDisruptionBudget** の仕様は単一ノードの OpenShift クラスターには適合せず、これにより、すべての Pod をエビクトできるわけではないことから、アップグレード機能が制限されていました。今回の更新により、**PodDisruptionBudget** の仕様がクラストポロジーに基づいて調整され、Kubernetes-NMState Operator が単一ノードの OpenShift クラスターでアップグレードできるようになりました。(BZ#2075491)

- 以前は、起動時に **br-ex** ブリッジをセットアップするときに、DHCP クライアント ID と IPv6 アドレス生成モードの設定が正しく機能せず、**br-ex** で予期しない IP アドレスが発生していました。今回の更新により、DHCP クライアント ID と IPv6 生成モードの設定が **br-ex** で適切に設定されるようになりました。(BZ#2058030)

- 以前は、CNI 定義の **gateway** フィールドに依存してデフォルトルートを削除し、独自のルートを挿入していたため、**egress-router-cni** Pod に一部のクラスター内部ルートがありませんでした。今回の更新では、**egress-router-cni** Pod が正しいルーティング情報を注入することで、Pod が外部および内部クラスターの宛先に到達できるようにしています。(BZ#2075475)

- 以前は、単一ノードの OpenShift で OVN raft クォーラムを作成するために、Pod の Disruption Budget (PDB: 停止状態の予算) が使用されていました。これにより、単一ノードの OpenShift クラスターで役に立たない **PodDisruptionBudgetAtLimit** アラートが発生しました。今回の更新により、これらのクラスターで **PodDisruptionBudgetAtLimit** アラートが発生しなくなりました。(BZ#2037721)

- 以前は、OVN-Kubernetes を使用している場合、**NetworkManager** の再起動での競合状態により、DHCP 解決がノードの起動時に **br-ex** ブリッジの設定を正常に完了できないことがありました。今回の更新により、**br-ex** のセットアップ時に **NetworkManager** が再起動されなくなり、競合状態がなくなりました。(BZ#2055433)

- これまでは、**PtpConfigSlave** ソースカスタムリソース (CR) がサポート対象外のネットワークトランスポート UDPv4 に設定されていたため、分散ユニット (DU) ノードでエラーが発生していました。今回の修正では、**PtpConfigSlave** ソース CR が UDPv4 ではなくネットワークトランスポート L2 を使用するように更新されました。その結果、DU ノードでエラーは検出されなくなりました。(BZ#2060492)

- これまでは、ネットワークポリシーの更新時に、すべての OpenShift Container Platform ポリシーロギング設定が更新されていました。そのため、同時またはそれ以降のネットワークポリシーで顕著なレイテンシーが発生しました。今回の更新により、新しいポリシーの追加時にすべてのネットワークポリシーが更新されなくなり、レイテンシーが解消されました。(BZ#2089392)

ネットワークパフォーマンスの向上

- 以前は、**systemd** サービスは、仮想デバイスを除く udev から見えるすべてのネットワークデバイスに対して、パフォーマンスプロファイルの予約済み CPU リストに従って、デフォルトの Recieve Packet Steering (RPS) マスクを設定していました。**crio** フックスクリプトは、保証された Pod の **/sys/devices** から見えるすべてのネットワークデバイスの RPS マスクを設定します。これにより、ネットワーク パフォーマンスに複数の影響が生じました。今回の更新では、**systemd** サービスは、**/sys/devices/virtual** の下にある仮想インターフェイスのデフォル

トの RPS マスクのみを設定します。**crio** フックスクリプトは、物理デバイスも除外するようになりました。この設定により、プロセスの過負荷、長いポーリング間隔、レイテンシーの急増などの問題が軽減されます。(BZ#2081852)

ノード

- 以前は、Pod マネージャーが Pod シークレットと config map の登録と登録解除を処理していました。このため、Pod シークレットを Pod 内にマウントできない場合がありました。今回の修正により、Pod ID は、kubelet が登録済み Pod の管理に使用するキーに含まれるようになりました。その結果、シークレットは期待どおりに適切にマウントされるようになります。(BZ#1999325)

- ガベージコレクションプロセスでのメモリーリークが原因で、メモリー不足のために Pod がノードで起動できない場合があります。この修正により、ガベージコレクションプロセスでメモリーリークが発生しなくなり、ノードが期待どおりに起動するようになります。(BZ#2065749)

- アップストリーム Kubernetes の変更により、kubelet は終了した Pod で readiness プローブを実行していませんでした。その結果、ロードバランサーまたはコントローラーが Pod の終了に反応するのが遅くなり、エラーが発生する可能性がありました。今回の修正により、Pod の終了時に readiness プローブが再び実行されるようになりました。(BZ#2089933)

- バグが原因で、API で他の Pod が完了したと報告された後に Pod が急速にスケジュールされた場合、kubelet は **OutOfCpu** エラーが発生した Pod を誤って拒否する可能性がありました。この修正により、kubelet は、実行中のすべてのコンテナーが停止し、新しいコンテナーが開始されなくなるまで待機してから、API で Pod のフェーズをターミナルと報告するようになりました。この変更後、存続期間の短い Pod が、成功または失敗のいずれかを報告する際に、やや時間がかかる場合があります (約 1 秒)。(BZ#2022507)

- 最近のバージョンの **prometheus-adapter** は追加の Pod メトリックを送信しているため、Vertical Pod Autoscaler (VPA) レコメンダーは、不要かつ反復的なメッセージを大量に生成しています。この修正により、VPA は余分なメトリックを認識して無視します。その結果、これらのメッセージは生成されなくなりました。(BZ#2102947)

OpenShift CLI (oc)

- 以前は、非推奨の古いイメージバージョンがソースとして使用された場合、**oc** カタログのミラーリングが失敗していました。現在は、イメージマニフェストのバージョンが自動的に検出され、ミラーリングが正常に機能します。(BZ#2049133)

- 以前は、フォールバック検証がいつ発生したかをログから把握することは困難でした。これを明確にするために、ログが改善されました。その結果、**must-gather run** の出力が、より明確になっています。(BZ#2035717)

- 以前は、無効な引数を指定して **must-gather** を実行した場合、一貫してエラーが報告されず、代わりに不可能な場合でもデータを収集しようとすることがありました。現在は、**must-gather** が無効なオプションで呼び出された場合、有用なエラー出力が提供されるようになりました。(BZ#1999891)

- 以前は、**oc adm catalog mirror** コマンドでエラーが発生した場合、そのまま続行され、**0** 終了コードが返されていました。**--continue-on-error** フラグが利用可能になり、エラーが発生した場合にコマンドを続行するか、ゼロ以外の終了コードで終了するかをユーザーが決定できるようになりました。(BZ#2088483)

- 今回の更新で、**--subresource** フラグが **oc adm policy who-can** コマンドに追加され、サブリソースで指定されたアクションを誰が実行できるかを確認できるようになりました。(BZ#1905850)

- 以前は、ユーザーは **oc project** コマンドでタブ補完を使用できませんでした。現在は、**oc project** の後にタブを押すと、プロジェクトが適切にリスト表示されます。(BZ#2080416)

- 以前は、スタートアッププローブがデバッグ Pod から削除されなかったため、スタートアッププローブが失敗した場合にデバッグ Pod で問題が発生する可能性がありました。**--keep-startup** フラグが追加されました。これはデフォルトでは **false** で、スタートアッププローブがデバッグ Pod からデフォルトで削除されることを意味します。(BZ#2056122)

- 以前は、**oc debug node** の呼び出し後にタイムアウトが指定されていなかったため、ユーザーがクラスターからログアウトされることはありませんでした。**TMOUT** 環境変数が追加され、非アクティブ状態が指定された時間経過すると、セッションが自動的に終了するようになりました。(BZ#2043314)

- この更新により、ユーザーがログアウトしている場合でも、**oc login** は Web コンソールの URL を表示するようになりました。(BZ#1957668)

- 以前は、コンテナーが見つからない場合に **oc rsync** コマンドが間違ったエラー出力を表示していました。このリリースでは、特定のコンテナーが実行されていない場合に、**oc rsync** コマンドが正しいエラーメッセージを表示するようになりました。(BZ#2057633)

- 以前は、大きなイメージは、クラスターにとって新しい場合、プルーニングすることができませんでした。これにより、サイズが大きすぎるイメージをフィルタリングする際に、最近のイメージが省略されてしまうことがありました。このリリースでは、指定されたサイズを超えるイメージをプルーニングできるようになりました。(BZ#2083999)

- 以前は、**gather** スクリプトにタイプミスがありました。その結果、Insights データが適切に収集されませんでした。このリリースでは、タイプミスが修正され、Insights データが **must-gather** によって適切に収集されるようになりました。(BZ#2106543)

- 以前は、**oc** CLI を使用して **EgressNetworkPolicy** リソースタイプをクラスターに適用できませんでした。このリリースでは、**EgressNetworkPolicy** リソースを作成、更新、および削除できるようになりました。(BZ#2071614)

Kubernetes コントローラーマネージャー

- 以前は、Pod ファイナライザーを使用してジョブを追跡するためのベータ機能がデフォルトで有効になっていました。場合によっては、Pod のファイナライザーが削除されていないために、Pod が常に削除されるわけではありませんでした。今回の更新により、機能ゲート **JobTrackingWithFinalizers** がデフォルトで無効になりました。その結果、削除中に Pod が取り残されることがなくなりました。(BZ#2075621)

- 以前は、CR レプリカ数がゼロになるたびに **PodDisruptionBudgetAtLimit** アラートが発生していました。今回の更新により、中断するアプリケーションがない場合、またはレプリカ数がゼロの場合に、アラートは発生しなくなりました。(BZ#2053622)

Operator Lifecycle Manager (OLM)

- この更新の前は、リソース名が 63 文字を超えると、無効なサブスクリプションラベルが作成されていました。63 文字の制限を超えるラベルを切り捨てることで問題が解決し、サブスクリプションリソースが Kubernetes API を拒否しなくなりました。(BZ#2016425)

- この更新の前は、Marketplace Operator のカタログソース Pod がノードのドレインを妨げていました。その結果、Cluster Autoscaler は効果的にスケールダウンできませんでした。今回の更新では、**cluster-autoscaler.kubernetes.io/safe-to-evict** アノテーションをカタログソース Pod に追加すると問題が修正され、Cluster Autoscaler が効果的にスケールダウンできるようになりました。(BZ#2053343)

- この更新の前は、Pod をスケジュールできなかった場合など、特定の状況で **collect-profiles** ジョブが完了するまでに長い時間がかかることがありました。その結果、十分な数のジョブがスケジュールされていても実行できない場合、スケジュールされたジョブの数が Pod クォータ制限を超えていました。今回の更新により、一度に 1 つの **collect-profiles** Pod のみが存在するようになり、**collect-profiles** ジョブが Pod のクォータ制限を超えなくなりました。(BZ#2055861)

- この更新の前は、パッケージサーバーは、リーダーの選出期間、更新期限、および再試行期間を定義するときに Pod トポロジーを認識していませんでした。その結果、パッケージサーバーは、単一ノード環境など、リソースが限られているトポロジーに負担をかけていました。今回の更新では、妥当なリース期間、更新期限、再試行期間を設定する **LeaderElection** パッケージが導入されました。この修正により、リソースが限られているクラスターの負担が軽減されます。(BZ#2048563)

- 以前は、**openshift-marketplace** namespace に不適切なカタログソースがありました。このため、すべてのサブスクリプションがブロックされました。今回の更新により、**openshift-marketplace** namespace に不適切なカタログソースがある場合、ユーザーは、元のアノテーションを使用して独自の namespace の品質の高いカタログソースから Operator にサブスクライブできるようになります。その結果、ローカルの namespace に不適切なカタログソースがある場合、ユーザーは namespace のどの Operator にもサブスクライブすることはできません。(BZ#2076323)

- 以前は、**operator-marketplace** プロジェクトのポーリング中に情報レベルのログが生成され、これによりログスパムが発生していました。この更新では、コマンドラインフラグを使用してログラインをデバッグレベルに下げ、ユーザーがログレベルをより詳細に制御できるようにします。その結果、ログスパムが減少します。(BZ#2057558)

- 以前は、Cluster Version Operator (CVO) によって管理される各コンポーネントは、プロジェクトのリポジトリーの root にある **/manifest** ディレクトリーで定義された YAML ファイルで設定されていました。**/manifest** ディレクトリーから YAML ファイルを削除する場合、**release.openshift.io/delete: "true"** アノテーションを追加する必要がありました。そうしないと、CVO はクラスターからリソースを削除しませんでした。今回の更新では、**/manifest** ディレクトリーから削除されたすべてのリソースを再導入し、**release.openshift.io/delete: "true"** アノテーションを追加して、CVO がリソースをクリーンアップできるようにしています。その結果、OLM コンポーネントに不要になったリソースはクラスターから削除されます。(BZ#1975543)

- 以前は、gRPC カタログソースで使用される **CheckRegistryServer** 関数は、カタログソースに関連付けられたサービスアカウントの存在を確認しませんでした。これにより、サービス アカウントのない異常なカタログ ソースが存在していました。この更新により、gRPC **CheckRegistryServer** 関数は、サービスアカウントが存在するかどうかを確認し、見つからない場合はサービスを再作成します。その結果、OLM は gRPC カタログソースが所有するサービスアカウントを再作成します (存在しない場合)。(BZ#2074612)

- 以前は、ユーザーがファイルベースのカタログイメージに対して **opm index prune** を実行したときに発生したエラーメッセージで、不正確な表現により、このコマンドがそのカタログ形式をサポートしていないことが不明確となっていました。今回の更新により、エラーメッセージが明確になり、コマンド **opm index prune** は SQLite ベースのイメージのみをサポートすることをユーザーが理解できるようになりました。(BZ#2039135)

- 以前は、Operator API の周りに壊れたスレッドセーフがありました。そのため、Operator リソースが適切に削除されませんでした。今回の更新により、Operator リソースが適切に削除されるようになりました。(BZ#2015023)

- 以前は、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しく決定され、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)

- OpenShift Container Platform 4.11 では、デフォルトのクラスター全体の Pod セキュリティーアドミッションポリシーは、すべての namespace の **baseline** に設定され、デフォルトの警告レベルは **restricted** に設定されています。この更新の前は、Operator Lifecycle Manager は、**operator -marketplace** namespace に Pod セキュリティーアドミッション警告を表示していました。この修正では、警告レベルを **baseline** に下げることで問題を解決しています。(BZ#2088541)

Operator SDK

- この更新の前は、Operator SDK は、サポートされているダウンストリームイメージではなくアップストリームイメージを使用して、Hybrid Helm ベースの Operator をスキャフォールディングしていました。今回の更新により、Operator SDK は、サポートされているダウンストリームイメージを使用して、Hybrid Helm ベースの Operator をスキャフォールディングします。(BZ#2039135)

- OpenShift Container Platform 4.11 では、Operator SDK により **arm64** Operator イメージをビルドすることができます。その結果、Operator SDK は、**arm64** をターゲットとする Operator イメージのビルドをサポートするようになりました。(BZ#2035899)

- 以前は、Operator SDK でスキャフォールディングされた Hybrid Helm Operators を実行している {product-tile} は、サポート対象のダウンストリームイメージではなく、アップストリームイメージを使用していました。今回の更新により、Hybrid Helm Operator のスキャフォールディングはダウンストリームイメージを使用するようになりました。(BZ#2066615)

OpenShift API サーバー

- 複数の Authentication Operator コントローラーが同時に同期していたため、Authentication Operator は設定の変更に対応するのに時間がかかりすぎていました。この機能は、Authentication Operator コントローラーがリソースを競合しないように、通常の同期期間にジッターを追加します。その結果、Authentication Operator が設定の変更に対応するのにかかる時間が短縮されました。(BZ#1958198)

- OpenShift Container Platform 4.11 では、外部 ID プロバイダーからの認証試行が監査ログに記録されるようになりました。その結果、外部 ID プロバイダーからのログイン試行の成功、失敗、およびエラーを監査ログで確認することができます。(BZ#2086465)

Red Hat Enterprise Linux CoreOS (RHCOS)

- 今回の更新以前は、マシンが PXE 経由で起動し、**BOOTIF** 引数がカーネルコマンドラインで指定されている場合に、マシンは 1 つのインターフェイスだけで DHCP を有効にして起動します。今回の更新により、**BOOTIF** 引数が指定されていても、マシンはすべてのインターフェイスで DHCP を有効にして起動するようになりました。(BZ#2032717)

- 以前のバージョンでは、VMware OVA イメージからプロビジョニングされたノードは、初回のプロビジョニング後に Ignition config を削除しませんでした。そのため、シークレットが Ignition 設定に保存される際にセキュリティーの問題が作成されました。今回の更新により、新規ノードでの初回プロビジョニング後に、Ignition 設定が VMware ハイパーバイザーから削除され、また既存ノードで以前の OpenShift Container Platform リリースからアップグレードできるようになりました。(BZ#2082274)

- 以前は、**toolbox** コマンドに指定された引数は、コマンドが最初に呼び出されたときに無視されていました。この修正により、ツールボックススクリプトが更新され、**podman container create** コマンドの開始後に、**podman start** コマンドおよび **podman exec** コマンドが続くようになりました。また、複数の引数と空白を配列として処理するようにスクリプトを変更しています。その結果、**toolbox** コマンドに渡された引数は、期待どおりに毎回実行されます。(BZ#2039589)

Performance Addon Operator

- 以前は、CNF cyclictest ランナーは **--mainaffinity** 引数を提供している必要があり、実行するスレッドをバイナリーに指示していましたが、cyclictest ランナーには **--mainaffinity** 引数がありませんでした。今回の更新により、**--mainaffinity** 引数が cyclictest ランナーに追加され、**cyclitest** コマンドに適切に渡されるようになりました。(BZ#2051540)

- 以前は、**oslat** コンテナーの仕様に **cpu-quota.crio.io: "disable"** アノテーションがなかったため、レイテンシーが大きくなっていました。その結果、作成時に **cpu-quay.crio.io:"disable"** アノテーションが Pod 定義にありませんでした。今回の更新により、Pod の作成時に **cpu-quota.crio.io:"disable"** アノテーションが追加され、その結果、**oslat** Pod の **specification** フィールドに表示されるようになります。(BZ#2061676)

Routing

- 以前は、Ingress Operator 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 Controller によって作成または所有されているかどうかを検証しませんでした。したがって、Ingress Operator は、所有権に関係なく、名前も namespace も同じ Kubernetes サービスを変更または削除し、予期しない動作を引き起こしていました。今回の更新により、サービスの変更または削除を試みる前に、Ingress Operator が既存の Kubernetes サービスの所有権を確認できるようになりました。所有権が一致しない場合、Ingress Operator はエラーを表示し、アクションを起こしません。その結果、Ingress Operator は、変更または削除する OpenShift Ingress namespace と同じ名前のカスタム Kubernetes サービスを変更または削除することができません。(BZ#2054200)

- 以前、OpenShift Container Platform 4.8 は、プラットフォームルートをカスタマイズするための API を追加しました。この API には、カスタマイズ可能なルートの現在のホスト名と、これらのルートに対するユーザーの目的のホスト名をそれぞれ報告するために、クラスターの ingress 設定に status フィールドと spec フィールドが含まれています。API は、これらの値に対する制約も定義しました。これらの制約は限定的であり、いくつかの有効な潜在的なホスト名を除外していました。その結果、API の制限的な検証により、ユーザーは、許可されるべきカスタムホスト名を指定できなくなり、また、許可されるべきドメインでクラスターをインストールできなくなりました。今回の更新により、ホスト名の制約が緩和され、ルートに有効なすべてのホスト名が許可され、OpenShift Container Platform ではユーザーが 10 進数を含む TLD でクラスタードメインを使用できるようになりました。(BZ#2039256)

- 以前は、Ingress Operator はクラスターの **spec.domain** パラメーターで設定された Ingress Controller が **spec.baseDomain** パラメーターと一致するかどうかをチェックしませんでした。これにより、Operator は DNS レコードを作成し、**DNSManaged** 条件を **false** に設定していました。この修正により、Ingress Operator は **spec.domain** パラメーターがクラスターの **spec.baseDomain** と一致するかどうかをチェックするようになりました。その結果、カスタム Ingress Controller の場合、Ingress Operator は DNS レコードを作成せず、**DNSManaged** 条件を false に設定します。(BZ#2041616)

- OpenShift Container Platform 4.10 では以前、HAProxy の must-gather 関数の実行に最大 1 時間かかることがありました。これは、終了状態のルーターが **oc cp** コマンドを遅らせた場合に発生する可能性があります。遅延は、Pod が終了するまで続きます。新しいリリースでは、**oc op** コマンドに 10 分の制限を設けることで、長時間の遅延を防止しています。(BZ#2104701)

- 以前は、Ingress Controller が削除されたときに、Ingress Operator はルートステータスをクリアせず、削除後もルートが Operator に残っていることを示していました。この修正により、Ingress Controller を削除したときにルートのステータスがクリアされ、削除後に Operator でルートがクリアされるようになります。(BZ#1944851)

- 以前は、**oc explain router.status.ingress.conditions** コマンドの説明ルートステータスの出力では、アプリケーションプログラミングインターフェイス (API) の不適切な表現が原因で、**Admitted** ではなく、**Currently only Ready** が表示されていました。この修正により、API

の表現が修正されています。その結果、コマンド出力は正しくなります。(BZ#2041133)

- 以前は、Ingress Operator は、**LoadBalancer-type** のサービスで Operator が管理するアノテーションをユーザーが変更したことを検出していました。その結果、Operator は Ingress Cluster Operator の **Upgradeable** ステータス条件を **False** 設定してアップグレードをブロックし、IngressOperator はサービスにアノテーションがない場合、誤って **Upgradeable** ステータス条件を **False** に設定し、アップグレードをブロックしてしまいました。現在、サービスのアノテーションをチェックするロジックは空のアノテーションを正しく処理し、Ingress Operator はアップグレードを誤ってブロックしなくなりました。(BZ#2097555)

- 以前は、Ingress Operator は、Operator が以前のバージョンの OpenShift Container Platform から **LoadBalancer-type** サービスに追加したファイナライザーを削除していました。今回の更新により、Ingress Operator はファイナライザーを削除しなくなりました。(BZ#2069457)

- Ingress Operator は、ingress カナリアルートに対してヘルスチェックを実行します。この更新の前は、接続時に **keepalive** デーモンが有効になっているため、ヘルスチェックの完了後に Ingress Operator がロード バランサー (LB) への TCP 接続を閉じませんでした。既存の接続を使用する代わりに、次のヘルスチェック用に新しい接続が作成されました。その結果、ロードバランサー上に接続が構築され、ロードバランサー上に多数の接続が作成されました。この更新により、カナリアルートへの接続時に **keepalive** デーモンが無効になり、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、閉じられるようになりました。(BZ#2037447)

- 以前は、Ingress Controller がルーターのデプロイメントで **allowPrivilegeEscalation** 値を false に設定しなかったため、ルーター Pod が誤った Security Context Constraint (SCC) に選択され、カスタム SCC との競合が発生していました。この修正により、**allowPrivilegeEscalation** 値が **true** に設定され、ルーター Pod が正しい SCC に選択され、カスタム SCC との競合が回避されるようになります。(BZ#2007246)

- 以前は、カナリアルートが Ingress Controller に認められない場合、Ingress Operator のステータス状態が **degraded** と表示されませんでした。その結果、カナリアルートは、ステータス条件が **not admitted** と表示されるはずであっても、**valid** と表示される可能性がありました。今回の更新により、Ingress Operator のステータスは、カナリアコントローラーのステータスをより正確に反映するようになりました。(BZ#2021446)

- 以前は、**openshift-router** プロセスが一時的に **SIGTERM** シャットダウンシグナルを無視していました。これが原因で、コンテナーが Kubernetes のシャットダウンリクエストを無視し、シャットダウンに 1 時間かかっていました。この更新により、ルーターは **SIGTERM** シグナルに応答するようになりました。(BZ#2076297)

- 以前は、許可されたルートの Ingress Controller が削除されるか、シャーディング設定が追加されると、誤った **admitted** ステータスが与えられました。今回の更新により、Ingress Controller は、 **unadmitted** ルートのステータスをクリアし、誤ったステータスシナリオを回避できるようになりました。(BZ#1944851)

- 以前は、バージョン 4.7 以前を使用してインストールされた OpenShift Container Platform クラスターは、**0.0.0.0/0** の **service.beta.kubernetes.io/aws-load-balancer-internal** アノテーションの値を維持していました。4.8 以降を使用してインストールされたクラスターには、アノテーションの値が **true** になります。アノテーションの値 **true** を確認する AWS クラウドプロバイダー実装は、値が **0.0.0.0/0** の場合、誤った結果を返します。そのため、4.10 へのクラスターのアップグレードが完了しませんでした。今回の更新により、アノテーションの値が **true** に正規化され、クラスターのアップグレードが完了するようになりました。(BZ#2055470)

スケーラビリティーおよびパフォーマンス

- この更新の前は、Node Feature Discovery (NFD) がすでにインストールされていたかどうかに関係なく、SRO はデフォルトで NFD をインストールしていました。NFD がインストールされていた場合、これが原因で SRO のデプロイメントが失敗していました。SRO はデフォルトで

NFD をデプロイしなくなりました。

ストレージ

- 以前は、OpenShift Container Platform に同梱されている Alibaba Container Storage Interface (CS) ドライバーは、ユーザーが 20 GiB 未満の永続ボリューム要求 (PVC) を作成すると、エラーを返しました。これは、Alibaba Cloud が 20 GiB を超えるボリュームしかサポートしないことが原因でした。この更新により、Alibaba CSI ドライバーは、すべてのボリュームサイズを自動的に 20 GiB 以上に増加し、より小さな PVC が動的にプロビジョニングされるようになりました。これにより、コストが増加する可能性があります。管理者は、コストを制限するために、制限された環境で namespace ごとに PVC カウントのクォータを使用することができます。(BZ#2057495)

- 以前のバージョンでは、Local Storage Operator (LSO) は、ノードの削除が PV の削除要求も発行するように、作成した永続ボリューム (PV) に所有者参照を追加していました。これにより、PV が Pod にアタッチされたまま **Terminating** 状態となる可能性がありました。LSO はその OwnerReference を作成しなくなりました。つまり、クラスター管理者は、ノードをクラスターから削除した後、未使用の PV を削除する必要があります。(BZ#2061447) 詳細は、Persistent storage using local volumes を参照してください。

- この修正により、read-only-many ボリュームが、GCP CSI ドライバーによって read-only として適切にプロビジョニングされるようになります。(BZ#1968253)

- OpenShift Container Platform では、アップストリームコミュニティーまたは VMware によって出荷された vSphere CSI ドライバーをインストールできます。Red Hat はこのドライバーをサポートしていませんが、Red Hat が出荷する vSphere CSI ドライバーよりも多くの機能を備えているため、クラスター管理者はインストールして使用することができます。OpenShift Container Platform は、アップストリームおよび VMware vSphere CSI ドライバーを使用して 4.11 にアップグレードできますが、サードパーティーの CSI ドライバーが存在するという警告が表示されます。詳細については、(BZ#2089419) および (BZ#2052071) を参照してください。

- 今回の更新により、Amazon Web Services (AWS) のデフォルトの認証情報要求が変更され、Key Managment Service (KMS) からの顧客管理キーを使用する暗号化されたボリュームのマウントが可能になりました。Cloud Creditial Operator (CCO) を使用して手動モードで認証情報要求を作成した管理者は、AWS でお客様が管理する鍵を使用して暗号化されたボリュームをマウントする場合、こ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#2049872)

- 以前は、IBM Cloud にデプロイされた OpenShift Container Platform クラスターを削除した後に、バックエンドのストレージボリュームが削除されませんでした。そのため、クラスターリソースを完全に削除できませんでした。今回の修正により、インストールプログラムおよび Container Storage Interface (CSI) ドライバーのサポートが追加され、クラスターの削除後にバックエンドボリュームが削除されるようになりました。(BZ#2047732)

Web コンソール (開発者パースペクティブ)

- この更新の前は、無効な devfile リポジトリー (devfile v2.2 より古い) が入力されると、**Git Import** フォームにエラーメッセージが表示されていました。この更新により、v2.2 より古い devfile はサポートされないというエラーメッセージが表示されるようになりました。(BZ#2046435)

- この更新の前は、**ConsoleLink CR** (openshift-blog) がクラスターで利用できない場合、ブログリンクは定義されていませんでした。ブログへのリンクをクリックしても、OpenShift ブログにリダイレクトされませんでした。今回の更新により、**ConsoleLink CR** (openshift-blog) がクラスターに存在しない場合でも、https://developers.redhat.com/products/openshift/whats-new へのフォールバックリンクが追加されます。(BZ#2050637)

- この更新の前に、kafka CR の API バージョンが更新されました。このバージョンは旧バージョンをサポートしていなかったため、**ブートストラップサーバー** を作成していても、空のブートストラップサーバーが **Create Event Source - KafkaSource**に表示されていました。今回の更新により、Kafka CR の更新された API は古いバージョンをサポートし、**Create Event Source - KafkaSource** フォームで **ブートストラップサーバー** リストをレンダリングします。(BZ#2058623)

- この更新の前に、**Import from Git** 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、プライベートリポジトリーの詳細を取得するためのシークレットがデコードされなかったため、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でした。今回の更新により、**Import from Git** フォームはシークレットをデコードして、プライベートリポジトリーの詳細をフェッチします。(BZ#2053501)

- この更新の前は、開発者の観点から、**Observe** ダッシュボードは、**Topology** ビューで選択したワークロードではなく、直近に表示したワークロードに対して開いていました。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 ストアを優先するために発生します。この更新により、**Observe** ダッシュボードは、URL のクエリーパラメーターに基づいてコンポーネントをレンダリングします。(BZ#2052953)

- この更新の前は、**パイプライン** は、クラスターに存在しない場合でも、デフォルトのストレージクラスとしてハードコードされた値 **gp2** で開始していました。今回の更新により、ハードコードされた値の代わりに、デフォルトで指定されたストレージクラス名を使用できるようになりました。(BZ#2084635)

- この更新の前は、大量のパイプラインログを実行しているときに、自動スクロール機能が動作せず、ログに古いメッセージが表示されていました。大量のパイプライン ログを実行すると、**scrollIntoView** メソッドへの呼び出しが大量に生成されました。この更新により、大量のパイプラインログで **scrollIntoView** メソッドへの呼び出しが生成されなくなり、スムーズな自動スクロール機能が提供されるようになりました。(BZ#2014161)

- この更新の前は、**Create RoleBinding** フォームを使用して **RoleBinding** を作成する場合、サブジェクト名は必須でした。サブジェクト名がない場合は、**Project Access** タブの読み込みに失敗していました。この更新により、**Subject Name** プロパティーのない **RoleBinding** は、**Project Access** タブに記載されなくなりました。(BZ#2051558)

- この更新の前は、イベントソースのシンクとトリガーは、それらがスタンドアロンであっても、**k-native service**、**Broker**、または **KameletBinding** をバックアップする一部であっても、すべてのリソースを表示していました。アドレス指定されたリソースが、シンクドロップダウンリストに表示するために使用されました。今回の更新で、スタンドアロンリソースのみをシンクとして表示するフィルターが追加されました。(BZ#2054285)

- この更新の前は、トポロジービューのサイドバーにある空のタブは、レンダリング前にフィルタリングされていませんでした。これにより、トポロジービューに **ワークロード** の無効なタブが表示されていました。この更新により、レンダリング前に空のタブが適切にフィルタリングされるようになりました。(BZ#2049483)

- この更新の前に、**Start Last Run** ボタンを使用してパイプラインを開始すると、作成された **PipelineRun** の **started-by** アノテーションが正しいユーザー名に更新されなかったため、triggered by のセクションに正しいユーザー名が表示されませんでした。この更新により、**started-by** アノテーションの値が正しいユーザー名に更新され、triggered by セクションに、パイプラインを開始した正しいユーザーのユーザー名が表示されるようになりました。(BZ#2046618)

- この更新の前は、**ProjectHelmChartRepository** CR がクラスターに表示されませんでした。そのため、この CR の API スキーマは、クラスター内でまだ初期化されませんでした。この更新により、**ProjectHelmChartRepository** がクラスターに表示されるようになりました。(BZ#2054197)

- この更新の前は、トポロジーでキーボードを使用してナビゲートすると、選択した項目が強調表示されませんでした。この更新により、キーボードを使用したナビゲーションで、選択されたアイテムがハイライトされ、スタイルが更新されるようになりました。(BZ#2039277)

- この更新の前は、Web ターミナルのレイアウトがデフォルトビューの外で開き、サイズを変更できませんでした。この更新により、Web ターミナルはデフォルトビュー内で開き、適切にサイズ変更されるようになりました。(BZ#2022253)

- この更新の前は、サイドバー項目の一部に namespace コンテキストが含まれていませんでした。その結果、別のブラウザーからリンクを開いた場合、または別のアクティブな namespace からリンクを開いた場合、Web コンソールは正しい namespace に切り替わりませんでした。この更新により、URL を開くときに正しい namespace が選択されるようになりました。(BZ#2039647)

- 以前は、コンソールを使用してテンプレートをインスタンス化する際に、そのパラメーターはシークレットリソースとして保存されていました。テンプレートが削除されてもシークレットは残りました。そのため、クラスター内に不要なシークレットがビルドされました。今回の更新により、テンプレートインスタンスにマップするシークレットに所有者の参照が追加されました。テンプレートインスタンスが削除されると、シークレットも削除されるようになりました。(BZ#2015042)

- 今回の更新により、**jsonData** プロパティーは非推奨となり、**ping** ソースの **data** に置き換えられました。(BZ#2084438)

- 以前は、OpenShift Container Platform Web コンソールのトポロジービューは 100 を超えるノードを持つクラスターで失敗または遅延していました。今回の更新により、トポロジービューで、100 を超えるノードを持つクラスターの **LimitExceeded** 状態が表示されるようになりました。代わりに **Search** ページを使用してリソースを表示するオプションが提供されます。または、**Show topology anyway** をクリックして、トポロジービューのロードを継続できます。(BZ#2060329)

- 以前は、サービスが複数のサービスポートを公開し、ルートのターゲットポートが **8080** の場合、ターゲットポートの変更を試みると、ポート **8080** サービスポートの代わりに別のサービスポートが更新されていました。今回の更新により、新しいターゲットポートが設定されている場合に、アクティブなターゲットポートに対応するサービスポートが置き換えられるようになりました。(BZ#2077943)

- 以前は、セルフホスト GitHub および Bitbucket からリポジトリー情報を取得するためにインスタンス API の管理に使用される **git** 検出は機能しませんでした。今回の更新により、セルフホスト GitHub および Bitbucket インスタンスリポジトリーの検出が機能するようになりました。(BZ#2038244)

- 以前は、**apiVersion** は **EventSource** 作成フォームの **Resource** ドロップダウンメニューに正しい形式で渡されませんでした。そのため、**EventSource** の作成で **InContext** が選択されず、**Resource** ドロップダウンメニューから除外されていました。今回の更新により、**Resource** ドロップダウンメニューに **InContext** からの **Resource** が含まれるようになりました。(BZ#2070020)

- 以前は、**Pipeline metrics** ページにはメトリッククエリーのすべての API 呼び出しが表示され、**404** エラーで失敗していました。今回の更新により、**prometheus-tenancy** API を使用してパイプラインのメトリックデータが取得されます。パイプラインメトリックページには、namespace への少なくとも閲覧権限を持つ非管理者ユーザーに、すべてのデータおよびグラフが表示されるようになりました。(BZ#2041769)

- 以前は、Crtl+space キーボードショートカットを使用して、クイック検索にアクセスしてモーダルを追加できましたが、同じキーボードショートカットを使用して閉じることができませんでした。今回の更新で、Ctrl+space キーボードショートカットを使用して、クイック検索を閉

じ、モーダルを追加できるようになりました。(BZ#2093586)

- 以前は、ユーザーが削除されても、ユーザー設定用に作成されたリソースは削除されませんでした。そのため、**openshift-console-user-settings** namespace に作成されたリソースは削除されませんでした。今回の更新により、作成時に **ownerReference** がメタデータに追加されるようになりました。これにより、ユーザーが存在しなくなったときにリソースが自動的に削除されます。(BZ#2019564)

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 4.9	OCP 4.10	OCP 4.11
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	GA
境界クロックとして設定される PTP デュアル NIC ハードウェア	-	-	TP
通常のクロックでの PTP イベント	TP	GA	GA
境界クロックのある PTP イベント	-	TP	GA
OpenShift ビルドでの共有リソース CSI ドライバーおよびビルド CSI ボリューム	-	TP	TP
サービスバインディング	TP	GA	GA
CSI ボリューム拡張	TP	TP	GA
CSI AliCloud Disk Driver Operator	-	GA	GA
CSI Azure Disk Driver Operator	TP	GA	GA
CSI Azure File Driver Operator	-	TP	GA

機能	OCP 4.9	OCP 4.10	OCP 4.11
CSI Azure Stack Hub Driver Operator	GA	GA	GA
CSI GCP PD Driver Operator	GA	GA	GA
CSI IBM VPC Block Driver Operator	-	GA	GA
CSI AWS EFS Driver Operator	TP	GA	GA
CSI vSphere Driver Operator	TP	GA	GA
CSI の自動移行 (AWS EBS、Azure ファイル、GCP ディスク、VMware vSphere)	TP	TP	TP
CSI 自動移行 (Azure Disk、OpenStack Cinder)	TP	TP	GA
CSI インラインの一時ボリューム	TP	TP	TP
CSI 汎用一時ボリューム	-	-	GA
Shared Resource CSI Driver	-	TP	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	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
プリエンプションを実行しない優先順位クラス	TP	TP	GA
Kubernetes NMState Operator	TP	GA	GA
Assisted Installer	TP	GA	GA
x86_64 アーキテクチャーでの **kdump**	TP	TP	GA
arm64 アーキテクチャーでの **kdump**	-	-	TP
s390x アーキテクチャーでの **kdump**	TP	TP	TP
ppc64le アーキテクチャーでの **kdump**	TP	TP	TP

機能	OCP 4.9	OCP 4.10	OCP 4.11
ARM プラットフォームでの Open Shift	-	GA	GA
Serverless functions	TP	TP	TP
Memory Manager	GA	GA	GA
Alibaba Cloud のクラウドコントローラーマネージャー	-	TP	TP
Amazon Web Services のクラウドコントローラーマネージャー	TP	TP	TP
Google Cloud Platform のクラウドコントローラーマネージャー	-	TP	TP
IBM Cloud 向けクラウドコントローラーマネージャー	-	TP	TP
Microsoft Azure のクラウドコントローラーマネージャー	TP	TP	TP
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	TP
VMware vSphere のクラウドコントローラーマネージャー	-	TP	TP
ドライバーツールキット	TP	TP	TP
Special Resource Operator(SRO)	TP	TP	TP
Simple Content Access	TP	GA	GA
Node Health Check Operator	TP	TP	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	GA
IPv6 デュアルスタック	GA	GA	GA
選択可能なクラスターインベントリー	-	TP	TP
異種クラスター	-	-	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	
異種クラスター	-	-	TP
動的プラグイン	-	TP	TP

機能	OCP 4.9	OCP 4.10	OCP 4.11
ハイブリッド Helm Operator	-	TP	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	GA
oc-mirror CLI プラグインを使用した非接続ミラーリング	-	TP	GA
RHEL の BuildConfigs で共有資格をマウントする	-	TP	TP
RHEL で共有シークレットをマウントする	-	GA	GA
RHOSP DCN のサポート	-	TP	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	TP
RHOSP 上のクラスターの OVS ハードウェアオフロード	-	TP	GA
外部 DNS Operator	-	GA	GA
Web Terminal Operator	TP	GA	GA
プラットフォームモニタリングメトリクスに基づいたアラートルール	-	-	TP
AWS Load Balancer Operator	-	-	TP
Node Observability Operator	-	-	TP
Java ベースの Operator	-	-	TP
OpenShift Container Platform のホスト型コントロールプレーン	-	-	TP
Cluster API によるマシンの管理	-	-	TP
Topology Aware Lifecycle Manager	-	TP	TP
installer-provisioned infrastructure を使用した Alibaba Cloud へのクラスターのインストール	-	TP	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 4.11 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。認証なしのアクセスが必要な理由が特に無い限り、無効にしてください。認証されていないアクセスを引き続き許可する場合は、それに伴ってリスクが増大することに注意してください。

警告

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

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

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

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

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

(BZ#1821771)

- **oc annotate** コマンドは、等号 (**=**) が含まれる LDAP グループ名では機能しません。これは、コマンドがアノテーション名と値の間に等号を区切り文字として使用するためです。回避策として、**oc patch** または **oc edit** を使用してアノテーションを追加します。(BZ#1917280)
- モニタリングスタックで、ユーザー定義アラート専用の Alertmanager インスタンスを有効にしてデプロイした場合、OpenShift Container Platform Web コンソールの **Developer** パースペクティブでアラートを消音することはできません。この問題は、4.11.8 で修正されました。

(BZ#2100860)

- 新しくインストールされた OpenShift Container Platform 4.11 クラスターでは、プラットフォームモニタリングアラートに **openshift_io_alert_source="platform"** ラベルがありません。この問題は、以前のマイナーバージョンからアップグレードされたクラスターには影響しません。現在、この問題に対する回避策はありません。(BZ#2103127)

- Red Hat OpenStack Platform (RHOSP) では、ポートプールが同時に実行されるさまざまな一括ポート作成要求で設定されると、潜在的な問題が発生する場合があります。これらの一括要求時に、いずれかの IP アドレスの IP の割り当てに失敗すると、Neutron は全ポートの操作を再試行します。この問題は以前のエラータで解決されました。ただし、ポートプールバッチに小さい値を設定して、大量のポート作成要求を回避することができます。(BZ#2024690)

- oc-mirror CLI プラグインは、バージョン 4.9 よりも前の OpenShift Container Platform カタログをミラーリングできません。(BZ#2097210)

- イメージセット設定の **archiveSize** 値がコンテナーイメージサイズよりも小さい場合に、oc-mirror CLI プラグインはターゲットミラーレジストリーに設定されたイメージをアップロードできず、カタログディレクトリーが複数のアーカイブにまたがる可能性があります。(BZ#2106461)

- OpenShift Container Platform 4.11 では、MetalLB Operator スコープが namespace からクラスターに変更され、これにより、以前のバージョンからアップグレードに失敗します。
回避策として、以前のバージョンの MetalLB Operator を削除します。MetalLB カスタムリソースの namespace またはインスタンスを削除し、新規 Operator バージョンをデプロイしないでください。これにより、MetalLB が動作して設定されます。

  詳細は、Upgrading the MetalLB Operator を参照してください。(BZ#2100180)

- 双方向転送検出 (BFD) プロファイルを削除し、ボーダーゲートウェイプロトコル (BGP) ピアリソースに追加された **bfdProfile** 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)

- Go 1.18 ライブラリーで信頼できない証明書を処理するための変更により、OpenShift Container Platform 4.11 の OpenShift CLI (**oc**) は macOS で適切に機能しません。この変更により、**oc login** およびその他の **oc** コマンドは、MacOS で実行しても、 **certificate is not trusted** エラーで失敗することがあります。Go 1.18 でエラー処理が適切に修正されるまで (Go の問題 #52010 で追跡)、回避策は代わりに OpenShift Container Platform 4.10 **oc** CLI を使用することです。OpenShift Container Platform 4.10 **oc** CLI を OpenShift Container Platform 4.11 クラスターで使用する場合、**oc serviceaccounts get-token <service_account>** コマンドを使用してトークンを取得することはできなくなりました。(BZ#2097830) (BZ#2109799)

- プロジェクトの開発者カタログを拡張する **Add Helm Chart Repositories** フォームには、現在既知の問題があります。**クイックスタート** ガイドでは、目的の namespace に **ProjectHelmChartRepository** CR を追加できると説明されていますが、これを実行するには kubeadmin からのパーミッションが必要である点については言及されていません。(BZ#2054197)

- 現在、既知の問題があります。TLS 検証を使用する **ProjectHelmChartRepository** カスタムリソース (CR) のインスタンスを作成する場合、リポジトリーをリスト表示して Helm 関連の操作を実行することはできません。現在、この問題に対する回避策はありません。(HELM-343)

- ベアメタル IBM Power で OpenShift Container Platform を実行している場合、Petitboot ブートローダーが、一部の RHCOS ライブイメージのブート設定を入力できないという既知の問題があります。このような場合、RHCOS をインストールするために PXE でノードを起動した

後、想定されたライブイメージディスクの設定が表示されないことがあります。
回避策として、Petitboot シェルから **kexec** を使用して手動で起動できます。

ライブイメージを保存しているディスク (この例では **nvme0n1p3**) を特定し、以下のコマンドを実行します。

```
# cd /var/petitboot/mnt/dev/nvme0n1p3/ostree/rhcos-*/
# kexec -l vmlinuz-*.ppc64le -i initramfs-*.img -c "ignition.firstboot rd.neednet=1 ip=dhcp
$(grep options /var/petitboot/mnt/dev/nvme0n1p3/loader/entries/ostree-1-rhcos.conf | sed
's,^options ,,')" && kexec -e
```

(BZ#2107674)

- 切断された環境では、SRO はメインレジストリーから DTK を取得しようとしません。代わりにミラーレジストリーから取得します。(BZ#2102724)

- プロセスカウンターは、**phc2sys** が実行されていないインターフェイス上の **phc2sys** プロセスに関する誤った情報を表示します。現在、この問題に対する回避策はありません。(OCPBUGSM-46005)

- デュアル NIC PTP 設定を持つノードのネットワークインターフェイスコントローラー (NIC) がシャットダウンされると、両方の PTP インターフェイスに対して障害イベントが生成されます。現在、この問題に対する回避策はありません。(OCPBUGSM-46004)

- ローバンドシステムでは、グランドマスタークロックが数時間切断されてから復旧した後、システムクロックは PTP の通常クロックと同期しません。現在、この問題に対する回避策はありません。(OCPBUGSM-45173)

- 以前は、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て、**type=LoadBalancer** のサービスが **internalTrafficPolicy=cluster** セットで設定されている場合、ホストルーティングテーブルに使用に適したルートが含まれていても、すべてのトラフィックがデフォルトのゲートウェイにルーティングされていました。現在は、常にデフォルトのゲートウェイを使用するのではなく、最適なルートが使用されるようになりました。(BZ#2060159)

- OVN クラスターに 75 を超えるワーカーノードがある場合、2000 以上のサービスとルートオブジェクトを同時に作成すると、同時に作成された Pod が **ContainerCreating** ステータスでハングする可能性があります。この問題が発生した場合、oc describe pod <podname> コマンドを入力すると、`FailedCreatePodSandBox...failed to configure pod interface: timed out waiting for OVS port binding (ovn-installed)' の警告とともにイベントが表示されます。現在、この問題に対する回避策はありません。(BZ#2084062)

- 現在、OVN-Kubernetes には、**NetworkManager** サービスが再起動するたびに、ノードがネットワーク接続を失い、回復する必要があるという既知の問題があります。(BZ#2074009)

- デフォルトの SCC (Security Context Constraints) により、汎用一時ボリュームを使用する Pod が **Pending** 状態のままになる可能性があります。カスタム SCC を作成して、この問題を回避することができます。詳細は、Pods with Generic Ephemeral Volumes fail with SCC errors を参照してください。回避策については、Allowing the use of generic ephemeral volumes を参照してください。(BZ#2100429)

- OpenShift サンドボックスコンテナーがある場合、クラスターのアップグレード時に Machine Config Operator (MCO) Pod が **CrashLoopBackOff** 状態に遷移し、Pod の **openshift.io/scc** アノテーションにデフォルト値の **hostmount-anyuid** ではなく **sandboxed-containers-operator-scc** が表示される問題が発生する可能性があります。

この場合は、**sandboxed-containers-operator-scc** SCC の **seLinuxOptions** ストラテジーを一時的に制限の少ない **RunAsAny** に変更し、承認プロセスが **hostmount-anyuid** SCC よりも優先しないようにします。

1. 以下のコマンドを実行して **seLinuxOptions** ストラテジーを変更します。

```
$ oc patch scc sandboxed-containers-operator-scc --type=merge --patch
'{"seLinuxContext":{"type": "RunAsAny"}}'
```

2. 以下のコマンドを実行して MCO Pod を再起動します。

```
$ oc scale deployments/machine-config-operator -n openshift-machine-config-operator --
replicas=0
```

```
$ oc scale deployments/machine-config-operator -n openshift-machine-config-operator --
replicas=1
```

3. 以下のコマンドを実行して、**sandboxed-containers-operator-scc** の **seLinuxOptions** ストラテジーを **MustRunAs** の元の値に戻します。

```
$ oc patch scc sandboxed-containers-operator-scc --type=merge --patch
'{"seLinuxContext":{"type": "MustRunAs"}}'
```

4. 以下のコマンドを実行して、**hostmount-anyuid** SCC が MCO Pod に適用されていることを確認します。

```
$ oc get pods -n openshift-machine-config-operator -l k8s-app=machine-config-operator -
o yaml | grep scc
openshift.io/scc: hostmount-anyuid
```

(KATA-1373)

- パイプラインメトリック API は、RHOSP 1.6 以降の必要な **pipelinerun/taskrun** ヒストグラムの値をサポートしません。その結果、**Pipeline → Details** ページの **Metrics** タブは、誤った値を表示する代わりに削除されます。現在、この問題に対する回避策はありません (リンク: BZ#2074767)。

- 一部の Alibabacloud サービスは、クラスターのすべてのリソースを指定されたリソースグループに配置していません。したがって、OpenShift Container Platform インストールプログラムによって作成された一部のリソースは、デフォルトのリソースグループに配置されます。現在、この問題に対する回避策はありません。(BZ#2096692)

- 各クラスターノードを再起動した後、クラスター Operators **network** と **kube-apiserver** は、クラスターの各ノードを再起動した後に **degraded** 状態になり、クラスターが異常になります。現在、この問題に対する回避策はありません。(BZ#2102011)

- **install-config.yaml** に **resourceGroupID** が指定されている場合、ブートストラップリソースの削除時にエラーが表示され、OpenShift Container Platform のインストールが失敗します。この問題を回避するには、**install-config.yaml** で **resourceGroupID** を指定しないでください。(BZ#2100746)

- RHEL コンピュートノードでのスケールアップには、既知の問題があります。新しいノードは **Ready** になる可能性がありますが、Ingress Pod はこれらのノードで **Running** に変わることができず、スケールアップは成功しません。回避策として、RHCOS ノードでのスケールアップは機能します。(BZ#2056387)

- Google Cloud Platform (GCP) で **machine** セットを作成した後、**capg-controller-manager** マシンが **Provisioning** で停止します。現在、この問題に対する回避策はありません。(BZ#2107999)

- Nutanix には、クラスターによって作成された永続ボリューム (PV) が **destroy cluster** コマンドによってクリーンアップされないという既知の問題があります。この問題の回避策として、PV を手動でクリーンアップする必要があります。(BZ#2108700)

- Prism Central 2022.x で 4096 ビットの証明書を使用すると、Nutanix のインストールに失敗するという既知の問題があります。代わりに、2048 ビットの証明書を使用します。(KCS)

- 現在、不正な構文または値を使用して **egressqos** を作成および編集すると、成功するという既知の問題があります。**egressqos** の誤った値は正常に作成されません。現在、この問題に対する回避策はありません。(BZ#2097579)

- 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、VMware vSphere に OpenShift Container Platform クラスターをインストールする目的でインストールプログラムを macOS で実行する場合、**x509: certificate is not standards compliant** として出力される証明書コンプライアンスの問題が存在します。この問題は、コンパイラーが新しくサポートされた macOS 証明書規格を認識しないという **golang** コンパイラーの既知の問題に関連しています。この問題に対する回避策はありません。(OSDOCS-5694)

- 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. 非同期エラータの更新

OpenShift Container Platform 4.11 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 4.11 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 4.11 バージョンの非同期リリースで発表されるエラータの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 4.11.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-2022:5069 - OpenShift Container Platform 4.11.0 イメージリリース、バグ修正およびセキュリティー更新アドバイザリー

発行日: 2022-08-10

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.0 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHSA-2022:5069 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-2022:5068 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 4.11.0 --pullspecs
```

1.9.2. RHSA-2022:6103 - OpenShift Container Platform 4.11.1 のバグ修正と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 4.11.1 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2022:6103 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2022:6102 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 4.11.1 --pullspecs
```

1.9.2.1. 機能

1.9.2.1.1. 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。

1.9.2.2. 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)

1.9.2.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.3. RHBA-2022:6143 - OpenShift Container Platform 4.11.2 バグ修正の更新

発行日: 2022-08-29

OpenShift Container Platform リリース 4.11.2 が公開されました。この更新に含まれるバグ修正のリストは、RHBA-2022:6143 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-2022:6142 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 4.11.2 --pullspecs
```

1.9.3.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.4. RHSA-2022:6287 - OpenShift Container Platform 4.11.3 のバグ修正とセキュリティー更新

発行日: 2022-09-06

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.3 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2022:6287 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-2022:6286 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 4.11.3 --pullspecs
```

1.9.4.1. 機能

1.9.5. スケーラビリティーおよびパフォーマンス

OpenShift Container Platform 4.11.3 以降、ユーザーは Root FS イメージ URL (**rootFSUrl**) を **agent_service_config.yaml** ファイルに設定する必要がなくなりました。**rootFSUrl** が自動的に処理されるようになりました。

1.9.5.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.6. RHBA-2022:6376 - OpenShift Container Platform 4.11.4 バグ修正の更新

発行日: 2022-09-12

OpenShift Container Platform リリース 4.11.4 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-2022:6376 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-2022:6375 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 4.11.4 --pullspecs
```

1.9.6.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.7. RHSA-2022:6536 - OpenShift Container Platform 4.11.5 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 4.11.5 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2022:6536 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-2022:6535 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 4.11.5 --pullspecs
```

1.9.7.1. 既知の問題

- デフォルトの Ingress コントローラーをシャーディングすると、**canary**、**oauth**、**console** などの OpenShift Container Platform ファクトリールートが壊れます。回避策として、一致するラベルおよび式をルートに手動で追加できます。(**BZ#2024946**)

1.9.7.2. バグ修正

- 以前は、**routeSelector** の更新により、ルーターのデプロイ前に Ingress コントローラーのルートステータスがクリアされていました。その結果、ルートステータスが正しく再入力されませんでした。今回の更新により、ルートステータスは **routeSelector** 更新でクリアされます。(**BZ#2110528**)

1.9.7.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.8. RHBA-2022:6659 - OpenShift Container Platform 4.11.6 バグ修正の更新

発行日: 2022-09-28

OpenShift Container Platform release 4.11.6 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-2022:6659 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-2022:6658 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 4.11.6 --pullspecs
```

1.9.8.1. OpenShift Container Platform 4.11 RAN の新機能

1.9.8.1.1. 更新に失敗した後のクラスターの回復

単一ノードの OpenShift の場合は、Topology Aware Lifecycle Manager (TALM) Operator を使用して、OpenShift Container Platform バージョンの更新前に現在のデプロイメントのバックアップを作成できます。更新が失敗した場合は、バックアップを使用してクラスターを更新前の状態に戻します。詳細は、アップグレード前のクラスターリソースのバックアップの作成 を参照してください。

1.9.8.1.2. PolicyGenTemplate カスタムリソース (CR) で chronyd を無効にする

以前のバージョンから OpenShift Container Platform 4.11 に更新する場合は、**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、Recommended cluster kernel configuration を参照してください。

1.9.8.2. OpenShift Container Platform 4.11 RAN の既知の問題

- RAN DU プロファイルを使用して単一ノードの OpenShift クラスターをデプロイした後、エラー **openvswitch: cpu_id mismatch with handler threads** が Open vSwitch カーネルログに継続的に生成されます。(OCPBUGSM-46165)

- セキュアブートが現在無効になっていて、ZTP を使用して有効にしようとすると、クラスターのインストールが開始しません。ZTP を使用してセキュアブートを有効にすると、仮想 CD が接続される前にブートオプションが設定されます。したがって、既存のハードディスクからの最初の起動では、セキュアブートが有効になります。システムが CD から起動しないため、クラスターのインストールが停止します。(OCPBUGSM-45085)

- クラスターのアップグレードを実行するために使用されるサブスクリプションポリシーで無効なサブスクリプションチャネルが指定されている場合、Topology Aware Lifecycle Manager は、ポリシーが適用された直後にアップグレードの成功を示します。これは、**Subscription** の状態が **AtLatestKnown** のままであるためです。(OCPBUGSM-43618)

- SRIOV-FEC Operator が個別のポリシーを介してインストールされ、**CatalogSource** がデフォルトのカタログソースの名前を再利用する場合は、デフォルトのカタログソースの管理との競合により、Operator のインストールが失敗する可能性があります。この問題を回避するには、SRIOV-FEC **CatalogSource** CR を **common-config-policy** に追加し、Operator サブスクリプションを **common-subscriptions-policy** に追加する必要があります。別のポリシーを使用して SRIOV-FEC Operator をインストールする場合の回避策として、この Operator の **CatalogSource** が一意の名前であることを確認する必要があります。(OCPBUGSM-39859)

- クラスター内の複数のノードに適用すると、**SiteConfig** ディスクパーティションの定義が失敗します。**SiteConfig** CR を使用してコンパクトクラスターをプロビジョニングする場合は、複数のノードで有効な **diskPartition** 設定を作成すると、Kustomize プラグインエラーで失敗します。(OCPBUGSM-44403)

- ZTP コンテナーを使用して **ArgoCD** リソースにパッチを適用すると、そのパッチは、そのリリースバージョンの最新のコンテナーバージョンに続くタグを指します。ZTP コンテナーをリリース内の特定のバージョンに固定する場合は、特定のバージョンを指すようにパッチファイル **argocd-openshift-gitops-patch.json** を更新する必要があります。(OCPBUGSM-44261)

- **BMCEventSubscription** CR を適用すると、Redfish イベントサブスクリプションの作成に失敗します。サブスクリプション YAML ファイルを作成して適用すると、アクティブな Redfish サブスクリプションが表示されなくなります。回避策として、API を直接呼び出してサブスクリプションを作成します。以下に例を示します。

  1. 次のコマンドを実行して、認証トークンを取得します。

     ```
     $ curl -i --insecure --request POST --header "OData-Version: 4.0" \
     --header "Content-Type: application/json" -d '{"UserName": <BMC_USERNAME>, \
     "Password": <BMC_PASSWORD>}'
     https://<BMC_IP>/redfish/v1/SessionService/Sessions/ |grep 'X-Auth-Token'
     ```

     出力例

     ```
     X-Auth-Token: 1234abcd5678efgh9012ijkl3456mnop
     ```

  2. 認証トークンを使用して、Redfish イベントサブスクリプションを作成します。

     ```
     $ curl -X POST -i --insecure --header "X-Auth-Token:
     1234abcd5678efgh9012ijkl3456mnop" \
     -H 'Content-Type: application/json' --data-raw '{"Protocol": "Redfish", "Context": \
     "Public", "Destination": "https://hw-event-proxy-openshift-hw-
     events.apps.example.com/webhook", \
     "EventTypes": ["Alert"]}' https://<BMC_IP>/redfish/v1/EventService/Subscriptions
     ```

  201 Created 応答と、Redfish イベントサブスクリプションが正常に作成されたことを示す **Location: https://<BMC_IP>/redfish/v1/EventService/Subscriptions/35** を含むヘッダーを受け取る必要があります。(OCPBUGSM-43707)

- GitOps ZTP パイプラインを使用して、切断された環境に単一ノードの OpenShift クラスターをインストールする場合、クラスターに 2 つの **CatalogSource** CR が適用されている必要があります。ノードを複数回再起動すると、**CatalogSource** CR の 1 つが削除されます。回避策として、カタログソースのデフォルト名 (**certified-operators** や **redhat-operators** など) を変更できます。(OCPBUGSM-46245)

- スケールテスト中に、いくつかのクラスターが更新に失敗します。Telecom vDU 設定が適用された OpenShift Container Platform 4.9.26 更新を開始した後、**ClusterVersion** CR で開始された 4.10.13 へのクラスター更新は 15% で失敗し、クラスター Operator がターゲットバージョンに更新されるのを待ちます。(OCPBUGSM-44655)

- ZTP GitOps パイプラインの単一ノード OpenShift インストール中に、Operator Lifecycle Manager レジストリーサーバーコンテナーが **READY** 状態にならないことがあります。新しい **CatalogSource** でサブスクリプションを作成すると、**CatalogSource** は **TRANSIENT_FAILURE** 状態のままになります。(OCPBUGSM-44041)

- Pod に調整されたオーバーライドを適用し、調整された Pod を削除して再起動を強制すると、Pod が再起動し、システムが正常に実行されるはずです。代わりに、**systemd** のハングが発生し、システムが応答を停止する可能性があります。(RHELPLAN-131021)

- ZT Systems マシンを静的 IPv6 アドレス設定のライブ ISO から起動すると、インターフェイス

リンクの準備が整う前に **NetworkManager** が正常に終了します。これにより、設定がないネットワークインターフェイスが残ります。回避策として、**AgentServiceConfig** CR で参照されている RHCOS ISO を編集して、**grub.cfg** ファイルのカーネルパラメーターに **rd.net.timeout.carrier** を追加します。

1. インストールするリリースの **rhcos-live** ISO イメージをプルします。次のコマンドを実行して、ハブクラスターの **AgentServiceConfig** CR から URL を取得できます。

```
$ oc get AgentServiceConfig agent -o yaml
```

2. イメージを **/mnt/iso/** ディレクトリーにマウントします。

```
$ mount rhcos-live.x86_64.iso /mnt/iso/
```

3. **iso-grub-cfg/** ディレクトリーを作成し、次のディレクトリーに移動します。

```
$ mkdir iso-grub-cfg/; pushd iso-grub-cfg/
```

4. **/mnt/iso/** ディレクトリーの内容を作業ディレクトリーにコピーします。

```
$ rsync -avH /mnt/iso/* .
```

5. GRUB 設定ファイルを開きます。

```
$ vim EFI/redhat/grub.cfg
```

   a. **rd.net.timeout.carrier=20** 文字列を **Linux** ブート行に追加します。

6. 次のコマンドを実行して、最初の作業ディレクトリーに戻ります。

```
$ popd
```

7. **iso-grub-cfg** ディレクトリーから ISO ファイルを生成します。

```
$ mkisofs -JR -graft-points -o rhcos-carrier-timeout.iso iso-grub-cfg
```

8. 更新された ISO イメージを、ハブクラスターからアクセスできるサーバーにプッシュします。

9. ハブクラスターで、インストールするリリースの **AgentServiceConfig** CR の **osImages** エントリーを更新して、更新された ISO イメージを指すようにします。

```
$ oc edit AgentServiceConfig agent
```

10. **url** フィールドを更新して、更新された ISO イメージの URL を指すようにします。

(OCPBUGSM-46336)

- DU プロファイルとワークロードテストアプリケーションを使用してベアメタル SNO を再起動すると、カーネルエラーが発生します。回避策として、追加のカーネルパラメーターをパフォーマンスプロファイルに追加できます。

```
apiVersion: performance.openshift.io/v2
```

```
kind: PerformanceProfile
spec:
  additionalKernelArgs:
  - rcutree.kthread_prio=11
```

(RHELPLAN-123262)

- ZTP クラスターのデプロイメント中に、ベアメタルホストイメージのプロビジョニングが、HTTP 412 エラーコードを参照するエラーで失敗する場合があります。

```
Deploy step deploy.deploy failed with HTTPError: HTTP PATCH
https://10.16.230.34/redfish/v1/Managers/1/VirtualMedia/EXT1 returned code 412.
Base.1.8.GeneralError: A general error has occurred. See ExtendedInfo for more
information. Extended information: [

{'MessageSeverity': 'Critical', 'MessageArgs': [], 'MessageId': 'Base.1.8.PreconditionFailed',
'Resolution': 'Try the operation again using the appropriate ETag.', '@odata.type':
'#Message.v1_1_0.Message', 'Message': 'The ETag supplied did not match the ETag
required to change this resource.'}]
```

この問題は、古いファームウェアを実行している Gen8 HP マシンや Gen9 HP マシンなど、さまざまなサーバーモデルに影響を与える可能性があります。Gen9 HP マシンの場合は、最新の iLO ファームウェアにアップグレードすると問題が解決する場合があります。Gen8 HP およびその他のマシンの場合、現在、この問題の回避策はありません。(OCPBUGS-1246)

- SE450 などの特定の Lenovo モデルでは、ZTP クラスターデプロイメント中のベアメタルホストイメージのプロビジョニングが、HTTP 400 ステータスコードと **PropertyNotWriteable** エラーで失敗する場合があります。

```
HTTP response for PATCH https://192.168.26.178/redfish/v1/Systems/1/Pending: status
code: 400, error: Base.1.8.GeneralError: A general error has occurred. See ExtendedInfo for
more information., extended: [{'MessageArgs': ['BootSourceOverrideEnabled'], 'Resolution':
'Remove the property from the request body and resubmit the request if the operation failed.',
MessageId': 'Base.1.8.PropertyNotWritable', 'Message': 'The property
BootSourceOverrideEnabled is a read only property and cannot be assigned a value.',
'@odata.type': '#Message.v1_1_0.Message', 'MessageSeverity': 'Warning'}]
```

現在、この問題に対する回避策はありません。(OCPBUGSM-46305)

- ベアメタルクラスターでのプライマリーノードの交換中に、新しいプライマリーホストが **Provisioning** 状態で停止しますが、ノードはクラスターに **Ready** としてレポートします。(OCPBUGSM-45772)

- イメージをディスクに書き込んだ後、仮想メディアが iDRAC コンソールで ISO を切断しない場合は、Red Hat Advanced Cluster Management (RHACM) を使用して、Dell PowerEdge R640 サーバーでのスポーククラスターの導入がブロックされます。回避策として、iDRAC コンソールの仮想メディアタブから ISO を手動で切断します。(OCPBUGSM-45884)

- デュアルスタックネットワーク環境では、デバイスと接続が、**nm-initrd-generator** ユーティリティーによって生成されたデフォルトの **dhcp6** プロファイルを使用した **ip-check** 状態でスタックします。この問題により、**/etc/resolve.conf** ファイルが生成されません。回避策として、**NetworkManager** サービスを再起動します。これにより、欠落している **/etc/resolve.conf** ファイルが生成され、インストールを続行できます。(RHELPLAN-127788、OCPBUGS-70)

- Dell ハードウェアで NVIDIA ブランドの Mellanox NIC を使用すると、事前設定された F5 アプリケーション受信バッファー (現在は 8K に設定) よりも大きい受信パケットが、誤った VLAN

タグで到着します。これにより、不規則に切り捨てられたパケットが NIC によって配信されます。(RHELPLAN-123058)

- 場合によっては、静的 IP で設定され、GitOps ZTP パイプラインを使用してデプロイされた単一ノードの OpenShift ノードが、Day 2 オペレーターの設定中に到達不能になることがあります。OpenShift Container Platform クラスターのインストールは正常に完了し、クラスターは正常です。再起動後、ネットワークインターフェイスがダウンしてノードに到達できなくなります。(OCPBUGSM-46688)

- Git リポジトリーから **SriovNetworkNodePolicy** ポリシーを削除した後、削除されたポリシーによって管理されている **SriovNetworkNodePolicy** リソースはスポーククラスターに残ります。(OCPBUGSM-34614)

- PTP Operator を 4.10 から 4.11 にアップグレードすると、OpenShift サブスクリプションは、no channel heads (entries not replaced by another entry) found in channel **"stable"** of package **"ptp-operator"** エラーが報告されます。ただし、Operator は正常にアップグレードされます。(OCPBUGSM-46114)

- 現在、ZTP ソース CR 内のすべての **PtpConfig** CR には、**phc2sysOpts** オプションが含まれています。したがって、ユーザーがユーザーの **PolicyGenTemplate** CR に **phc2sysOpts** を含めなくても、**phc2sysOpts** オプションがスポーク PTP 設定に追加されます。デュアル NIC を使用する PTP が ZTP を介して設定されていると、ユーザーは、ZTP の完了後に **phc2sysOpts** オプションを削除するために 1 つの **PtpConfig** CR を更新する必要があります。(OCPBUGSM-47798)

- セキュアブートが **stalld** で有効になっている場合、サービスは **/sys/kernel/debug/sched_features** ファイルを開くことができないため、開始に失敗します。(OCPBUGSM-1466)

- セキュアブートが有効になっている場合は、**kdump** サービスが **kexec: failed to load kdump kernel** エラーで起動に失敗することがあります。この問題を回避するには、efi=runtime をカーネル引数に追加します。(OCPBUGSM-97)

- SNO クラスターを OCP 4.10 から OCP 4.11 にアップグレードすると、アップグレードプロセス中に SNO クラスターが 3 回再起動することがあります。(OCPBUGSM-46704)

- Supermicro サーバーが ZTP を介してデプロイメントされている場合は、不適切な起動デバイスが選択され、インストールが開始されない可能性があります。(OCPBUGSM-369)

- デフォルトの **dns-default** Pod に **"target.workload.openshift.io/management:"** アノテーションがありません。その結果、ワークロードパーティショニング機能が SNO で有効になっていると、Pod リソースは変更されず、予約済みの CPU セットに固定されません。回避策として、クラスター管理者は次のコマンドを使用して注釈を手動で追加できます。

  ```
  $ oc annotate pod dns-default
  target.workload.openshift.io/management='{"effect":"PreferredDuringScheduling"}' -n
  openshift-dns
  ```

  (OCPBUGSM-753)

1.9.8.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.9. RHSA-2022:6732 - OpenShift Container Platform 4.11.7 バグ修正の更新

発行日: 2022-10-03

OpenShift Container Platform release 4.11.7 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-2022:6732 アドバイザリーにまとめられています。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 4.11.7 --pullspecs
```

1.9.9.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.10. RHBA-2022:6809 - OpenShift Container Platform 4.11.8 バグ修正の更新

発行日: 2022-10-12

OpenShift Container Platform release 4.11.8 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-2022:6809 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-2022:6808 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 4.11.8 --pullspecs
```

1.9.10.1. バグ修正

- 以前は、モニタリングスタックで、ユーザー定義アラート専用の Alertmanager インスタンスを有効にしてデプロイした場合、OpenShift Container Platform Web コンソールの Developer パースペクティブでアラートを消音することはできません。今回の更新により、開発者の観点からユーザー定義のアラートを無効にすることができます。(**OCPBUGS-1790**)

1.9.10.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.11. RHBA-2022:6897 - OpenShift Container Platform 4.11.9 バグ修正の更新

発行日: 2022-10-17

OpenShift Container Platform release 4.11.9 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-2022:6897 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-2022:6896 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 4.11.9 --pullspecs
```

1.9.11.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.12. RHSA-2022:7201 - OpenShift Container Platform 4.11.12 バグ修正およびセキュリティー更新

発行日: 2022-11-02

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.12 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2022:7201 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-2022:7200 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 4.11.12 --pullspecs
```

1.9.12.1. 既知の問題

- クラスターが 4.9 以下のバージョンから段階的に更新される場合、**openshift-dns namespace** には、将来のバージョン更新に必要な Pod セキュリティーラベルが含まれていない可能性があります。(**OCPBUGS-1549**)

1.9.12.2. 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。

1.9.12.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.13. RHBA-2022:7201 - OpenShift Container Platform 4.11.13 バグ修正の更新

発行日: 2022-11-09

OpenShift Container Platform リリース 4.11.13 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-2022:7290 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-2022:7289 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 4.11.13 --pullspecs
```

1.9.13.1. 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。

1.9.13.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.14. RHSA-2022:8535 - OpenShift Container Platform 4.11.16 バグ修正およびセキュリティー更新

発行日: 2022-11-24

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.16 が利用可能になりました。このリリースには IBM powerbuild はありません。更新に含まれるバグ修正のリストは、RHSA-2022:8535 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-2022:8534 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 4.11.16 --pullspecs
```

1.9.14.1. 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。

1.9.14.2. バグ修正

- 以前は、Azure Disk Encryption Set (DES) またはResource Group (RG) 名を指定するときに大文字を使用すると、検証が失敗していました。このリリースでは、DES および RG 名に大文字と小文字を使用できるようになりました。(**OCPBUGS#4826**)

1.9.14.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.15. RHBA-2022:8627 - OpenShift Container Platform 4.11.17 バグ修正およびセキュリティー更新

発行日: 2022-11-28

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.17 が利用可能になりました。このリリースには IBM powerbuild はありません。この更新に含まれるバグ修正の一覧は、RHBA-2022:8627 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-2022:8626 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 4.11.17 --pullspecs
```

1.9.15.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.16. RHBA-2022:8698 - OpenShift Container Platform 4.11.18 バグ修正の更新

発行日: 2022-12-05

OpenShift Container Platform リリース 4.11.18 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-2022:8698 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-2022:8697 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 4.11.18 --pullspecs
```

1.9.16.1. 機能拡張

- 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。

1.9.16.2. 主な技術上の変更点

- 以前に名前が付けられた異種クラスターは、OpenShift Container Platform ドキュメントでマルチアーキテクチャーと呼ばれるようになりました。詳細は、マルチアーキテクチャークラスターの設定 を参照してください。

1.9.16.3. 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-4081)

- 以前は、ロードされたクラスターでの **kube-apiserver** のロールアウト時間が長く、5 分のロールアウトタイムアウトを超える場合がありました。今回の更新により、ロールアウト時間が短縮され、5 分のしきい値以内になりました。(OCPBUGS-3182)

1.9.16.4. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.17. RHSA-2022:8893 - OpenShift Container Platform 4.11.20 バグ修正およびセキュリティー更新

発行日: 2022-12-15

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.20 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2022:8893 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-2022:8892 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 4.11.20 --pullspecs
```

1.9.17.1. バグ修正

- 以前は、OpenShift Container Platform インストールプログラムは、Google Cloud Platform (GCP) にクラスターをインストールするときに、リージョンの不完全なリストをユーザーに提示していました。今回の更新により、インストールプログラムには、サポートされているすべての地域が含まれます。(OCPBUGS-3023)

1.9.17.2. 既知の問題

- **spec.endpointPublishingStrategy.loadBalancer.scope** フィールドを設定してデフォルトの Ingress Controller のルータースコープを切り替えると、Ingress Operator が劣化します。その結果、Web コンソール URL などのそのエンドポイントを使用するルートにアクセスできなくなります。回避策として、ルーター Pod の 1 つを再起動すると、**loadbalancer** の下にある複数のインスタンスが **inService** に戻ります。(OCPBUGS-2554)

1.9.17.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.18. RHSA-2022:9107 - OpenShift Container Platform 4.11.21 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 4.11.21 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2022:9107 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 4.11.21 --pullspecs
```

1.9.18.1. バグ修正

- 以前は、Red Hat OpenStack Platform (RHOSP) の認証情報をローテーションした後、Cinder CSI ドライバーは帯域外で再起動するまで古い認証情報を使用し続けていました。古い認証情報が有効でなくなった場合は、すべてのボリューム操作が失敗しました。今回の更新により、RHOSP 認証情報がローテーションされると、Cinder CSI ドライバーが自動的に更新されます。(OCPBUGS-4103)

- 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-2901)

- 以前は、ゾーンを持つリージョンで **vmSize** が無効な場合に可用性セットが作成されていました。ただし、可用性セットは、ゾーンがないリージョンでのみ作成する必要があります。今回の更新により、正しい **vmSize** が提供され、マシンセットに対して可用性セットが提供されなくなりました。(OCPBUGS-2123)

1.9.18.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.19. RHBA-2023:0027 - OpenShift Container Platform 4.11.22 バグ修正の更新

発行日: 2023-01-09

OpenShift Container Platform リリース 4.11.22 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-2023:0027 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 4.11.22 --pullspecs
```

1.9.19.1. バグ修正

- OpenShift Container Platform 4.11 リリースでは、**install-config.yaml** ファイルが更新され、**me-west1** (イスラエルのテルアビブ) リージョンがリストされるようになりました。**openshift-install** バイナリーを実行して OpenShift Container Platform をインストールした後、選択したクラスターの **me-west1** リージョンを選択できます。(OCPBUGS-4720)

- 以前は、一部のオブジェクトストレージインスタンスが、コンテンツが表示されるはずのときに **204 No Content** エラーメッセージ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。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-5078)

- 以前は、OpenShift Container Platform 4.11.ec4 ビルドのデプロイメントは、最新の RHCOS イメージ **412.86.202210072120-0** および **rhel-86** イメージで失敗しました。その結果、Red Hat Enterprise Linux CoreOS (RHCOS) ノードが起動時に停止します。今回の更新により、デプロイメントは正常に完了します。(OCPBUGS-2321)

1.9.19.2. 既知の問題

- ノードに対して約 470 個を超えるコンテナーを持つ 4.11 以降 の **arm64** クラスターでは、追加の Pod の作成が次のエラーで失敗する可能性があります。

  ```
  runc create failed: unable to start container process: unable to init seccomp: error loading seccomp filter into kernel: error loading seccomp filter: errno 524"
  ```

  これは、ワーカーノードで作成できる seccomp プロファイルの数が CoreOS によって制限されているためです。これは、アップグレード、ワーカーノードの障害、または Pod のスケール

アップ中に、Pod ごとに複数のコンテナーを持つクラスターで発生する可能性が最も高くなります。これは、OpenShift Container Platform の以降のバージョンで修正される予定です。(OCPBUGS-2637)

1.9.19.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.20. RHSA-2023:0069 - OpenShift Container Platform 4.11.24 バグ修正およびセキュリティー更新

発行日: 2023-01-19

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.24 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2023:0069 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-2023:0068 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 4.11.24 --pullspecs
```

1.9.20.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.21. RHSA-2023:0245 - OpenShift Container Platform 4.11.25 バグ修正およびセキュリティー更新

発行日:2023-01-23

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.25 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2023:0245 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-2023:0244 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 4.11.25 --pullspecs
```

1.9.21.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.22. RHSA-2023:0565 - OpenShift Container Platform 4.11.26 のバグ修正とセキュリティー更新

発行日: 2023-02-07

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.26 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2023:0565 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-2023:0564 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 4.11.26 --pullspecs
```

1.9.22.1. 既知の問題

- このリリースでは、機能のリグレッションがあります。静的な MAC アドレスが設定された SR-IOV セカンダリーネットワークインターフェイスが Pod にアタッチされている場合には、ネットワークの接続性が完全でない場合があります。この問題は、インテルイーサネットネットワークアダプター X710 製品 (i40e/iavf Linux カーネルドライバー) をベースにする SR-IOV 仮想機能にのみ影響します。詳細は、OCPBUGS-5139 を参照してください。

1.9.22.2. バグ修正

- 以前のリリースでは、**cluster-image-registry-operator** は、Swift に到達できなかった場合に、デフォルトで永続ボリューム要求 (PVC) を使用していました。今回の更新により、Red Hat OpenStack Platform (RHOSP) API への接続の失敗またはその他の偶発的な失敗により、**cluster-image-registry-operator** がプローブを再試行するようになりました。再試行中に、RHOSP カタログが問題なく見つかり、オブジェクトストレージが含まれていない場合、または RHOSP カタログがあり、現在のユーザーにコンテナーをリストするパーミッションがない場合に、デフォルトで PVC が使用されます。(OCPBUGS-5578)

- 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 detail ページ** で問題が発生しなくなりました。(OCPBUGS-6689)

1.9.22.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.23. RHSA-2023:0651 - OpenShift Container Platform 4.11.27 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 4.11.27 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2023:0651 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-2023:0650 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 4.11.27 --pullspecs
```

1.9.23.1. 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。(OCPBUGS-5459)

1.9.23.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.24. RHSA-2023:0774 - OpenShift Container Platform 4.11.28 のバグ修正とセキュリティー更新

発行日: 2023-02-21

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.28 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2023:0774 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-2023:0773 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 4.11.28 --pullspecs
```

1.9.24.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.25. RHSA-2023:0895 - OpenShift Container Platform 4.11.29 のバグ修正とセキュリティー更新

発行日: 2023-02-28

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.29 が利用可能になりました。更新に含まれるバグ修正のリストは RHSA-2023:0895 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 4.11.29 --pullspecs
```

1.9.25.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.26. RHSA-2023:1030 - OpenShift Container Platform 4.11.30 のバグ修正とセキュリティー更新

発行日: 2023-03-07

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.30 が利用可能になりました。更新に含まれるバグ修正のリストは RHSA-2023:1030 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-2023:1029 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 4.11.30 --pullspecs
```

1.9.26.1. バグ修正

- 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 Secret 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-7494)

1.9.26.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.27. RHSA-2023:1158 - OpenShift Container Platform 4.11.31 バグ修正およびセキュリティー更新

発行日: 2023-03-14

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.31 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-2023:1158 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-2023:1157 アドバイザリーによって提供されています。

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 4.11.31 --pullspecs
```

1.9.27.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.28. RHBA-2023:1296 - OpenShift Container Platform 4.11.32 バグ修正およびセキュリティー更新

発行日: 2023-03-22

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.32 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-2023:1296 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-2023:1295 アドバイザリーによって提供されています。

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 4.11.32 --pullspecs
```

1.9.28.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.29. RHBA-2023:1396 - OpenShift Container Platform 4.11.33 バグ修正

発行日: 2023-03-28

OpenShift Container Platform リリース 4.11.33 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:1396 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-2023:1395 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 4.11.33 --pullspecs
```

1.9.29.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.30. RHSA-2023:1504 - OpenShift Container Platform 4.11.34 のバグ修正とセキュリティー更新

発行日: 2023-04-04

OpenShift Container Platform リリース 4.11.34 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2023:1504 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2023:1503 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 4.11.34 --pullspecs
```

1.9.30.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.31. RHBA-2023:1650 - OpenShift Container Platform 4.11.35 バグ修正

発行日: 2023-04-12

OpenShift Container Platform リリース 4.11.35 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:1650 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-2023:1649 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 4.11.35 --pullspecs
```

1.9.31.1. バグ修正

- 以前は、OpenStack **clouds.yaml** ファイルがローテーションされた場合、新しいクラウド認証情報を取得するために **machine-api-provider-openstack** を再起動する必要がありました。その結果、**MachineSet** がゼロにスケールする機能が影響を受ける可能性があります。この変更により、クラウド認証情報はキャッシュされなくなり、**machine-api-provider-openstack** が必要なときに対応するシークレットを読み取ります。(OCPBUGS-10954)

1.9.31.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.32. RHBA-2023:1733 - OpenShift Container Platform 4.11.36 バグ修正

発行日: 2023-04-13

OpenShift Container Platform リリース 4.11.36 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:1733 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 4.11.36 --pullspecs
```

1.9.32.1. 更新

すべての OpenShift Container Platform 4.11 ユーザーは、このリリースで修正された唯一の欠陥がインストール時間に限定されていることに注意してください。したがって、以前にインストールされたクラスターをこのバージョンに更新する必要はありません。

1.9.33. RHBA-2023:1760 - OpenShift Container Platform 4.11.37 バグ修正

発行日: 2023-04-19

OpenShift Container Platform リリース 4.11.37 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2023:1760 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-2023:1759 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 4.11.37 --pullspecs
```

1.9.33.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.34. RHBA-2023:1863 - OpenShift Container Platform 4.11.38 バグ修正の更新

発行日: 2023-04-26

OpenShift Container Platform リリース 4.11.38 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:1863 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-2023:1862 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 4.11.38 --pullspecs
```

1.9.34.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.35. RHSA-2023:2014 - OpenShift Container Platform 4.11.39 のバグ修正とセキュリティー更新

発行日: 2023-05-02

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.39 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:2014 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-2023:2056 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 4.11.39 --pullspecs
```

1.9.35.1. バグ修正

- 以前は、シークレットのサイズ制限が 1 MB だったため、Ingress Operator は、多数の Ingress Controller を備えたクラスターで **router-certs** シークレットを公開できませんでした。その結果、**router-certs** シークレットを使用してクラスター Ingress ドメインにアクセスする Authentication Operator は、OAuth の目的で使用する最新の証明書を持っていない可能性があります。この更新により、Ingress Operator は、クラスター Ingress ドメインを所有する Ingress Controller に対してのみ証明書とキーを公開するため、シークレットがサイズ制限を超えないようになります。この更新により、Authentication Operator が OAuth 認証用の最新の証明書を読み取って使用できるようになります。(OCPBUGS-8000)

1.9.35.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.36. RHBA-2023:2694 - OpenShift Container Platform 4.11.40 バグ修正の更新

発行日: 2023-05-18

OpenShift Container Platform リリース 4.11.40 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:2694 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-2023:2693 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 4.11.40 --pullspecs
```

1.9.36.1. バグ修正

- 以前は、OpenShift Web コンソールで Knative (**kn**) サービスを削除しても、関連付けられた **<kn-service-name>-github-webhook-secret** Webhook は削除されませんでした。元のサービスと同じ名前を保持したまま Knative サービスを再作成しようとすると、操作は失敗します。この更新により、OpenShift Web コンソールで Knative (**kn**) サービスを削除すると、関連付けられた Webhook がサービスと同時に削除されます。操作が失敗することなく、削除されたサービスと同じ名前で Knative サービスを再作成できるようになりました。(OCPBUGS-7949)

1.9.36.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.37. RHBA-2023:3213 - OpenShift Container Platform 4.11.41 バグ修正の更新

発行日: 2023-05-24

OpenShift Container Platform リリース 4.11.41 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:3213 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-2023:3212 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 4.11.41 --pullspecs
```

1.9.37.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.38. RHSA-2023:3309 - OpenShift Container Platform 4.11.42 のバグ修正とセキュリティー更新

発行日 2023 年 5 月 31 日

OpenShift Container Platform リリース 4.11.42 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:3309 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-2023:3308 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 4.11.42 --pullspecs
```

1.9.38.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.39. RHSA-2023:3542 OpenShift Container Platform 4.11.43 のバグ修正とセキュリティー更新

発行日: 2023 年 6 月 14 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.43 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:3542 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-2023:3541 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 4.11.43 --pullspecs
```

1.9.39.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.40. RHSA-2023:3915 - OpenShift Container Platform 4.11.44 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 4.11.44 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-2023:3915 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-2023:3914 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 4.11.44 --pullspecs
```

1.9.40.1. バグ修正

- 以前は、クライアント TLS (mTLS) がイングレスコントローラーで設定されており、クライアント CA バンドルの認証局 (CA) をダウンロードするには 1MB を超える証明書失効リスト (CRL) を必要としたため、**ConfigMap** オブジェクトのサイズ制限CRL **ConfigMap** オブジェクトを更新できませんでした。これは、**ConfigMap** オブジェクトのサイズ制限が原因です。CRL が欠落しているため、有効なクライアント証明書を使用した接続が、エラー **unknown ca** で拒否される可能性がありました。この更新により、各イングレスコントローラーの CRL **ConfigMap** オブジェクトは存在しなくなります。代わりに、CRL **ConfigMap** オブジェクトが各ルーター Pod によって直接ダウンロードされ、有効なクライアント証明書による接続が拒否されなくなります。(OCPBUGS-14456)

- 以前は、クライアント TLS (mTLS) が Ingress コントローラー上で設定されていたため、配布元の認証局 (CA) と発行元の CA が一致せず、間違った証明書失効リスト (CRL) がダウンロードされていました。その結果、正しい CRL の代わりに間違った CRL がダウンロードされ、有効なクライアント証明書を使用した接続が **unknown ca** のエラーメッセージで拒否されていました。この更新により、ダウンロードした CRL はそれらを配布元の CA によって追跡されるようになりました。これにより、有効なクライアント証明書が拒否されなくなります。(OCPBUGS-14457)

1.9.40.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.41. RHSA-2023:4053 OpenShift Container Platform 4.11.45 のバグ修正とセキュリティー更新

発行日: 2023-07-19

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.45 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:4053 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-2023:4052 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 4.11.45 --pullspecs
```

1.9.41.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.42. RHSA-2023:4310 OpenShift Container Platform 4.11.46 のバグ修正とセキュリティー更新

発行日: 2023 年 8 月 2 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.11.46 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:4310 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-2023:4312 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 4.11.46 --pullspecs
```

1.9.42.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.43. RHBA-2023:4614 OpenShift Container Platform 4.11.47 バグ修正の更新

発行日: 2023 年 8 月 16 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は RHBA-2023:4614 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-2023:4616 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 4.11.47 --pullspecs
```

1.9.43.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.44. RHBA-2023:6153 - OpenShift Container Platform 4.14.1 バグ修正の更新

発行日: 2024 年 3 月 27 日

OpenShift Container Platform リリース 4.13.12 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。この更新には 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 4.11.48 --pullspecs
```

1.9.44.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.45. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:3911 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 4.11.49 --pullspecs
```

1.9.45.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.46. RHBA-2023:6153 - OpenShift Container Platform 4.14.1 バグ修正の更新

発行日: 2024 年 3 月 27 日

OpenShift Container Platform リリース 4.13.12 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 4.11.50 --pullspecs
```

1.9.46.1. 機能

1.9.46.1.1. Google Cloud Provider クラスター用のカスタム Red Hat Enterprise Linux CoreOS (RHCOS) イメージの使用

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

- **controlPlane.platform.gcp.osImage.project**
- **controlPlane.platform.gcp.osImage.name**
- **compute.platform.gcp.osImage.project**
- **compute.platform.gcp.osImage.name**
- **platform.gcp.defaultMachinePlatform.osImage.project**

- **platform.gcp.defaultMachinePlatform.osImage.name**

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

1.9.46.2. バグ修正

- 以前は、Manila CSI ドライバー Operator で使用されるクラウド認証情報がキャッシュされ、これらの認証情報がローテーションされると認証の問題が発生していました。今回の更新で、この問題は解決されました。(OCPBUGS-18782)

1.9.46.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.47. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、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 4.11.52 --pullspecs
```

1.9.47.1. 既知の問題

Python への最近のセキュリティー更新により、ベアメタルプラットフォーム上のホストのプロビジョニングに失敗していました。この問題が解決されるまで、OpenShift Container Platform クラスターをベアメタルプラットフォームのバージョン 4.11.52 にアップグレードしないでください。このバージョンにアップグレードして、この問題が修正されていない場合は、ノードをスケーリングできません。(OCPBUGS-20486)

1.9.47.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.48. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、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 4.11.53 --pullspecs
```

1.9.48.1. バグ修正

- 以前のバージョンでは、**EndpointSlice** ポートがポート番号なしで作成されると、**CoreDNS** がクラッシュしました。今回の更新により、検証が **CoreDNS** に追加されるため、この状況ではサーバーがクラッシュしなくなりました。(OCPBUGS-20359)

1.9.48.2. 既知の問題

- Python への最近のセキュリティー更新により、ベアメタルプラットフォーム上のホストのプロビジョニングに失敗していました。この問題が解決されるまで、OpenShift Container Platform クラスターをベアメタルプラットフォームのバージョン 4.11.53 にアップグレードしないでください。このバージョンにアップグレードして、この問題が修正されていない場合は、ノードをスケーリングできません。(OCPBUGS-20486)

1.9.48.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.49. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2023 年 11 月 29 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:3911 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 4.11.54 --pullspecs
```

1.9.49.1. 機能

1.9.49.1.1. apiserver.config.openshift.io が Insights Operator によって追跡されるようになりました

Insights Operator の実行後、**APIServer.config.openshift.io** の監査プロファイルに関する情報とともに、パス **config/apiserver.json** のアーカイブで新しいファイルが利用できるようになります。

監査プロファイルにアクセスすると、どの監査ポリシーが共通であること、最も一般的に使用されるプロファイル、業界間のどのような違い、どのようなカスタマイズが適用されるかを理解するのに役立ちます。

1.9.49.2. バグ修正

- 以前は、ユーザーがコンテナー間でファイルをコピーすると、タイムスタンプは保持されませんでした。今回のリリースでは、コンテナー間でファイルをコピーするときにタイムスタンプを保持するための **-p** フラグが追加されました。(OCPBUGS-23041)

1.9.49.3. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.50. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:3911 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 4.11.55 --pullspecs
```

1.9.50.1. バグ修正

- 以前は、マスターノードが追加のネットワークに接続されている場合、OpenStack Platform で 4.12 へのアップグレードが失敗する可能性がありました。アップグレード中に、両方のプロバイダーが同時にアクティブになり、短期間はアクティブになり、異なるノード IP を報告することができます。この動作は、ツリー内クラウドプロバイダーから外部クラウドプロバイダーに切り替える際の既知の競合状態によるものです。このリリースでは、両方のプロバイダーが同じプライマリーノード IP を報告するアノテーションが追加され、ノード IP のフラッピングを防ぎます。(OCPBUGS-20122)

1.9.50.2. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.51. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、RHSA-2023:3911 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 4.11.56 --pullspecs
```

1.9.51.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.52. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、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 4.11.57 --pullspecs
```

1.9.52.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.53. RHSA-2023:3615 - OpenShift Container Platform 4.12.22 バグ修正の更新およびセキュリティー更新

発行日: 2024 年 3 月 27 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.15.5 が利用可能になりました。更新に含まれるバグ修正は、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 4.11.58 --pullspecs
```

1.9.53.1. 更新

既存の OpenShift Container Platform 4.15 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。