OpenShift Container Platform 4.7

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: 2021-10-17

OpenShift Container Platform 4.7 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

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

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

目次

第1章 OPENSHIFT CONTAINER PLATFORM 4.7 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、エンタープライズレベルの最新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. 本リリースについて

OpenShift Container Platform (RHSA-2020:5633) が公開されました。本リリースでは、CRI-O ランタイムで Kubernetes 1.20 を使用します。以下では、OpenShift Container Platform 4.7 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 4.7 クラスターは https://cloud.redhat.com/openshift でご利用いただけます。OpenShift Container Platform 向けの Red Hat OpenShift Cluster Manager アプリケーションを使って、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 4.7 は、Red Hat Enterprise Linux (RHEL) 7.9 以降、および Red Hat Enterprise Linux CoreOS (RHCOS) 4.7 でサポートされます。

コントロールプレーン (マスターマシンとしても知られている) 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 (ワーカーマシンとしても知られている) には RHCOS または Red Hat Enterprise Linux (RHEL) 7.9 以降のいずれかを使用できます。

重要

コンピュートマシン用にサポートされているのは Red Hat Enterprise Linux (RHEL) バージョン 7.9 以降であるため、RHEL コンピュートマシンをバージョン 8 にアップグレードすることはできません。

OpenShift Container Platform 4.7 のリリースでは、バージョン 4.4 のライフサイクルは終了します。詳細は、Red Hat OpenShift Container Platform ライフサイクルポリシー を参照してください。

1.2. 多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、弊社の CTO、Chris Wright のメッセージを参照してください。

1.3. 新機能および改良された機能

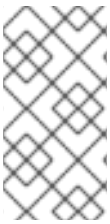
今回のリリースでは、以下のコンポーネントおよび概念に関連する拡張機能が追加されました。

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. LUKS、RAID、および FBA DASD のディスクプロビジョニングの強化

OpenShift Container Platform 4.7 には、ベアメタルデプロイメントのディスクのプロビジョニングについてのいくつかの改善点が含まれています。現時点で、以下の機能は新規の 4.7 クラスターについてのみサポートされています。

- LUKS ディスク暗号化のネイティブ Ignition サポートは、暗号化したルートファイルシステムのさらなる設定の容易性をもたらし、追加のデータファイルシステムの暗号化サポートも提供します。
- RHCOS は、s390x の場合を除くブートディスクのミラーリングをサポートするようになりました。ディスクに障害が発生した場合の冗長性が提供されます。詳細は、インストール時のディスクのミラーリングについて参照してください。
- s390x 上の RHCOS は、固定ブロックアーキテクチャー (FBA) タイプのダイレクトアクセスストレージデバイス (DASD) ディスクにインストールできます。
- RHCOS は、マルチパス化されるプライマリーディスクをサポートするようになりました。



注記

新規クラスターでは、レガシーの **/etc/clevis.json** ファイルがマシン設定に含まれるとプロビジョニングに失敗するため、LUKS 設定はネイティブの Ignition メカニズムを使用する必要があります。OpenShift Container Platform 4.6 以前からアップグレードしているクラスターでは、LUKS は **/etc/clevis.json** を使用してのみ設定できます。

1.3.1.2. bootupd の使用によるブートローダーの更新

bootupd を使用する RHCOS ユーザーは、最新のアーキテクチャーで実行される UEFI およびレガシー BIOS ブートモードのファームウェアおよびブートの更新を管理する複数のディストリビューションに対応可能な、システムに依存しない更新ツールにアクセスできます。

1.3.1.3. RHCOS が RHEL 8.4 を使用するように

RHCOS は、OpenShift Container Platform 4.7.24 以降で Red Hat Enterprise Linux (RHEL) 8.4 パッケージを使用するようになりました。これにより、NetworkManager 機能などの最新の修正、機能、拡張機能、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。OpenShift Container Platform 4.6 は延長アップデートサポート (EUS) リリースです。このリリースは、ライフサイクル全体に対して RHEL 8.2 EUS パッケージを引き続き使用します。

1.3.1.4. RHCOS が kdump サービスに対応 (テクノロジープレビュー)

kdump サービスは、カーネル問題のデバッグ用のクラッシュダンプの仕組みを提供するために RHCOS のテクノロジープレビューに導入されています。このサービスを使用して、後の分析用にシステムメモリーの内容を保存できます。**kdump** サービスはクラスターレベルで管理されず、ノードごとに手動で有効にし、設定する必要があります。詳細は、kdump の有効化について参照してください。

1.3.1.5. Ignition の更新

以下の Ignition の更新が利用可能になりました。

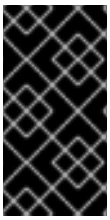
- RHCOS が Ignition 設定仕様 3.2.0 をサポートするようになりました。今回の更新により、ディスクパーティションのサイズ変更、LUKS で暗号化されたストレージ、および **gs://** URL のサポートが提供されるようになりました。
- GovCloud または AWS China などのデフォルト以外の AWS パーティションで実行される場合、Ignition は同じパーティションから **s3://** リソースを取得するようになりました。
- Ignition が AWS EC2 インスタンスメタデータサービスバージョン 2 (IMDSv2) をサポートするようになりました。

1.3.1.6. DHCP リースの取得の試行時に使用されるタイムアウト値の設定

以前のバージョンでは、DHCP リースの取得にデフォルトの 45 秒よりも長い時間がかかるため、RHCOS DHCP カーネルパラメーターは予想通りに機能しませんでした。今回の修正により、DHCP リースの取得の試行時に使用されるタイムアウト値を設定できるようになりました。詳細は、BZ#1879094 を参照してください。

1.3.1.7. RHCOS によるマルチパスのサポート

RHCOS はプライマリーディスクでのマルチパスをサポートするようになり、ハードウェア障害に対する対障害性が強化され、マルチパスの上部に RHCOS を設定してホストの可用性を強化できるようになりました。詳細は、BZ#1886229 を参照してください。



重要

説明されているように、マシン設定内のカーネル引数でのみマルチパスを有効にします。インストール時にマルチパスを有効にしないでください。

詳細は、RHCOS のカーネル引数でのマルチパスの有効化について参照してください。

重要

IBM Z および LinuxONE でマルチパスを有効にするには、インストール時に追加の手順が必要です。

詳細は、Red Hat Enterprise Linux CoreOS (RHCOS) マシン について参照してください。

1.3.1.8. Instance Metadata Service Version 2 (IMDSv2) からの AWS の設定の取得

Ignition がInstance Metadata Service Version 2 (IMDSv2) からの AWS の設定の取得をサポートするようになりました。今回の機能拡張により、AWS EC2 インスタンスは IMDSv1 を無効にして作成できるようになり、インスタンスユーザーデータから Ignition 設定を読み取るのに IMDSv2 が必要になりました。その結果、Ignition は IMDSv1 が有効かどうかにかかわらず、インスタンスのユーザーデータから設定を正常に読み取ります。詳細は、BZ#1899220 を参照してください。

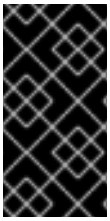
1.3.1.9. Qemu ゲストエージェントが RHCOS に追加される

Qemu ゲストエージェントがデフォルトで RHCOS に組み込まれるようになりました。今回の機能拡張により、Red Hat Virtualization (RHV) 管理者は、RHCOS についての役立つ情報を RHV 管理インターフェースに戻すことで、RHCOS ノードについての豊富な情報を表示できるようになりました。詳細は、BZ#1900759 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. クラスターの AWS C2S シークレットリージョンへのインストール

Amazon Web Services (AWS) のクラスターを Commercial Cloud Services (C2S) シークレットリージョンにインストールできるようになりました。C2S リージョンには Red Hat によって公開される RHCOS AMI がないため、そのリージョンに属するカスタム AMI をアップロードする必要があります。また、クラスターのインストール時に **install-config.yaml** ファイルの **additionalTrustBundle** フィールドに C2S の CA 証明書を含める必要もあります。C2S シークレットリージョンにデプロイされたクラスターには、インターネットへのアクセスがありません。そのため、プライベートイメージレジストリーを設定する必要があります。



重要

現時点で、現在の OpenShift Container Platform の制限により、AWS C2S シークレットリージョンにインストールされたクラスターで、テクノロジープレビュー機能である AWS Secure Token Service (STS) を使用することはできません。これには、C2S Access Portal (CAP) で提供される一時的な認証情報の使用が含まれます。

インストールプログラムは、C2S リージョンにデプロイされたクラスターの破棄をサポートしません。クラスターのリソースは手動で削除する必要があります。

詳細は、AWS government およびシークレットリージョン について参照してください。

1.3.2.2. 個人の暗号化キーを使用したディスク暗号化による GCP へのクラスターのインストール

クラスターを Google Cloud Platform (GCP) にインストールし、個人の暗号化キーを使用して仮想マシンと永続ボリュームの両方を暗号化できるようになりました。これは、**install-config.yaml** ファイルで **controlPlane.platform.gcp.osDisk.encryptionKey**、**compute.platform.gcp.osDisk.encryptionKey**、または **gcp.defaultMachinePlatform.osDisk.encryptionKey** フィールドを設定して実行できます。

1.3.2.3. ベアメタルマシンを使用する RHOSP へのクラスターのインストール

ベアメタルマシンを使用する独自の Red Hat OpenStack Platform (RHOSP) インフラストラクチャーにクラスターをインストールできます。クラスターには、ベアメタル上でコントロールプレーンとコンピュートマシンの両方を実行させることも、コンピュートマシンのみを実行させることもできます。詳細は、ベアメタルマシンを使用したクラスターのデプロイ について参照してください。

この機能は、Kuryr を使用するクラスターではサポートされません。

1.3.2.4. インストール時の RHOSP 要件の検証の強化

OpenShift Container Platform インストーラーは、RHOSP へのクラスターのインストールを試行する前に追加の検証を実行するようになりました。これらの新規の検証には以下が含まれます。

- リソースクォータ
- Floating IP アドレスの重複
- カスタムクラスター OS イメージの可用性

1.3.2.5. RHOSP 上の新規コンピュートマシンのカスタムサブネット

任意のネットワークおよびサブネットを使用する RHOSP で実行されるクラスターにコンピュートマシンを作成できるようになりました。

1.3.2.6. RHOSP 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 Playbook へのアクセスが容易になる

独自の RHOSP インフラストラクチャーにクラスターをインストールするための Ansible Playbook は、インストールドキュメントのスクリプトを使用して取得できるようにパッケージ化されました。

1.3.2.7. RHOSP での QEMU ゲストエージェントのサポート

インストール時に QEMU ゲストエージェントのサポートを有効にできるようになりました。

1.3.2.8. RHOSP のクラスターの永続ボリューム制限の引き上げ

インストール時に、RHOSP のクラスターに 26 を超える永続 Cinder ボリュームが含まれるようにノードを設定できるようになりました。

1.3.2.9. install-config.yaml ファイルの computeFlavor プロパティーが非推奨になる

install-config.yaml ファイルで使用される **computeFlavor** プロパティーは非推奨になりました。代替方法として、**platform.openstack.defaultMachinePlatform** プロパティーでマシンプールフレーバーを設定できるようになりました。

1.3.2.10. インストーラーでプロビジョニングされるインフラストラクチャーのクラスターについてのブートストラップホストの静的 DHCP 予約の使用

以前のバージョンの OpenShift Container Platform 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するベアメタルインストールのブートストラップホストに静的 IP アドレスを割り当てることができませんでした。ブートストラップ仮想マシンで使用される MAC アドレスを指定できるようになりました。つまり、ブートストラップホストに静的 DHCP 予約を使用できます。詳細は、BZ#1867165 を参照してください。

1.3.2.11. インストーラーでプロビジョニングされるインストールの機能拡張

ベアメタルノードでのインストーラーでプロビジョニングされるインストールのインストーラーは、Ignition ファイルなどのインストール時に必要なデータファイルを保存するためにストレージプールを自動的に作成できるようになりました。

ベアメタルノードのインストーラーでプロビジョニングされるインストールのインストーラーはサーベイを提供し、ユーザーに対して最小限の質問を尋ねし、妥当なデフォルト値で **install-config.yaml** ファイルを生成します。生成された **install-config.yaml** ファイルを使用してクラスターを作成するか、またはクラスターを作成する前にファイルを手動で編集できます。

1.3.2.12. インストーラーでプロビジョニングされるクラスターによる DHCP リースの静的 IP アドレスへの変換が可能になる

ベアメタルクラスターにインストーラーでプロビジョニングされるインストールでデプロイされるクラスターノードは、静的 IP アドレスでデプロイできます。ノードが静的 IP アドレスを使用するようにクラスターをデプロイするには、クラスターノードに無限リースを提供するよう DHCP サーバーを設定します。インストーラーが各ノードのプロビジョニングを終了すると、dispatcher スクリプトが各プロビジョニングノードで実行され、DHCP サーバーが提供する同じ静的 IP アドレスを使用して、DHCP の無限リースを静的 IP アドレスに変換します。

1.3.2.13. マシン設定プールのパフォーマンスが低下している場合、更新は即時にブロックされます。

マシン設定プール (MCP) が **degraded** 状態の場合、Machine Config Operator (MCO) はその **Upgradeable** ステータスを **False** として報告するようになりました。その結果、すべてのマシン設定プールが正常な状態になるまで、(4.7 から 4.8 などの) マイナーバージョン内での更新を実行できなくなりました。以前のバージョンでは、パフォーマンスが低下したマシン設定プールがある場合に、Machine Config Operator はその **Upgradeable** ステータスを **false** と報告しませんでした。更新が許可されても、マシン設定プールが低下している場合、最終的には Machine Config Operator の更新時に失敗するようになりました。z-stream リリース内の更新 (例: 4.7.1 から 4.7.2) の場合、この動作に関連する変更はありません。そのため、z-stream の更新を実行する前に、マシン設定プールのステータスをチェックする必要があります。

1.3.3. Web コンソール

1.3.3.1. Web コンソールのローカライズ

Web コンソールがローカライズされ、世界のユーザー向けに言語サポートが提供されるようになりました。現時点では、英語、日本語、および簡体字中国語のサポートが提供されています。ブラウザーの設定に従って言語が表示されますが、ブラウザーのデフォルトを上書きするよう言語を選択することもできます。**User** ドロップダウンメニューから、**Language preferences** を選択して言語設定を更新します。日時のローカライズもサポートされています。

1.3.3.2. クイックスタートチュートリアル

クイックスタートは、ユーザータスクに関するガイド付きチュートリアルです。Web コンソールでは、**Help** メニューでクリックスタートにアクセスできます。これらは、アプリケーション、Operator、または他の製品オファリングを使用する場合に役立ちます。

詳細は、Web コンソールでのクイックスタートチュートリアルの作成について参照してください。

1.3.3.3. Insights プラグイン

Insights プラグイン は OpenShift Container Platform Web コンソールに統合されるようになりました。Insights は、問題の合計数や問題の合計リスクなど、クラスターの正常性データを提供します。リスクには、**Critical**、**Important**、**Moderate**、または **Low** としてラベルが付けられます。Red Hat OpenShift Cluster Manager に簡単に移動して問題および問題の修正方法についての詳細を参照できます。

1.3.3.4. Developer パースペクティブ

- コンソールは、Red Hat Operator がコンソールを拡張する独自のユーザーインターフェースをビルドし、パッケージ化することを可能にする、拡張性のあるメカニズムを提供するようになりました。またこれにより、お客様および Operator が独自のクイックスタートを追加できるようになりました。**Administrator** および **Developer** パースペクティブの両方からヒント、フィルター、およびアクセスが追加され、クイックスタートおよび関連のコンテンツがよりアクセスしやすくなりました。

- トポロジーの **List** および **Graph** ビューでデプロイされたワークロードとアプリケーションのグループをすぐに検索し、それらをアプリケーションに追加できるようになりました。

- ユーザー設定の永続ストレージが提供され、あるマシンまたはブラウザーから別のブラウザーに移行してもユーザーエクスペリエンスの一貫性が保たれるようになりました。

- OpenShift GitOps Operator をクラスターにインストールしている場合、**Environments** ビューの **Argo CD** リンクを使用して Argo CD ユーザーインターフェースに移動できます。

- **Developer Catalog** 機能および **Form** または **YAML** オプションへのインコンテキスト (in-context) のメニューのマッピングなどのユーザービリティーの強化により、Pipeline、Helm、およびイベントソース設定をより容易に更新できるようになりました。

- Operator Backed、Helm、ビルダーイメージ、テンプレートおよびイベントソースなどの指定されたサービスについてのフィルターされたエントリーを表示する機能が、**Developer Catalog** に追加されました。

- Quay Security Operator をクラスターにインストールした後に、以下を実行します。

  - 選択したプロジェクトについての以下の脆弱性の一覧を表示できます。

    - 脆弱性および脆弱なイメージの合計数
    - すべての脆弱なイメージの重大度ベースの数
    - 修正可能な脆弱性の数
    - 脆弱なイメージごとの影響を受ける Pod 数

  - 脆弱性の重大度の詳細を確認し、そのリポジトリーに保存される脆弱なイメージのマニフェストのコンテキストで Quay ユーザーインターフェースを起動して、脆弱性の詳細を取得できます。

- OpenShift Virtualization Operator をクラスターにインストールした後に、**+Add** ビューで **Virtual Machines** オプションを選択し、**Developer Catalog** のテンプレートを使用して仮想マシンを作成できます。

- Web 端末がさらに使いやすくなりました。

  - すべてのユーザーは、権限レベルに関係なく、コンソールの Web 端末にアクセスできます。

  - Web 端末が長期間非アクティブになると、停止し、ユーザーに再起動するオプションを提供します。

- Pipeline ワークフローが強化されました。

  - Pipeline の作成プロセスでは、パイプラインをデフォルトのビルド設定システムでより適切に使用できるようになりました。ビルド設定は、デフォルトでは **Import from git** ワークフローを使用してパイプラインと共に作成されなくなり、パイプラインはアプリケーションの作成直後に起動します。

  - パイプラインは、**Pipeline builder** オプションまたは **YAML view** オプションのいずれかを使用して **Pipeline builder** ページで設定できるようになりました。Operator によってインストールされた、再利用可能なスニペットおよびサンプルを使用して、詳細な Pipeline を作成することもできます。

  - **PipelineRun** ページには、関連付けられたタスクの実行を一覧表示する **TaskRuns** タブが含まれるようになりました。必要なタスク実行をクリックして、タスク実行の詳細を表示し、パイプラインをデバッグできます。

  - **Pipeline Details** ページで、パイプラインごとに、パイプラインの実行時間、タスクの実行時間、1日あたりのパイプラインの実行数および成功率などのメトリクスを確認できるようになりました。

  - **Events** タブが **Pipeline Run details**および **Task Run details**ページで選択できるようになり、ここには特定の PipelineRun または TaskRun のイベントが表示されます。

- サーバーレスがさらに使いやすくなりました。
  - **Administrator** パースペクティブから **Serving** および **Eventing** ページにアクセスし、コンソールを使用してサーバーレスコンポーネントを作成できます。
  - イベントソース作成ワークフローを使用して Camel コネクターを作成できます。
- Helm チャートのユーザビリティーが強化されました。
  - クラスター管理者として、以下を実行できます。
    - チャートリポジトリーを追加または削除します。
    - Helm チャートを使用する機能を削除します。
    - クイックスタートで Helm チャートリポジトリーの管理方法を確認します。
  - 開発者は、以下を実行できます。
    - 同じ名前のチャートをチャートリポジトリーごとに区別するには、カタログのチャートカードにあるチャートリポジトリーの名前を参照します。
    - カードのカタログレベルでチャートについての洞察を得ることができます。
    - 複数のリポジトリーが設定されている場合には、チャートリポジトリーでカタログをフィルターします。

1.3.3.5. IBM Z および LinuxONE

本リリースでは、IBM Z および LinuxONE は OpenShift Container Platform 4.7 と互換性があります。インストール手順については、 z/VM を使用したクラスターの IBM Z および LinuxONE へのインストールや、ネットワークが制限された環境での z/VM を使用したクラスターの IBM Z および LinuxONE へのインストールについて参照してください。

主な機能拡張
以下の新機能は、OpenShift Container Platform 4.7 の IBM Z および LinuxONE でサポートされます。

- RHEL 8.3 以降の KVM は、IBM Z および LinuxONE での OpenShift Container Platform 4.7 のユーザーによってプロビジョニングされるインストールのハイパーバイザーとしてサポートされます。インストール手順については、RHEL KVM を使用したクラスターの IBM Z および LinuxONE へのインストールについて参照してください。
- マルチパス化
- OpenShift Pipelines TP
- OpenShift Service Mesh
- OpenShift Container Platform 4.7 の初回インストールを含む OVN-Kubernetes
- 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
- SCSI ディスク上の z/VM Emulated FBA デバイス

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。

- CodeReady Workspaces
- Developer CLI - odo
- 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)

制限
IBM Z および LinuxONE の OpenShift Container Platform については、以下の制限に注意してください。

- IBM Z 向けの OpenShift Container Platform には、以下のテクノロジープレビューが含まれていません。
  - Precision Time Protocol (PTP) ハードウェア
  - CSI ボリュームスナップショット
- 以下の OpenShift Container Platform 機能はサポートされていません。
  - ログ転送
  - OpenShift Virtualization
  - CodeReady Containers (CRC)
  - OpenShift Metering
  - Multus CNI プラグイン
  - FIPS 暗号
  - etcd に保存されるデータの暗号化
  - 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
  - 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
  - OpenShift Serverless
  - Helm コマンドラインインターフェース (CLI) ツール
  - オーバーコミットの制御およびノード上のコンテナーの密度の管理
  - CSI ボリュームのクローン作成
  - NVMe
  - 4k FCP ブロックデバイス
- ワーカーノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続共有ストレージは、NFS 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。

- これらの機能は、4.7 の IBM Z の OpenShift Container Platform についてのみ利用できます。
  - IBM System Z/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)。

1.3.3.6. IBM Power Systems

本リリースでは、IBM Power Systems は OpenShift Container Platform 4.7 と互換性があります。インストール手順については、IBM Power Systems へのクラスターのインストール、またはネットワークが制限された環境での IBM Power Systems へのクラスターのインストールについて参照してください。

主な機能拡張
以下の新機能は、OpenShift Container Platform 4.7 の IBM Power Systems でサポートされます。

- マルチパス化
- OpenShift Pipelines TP
- OpenShift Service Mesh
- OpenShift Container Platform 4.7 の初回インストールを含む OVN-Kubernetes
- 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
- 4K ディスクのサポート

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

- 現時点で、4 つの Operator がサポートされています。
  - Cluster-Logging-Operator
  - Cluster-NFD-Operator
  - Elastic Search-Operator
  - Local Storage Operator
- Developer CLI - odo
- CodeReady Workspaces
- iSCSI を使用した永続ストレージ
- HostPath

制限
IBM Power Systems の OpenShift Container Platform については、以下の制限に注意してください。

- 以下の OpenShift Container Platform 機能はサポートされていません。
  - OpenShift Metering
  - OpenShift Serverless

- OpenShift Virtualization
- CodeReady Containers (CRC)

- ワーカーノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続ストレージは、ローカルボリューム、Network File System (NFS)、OpenStack Cinder、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。

1.3.4. セキュリティーおよびコンプライアンス

1.3.4.1. ユーザーが所有する OAuth アクセストークンの管理

ユーザーは独自の OAuth アクセストークンを管理できるようになりました。これにより、ユーザーはトークンを確認して、タイムアウトしたか、または不要になったトークンを削除できます。

詳細は、ユーザーが所有する OAuth アクセストークンの管理について参照してください。

1.3.4.2. インストール後の GCP ルート認証情報の削除についての Cloud Credential Operator のサポート

Cloud Credential Operator が Mint モードで使用する GCP の管理者レベルの認証情報を削除したり、ローテーションしたりできるようになりました。このオプションでは、インストール時に管理者レベルの認証情報が必要ですが、認証情報はクラスターに永続的に保存されないため、有効期間を長くする必要はありません。

1.3.4.3. Compliance Operator の CIS Kubernetes ベンチマークプロファイル

Compliance Operator を使用して Center for Internet Security (CIS) Kubernetes ベンチマークチェックを実行できるようになりました。OpenShift Container Platform の CIS プロファイルは CIS Kubernetes チェックに基づいています。

CIS OpenShift Container Platform Benchmark が公開されるまで、『Red Hat OpenShift Container Platform Hardening Guide』を参照してください。

1.3.4.4. インストーラーでプロビジョニングされるクラスターの Secure Boot サポート

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ベアメタルノードで使用する場合に、Secure Boot でクラスターをデプロイできるようになりました。Secure Boot でクラスターをデプロイするには、UEFI ブートモードと Red Fish 仮想メディアが必要です。Secure Boot で自己生成したキーを使用することはできません。

1.3.4.5. Advanced Cluster Management 2.2 の統合

Red Hat Advanced Cluster Management 2.2 が Compliance Operator と統合しました。

1.3.5. ネットワーク

1.3.5.1. OpenShift SDN クラスターネットワークプロバイダーから OVN-Kubernetes クラスターネットワークプロバイダーに移行するためのプラットフォームサポートの拡張

OVN-Kubernetes クラスターネットワークプロバイダーへの移行 は、以下のプラットフォームのインストーラーでプロビジョニングされるクラスターでサポートされます。

- ベアメタルハードウェア
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- Red Hat OpenStack Platform (RHOSP)
- VMware vSphere

1.3.5.2. API サーバー、ロードバランサー、およびノードについてのネットワーク接続のヘルスチェック

クラスターネットワークの接続の問題の診断を容易にするために、Cluster Network Operator (CNO) は接続チェックコントローラーを実行し、クラスターでの接続ヘルスチェックを実行するようになりました。接続テストの結果は、**openshift-network-diagnostics** namespace の **PodNetworkConnectivity** オブジェクトで利用できます。詳細は、エンドポイントへの接続の確認について参照してください。

1.3.5.3. DNS ルールについての OVN-Kubernetes egress ファイアウォールのサポート

egress ファイアウォールルールを設定する際に、IP アドレスの代わりに DNS ドメイン名を使用できるようになりました。OVN-Kubernetes クラスターネットワークプロバイダーの egress ファイアウォール実装への DNS サポートの追加に伴い、同等の機能が OpenShift SDN クラスターネットワークプロバイダーの egress ファイアウォール実装で実行できるようになりました。

1.3.5.4. コンテナー内の DPDK モードの SR-IOV 仮想機能と対話するライブラリー

Data Plane Development Kit (DPDK) モードで SR-IOV Virtual Function (VF) と対話するコンテナーの場合、**app-netutil** ライブラリーは **GetCPUInfo()**、**GetHugepages()**、および **GetInterfaces()** などの機能を提供できるようになりました。詳細は、コンテナーアプリケーションで使用する DPDK ライブラリーについて参照してください。

1.3.5.5. Egress ルーター CNI (テクノロジープレビュー)

egress ルーター CNI プラグインは、テクノロジープレビューとして導入されています。このプラグインを使用して、リダイレクトモードで egress ルーターをデプロイできます。この egress ルーターは、OpenShift SDN に対して OVN-Kubernetes と同等の機能を提供しますが、リダイレクトモードのみに対応します。プラグインは HTTP プロキシーまたは DNS プロキシーモードを実行しません。これは OpenShift SDN の実装と異なる点です。詳細は、リダイレクトモードでの egress ルーター Pod のデプロイについて参照してください。

1.3.5.6. Pod 間の暗号化されたトラフィックについての OVN-Kubernetes IPsec のサポート

クラスターのインストール時に、IPsec を有効にして OVN-Kubernetes クラスターネットワークプロバイダーを設定できます。IPsec を有効にすると、Pod 間のすべてのクラスターネットワークトラフィックは、暗号化された IPsec トンネルで送信されます。クラスターのインストール後に IPsec を有効または無効にすることはできません。

IPsec トンネルは、ホストネットワークを使用するように設定されている Pod 間のネットワークトラフィックには使用されません。ただし、ホストネットワークの Pod から送信され、クラスターネットワークを使用する Pod によって受信されるトラフィックは IPsec トンネルを使用します。詳細は、IPsec 暗号化の設定について参照してください。

1.3.5.7. Red Hat OpenStack Platform (RHOSP) を使用したデプロイメント用の SR-IOV ネットワークポリシーの強化

SR-IOV ネットワーク Operator は、SR-IOV ネットワークノードポリシーのカスタムリソースで追加のフィールドの **spec.nicSelector.netFilter** をサポートするように強化されています。新規フィールドを使用し、ネットワーク ID で RHOSP ネットワークを指定することができます。詳細は、SR-IOV ネットワークデバイスの設定について参照してください。

1.3.5.8. Pod セレクターのないサービスについての RHOSP Kuryr のサポート

RHOSP で実行され、Kuryr を使用するクラスターは、Pod セレクターが指定されていないサービスをサポートするようになりました。

1.3.5.9. HTTP ヘッダー名の調整

レガシーアプリケーションが HTTP ヘッダー名の大文字を認識する場合、Ingress Controller の **spec.httpHeaders.headerNameCaseAdjustments** API フィールドを、修正されるまでレガシーアプリケーションに対応するソリューションに使用します。

OpenShift Container Platform は HAProxy 2.2 に対して更新されます。これはデフォルトで、**Host: xyz.com** を **host: xyz.com** に変更するなど HTTP ヘッダー名を大文字から小文字に変換します。HAProxy 2.2 が利用可能な場合、OpenShift Container Platform をアップグレードする前に、**spec.httpHeaders.headerNameCaseAdjustments** を使用して必要な設定を追加するようにしてください。

1.3.5.10. Kubernetes NMState Operator (テクノロジープレビュー)

OpenShift Container Platform 4.7 は、Kubernetes NMState Operator をテクノロジープレビュー機能として使用し、クラスターノードのセカンダリーネットワークインターフェースで、インストール後のステートドリブンのネットワーク設定を提供します。詳細は、Kubernetes NMState の使用 (テクノロジープレビュー) について参照してください。

注記

設定は、Pod のスケジュール前に行われる必要があります。

1.3.5.11. ネットワークポリシーによるホストネットワーク Ingress コントローラーの選択のサポート

OpenShift SDN または OVN-Kubernetes クラスターネットワークプロバイダーを使用する場合、Ingress コントローラーがクラスターネットワークまたはホストネットワークで実行されるかどうかにかかわらず、ネットワークポリシールールの Ingress コントローラーからトラフィックを選択することができます。ネットワークポリシールールでは、policy **-group.network.openshift.io/ingress=""** namespace セレクターラベルが Ingress コントローラーからのトラフィックに一致します。引き続き **network.openshift.io/policy-group: ingress** namespace セレクターラベルを使用できますが、これは OpenShift Container Platform の今後のリリースで削除できるレガシーラベルです。

OpenShift Container Platform の以前のリリースでは、以下の制限がありました。

- OpenShift SDN 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は、network. **openshift.io/policy-group="ingress"** ラベルを **default namespace** に適用することによってのみ、ホストネットワーク上の Ingress コントローラーからトラフィックを選択できます。
- 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は、ホストネットワーク上の Ingress コントローラーからのトラフィックを選択できませんでした。

詳細は、「ネットワークポリシーについて」を参照してください。

1.3.5.12. ネットワークポリシーによるホストネットワークトラフィックの選択のサポート

OVN-Kubernetes クラスターネットワークプロバイダーまたは OpenShift SDN クラスターネットワークプロバイダーのいずれかを使用する場合は、**policy-group.network.openshift.io/host-network: ""** namespace セレクターを使用して、ネットワークポリシールールでホストネットワークトラフィックを選択できます。

1.3.6. ストレージ

1.3.6.1. CSI ボリュームスナップショットを使用した永続ストレージが一般に利用可能になる

Container Storage Interface (CSI) を使用して、ボリュームスナップショットのサポートを提供する CSI ドライバーを使用する場合にボリュームスナップショットを作成し、復元し、削除することができます。この機能は以前は OpenShift Container Platform 4.4 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 4.7 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、CSI ボリュームスナップショットの使用について参照してください。

1.3.6.2. GCP PD CSI Driver Operator を使用した永続ストレージ (テクノロジープレビュー)

Google Cloud Platform (GCP) 永続ディスク (PD) CSI ドライバーは、GCP 環境に自動的にデプロイされ、管理されるため、ドライバーを手動でインストールしなくてもこれらのボリュームを動的にプロビジョニングできます。このドライバーを管理する GCP PD CSI Driver Operator はテクノロジープレビュー機能としてご利用いただけます。

詳細は、OpenStack Manila CSI Driver Operator について参照してください。

1.3.6.3. OpenStack Cinder CSI Driver Operator を使用した永続ストレージ

CSI を使用して、OpenStack Cinder の CSI ドライバーを使用した永続ボリュームのプロビジョニングを実行できるようになりました。

詳細は、OpenStack Manila CSI Driver Operator について参照してください。

1.3.6.4. vSphere Problem Detector Operator

vSphere Problem Detector Operator は、vSphere 環境にインストールされた OpenShift Container Platform クラスターの機能を定期的にチェックします。vSphere Problem Detector Operator は Cluster Storage Operator によってデフォルトでインストールされ、これを使用して vSphere クラスターで設定およびパーミッションなどの一般的なストレージの問題を迅速に特定し、トラブルシューティングすることができます。

1.3.6.5. Local Storage Operator がカスタムリソースを収集する

Local Storage Operator に must-gather イメージが含まれるようになり、診断目的でこの Operator に固有のカスタムリソースを収集できるようになりました。詳細は、BZ#1756096 を参照してください。

1.3.6.6. AWS EFS (テクノロジープレビュー) 機能の外部プロビジョナーが削除される

Amazon Web Services (AWS) Elastic File System (EFS) テクノロジープレビュー機能が削除され、サポートされなくなりました。

1.3.7. レジストリー

1.3.7.1. Open Container Initiative イメージのサポート

OpenShift Container Platform 内部レジストリーおよびイメージストリームが Open Container Initiative (OCI) イメージに対応するようになりました。OCI イメージは、Docker **schema2** イメージを使用するのと同じ方法で使用できます。

1.3.7.2. 新規イメージストリームメトリクス

クライアントが docker レジストリー v1 プロトコルを使用してイメージストリームのインポートを使用しているかどうかを把握する必要があり、今回の機能拡張で Operator メトリクスを Telemetry にインポートできるようになりました。プロトコル v1 の使用に関連するメトリクスが Telemetry に表示されるようになりました。詳細は、BZ#1885856 を参照してください。

1.3.8. Operator ライフサイクル

1.3.8.1. 安全な Operator のアップグレード

アップグレードをより堅牢にするには、Operator が更新対象のサービスとアクティブに通信することが推奨されます。サービスが OpenShift Virtualization での仮想マシン (VM) のライブマイグレーションやデータベースの復元などの重要な操作を処理している場合、その時点で関連する Operator をアップグレードすることは安全でない可能性があります。

OpenShift Container Platform 4.7 では、 Operator は新規の **OperatorCondition** リソースを利用して、関連するサービスが重要な操作を実行する場合など、アップグレードが不可能な状態を Operator Lifecycle Manager (OLM) に通信できます。アップグレードが不可能な状態は、Operator が操作を終了してアップグレードの準備状態を報告するまで、承認が自動または手動で行われるかにかかわらず、保留中の Operator のアップグレードを遅延します。

OLM によるこの通信チャネルの使用方法についての詳細は、Operator の状態について参照してください。

クラスター管理者による OLM の状態の上書きについての詳細は、Operator 状態の管理について参照してください。

Operator 開発者が通信チャネルを使用するためにプロジェクトを更新する方法についての詳細は、Operator の状態の有効化について参照してください。

1.3.8.2. プルシークレットのカタログソースへの追加

Operator Lifecycle Manager (OLM) によって管理される Operator に関連する特定のイメージが、認証コンテナーイメージレジストリー (プライベートレジストリー) でホストされる場合、OLM および OperatorHub はデフォルトでイメージをプルできません。アクセスを有効にするために、レジストリーの認証情報が含まれるプルシークレットを作成できます。

カタログソースの 1 つ以上のシークレットを参照することで、これらの必要なイメージの一部を OperatorHub で使用するためにプルできますが、他のイメージにはグローバルクラスタープルシークレットまたは namespace スコープのシークレットへの更新が必要です。

詳細は、プライベートレジストリーからの Operator のイメージへのアクセスについて参照してください。

1.3.8.3. Operator カタログのコンテナーのコンテナーイメージレジストリーへのミラーリング

クラスター管理者は **oc adm catalog mirror** コマンドを使用して、Operator カタログのコンテンツをコンテナーイメージレジストリーにミラーリングできます。今回の機能拡張により、**oc adm catalog mirror** コマンドが更新され、操作に使用されるインデックスイメージをレジストリーにもミラーリングできるようになりました。これは以前は **oc image mirror** コマンドを必要とする別のステップで実行されました。詳細は、BZ#1832968 を参照してください。

1.3.8.4. より優れたエクスペリエンスに向けた新たなインストール計画の作成

ユーザー承認を待機している **InstallPlan** オブジェクトを削除すると、Operator のインストールが完了しないため、Operator はリカバリー不可能な状態になります。今回の機能拡張により、Operator Lifecycle Manager (OLM) が更新され、以前に保留されていたものが削除される場合に新規インストール計画が作成されるようになりました。その結果、ユーザーは新規のインストール計画を承認し、Operator のインストールを続行できるようになりました。(BZ#1841175)

1.3.8.5. イメージのローカルファイルへのミラーリングによる非接続レジストリーへのイメージのミラーリング

今回の機能拡張により、**oc adm catalog mirror** コマンドが更新され、イメージをローカルファイルにミラーリングして、イメージの非接続レジストリーへのミラーリングをサポートするようになりました。以下は例になります。

```
$ oc adm catalog mirror <source_registry>/<repository>/<index_image>:<tag> file:///local/index
```

ローカルの **v2/local/index** ディレクトリーを非接続ネットワーク内の場所に移動し、ローカルファイルを非接続レジストリーにミラーリングできます。

```
$ oc adm catalog mirror file:///v2/local/index <disconnected_registry>/<repository>
```

詳細は、BZ#1841885 を参照してください。

1.3.9. Operator の開発

1.3.9.1. Operator SDK が完全にサポートされるようになりました。

OpenShift Container Platform 4.7 の時点で、Operator SDK は完全にサポートされる Red Hat オファリングになりました。Operator SDK v1.3.0 のダウンストリームのリリースにより、Operator SDK の公式にサポートされているツールおよび Operator SDK のブランドツールが Red Hat から直接ダウンロードできるようになりました。

Operator SDK CLI は、Operator の開発者および ISV (独立系ソフトウェアベンダー)パートナーが優れたユーザーエクスペリエンスを提供し、OpenShift ディストリビューションと Operator Lifecycle Manager (OLM) と互換性のある Operator を作成する支援をします。

Operator SDK を使用すると、Kubernetes ベースのクラスター (OpenShift Container Platform など) へのクラスター管理者のアクセスのある Operator の作成者は、Go、Ansible、または Helm をベースに独自の Operator を開発できます。Go ベースの Operator の場合、Kubebuilder はスキャフォールディングソリューションとして SDK に組み込まれます。つまり、既存の Kubebuilder プロジェクトは SDK でそのまま使用でき、引き続き機能します。

以下の機能は、Operator SDK の機能の一部のハイライトです。

Operator Bundle Format のネイティブサポート

Operator SDK には、OpenShift Container Platform 4.6 に導入された Operator Bundle Format のネイティブサポートが含まれます。OLM の Operator をパッケージ化するために必要なすべてのメタデータが自動生成されます。Operator 開発者はこの機能を使用し、OLM および OpenShift ディストリビューションの Operator を CI パイプラインから直接パッケージ化し、テストすることができます。

Operator Lifecycle Manager の統合

Operator SDK は、それぞれの Operator をワークステーションから OLM を使用して簡単にテストできるような単純化されたエクスペリエンスを提供します。**run bundle** サブコマンドを使用して Operator をクラスターで実行し、OLM によって管理される際に Operator が正常に動作するかどうかをテストできます。

Webhook の統合

Operator SDK は OLM を使用した Webhook 統合をサポートします。これは、受付またはカスタムリソース定義 (CRD) 変換 Webhook を持つ Operator のインストールを単純化します。この機能により、クラスター管理者は Webhook を手動で登録し、TLS 証明書を追加し、証明書のローテーションを設定する必要がなくなります。

検証スコアカード

Operator の作成者は、Operator が適切にパッケージ化されていることと、構文エラーがないことを確認する必要があります。Operator を検証するには、Operator SDK で提供されるスコアカードツールを、関連するカスタムリソース (CR) および Operator に必要なすべてのリソースを作成して開始します。スコアカードは、その後に API サーバーへの呼び出しを記録し、一部のテストを実行するために使用されるプロキシーコンテナーを Operator のデプロイメントに作成します。実行されるテストは CR の一部のパラメーターも検査します。

アップグレードの準備状態 **(readiness)** についてのレポート

Operator 開発者は Operator SDK を使用して、OLM へのアップグレードの準備状態についてのレポートを含む、Operator の状態についてのコードのスキャフォールディングサポートを利用できます。

Operator のアップグレードのトリガー

インデックスイメージおよびカタログソースを手動で管理しなくても、Operator SDK で OLM 統合を使用して Operator のアップグレードを迅速にテストできます。**run bundle-upgrade** サブコマンドは、より新しいバージョンのバンドルイメージを指定することにより、インストールされた Operator をトリガーしてそのバージョンにアップグレードするプロセスを自動化します。

注記

Operator SDK v1.3.0 は Kubernetes 1.19 をサポートします。

Operator SDK についての詳細は、Operator の開発について参照してください。

1.3.10. ビルド

buildah バージョンのビルドログへの出力
現在のバージョンでは、OpenShift Container Platform がビルドを実行し、ログレベルが 5 以上である場合、クラスターは buildah バージョン情報をビルドログに書き込みます。この情報は、Red Hat のエンジニアリングチームによるバグレポートの再現に役立ちます。以前のバージョンでは、このバージョン情報はビルドログで利用できませんでした。

ミラーリングの **Cluster Samples Operator** のサポート
OpenShift Container Platform は **imagestreamtag-to-image** という名前の設定マップを **openshift-**

cluster-samples-operator namespace に作成するようになりました。これには、各ストリームタグについてのエントリー、設定されるイメージが含まれます。この設定マップを、イメージストリームがインポートできるようにミラーリングする必要のあるイメージについての参照情報として使用できます。

詳細は、ミラーリングの Cluster Samples Operator のサポート について参照してください。

1.3.11. マシン API

1.3.11.1. AWS で実行されるマシンセットが専有インスタンス (Dedicated Instance) インスタンスをサポートする

AWS で実行されるマシンセットが専有インスタンス (Dedicated Instance) をサポートするようになりました。マシンセット YAML ファイルの **providerSpec** フィールドで専用のテナンシーを指定して専有インスタンス (Dedicated Instance) を設定します。

詳細は、「マシンを専有インスタンス (Dedicated Instance) としてデプロイするマシンセット」を参照してください。

1.3.11.2. GCP で実行されるマシンセットがお客様が管理する暗号化キーをサポート

GCP で実行されるマシンセットのお客様が管理するキーで暗号化を有効できるようになりました。ユーザーは、マシンセット YAML ファイルの **providerSpec** フィールドで暗号化キーを設定できます。この鍵は、顧客のデータの暗号化に使用されず、データ暗号化キーの暗号化に使用されます。

詳細は、「マシンセットの顧客管理の暗号鍵の有効化」を参照してください。

1.3.11.3. マシン API コンポーネントはクラスター全体のプロキシー設定を有効にする

マシン API がクラスター全体のプロキシー設定を有効にするようになりました。クラスター全体のプロキシーが設定されると、すべてのマシン API コンポーネントは設定されたプロキシー経由でトラフィックをルーティングします。

1.3.11.4. 一部のマシン設定の更新により自動再起動が実行されなくなる

Machine Config Operator (MCO) は、以下のマシン設定の変更について対応するすべてのノードを自動的に再起動しなくなりました。

- マシン設定の **spec.config.ignition.passwd.users.sshAuthorizedKeys** パラメーターの SSH キーへの変更
- **openshift-config** namespace でのグローバルプルシークレットまたはプルシークレットへの変更
- **ImageContentSourcePolicy** オブジェクトの追加または編集など、**/etc/containers/registries.conf** ファイルへの変更

詳細は、Machine Config Operator について参照してください。

1.3.11.5. BareMetalHost API によるソフトシャットダウンのサポート

OpenShift Container Platform 4.6 では、BareMetalHost API のオンラインフラグが **false** に設定される場合、Bare Metal Operator はノードを「ハード (hard)」シャットダウンします。 つまり、オペレーティングシステムやワークロードに反応する時間を残さずに電源をオフにします。OpenShift Container Platform 4.7 以降のリリースでは、API はノードのオペレーティングシステムにシャットダウンするシ

グナルを送信してから、ノードが「ソフト (soft)」モードで電源オフになるのを待機します。オペレーティングシステムが 3 分以内にノードをシャットダウンしない場合、Bare Metal Operator は「ハード (hard)」シャットダウンを実行します。

OpenShift Container Platform 4.8 は、ノードに既知の問題がある場合などに、修復の目的で「ハード (hard)」シャットダウンを実行します。修復の目的で「ハード (hard)」シャットダウンを実行する動作は OpenShift Container Platform 4.7 にバックポートされます。

1.3.11.6. マシンのヘルスチェックタイマーの例の更新

マシンヘルスチェックについて で説明されているマシンのヘルスリソースの例は、ヘルスチェックタイマーの値が短くなるように更新されました。

1.3.11.7. 電源ベースの修復が正常に更新しない場合に正常でないノードの再プロビジョニング

OpenShift Container Platform 4.7 以降、電源操作が正常に完了しない場合の電源ベース修復中に、ベアメタルマシンコントローラーは正常でないノードの再プロビジョニングをトリガーします。ノードがマスターノードであるか、外部で以前にプロビジョニングされたノードである場合には、例外になります。

1.3.11.8. クラスター内の新しいホストをプロビジョニングする際の重複する MAC アドレスの診断

クラスターの既存のベアメタルノードの MAC アドレスが、クラスターに追加しようとしているベアメタルホストの MAC アドレスと一致する場合には、クラスターに新規ノードをプロビジョニングする時に、インストールが失敗し、失敗したベアメタルホストの登録エラーが表示されます。

openshift-machine-api namespace で実行されているベアメタルホストを調べることで、重複する MAC アドレスを診断できます。

詳細は、クラスター内の新しいホストをプロビジョニングする際の重複する MAC アドレスの診断 を参照してください。

1.3.12. ノード

1.3.12.1. Descheduler が一般に利用可能になる

Descheduler が一般に利用可能になりました。Descheduler は実行中の Pod をエビクトし、Pod がより適したノードに再スケジュールできるようにします。以下の Descheduler プロファイルのいずれかを有効にすることができます。

- **AffinityAndTaints**: Pod 間の非アフィニティー、ノードアフィニティー、およびノードテイントに違反する Pod をエビクトします。
- **TopologyAndDuplicates**: ノード間で同様の Pod または同じトポロジードメインの Pod を均等に分散できるように Pod をエビクトします。
- **LifecycleAndUtilization**: 長時間実行される Pod をエビクトし、ノード間のリソース使用状況のバランスを取ります。

注記

GA に伴い、Descheduler プロファイルを有効にし、Descheduler の間隔を設定できるようになりました。テクノロジープレビューとして利用可能であったその他の設定は利用できなくなりました。

詳細は、Descheduler を使用した Pod のエビクト について参照してください。

1.3.12.2. スケジューラープロファイル (テクノロジープレビュー)

スケジューラープロファイルを指定して、Pod をノードにスケジュールする方法を制御できます。これは、スケジューラーポリシーを設定する代わりに実行されます。以下のスケジューラープロファイルを利用できます。

- **LowNodeUtilization**: このプロファイルは、ノードごとにリソースの使用量を減らすためにノード間で Pod を均等に分散しようとします。
- **HighNodeUtilization**: このプロファイルは、ノードごとに使用率が高いノード数を最小限に抑えるために、できるだけ少ないノードに可能な限り多くの Pod の配置を試みます。
- **NoScoring**: これは、すべてのスコアプラグインを無効にして最速のスケジューリングサイクルを目指す低レイテンシープロファイルです。これにより、スケジューリングの高速化がスケジューリングにおける意思決定の質に対して優先されます。

詳細は、スケジューラープロファイルを使用した Pod のスケジューリング について参照してください。

1.3.12.3. メモリー使用率の自動スケーリングが一般に利用可能になる

メモリー使用率の自動スケーリングが一般に利用可能になりました。Horizontal Pod Autoscaler カスタムリソースを作成し、直接の値または要求されるメモリーのパーセンテージのいずれかで指定する平均のメモリー使用率を維持するために、デプロイメント設定またはレプリケーションコントローラーに関連付けられた Pod を自動的にスケーリングできます。詳細は、メモリー使用率のための Horizontal Pod Autoscaler オブジェクトの作成について参照してください。

1.3.12.4. RHOSP 上のクラスターのゼロマシンへの自動スケーリング

RHOSP で実行されるクラスターでは、ゼロマシンへの自動スケーリングが可能になりました。

1.3.12.5. 優先順位クラスのプリエンプションを実行しないオプション (テクノロジープレビュー)

preemptionPolicy フィールドを **Never** に設定して、優先順位クラスをプリエンプションを実行しないように設定できます。優先順位クラスの設定のある Pod は、優先順位の低い Pod よりも前のスケジュールキューに置かれますが、これらは他の Pod のプリエンプションは実行しません。

詳細は、プリエンプションは実行しない優先順位クラス について参照してください。

1.3.12.6. CRI-O を使用したノードホストプロセスの CPU の指定

CRI-O は、ノードホストプロセスの CPU の指定に対応するようになりました (kubelet、CRI-O など)。**crio.conf** ファイルで **infra_ctr_cpuset** パラメーターを使用すると、ノードホストプロセスの CPU を予約できます。これにより、Guaranteed CPU を必要とする OpenShift Container Platform Pod

が他のプロセスがそれらの CPU で実行されない状態で動作できるようになります。Guaranteed CPU を要求する Pod は、ノードホストプロセスと CPU 時間について競合する必要はありません。詳細は、BZ#1775444 を参照してください。

1.3.13. Red Hat OpenShift Logging

クラスターロギングが **Red Hat OpenShift Logging** に
今回のリリースにより、**Cluster Logging** は **Red Hat OpenShift Logging** バージョン 5.0 になりました。詳細は、『Red Hat OpenShift Logging 5.0 リリースノート 』を参照してください。

1.3.14. モニタリング

1.3.14.1. アラートルールの変更

OpenShift Container Platform 4.7 には、以下のアラートルールの変更が含まれます。

例1.1 アラートルールの変更

- **AlertmanagerClusterCrashlooping** アラートが追加されました。重大なアラートは、クラスター内の Alertmanager インスタンスの半分以上がクラッシュループしている場合に通知を出します。
- **AlertmanagerClusterDown** アラートが追加されました。重大なアラートは、クラスター内の Alertmanager インスタンスの半分以上が停止している場合に通知を出します。
- **AlertmanagerClusterFailedToSendAlerts** アラートが追加されました。重大なアラートは、クラスター内のすべての Alertmanager インスタンスが通知の送信に失敗した場合に通知を出します。
- **AlertmanagerFailedToSendAlerts** アラートが追加されました。警告のアラートは、Alertmanager インスタンスが通知の送信に失敗した場合に通知を出します。
- **etcdBackendQuotaLowSpace** アラートが追加されました。重大なアラートは、etcd クラスターのデータベースのサイズが etcd インスタンスで定義されるクォータを超える場合に通知を出します。
- **etcdExcessiveDatabaseGrowth** アラートが追加されました。警告アラートは、4 時間の間に etcd インスタンスのデータベースのサイズの 50% の増加を生じさせる etcd 書き込み増加が観察される場合に通知を出します。
- **etcdHighFsyncDurations** アラートが追加されました。重大なアラートは、etcd クラスターの 99 番目のパーセンタイルの **fsync** 期間が高すぎる場合に通知を出します。
- **KubeletClientCertificateRenewalErrors** アラートが追加されました。警告アラートは、Kubelet がそのクライアント証明書の更新に失敗した場合に通知を出します。
- **KubeletServerCertificateRenewalErrors** アラートが追加されました。警告アラートは、Kubelet がそのサーバー証明書の更新に失敗した場合に通知を出します。
- **NTODegraded** アラートが追加されました。警告アラートは、Node Tuning Operator のパフォーマンスが低下する場合に通知を出します。
- **NTOPodsNotReady** アラートが追加されました。警告アラートは、ノード上の特定の Pod が準備状態にない場合に通知を出します。

- **PrometheusOperatorNotReady** アラートが追加されました。警告アラートは、Prometheus Operator インスタンスが準備状態にない場合に通知を出します。
- **PrometheusOperatorRejectedResources** アラートが追加されました。警告アラートは、特定のリソースが Prometheus Operator によって拒否される場合に通知を出します。
- **PrometheusOperatorSyncFailed** アラートが追加されました。警告アラートは、Prometheus Operator のコントローラーが特定オブジェクトの調整に失敗した場合に通知を出します。
- **PrometheusTargetLimitHit** アラートが追加されました。警告アラートは、一部の収集設定がターゲットの制限を超えるために Prometheus がターゲットをドロップした場合に通知を出します。
- **ThanosSidecarPrometheusDown** アラートが追加されました。重大アラートは、Thanos サイドカーが Prometheus に接続できないことを示す通知を出します。
- **ThanosSidecarUnhealthy** アラートが追加されました。重大アラートは、Thanos サイドカーが指定された期間に正常ではないことを示す通知を出します。
- **NodeClockNotSynchronising** が更新され、chrony タイムサービス **chronyd** を使用する環境での誤検知 (false positive) の発生を防ぐようになりました。
- **NodeNetworkReceiveErrs** アラートが更新され、レポートされるエラーの数が少ない場合にアラートが実行されなくなりました。ルールは、エラーの絶対数ではなく、パケットの合計に対するエラーの割合を使用します。
- **NodeNetworkTransmitErrs** アラートが更新され、レポートされるエラー数が少ない場合にアラートが実行されなくなりました。ルールは、エラーの絶対数ではなく、パケットの合計に対するエラーの割合を使用します。
- 重大度が warning および critical の **etcdHighNumberOfFailedHTTPRequests** アラートが削除されます。これらのアラートは、etcd インスタンスで高い割合の HTTP 要求が失敗する場合に実行されます。

注記

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

1.3.14.2. 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更新

OpenShift Container Platform 4.7 には、以下のモニタリングスタックコンポーネントおよび依存関係に対するバージョンの更新が含まれます。

- Prometheus Operator: バージョン 0.44.1
- Thanos: バージョン 0.17.2

1.3.14.3. Prometheus Operator の AlertmanagerConfig CRD はサポートされない

Prometheus Operator の **AlertmanagerConfig** カスタムリース定義 (CRD) を使用した Alertmanager 設定の変更はサポートされません。

詳細は、モニタリングのサポートに関する考慮事項について参照してください。

1.3.14.4. 新規 API パフォーマンスモニタリングダッシュボード

API Performance ダッシュボードが Web コンソールから利用できるようになりました。このダッシュボードは、Kubernetes API サーバーまたは OpenShift API サーバーのパフォーマンス問題のトラブルシューティングを行う際に使用できます。**Monitoring → Dashboards** に移動し、**API Performance** ダッシュボードを選択して、Web コンソールの **Administrator** パースペクティブから **API Performance** ダッシュボードにアクセスできます。

このダッシュボードは、以下のような API サーバーメトリクスを提供します。

- 要求期間
- 要求レート
- 要求の終了
- 進行中 (in flight) の要求
- 中止された要求
- etcd 要求期間
- etcd オブジェクト数
- 長時間実行される要求
- 応答ステータスコード
- 応答サイズ
- 優先順位およびフェアネス (fairness)

1.3.14.5. Grafana で namespace (Pod) および Pod Kubernetes ネットワークダッシュボードが有効にされる

Grafana で **Namespace (Pods)** および **Pod** Kubernetes ネットワークダッシュボードが有効にされました。**Monitoring → Dashboards → Grafana UI** の順に移動し、Web コンソール の **Administrator** パースペクティブから **Namespace (Pod)** および **Pod** ダッシュボードにアクセスできます。

これらのダッシュボードは、以下のようなネットワークのメトリクスを提供します。

- namespace ごとまたは Pod ごとに受信される現在のバイト数のレート。
- namespace ごとまたは Pod ごとに送信される現在のバイト数のレート
- 受信される帯域幅
- 送信される帯域幅
- 受信パケットのレート
- 送信パケットのレート
- 受信されたパケットのレート

- 送信パケットのドロップレート

1.3.14.6. ベアメタルクラスターについてのハードウェア Telemetry の HWMon データ収集

HWMon データ収集は、ベアメタルクラスターの CPU 温度やファン回転数などのハードウェアのヘルス Telemetry について有効にされます。

1.3.14.7. Thanos Querier のログレベル設定フィールド

デバッグなどの目的で、Thanos Querier の **logLevel** フィールドを設定できるようになりました。

1.3.14.8. ユーザー定義プロジェクトのモニタリングについてのメモリー制限を config-reloader コンテナーで削除する

Prometheus および Thanos Ruler Pod について、メモリー制限が **openshift-user-workload-monitoring** namespace の **config-reloader** コンテナーで削除されました。今回の更新により、**config-reloader** コンテナーの OOM による強制終了が発生しなくなりました。この強制終了は、以前はコンテナーが定義された制限よりも多くのメモリーを使用する場合に発生しました。

1.3.14.9. 独自のサービスをモニタリングするための非推奨のテクノロジープレビュー設定が削除される

ユーザーの独自のサービスのモニタリングを可能にする以前のテクノロジープレビュー設定は削除され、OpenShift Container Platform 4.7 でサポートされなくなりました。**techPreviewUserWorkload** フィールドは **cluster-monitoring-config ConfigMap** オブジェクトから削除され、サポートされなくなりました。

ユーザー定義プロジェクトのモニタリングについての詳細は、モニタリングスタックについて参照してください。

1.3.15. スケーリング

1.3.15.1. クラスターの最大数

OpenShift Container Platform 4.7 のクラスターの最大値に関するガイダンスが更新されました。

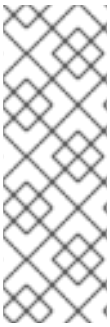
ご使用の環境のクラスター制限を見積もるには、OpenShift Container Platform Limit Calculator を使用できます。

1.3.15.2. Intel vRAN Dedicated Accelerator ACC100 でのデータプレーンのパフォーマンスの最適化

OpenShift Container Platform 4.7 は、ワイヤレス FEC Accelerator の OpenNESS SR-IOV Operator をサポートします。

この Operator は、低電力、低コスト、低レイテンシーを実現する vRAN デプロイメントの要件をサポートし、さまざまなユースケースでパフォーマンスの上下を管理する機能も提供します。最もコンピュート集中型の 4G および 5G ワークロードの 1 (L1) forward error correction (FEC) の 1 つで、信頼できないまたはノイズのある通信チャネルにおけるデータ送信エラーを解決します。

5G の使用が増え、5G ネットワークに依存するユーザーが増加するにつれ、5G レベルの高パフォーマンスを維持するには高パフォーマンス FEC を提供することが極めて重量です。FEC は、Wireless FEC Accelerator 用の OpenNESS SR-IOV Operator を使用した Intel vRAN Dedicated Accelerator ACC100 カードでサポートされるようになりました。



注記

ワイヤレス FEC Accelerator の OpenNESS SR-IOV Operator は OpenShift Container Platform 4.7.8 でサポートされます。異なる OpenShift Container Platform バージョンが必要な場合には、Intel® Premier Support Access または openness.n3000.operator@intel.com のプレミアサポートポータルから Intelにお問い合わせください。

詳細は、OpenNESS Operator for Wireless FEC Accelerators を参照してください。

詳細は、Intel vRAN Dedicated Accelerator ACC100 でのデータプレーンパフォーマンスの最適化 を参照してください。

1.3.15.3. テストによる CPU レイテンシーの判別

CNF-test コンテナーの一部であるレイテンシーテストでは、分離された CPU レイテンシーが要求される上限を下回るかどうかを測定する方法を提供します。

レイテンシーテストの実行に関する詳細は、 レイテンシーテストの実行について参照してください。

1.3.15.4. Performance Addon Operator の新規の globalDisableIrqLoadBalancing 機能により、Guaranteed Pod の CPU についてグローバルデバイス割り込み処理を無効にできます。

Performance Addon Operator は、それらをクラスターおよびオペレーティングシステムのハウスキーピング用の予約された CPU に分割し、ワークロード用に分離された CPU を管理します。新規のパフォーマンスプロファイルフィールドの **globallyDisableIrqLoadBalancing** は、分離された CPU セットでデバイス割り込みが処理されるかどうかを管理するために使用できます。

新規 Pod アノテーションの **irq-load-balancing.crio.io** および **cpu-quota.crio.io** は、Pod についてデバイス割り込みが処理されるかどうかを定義するために **globallyDisableIrqLoadBalancing** と共に使用されます。CRI-O は (設定されている場合)、Pod が実行されている場合にのみデバイス割り込みを無効にします。

詳細は、Guaranteed Pod の分離された CPU のデバイス割り込み処理の管理 について参照してください。

1.3.15.5. 新しい VRF CNI プラグインにより、セカンダリーネットワークを VRF に割り当てることができます。

追加のネットワークの VRF への割り当てを可能にする新規の VRF CNI プラグインが利用可能になりました。CNO カスタムリソースの **rawConfig** 設定を使用してセカンダリーネットワークを作成し、その VRF を設定する場合、Pod に作成されるインターフェースは VRF に関連付けられます。さらに、VRF CNI プラグインを使用して SR-IOV ネットワークを VRF に割り当てることもできます。

詳細は、「セカンダリーネットワークの VRF への割り当て」および「SR-IOV ネットワークの VRF への割り当て」を参照してください。

1.3.15.6. xt_u32 エンドツーエンドテストが CNF について有効にされる

XT_u32 は iptables カーネルモジュールであり、任意のコンテンツに基づいてパケットのフィルタリングを可能にします。ヘッダー以外に、他の iptables モジュールでは対応していない特殊なプロトコルなどを確認できます。

詳細は、プラットフォーム検証のエンドツーエンドテストの実行について参照してください。

1.3.16. Insights Operator

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

OpenShift Container Platform 4.7 では、Insights Operator は以下の追加情報を収集します。

- 無効な Operator Lifecycle Manager (OLM) インストールを特定するための上位 100 の **InstallPlan** エントリー
- Kubernetes のデフォルト namespace および **openshift*** の組み込み namespace からのサービスアカウント
- コンテナーストレージ制限を確認するための **ContainerRuntimeConfig** および **MachineConfigPools** 設定ファイル
- 非管理状態の Operator を特定するための、利用可能なすべての **operator.openshift.io** コントロールペインリソースの設定ファイル
- **netID** および egress IP アドレスを含む **NetNamespaces** 名
- バージョン情報を含む、インストールされた Operator Lifecycle Manager Operator の一覧
- **openshift-image-registry** 設定で使用される場合の永続ボリュームの定義
- **openshift-apiserver-operator** namespace の Pod の特定ログエントリーの表示
- **openshift-sdn** namespace の **sdn** Pod の特定ログエントリーの表示

この追加情報により、Red Hat は、Red Hat OpenShift Cluster Manager で改善された修復手順を提供できるようになりました。

1.3.17. 認証および認可

1.3.17.1. 認証情報の AWS Security Token Service (STS) を使用した OpenShift Container Platform の実行 (テクノロジープレビュー)

Cloud Credential Operator (CCO) を Amazon Web Services Security Token Service (AWS STS) を使用するように設定できます。CCO が STS を使用するように設定されている場合、短期的で限定的なセキュリティー認証情報を提供する IAM ロールをコンポーネントに割り当てます。

詳細は、Amazon Web Services Secure Token Service (AWS STS) のサポート について参照してください。

1.3.18. マシン管理

1.3.18.1. ベアメタルクラスターの電源ベースのヘルスチェックによる修復

インストーラーでプロビジョニングされるインフラストラクチャー (IPI) を使用してインストールされるベアメタルの電源ベースの修復が利用できるようになりました。**MachineHealthCheck** CR を設定して、ノードの再プロビジョニングではなく、電源サイクルをもとにする、電源ベースの修復をトリガーできます。

この修復は、ベアメタル環境でステートフルワークロードとコンピュート容量を復元する時間を大幅に短縮します。詳細は、ベアメタルの電源ベースの修復について を参照してください。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.7 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。

Operator Lifecycle Manager が Kubernetes 1.20 を使用するように更新される
Operator Lifecycle Manager (OLM) は、Kubernetes リリースが利用可能になる時点でその最新リリースに対応します。OLM が提供する **ClusterServiceVersion** (CSV) リソースは数多くのコア Kubernetes リソースで構成されます。OLM が Kubernetes の依存関係を増やすと、埋め込まれたリソースも更新されます。

OpenShift Container Platform 4.7 の時点で、OLM とその関連付けられたコンポーネントが Kubernetes 1.20 を使用するように更新されています。通常、Kubernetes にはこれまでのいくつかのバージョンとの後方互換性があります。Operator の作成者は互換性を維持し、更新されたリソースを活用するために、プロジェクトを最新の状態に維持することが推奨されます。

後方互換性の保証についての詳細は、「OpenShift Container Platform のバージョン管理ポリシー」を参照してください。

アップストリーム Kubernetes プロジェクトのバージョン差異についてのポリシーの詳細は、Kubernetes ドキュメントを参照してください。

スケジューラーで Pod トポロジー分散制約が使用されるように
OpenShift Container Platform 4.7 のデフォルトスケジューラーは、Pod トポロジー分散制約を使用して Pod の配置を制御するようになりました。Pod レプリカを適切に分散するために、ノードに必要なラベルがあることを確認します。

注記

デフォルトで、スケジューラーは **kubernetes.io/hostname** および **topology.kubernetes.io/zone** ノードラベルが必要です。ノードがこれらのラベルを使用しない場合は、デフォルトの制約ではなく、独自の Pod トポロジー分散制約を定義します。

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

1.5. 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、または削除されました。

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 4.7 で非推奨となり、削除された主な機能の最新の一覧については、以下の表を参照してください。非推奨になったか、または削除された機能の詳細情報は、表の後に記載されています。

以下の表では、機能は以下のステータスでマークされています。

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

表1.1 非推奨および削除機能のトラッカー

機能	OCP 4.5	OCP 4.6	OCP 4.7
OperatorSource オブジェクト	DEP	REM	REM
Package Manifest Format (Operator Framework)	DEP	DEP	DEP
oc adm catalog build	DEP	DEP	DEP
oc adm catalog mirror の **--filter-by-os** フラグ	GA	GA	DEP
v1beta1 CRD	DEP	DEP	DEP
Docker Registry v1 API	GA	DEP	DEP
メータリング Operator	GA	DEP	DEP
スケジューラーポリシー	GA	GA	DEP
Cluster Samples Operator の **ImageChangesInProgress** 状態	GA	GA	DEP
Cluster Samples Operator の **MigrationInProgress** 状態	GA	GA	DEP
OpenShift Container Platform リソースの **apiVersion** での **v1** の使用	GA	GA	DEP
独自の RHEL 7 コンピュートマシンの持ち込み	GA	DEP	DEP
AWS EFS の外部プロビジョナー	REM	REM	REM

1.5.1. 非推奨の機能

1.5.1.1. スケジューラーポリシー

スケジューラーポリシーを使用して Pod 配置を制御することは非推奨となり、今後のリリースで削除される予定です。テクノロジープレビューの代替オプションについての詳細は、「スケジューラープロファイルを使用した Pod のスケジューリング」を参照してください。

1.5.1.2. filter-by-os フラグを使用したカタログのミラーリング

以前のバージョンでは、**oc adm catalog mirror** コマンドを使用してカタログをミラーリングする場合、**--filter-by-os** フラグはミラーリングされたコンテンツのアーキテクチャーをフィルターできました。これにより、マニフェストではなくマニフェストの一覧を参照するカタログのそれらのイメージへの参照が破損しました。**--filter-by-os** フラグは、プルおよび展開されるインデックスイメージのみをフィルターするようになりました。明確化するために、新規の **--index-filter-by-os** フラグが追加され、これを代わりに使用する必要があります。

--filter-by-os フラグは非推奨になりました。

1.5.1.3. Cluster Samples Operator の ImageChangesInProgress 状態

イメージストリームイメージのインポートは、Cluster Samples Operator 設定リソースの状態別にリアルタイムで追跡されなくなりました。進行中のイメージストリームは、**ClusterOperator** インスタンスの **openshift-samples** への更新に直接影響を与えなくなりました。イメージストリームに関連する長いエラーが Prometheus アラートによって報告されるようになりました。

1.5.1.4. Cluster Samples Operator の MigrationInProgress 状態

アップグレードの追跡は、他の状態で実行でき、個別のイメージストリーム設定マップと **imagestream-to-image** 設定マップの両方を使用できます。

1.5.1.5. OpenShift Container Platform リソースに apiVersion の v1 を使用する

現時点で、**oc** は YAML または JSON リソースの **apiVersion** を **v1** からオブジェクトの正しい値に修正します。たとえば、**v1** は **DeploymentConfig** オブジェクトの **apps.openshift.io/v1** に修正されます。この動作は非推奨となり、今後のリリースで削除される予定です。***.openshift.io** が含まれるすべてのリソースが API インデックス にある **apiVersion** 値と一致している必要があります。

今回のリリースにより、オブジェクトにない場合に **apiVersion** の正しい値が表示する警告が追加されました。

```
Using non-groupfied API resources is deprecated and will be removed in a future release, update apiVersion to "apps.openshift.io/v1" for your resource
```

このメッセージが表示されたら、リソースファイルを更新して正しい値を使用してください。

1.5.2. 削除された機能

1.5.2.1. インストーラーでプロビジョニングされるクラスターには provisioningHostIP または bootstrapProvisioningIP が不要になる

ベアメタルノードでインストーラーでプロビジョニングされるインストールを使用する場合、OpenShift Container Platform 4.6 では、**provisioning** ネットワークなしでデプロイされる際に、**baremetal** ネットワークからの 2 つの IP アドレスを **provisioningHostIP** および **bootstrapProvisioningIP** 設定に提供する必要がありました。ベアメタルノードで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、**provisioning** ネットワークなしでデプロイする場合、これらの IP アドレスおよび設定は OpenShift Container Platform 4.7 で不要になりました。

1.5.2.2. サンプルイメージストリームから削除されたイメージ

以下のイメージは、OpenShift Container Platform で提供されるサンプルイメージストリームに含まれなくなりました。

```
registry.redhat.io/ubi8/go-toolset:1.13.4
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.8.1
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.8.0
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.8.1
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.8.1
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.8.1
```

```
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.8.1
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.8.0
```

1.5.2.3. oc 項目の削除

今回のリリースにより、**oc** で使用される以下の項目が削除されました。

- **--config** オプション。
- **OC_EDITOR** 環境変数。
- **convert** サブコマンド。

1.5.2.4. AWS EFS (テクノロジープレビュー) 機能の外部プロビジョナーが削除される

Amazon Web Services (AWS) Elastic File System (EFS) テクノロジープレビュー機能が削除され、サポートされなくなりました。

1.6. バグ修正

api-server-auth

- 以前のバージョンでは、**openshift-service-ca** namespace には **openshift.io/run-level: 1** のラベルが付けられました。これにより、この namespace の Pod は追加の権限で実行されました。このラベルは削除され、この namespace の Pod は適切な権限で実行されるようになりました。(BZ#1806915)
- 以前のバージョンでは、**openshift-service-ca-operator** namespace に **openshift.io/run-level: 1** のラベルが付けられました。これにより、この namespace の Pod は追加の権限で実行されました。新規インストールの場合にこのラベルは削除され、この namespace の Pod は適切な権限で実行されるようになりました。アップグレードされたクラスターの場合、このラベルを手動で削除し、影響を受ける Pod を再起動することができます。(BZ#1806917)
- 以前のバージョンでは、**openshift-oauth-apiserver** namespace の OAuth API サーバー Pod を収集するための設定がなく、OAuth API サーバー Pod のメトリクスは Prometheus でクエリーできませんでした。不足している設定が追加され、OAuth API サーバーメトリクスが Prometheus で利用可能になりました。(BZ#1887428)
- 以前のバージョンでは、Cluster Authentication Operator コードの満たされていない条件により、ログが実際に実行されていないデプロイメントに対する更新についてのメッセージで一杯になりました。Operator のステータスを更新するかどうかを判断するためのロジックが更新され、Cluster Authentication Operator ログで実際に生じていないデプロイメント更新についてのメッセージを受信しなくなりました。(BZ#1891758)
- 以前のバージョンでは、Cluster Authentication Operator は **cluster** という名前の設定リソースのみを監視しました。これにより、Operator は **default** という名前の Ingress 設定の変更を無視しました。これにより、Ingress がカスタムノードセレクターで設定されている場合にスケジュール可能なワーカーノードがないと誤って仮定されました。Cluster Authentication Operator は名前に関係なくすべてのリソースを監視し、Operator は適切に Ingress 設定の変更を監視し、ワーカーノードの可用性を調整するようになりました。(BZ#1893386)

ベアメタルハードウェアのプロビジョニング

- 以前のバージョンでは、一部のシステムでは、インストーラーは準備状態になり、失敗する前に Ironic と通信しました。今回のリリースでは、これは発生しなくなりました。(BZ#1902653)

- 以前のバージョンでは、Dell システムで仮想メディアを使用する場合に、仮想メディアは、デプロイメントを開始する前にすでに割り当てられていると失敗する可能性がありました。これが生じると、Ironic が再試行するようになりました。(BZ#1910739)

- 以前のバージョンでは、マスターノードはプロビジョニングインターフェースの IPv6 リンクローカルアドレスを失い、これにより、プロビジョニングが IPv6 で機能しなくなりました。この発生を防ぐために、回避策が **toggle addr_gen_mode** に追加されました。(BZ#1909682)

- 以前のバージョンでは、**cluster-baremetal-operator** は誤ったロギングライブラリーを使用していました。この問題により、コマンドライン引数が他の Operator と一貫性がなく、すべての Kubernetes ライブラリーのログが記録される訳ではありませんでした。この問題は、ロギングライブラリーの切り替えにより修正されています。(BZ#1906143)

- インターフェースで IPv6 を使用する場合、一定の時間が経過すると、Network Manager はリンクローカル IPv6 アドレスを削除します。この問題により、IPv6 リンクローカルアドレスの削除後に PXE ブートがノードに対して失敗しました。インターフェース IPv6 addr_gen_mode を切り替えるための回避策が追加され、リンクローカルアドレスが再び追加されるようになりました。(BZ#1901040)

- 以前のバージョンでは、Supermicro ノードは、ディスクへのデプロイメントに成功すると再起動時に PXE に対してブートしました。この問題は、**BootSourceOverrideTarget** の設定時に **BootSourceOverrideEnabled** を常に設定することにより修正されました。Supermicro ノードがデプロイメント後に永続的にディスクに対して起動するようになりました。(BZ#1918558)

- **baremetal** IPI に同梱されるサービスエージェントイメージは、UEFI セキュアブートが有効にされたシステムで実行できるようになりました。ネットワークブートはセキュアなブートと互換性がないため、この場合は仮想メディアを使用する必要があります。(BZ#1893648)

- ノードの自動検出は **baremetal** IPI で有効にされなくなりました。これは適切に処理されず、ベアメタルホストの登録の重複が発生しました。(BZ#1898517)

- 以前のバージョンでは、syslinux-nonlinux パッケージは、ベアメタルのプロビジョニングイメージに含まれていませんでした。このため、BIOS ブートモードを使用するマシンへの仮想メディアのインストールは失敗しました。パッケージはイメージに含まれるようになりました。(BZ#1862608)

- 以前のバージョンでは、一部の Dell ファームウェアバージョンは、Redfish PowerState を誤って報告していました。Dell iDRAC ファームウェアをバージョン 4.22.00.53 に更新すると、問題は解決されます。(BZ#1873305)

- 以前のバージョンでは、Redfish は BIOS 設定値の取得や設定が可能なインターフェース一覧にはありませんでした。そのため、BIOS 設定で Redfish を使用することはできませんでした。Redfish が一覧に含まれているようになり、BIOS 設定で使用できるようになりました。(BZ#1877105)

- 以前のバージョンでは、BIOS 設定の設定に使用する Redfish インターフェースが適切に実装されませんでした。その結果、Dell iDRACs は BIOS 設定値を設定できませんでした。実装エラーが修正されました。Redfish インターフェースは BIOS 設定を設定できるようになりました (BZ#1877924)。

- 以前のバージョンでは、Supermicro が IPMI で ートデバイスの設定を処理する方法の違いにより、イメージがディスクに書き込まれた後に IPMI および UEFI を使用する Supermicro ノードが失敗しました。Supermicro ノードが適切な IPMI コードを渡して、ディスクから起動するよ

うになりました。その結果、デプロイメント後に Supermicro ノードが正しくディスクから起動されるようになりました。(BZ#1885308)

- 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のベアメタルインストールは、無効なルートデバイスのヒントが提供される場合でも、警告なしでイメージの書き込みを省略しなくなりました。(BZ#1886327)

- 以前のバージョンでは、Supermicro ノードのブートモード情報が不完全であるために、Redfish を使用したデプロイメントが失敗しました。ブートモード情報が含まれるようになりました。これにより、Redfish を使用して Supermicro ノードをデプロイすることができます。(BZ#1888072)

- 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に組み込まれた Ironic API サービスは、8 つのワーカーではなく 4 つのワーカーを使用するようになりました。その結果、RAM の使用率が減少します。(BZ#1894146)

ビルド

- 以前のバージョンでは、Dockerfile ビルドは **/etc/pki/ca-trust** ディレクトリーのパーミッションを変更したり、その中にファイルを作成したりすることができませんでした。この問題は、バージョン 4.6 の BZ#1826183 の修正によって生じました。この修正により、ビルドの CA を含む HTTPS プロキシーのサポートが追加され、**/etc/pki/ca-trust** が常にマウントされました。その結果、独自の CA を含むビルドや、システムの信頼ストアを変更したビルドがランタイム時に適切に機能できなくなりました。現在のリリースでは、この問題はバグ 1826183 を元に戻すことで修正されています。独自の CA を含むビルダーイメージが再び機能するようになりました。(BZ#1891759)

- 以前のバージョンでは、OpenShift Container Platform バージョン 4.5 からバージョン 4.6 にアップグレードした後に、ビルドはソースコードのプルに使用された Git 設定にプロキシー情報を追加していないため、プライベートリポジトリーからの **git clone** の実行に失敗しました。そのため、クラスターがグローバルプロキシーを使用し、ソースがプライベート Git リポジトリーからプルされた場合、ソースコードはプルできませんでした。Git は、クラスターがグローバルプロキシーを使用する場合に適切に設定され、**git clone** コマンドはクラスターがグローバルプロキシーを使用する場合にプライベート Git リポジトリーからソースコードをプルできるようになりました。(BZ#1896446)

- 以前のバージョンでは、ノードのプルシークレット機能は機能しませんでした。**forcePull: true** が Source および Docker ストラテジービルドに設定されている場合、ノードのプルシークレットは使用されませんでした。そのため、ビルドはクラスター全体のプルシークレットを必要とするイメージのプルに失敗しました。ノードのプルシークレットはユーザーによって提供されるプルシークレットと常にマージされるようになりました。その結果、ビルドは **forcePull: true** が設定されている場合にイメージをプルでき、ソースレジストリーにはクラスター全体のプルシークレットが必要になります。(BZ#1883803)

- 以前のバージョンでは、OpenShift Container Platform のビルドは、Git SCP 形式の SSH の場所に対応しない Golang URL の解析により、SCP 形式の SSH の場所が指定されている場合に **git clone** で失敗しました。その結果、OpenShift Container Platform ビルドおよび S2I (Source-to-Image) は、それらのタイプのソース URL が指定されていると失敗しました。今回のリリースより、ビルドおよび S2I は Golang URL の解析をバイパスし、 **ssh://** プレフィックスを取り除き、Git SCP 形式の SSH の場所に対応するようになりました (BZ#1884270)

- 以前のバージョンでは、認証キーが base64 でエンコードされていない無効なビルドプルシークレットによって生じるビルドエラーは、ビルドスタックで伝播されませんでした。そのため、これらのエラーの根本的な原因を特定することは困難でした。現在のリリースではこの問題は修正され、これらのタイプのビルドエラーはビルドスタックで伝播されるようになりました。ユーザーが無効なビルドプルシークレットキーの根本的な原因を判別することがより容易になりました。(BZ#1918879)

クラウドコンピュート

- 以前のバージョンでは、マシン API は認証情報シークレットが無効な場合にユーザーにフィードバックを提供しないため、クラウドプロバイダーの認証情報に問題がある場合の診断が困難でした。マシンセットの作成時または更新時に認証情報に問題がある場合（認証情報のシークレットが存在しないか、またはフォーマットが正しくない場合など）にユーザーに警告が表示されるようになりました。(BZ#1805639)

- 以前のバージョンでは、ベアメタルアクチュエーターは、**Machine** オブジェクトも削除して基礎となるホストを削除しましたが、これはマシンコントローラーの意図される操作ではありません。今回の更新により、ホストの検索に失敗した場合に **InsufficientResourcesMachineError** エラーの理由をマシンに設定し、ホストのないマシンが最初にスケールダウンされるようになりました。マシンは、ホストのプロビジョニング解除時に **Failed** フェーズに移行します。マシンヘルスチェックが失敗したマシンを削除し、**Machine** オブジェクトは自動的に削除されなくなりました。(BZ#1868104)

- 以前のバージョンでは、マシンが **Failed** 状態になると、クラウドプロバイダーの状態は調整されませんでした。マシンのステータスでは、仮想マシンを削除できる場合に、削除後にクラウド仮想マシンの状態を **Running** と報告しました。マシンのステータスは、マシンが **Failed** 状態にある場合にクラウド仮想マシンの観察される状態を **Unknown** と、より正確に反映するようになりました。(BZ#1875598)

- 以前のバージョンでは、複数のマシン API カスタムリソース定義に、対応する参照ドキュメントに対するテンプレートスキーマの説明に破損したリンクが含まれていました。リンクが正しいアップストリームの場所に対して更新され、破損しなくなりました。(BZ#1876469)

- 以前のバージョンでは、コマンドの **oc explain Provisioning** は、古いバージョンの CRD 定義が使用されているためにカスタムリソース定義 (CRD) の説明を返しませんでした。CRD バージョンが更新され、**Provisioning** CRD の **oc explain** で予想される情報を返すようになりました。(BZ#1880787)

- 以前のバージョンでは、ユーザーがディスクサイズが推奨される最小サイズよりも小さいマシンの作成または更新を行う場合、ディスクサイズが低レベルの状態にあると、マシンは警告なしに起動に失敗しました。ディスクサイズは初期のイメージサイズよりも大きくなければなりません。ユーザーには、ディスクサイズのレベルが低下しており、これによりマシンまたはマシンセットが起動しない可能性があることを示す警告が通知されるようになりました。(BZ#1882723)

- 以前のバージョンでは、マシンの状態が調整時に永続化されませんでした。そのため、**Machine** オブジェクトの **instance-state** アノテーションと **providerStatus.instanceState** には異なる値が表示されることがありました。マシンの状態が調整されたマシンで複製され、**instance-state** アノテーションが **providerStatus.instanceState** の値に一致するようになりました。(BZ#1886848)

- 以前のバージョンでは、**publicIP** オプションが **MachineSet** リソースオブジェクトで true に設定されている場合に、非接続環境の Microsoft Azure で実行されるマシンセットは起動とスケーリングに失敗しました。今回のリリースより、マシンの防ぐために、ユーザーは無効な **publicIP** 設定で、非接続環境のマシンセットを作成できなくなりました。(BZ#1889620)

- 以前のバージョンでは、マシンの作成時に、特定のエラーのみが **mapi_instance_create_failed** の失敗メトリクスの更新を生じさせました。マシンの作成において発生するすべてのエラーが **mapi_instance_create_failed** メトリクスを適切に増分するようになりました。(BZ#1890456)

- 以前のバージョンでは、クラスター Autoscaler は特定の状況におけるノードのスケーリングの意思決定用にテンプレートノードを使用しました。**nodeAffinity** 述語は意図された通りにスケールアップできず、保留中の Pod をスケジュールできないことがありました。今回の更新に

より、クラスター Autoscaler がスケールアップでき、ノードのアフィニティーチェックを渡すことができるように、テンプレートノードにできるだけ多くのラベルが含まれるようになりました。(BZ#1891551)

- 以前のバージョンでは、マシンセットのデフォルトの削除の優先順位 (**random**) では、ビルド中のノードよりも **Ready** 状態のノードが優先されることはありませんでした。とくに多数のマシンをスケーリングする場合に、マシンセットをスケールアップしてからすぐにスケールダウンすると **Ready** 状態のすべてのノードが削除される可能性がありました。これにより、クラスターが利用できなくなる可能性がありました。今回のリリースより、低い優先順位がまだ **Ready** 状態にないマシンに割り当てられるようになりました。そのため、大規模なマシンのスケールアップの直後にスケールダウンが実行されると、ワークロードを実行しているマシンを削除する前にビルド中のマシンが削除されます。(BZ#1903733)

Cluster Version Operator

- 以前のバージョンでは、インストールおよびアップグレードプロセスのメッセージには、完了前でも現在のプロセスが 100% 完了していると表示されました。この正しくないメッセージは丸めエラーによって生じました。今回のリリースより、パーセンテージは丸められず、メッセージには終了したサブプロセスの数と正確な完了度 (percent complete) の値が表示されるようになりました。(BZ#1768255)

- 以前のバージョンでは、Cluster Version Operator (CVO) は、チャネルメンバーシップやエラータ URI などの Cincinnati メタデータをマージする際にプル仕様を実際の **available-update** および **current-target** の値と比較しました。有効な代替プル仕様を使用するミラーリングされたリリースイメージからインストールしているか、またはこれに対して更新している場合、Cincinnati メタデータを受信されませんでした。CVO は、どのレジストリーがイメージをホストするかにかかわらず、リリースをダイジェストで比較し、チャネルメンバーシップなどの Cincinnati メタデータを適切に関連付けるようになりました。(BZ#1879976)

- 以前のバージョンでは、metrics-serving goroutine の競合状態により、CVO がシャットダウン時に停止した状態になる可能性がありました。管理対象オブジェクトの調整やモニタリングなどの CVO 動作は機能せず、更新やインストールがフリーズする可能性がありました。CVO は数分後にタイムアウトし、停止状態のメトリクスの goroutine を破棄し、意図された通りにシャットダウンするようになりました。(BZ#1891143)

- 以前のバージョンでは、一部の CVO ログメッセージは、適切に検出されていた変更タイプの変数をレンダリングしませんでした。変数が正しくレンダリングされ、エラーメッセージが意図された通りに表示されるようになりました。(BZ#1921277)

CNF プラットフォーム検証

- 以前のバージョンでは、プラットフォーム検証用にエンドツーエンドテストを実行すると、マシン設定に設定仕様が含まれていない場合に SCTP 検証ステップでエラーが生じました。今回のバグ修正により、設定仕様が見つからない場合に SCTP テストが省略されるようになりました。(BZ#1889275)

- 以前のバージョンでは、Performance Addon Operator が 2 つ以上の NUMA ノードを持つホストで **hugepages** テストを実行し、パフォーマンスプロファイルがノード全体に分散される Huge Page を要求すると、テストは失敗しました。今回のバグ修正により、**hugepages** テストで NUMA ノードの Huge Page の数を判別する方法が修正されました。(BZ#1889633)

config-operator

- 以前のバージョンでは、OpenShift Container Platform 4.1 以降アップグレードされたクラスターでアップグレードを実行中に、非推奨の **status.platformStatus** フィールドは設定されませんでした。そのため、アップグレードが失敗する可能性がありました。今回の修正により、

Cluster Config Operator がこのフィールドを設定するように変更されました。その結果、このフィールドが変更されない場合でもアップグレードは失敗しなくなりました。(BZ#1890038)

コンソール **kubevirt** プラグイン

- 以前のバージョンでは、ストレージクラスは **DataVolume** ソースの永続ボリューム要求 (PVC) から VM ディスク一覧に伝播しませんでした。ストレージクラスが Web コンソールの仮想マシンディスク一覧に表示されるようになりました。(BZ#1853352)
- 以前のバージョンでは、インポートされた SR-IOV ネットワークを別のネットワークインターフェースタイプに設定できました。今回の修正により、インポートされた SR-IOV ネットワークは SR-IOV ネットワークインターフェースタイプのみに設定されるようになりました。(BZ#1862918)
- 以前のバージョンでは、仮想マシン名がクラスターで再使用されると、イベント画面に表示される仮想マシンイベントが正しくフィルターされず、両方の仮想マシンのイベントが混在しました。今回のリリースより、イベントが適切にフィルターされ、イベント画面には現在の仮想マシンに属するイベントのみが表示されるようになりました。(BZ#1878701)
- 以前のバージョンでは、**VM Import** ウィザードによって作成された **V2VVMWare** および **OvirtProvider** オブジェクトが適切にクリーンアップされませんでした。**V2VVMWare** および **OvirtProvider** オブジェクトは予想通りに削除されるようになりました。(BZ#1881347)
- 以前のバージョンでは、使用状況データは仮想マシンが関連付けられていない仮想マシンのある Virtual Machine Interface (VMI) について表示されませんでした。VMI の使用状況データが利用可能な場合には、これが表示されるようになりました。(BZ#1884654)
- 以前のバージョンでは、PVC のクローンが作成されると、その仮想マシンの状態が **Pending** と報告されましたが、追加情報は表示されませんでした。PVC のクローン作成時に、仮想マシンの状態が進捗バーと Pod または PVC へのリンクが含まれる追加の情報と共に インポート されるようになりました。(BZ#1885138)
- 以前のバージョンでは、仮想マシンのインポートステータスに正しくない仮想マシンのインポートプロバイダーが表示されました。仮想マシンのインポートステータスに正しい仮想マシンのインポートプロバイダーが表示されるようになりました。(BZ#1886977)
- 以前のバージョンでは、デフォルトの Pod ネットワークインターフェースタイプは間違った値に設定されました。デフォルトの Pod ネットワークインターフェースタイプは masquerade に設定されるようになりました。(BZ#1887797)

コンソールストレージプラグイン

- 以前のバージョンでは、Local Storage Operator (LSO) のインストール時に、ノードのディスクは表示されませんでした。また、そのノードでディスクの検出を開始する方法はありませんでした。LSO のインストール時に、検出が実行されていない場合に、**Disk** タブが有効にされ、**Discover Disks** オプションが選択可能になりました。(BZ#1889724)
- 今回の更新により、**Disk Mode** オプションの名前が **Volume Mode** 変更されました。(BZ#1920367)

Web コンソール **(Developer** パースペクティブ**)**

- 以前のバージョンでは、ユーザーのパーミッションが不十分であるために、他のプロジェクトからイメージをプルするためのユーザーのアクセスは拒否されました。今回のバグ修正により、ロールバインディングについてのすべてのユーザーインターフェースのチェックが削除され、ユーザーのコマンドラインの使用に役立つ **oc** コマンドアラートが表示されるようになり

ました。今回のバグ修正により、ユーザーの異なる namespace からのイメージの作成がブロックされなくなり、他のプロジェクトからイメージをデプロイできるようになりました。(BZ#1894020)

- コンソールでは、仕様の **resources** および **service account** フィールドを使用する **KafkaSource** オブジェクトの以前のバージョンを使用していました。**KafkaSource** オブジェクトの最新の **v1beta1** バージョンでは、ユーザーが v1beta1 バージョンで **KafkaSource** オブジェクトを作成できないために、これらのフィールドが削除されました。この問題は修正され、ユーザーは v1beta1 バージョンで **KafkaSource** オブジェクトを作成できるようになりました。(BZ#1892653)

- 以前のバージョンでは、**.git** サフィックスを使用して Git リポジトリーからのソースコードでアプリケーションを作成し、編集ソースコードリンクをクリックすると、「**page not found**」エラーが表示されました。今回の修正により、リポジトリー URL から **.git** サフィックスが削除され、SSH URL を HTTPS URL に変換できるようになりました。生成されたリンクは正しいリポジトリーページにつながります。(BZ#1896296)

- 以前のバージョンでは、基礎となる **SinkBinding** リソースが **Container Source** および **KameletBinding** リソースの場合に作成される実際のソースと共に **Topology** ビューに表示され、これはユーザーに混乱をもたらす可能性がありました。この問題は修正されました。イベントソース用に作成された実際のリソースが **Topology** ビュー に表示され、基礎となる **SinkBinding** リソースは (作成されている場合に) サイドバーに表示されるようになりました。(BZ#1906685)

- 以前のバージョンでは、イベントカスタムリソースを作成せずに Serverless Operator をインストールすると、チャネルカードが表示されました。カードをクリックすると、混乱を生じさせるアラートメッセージが表示されました。この問題は修正されています。適切なアラートメッセージを含むチャネルカードは、チャネルのカスタムリソース定義が存在する場合にのみ表示されるようになりました。(BZ#1909092)

- 以前のバージョンでは、Web 端末接続を閉じると、そのセッションからの端末出力がすべて非表示になりました。この問題は修正されています。端末の出力は、セッション終了後も保持されるようになりました。(BZ#1909067)

- テクノロジープレビューのバッジは、 OpenShift Container Platform 4.6 の GA リリースと表示されていても Eventing ユーザーインターフェースに表示されていました。テクノロジープレビューのバッジが削除され、変更は OpenShift Container Platform 4.6.9 バージョンにバックポートされました。(BZ#1894810)

- 以前のバージョンでは、デプロイメントがコンソール編集フローを使用して編集されている場合には、デプロイメントのボリュームマウントは保持されませんでした。変更されたデプロイメント YAML は、Pod テンプレート仕様のボリュームマウントを書き換えるか、または削除しました。この問題は修正されています。ボリュームマウントは、コンソールの編集フローを使用してデプロイメントが編集されている場合でも保持されるようになりました。(BZ#1867965)

- 複数のトリガーで Knative サービスにサブスクライブしているものと、サブスクライバーとして In Memory Channel にサブスクライブしているものがある場合、Knative リソースは **Topology** ビュー に表示されませんでした。この問題は修正され、Knative データモデルは適切なデータを返し、Knative リソースが **Topology** ビューに表示されるようになりました。(BZ#1906683)

- 以前のバージョンでは、コードの取得中の無効な設定が原因で、非接続環境の Helm チャートは **Developer Catalog** に表示されませんでした。この問題は、プロキシー環境変数が考慮されるようにすることで修正され、Helm チャートは **Developer Catalog** に表示されるようになりました。(BZ#1918748)

- Pipeline の実行時に、**TaskRun** リソースのログタブには、出力のコマンドの後に文字列 **undefined** が表示されました。これは、一部の内部文字列操作がログ出力に **undefined** を出力する一部のエッジケースによって生じました。この問題は修正され、Pipeline のログ出力はログストリームの空の行をドロップしなくなり、文字列の **undefined** を出力しなくなりました。(BZ#1915898)

- 以前のバージョンでは、**Add** フローの **Port** 一覧では、公開されたポートのみにオプションを指定でき、カスタムポートは指定できませんでした。この一覧は typeahead 選択メニューに置き換えられ、アプリケーションの作成時にカスタムポートを指定できるようになりました。(BZ#1881881)

- 以前のバージョンでは、条件付きタスクが失敗すると、完了したパイプライン実行で、失敗した条件付きタスクごとに永続的な保留状態のタスクが表示されました。この問題は、失敗した条件付きタスクを無効にし、省略 (skipped) アイコンをそれらのタスクに追加することで修正されています。これにより、パイプライン実行の状態をより明確に把握することができます。(BZ#1880389)

- 以前のバージョンでは、Pod のスケールアップボタンまたはダウンボタンが単一の Pod リソースで利用可能であり、ユーザーがスケールダウンボタンを押すと、ページはクラッシュしました。この問題は、単一の Pod リソースのスケールアップまたはダウンボタンを非表示にすることで修正されています。(BZ#1909678)

- 以前のバージョンでは、helm リリースをインスタンス化するためにチャートをダウンロードする際にチャート URL にアクセスできませんでした。これは、Helm チャートリポジトリーで参照されるリモートリポジトリーからの **index.yaml** ファイルがフェッチされ、そのまま使用されるために生じました。これらのインデックスファイルには、相対チャート URL が含まれているものもあります。この問題は相対チャート URL を絶対 URL に変換することによって修正され、これによりチャート URL にアクセスできるようになりました。(BZ#1912907)

- Serverless 0.10 では、サポートされる最新バージョンが、**trigger**、**subscription**、**channel**、および **IMC** について更新されました。それぞれに対応する静的モデルには、**beta** の API バージョンが表示されました。イベントリソースの API バージョンが **v1** に更新され、UI にサポートされる最新バージョンが表示されるようになりました。(BZ#1890104)

- 以前のバージョンでは、特定のデプロイメントから **All workloads** などのように、ユーザーが **Monitoring Dashboard** タブでワークロードを切り替えると、ダッシュボードには白いキャンバスが表示され、チャートは表示されませんでした。この問題は修正され、ユーザーがワークロードを切り替える際にダッシュボードににチャートが表示されるようになりました。(BZ#1911129)

- 以前のバージョンでは、**critical** および **warning** などの重大度レベルのモニタリングアラートは **info** レベルのアラートとして処理されました。そのため、**Monitoring Alert** アイコンは、これらのアラートの **Topology** ビューのワークロードに表示されませんでした。この問題は修正され、**critical** などのアラートは **warning** レベルのアラートとして処理され、 **Monitoring Alert** アイコンが表示されるようになりました。(BZ#1925200)

- 以前のバージョンでは、Helm インストールの **YAML** ビュー では、YAML コードのみが表示されました。**Schema** ビューアーが YAML エディターに追加され、スキーマとその説明が表示されるようになりました。(BZ#1886861)

- 以前のバージョンでは、すべての Pod は、外部プライベートイメージレジストリーにアクセスするためにイメージのプルシークレットが追加された後でも、**ErrImagePull** および **ImagePullBackOff** エラーを出して失敗しました。これは、外部イメージレジストリーのパーミッションがなく、クラスターは指定されたシークレットなしに外部 URL から直接コンテナーイメージを読み込もうとしてイメージのダウンロードに失敗することによります。そのため、デプロイメントは、サービスアカウントまたはデプロイメントが手動で更新されるまで停止しました。この問題は修正され、新規デプロイメントは内部プライベートコンテナーレジスト

リーから Pod を起動し、サービスアカウントまたはデプロイメントへの追加の変更なしに外部のプライベートコンテナーレジストリーからコンテナーイメージをインポートできるようになりました。(BZ#1924955)

- サンプルアプリケーションの作成時に、**Developer** パースペクティブは、相互に依存し、特定の順序で実行する必要のある複数のリソースを作成します。以前のバージョンでは、受付プラグインはこれらのリソースのいずれも確認できず、**Developer** パースペクティブでサンプルアプリケーションを生成できないことがありました。この問題は修正されています。このコードはリソースを必要な順序で作成するため、サンプルアプリケーションの作成の安定性が高くなります。(BZ#1933665)

- 以前のバージョンでは、API サーバーはリソースの作成に失敗し、リソースクォータのリソースの更新中の競合により 409 の競合状態の応答ステータスコードを返すことがありました。この問題は修正されています。409 ステータスコードを受信すると、OpenShift Web コンソールは要求を最大 3 回再試行するようになりました。引き続き 409 のステータスコードを受信する場合には、コンソールにエラーメッセージが表示されます。(BZ#1928228)

- 以前のバージョンでは、ユーザーが **Topology** ビューに移動すると、openshift **namespace** にテンプレートがない場合はエラーが生じました。このエラーが発生した場合は、空のページが表示されます。この問題は、テンプレートが **openshift** namespace に存在しないというエッジケースを処理することで修正されています。**Topology** ビューに移動し、予想通りにロードできるようになりました。(BZ#1952293)

- OpenShift Pipeline は GA 機能であったにも拘らず、テクノロジープレビューのバッジは Web コンソールの OpenShift Pipeline ワークフローに表示されていました。テクノロジープレビューのバッジが削除されました。(BZ#1945153)

- 以前のバージョンでは、プライベートリポジトリーの Git Import フローで作成されたパイプラインは実行できませんでした。これは、パイプライン **ServiceAccount** オブジェクトが、プライベート Git リポジトリーの Git import フローで作成されたシークレットを使用しないために生じました。今回の更新により、シークレット名をパイプライン **ServiceAccount** オブジェクトのアノテーションに追加し、パイプライン固有のアノテーションを指定されるシークレットに追加できるようになりました。その結果、プライベート Git リポジトリーのパイプラインは正常に実行されます。(BZ#1970485)

- 以前のバージョンでは、Start Pipeline モーダルは空の文字列を有効なエントリーとして認識しなかったため、値を入力する必要がありました。これは、OpenShift Pipelines Operator は空の文字列を有効な パラメーターのデフォルト として認識している場合でも生じました。今回の更新により、オプションで空白の文字列を入力できるようになりました。(BZ#1966275)

- 以前のバージョンでは、アノテーションはメタデータと共に Knative サービスの仕様に渡されていました。その結果、デコレーターはトポロジー内の Knative サービスの関連するリビジョンに表示されました。現在のリリースでは、アノテーションを Knative サービスメタデータにのみ渡すことで、この問題を修正しています。今回のバージョンでは、デコレーターはトポロジーの Knative サービスに対してのみ表示され、関連付けられたリビジョンには表示されなくなりました。(BZ#1954962)

- 以前のバージョンでは、ユーザーは **Developer** パースペクティブからプライベートサービスとして Knative サービスを作成できませんでした。この問題は、「**networking.knative.dev/visibility': 'cluster-local**」 ラベルを更新して修正されています。(BZ#1970796)

DNS

- 以前のバージョンでは、一部のノードの **/etc/hosts** ファイルに無効なエントリーが含まれるため、クラスターで断続的な DNS 解決のエラーが発生する可能性がありました。今回のリリースより、無効なエントリーを持つ **/etc/hosts** ファイルがある場合でも DNS 解決が失敗しなくな

りました。(BZ#1882485)

etcd

- 以前のバージョンでは、etcd readiness プローブで **lsof** および **grep** コマンドが使用されました。これにより、機能しないプロセスが残される可能性がありました。etcd readiness プローブは TCP ポートプローブを使用するようになり、これはよりコストの低いプローブであり、機能しないプロセスが作成されることはなくなりました。(BZ#1844727)

- 以前のバージョンでは、IP アドレスがコントロールプレーンノードで変更されると、ディスク上の証明書が無効になり、etcd がピアとの接続に失敗する理由についての不明確な etcd のエラーメッセージが出されました。コントロールプレーンノードの IP アドレスの変更が検出され、イベントが報告され、 **EtcdCertSignerController** に **Degraded** のマークが付けられるようになりました。(BZ#1882176)

- 以前のバージョンでは、etcd クラスターのメンバーが 3 メンバー未満の場合に新規の静的 Pod のリビジョンが発生する可能性があり、これが生じると、一時的にクォーラム (定足数) が失われました。すべてのコントロールプレーンノードが利用できない場合に静的 Pod のリビジョンは回避されるようになり、クォーラム (定足数) が一時的に失われることがなくなりました。(BZ#1892288)

- 以前のバージョンでは、etcd バックアップには、バックアップが取られたコントロールプレーンノードに固有のリカバリー YAML ファイルが含まれました。そのため、あるコントロールプレーンノードから取得されるバックアップは別のコントロールプレーンノードで復元できませんでした。リカバリー YAML ファイルはより汎用的になり、etcd バックアップはすべてのコントロールプレーンノードで復元できるようになりました。(BZ#1895509)

- 以前のバージョンでは、etcd バックアップスクリプトは最後の変更されたタイムスタンプを使用して最新のリビジョンを判別していました。これにより、正しくない静的 Pod リソースが etcd バックアップに保存されました。etcd バックアップスクリプトはマニフェストファイルを使用して最新のリビジョンを判別し、正しい静的 Pod リソースが etcd バックアップに保存されるようになりました。(BZ#1898954)

- 以前のバージョンでは、IPv4 CIDR が install-config マシンネットワーク CIDR 配列の最初の要素でない限り、ブートストラップのレンダリングロジックは、IPv6 デュアルスタックモードを使用する場合に使用可能なマシンネットワーク CIDR を検出できませんでした。解析ロジックはすべてのマシンネットワーク CIDR をループするように修正され、IPv4 アドレスはデュアルスタックモードでマシンネットワーク CIDR 間で正しく読み込まれるようになりました。(BZ#1907872)

- 以前のバージョンでは、**openshift-etcd** namespace が削除されると、**etcd-endpoints** 設定マップは再作成されず、クラスターは回復しませんでした。**etcd-endpoints** 設定マップがない場合はこれが再作成されるようになり、クラスターを回復できるようになりました。(BZ#1916853)

イメージレジストリー

- 最後の Kubernetes の更新により API のタイムアウトが実行されました。このタイムアウトにより、34 秒後にすべての長期的に続く要求がドロップされます。大規模なリポジトリーをインポートする場合 (とくに複数のタグを持つリポジトリーの場合) に、タイムアウトに達すると、以前のバージョンのようにインポートを正常に実行できません。**oc** クライアントに異なるタイムアウトを設定するためのフラグがありますが、サンプルがないために、クライアントが API のタイムアウトをバイパスする方法を把握するのが困難でした。**oc** help でフラグの使用法が示されることにより、クライアントがこのオプションを検索するのが容易になりました。(BZ#1878022)

- 以前のバージョンでは、同じロギングパッケージの 2 つの異なるバージョンを使用すると、

Operator ログが部分的に失われました。今回の修正により、ロギングパッケージのバージョンが等しいバージョンとなり、Operator で使用されるアップグレードされたロギングパッケージは client-go で使用されるパッケージに一致するようになりました。ログが失われることはなくなりました。(BZ#1883502)

- 以前のバージョンでは、プルーナーはイメージストリームを使用してレジストリー名を検出しようとしましたが、イメージストリームがない場合、プルーナーはレジストリー名の検出に失敗しました。今回の修正により、Image Registry Operator はレジストリー名と共にプルーナーを提供するようになりました。プルーナーはレジストリー名を検出するためにイメージストリームの有無に依存しなくなりました。(BZ#1887010)

- 以前のバージョンでは、Operator Pod にはメモリー要求がありませんでした。ノードでのメモリー不足が発生した場合、Operator は他の **BestEffort** コンテナーの前にメモリー不足になるために強制終了する可能性がありました。今回の修正により、メモリー要求が追加されました。今回のリリースより、Operator は、他の **BestEffort** コンテナーがノードにある場合にメモリー不足になっても強制終了されなくなりました。(BZ#1888118)

- 以前のバージョンでは、プルーナーはイメージストリームを使用してレジストリー名を検出しようとしましたが、イメージストリームがない場合、プルーナーはレジストリー名の検出に失敗しました。今回の修正により、Image Registry Operator は、レジストリーが設定されている場合にプルーナにレジストリー名を提供し、レジストリーがインストールされていない場合には、レジストリープルーニングを無効にするようになりました。(BZ#1888494)

- 以前のバージョンでは、Operator ステータスの定義時に使用できる Operand デプロイメントのステータスに関する分析がありませんでした。一部のシナリオでは、Image Registry Operator は自らについて 2 つの矛盾する情報を表示しました。ユーザーには、Not Available (利用不可) であると同時に Not Degraded (低下していない) と通知しました。これらの 2 つの状態は、デプロイメントでイメージレジストリーの稼働の試行を停止した後も依然として提示されました。このシナリオでは、Degraded フラグを Operator で設定する必要があります。イメージレジストリーのデプロイメントを考慮して、Operator は、アプリケーションの実行を試行する際に Operand デプロイメントが進捗期限に達すると、自らを Degraded に設定するようになりました。デプロイメントの失敗時に、進捗期限に達すると、Operator は自らのステータスを Degraded に設定します。Operator は、引き続き Operator デプロイメントが進行中に Progressing と報告します。(BZ#1889921)

- 以前のバージョンでは、Image Registry Operator は明示的なコマンドが提供されるため、そのエントリーポイントを使用しませんでした。クラスター全体の **trusted-ca** は Operator で使用されず、Operator はカスタム **trusted-ca** なしでは機能しないストレージプロバイダーに接続できませんでした。今回の修正により、Pod 仕様から明示的なコマンドが削除されました。イメージエントリーポイントは、**trusted-ca** を適用するコンテナーで使用されるようになりました。(BZ#1892799)

- 以前のバージョンでは、プルーナーのデフォルトのログレベルは **2** でした。そのため、エラーが発生すると、プルーナーはスタックトレースをダンプしました。今回の修正により、デフォルトのログレベルは **1** に変更されました。今回のリリースより、スタックトレースなしでエラーメッセージのみが出力されるようになりました。(BZ#1894677)

- 以前のバージョンでは、**configs.imageregistry.operator.openshift.io** ステータスフィールドは Operator の同期中に更新されませんでした。つまり、ステータスフィールドには最新の適用済みの swift 設定が表示されませんでした。今回の修正により、同期プロセスで **configs.imageregistry.operator.openshift.io** ステータスが仕様の値に更新されるようになりました。仕様およびステータスフィールドは、適用された設定を示すステータスフィールドと同期します。BZ#1907202)

- 以前のバージョンでは、HTTP/2 プロトコルの再試行がないと関連する再試行可能なエラーが生じ、ミラーリングがエラーメッセージを出してキャンセルされました。今回の修正により、エラーメッセージが HTTP/2 プロトコル関連のエラーに対応する場合、再試行が追加されまし

た。これらのエラーが生じる場合に、複数回の試行後にミラー操作がキャンセルされるようになりました。(BZ#1907421)

- 以前のバージョンでは、**node-ca** デーモンセットの明示的なユーザーおよびグループ ID がない場合に、**node-ca** Pod で使用されているユーザーおよびグループの解釈する際に混乱が生じました。今回の修正により、**node-ca** デーモンセットに **runAsUser** および **runAsGroup** 設定が提供されます。**node-ca** DaemonSet YAML ファイルを検査する際に、ユーザーおよびグループの定義が明確になりました。(BZ#1914407)

ImageStreams

- 以前のバージョンでは、イメージプルーナーでは、使用中のイメージの一覧を収集する際に **StatefulSet**、**Job**、および **Cronjob** オブジェクトによって使用されるイメージを考慮しませんでした。そのため、誤ったイメージをプルーニングする可能性がありました。イメージプルーナーでは、イメージ一覧の作成時にこれらのオブジェクトによって使用されるイメージを考慮に入れるようになりました。これらのオブジェクトによって使用されるイメージはプルーニングされなくなりました。(BZ#1880068)

- 以前のバージョンでは、新規に作成されたイメージストリームは **publicDockerImageRepository** 値で装飾されませんでした。ウォッチャーは、新規オブジェクトの **publicDockerImageRepository** 値を受信しませんでした。イメージストリームは正しい値で装飾されるようになりました。その結果、ウォッチャーは **publicDockerImageRepository** 値を持つイメージストリームを取得するようになりました。(BZ#1912590)

Insights Operator

- 以前のバージョンでは、誤ったエラー処理により、Operator は監視するファイルで変化が生じるとそのプロセスをあいまいな方法で終了しました。Operator のエラー処理が改善されました。今回のリリースより、Operator は実行を継続し、監視するファイルが変更される場合でも終了プロセスシグナルを送信しなくなりました。(BZ#1884221)

- 以前のバージョンでは、Operator はレポートのアーカイブ中にリソースの namespace を使用しませんでした。そのため、異なる namespace の同じ名前を持つリソースが上書きされました。Operator はデータのアーカイブ中に namespace と共にレポートパスを使用するようになりました。その結果、すべてのレポートが namespace ごとに収集されます。(BZ#1886462)

インストーラー

- 以前のバージョンでは、virtual-media が使用されると、fast-track モードはノードが操作と操作の間で再起動されるために、予想通りに機能しませんでした。この問題は修正されています。(BZ#1893546)

- 以前のバージョンでは、デュアルスタックのデプロイメントを使用する場合、ワーカーノードのホスト名はデプロイメントの前に検査される名前と一致しませんでした。これにより、ノードで手動の承認が必要でした。これは修正されています。(BZ#1895909)

- コントロールプレーンとデプロイされるホスト間に最大 1 時間までの小規模なクロックスキューがある場合に、ベアメタルのプロビジョニングは失敗しなくなりました。(BZ#1906448)

- vCenter ホスト名に大文字が含まれる場合、VMware vSphere の OpenShift Container Platform インストールプログラムでは、最終的に失敗するまでにクラスターの完了を待機する長い時間がかかりました。インストールプログラムは、初期プロセスで vCenter ホスト名に大文字が含まれていないことを検証し、待機時間を回避できるようになりました。(BZ#1874248)

- 以前のバージョンでは、OpenShift Container Platform インストールプログラムの内部

Terraform バックエンドは、Amazon Web Services (AWS) の場合のように Terraform コアから Terraform プロバイダーへの大規模な入力をサポートしませんでした。**bootstrap.ign** ファイルが文字列として AWS プロバイダーに渡されると、入力制限を超える可能性があり、ブートストラップ Ignition S3 バケットの作成時にインストールプログラムが失敗する可能性がありました。今回のバグ修正により、Terraform バックエンドは、**bootstrap.ign** をディスク上のパスとして渡すように変更され、AWS プロバイダーは入力サイズの制限を無視して大規模なファイルを読み取れるようになりました。今回のリリースより、入力制限よりも大きなブートストラップ Ignition ファイルを作成する Cal effort インストールの実行時に、インストールプログラムが正常に実行されるようになりました。(BZ#1877116)

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) の起動前 (pre-flight) のインストーラーの検証がフレーバーのメタデータに対して実行されました。これにより、インストールの完了に必要な容量がある可能性のある、**baremetal** と検出されるフレーバーへのインストールが阻止される可能性がありました。通常、これは RHOSP 管理者がベアメタルフレーバーに適切なメタデータを設定しないことによって生じます。**baremetal** と検出されるフレーバーでの検証が省略され、間違って失敗がが報告されることがなくなりました。(BZ#1878900)

- 以前のバージョンでは、GCP および Azure にインストールされるクラスターの **Manual** 認証情報モードは許可されませんでした。このため、ユーザーは手動の認証情報を使用してクラスターを GCP または Azure にインストールできませんでした。インストールプログラムは、GCP および Azure 用に提供される手動の認証情報を検証できるようになりました。(BZ#1884691)

- 以前のバージョンでは、インストールプログラムは、Azure にインストールされたクラスターを破棄する前にリソースグループが存在することを検証しませんでした。これにより、インストールプログラムがエラーを出して継続的にループしました。インストールプログラムは、クラスターを破棄する前にリソースグループが存在することを検証でき、クラスターを正常に破棄できるようになりました。(BZ#1888378)

- 以前のバージョンでは、インストールプログラムは、共有リソースでクラスターを作成する際に、AWS アカウントに **UnTagResources** パーミッションがあることをチェックしませんでした。そのため、クラスターを破棄する際に、インストールプログラムには既存のネットワークに追加されたタグを削除するパーミッションがありませんでした。今回のバグ修正により、共有ストレージリソースでクラスターを作成する際に、**UnTagResources** の有無をチェックし、インストールプロセスの終了前にアカウントに適切なパーミッションがあることを確認できるようになりました。(BZ#1888464)

- **openshift-install destroy cluster** コマンドが適切に機能するには、インストールプログラムが最初に作成するクラスターオブジェクトを削除する必要があります。一部の例では、ホストされるゾーンオブジェクトがすでに削除され、これによりインストールプログラムがハングすることがありました。インストールプログラムは、オブジェクトがすでに削除されている場合にオブジェクトの削除を省略し、これによりクラスターが正常に破棄されるようになりました。(BZ#1890228)

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) のコントロールプレーンポートには追加のユーザー定義のセキュリティーグループが割り当てられませんでした。これにより、ユーザー定義のセキュリティーグループルールがコントロールプレーンノードに適切に適用されませんでした。追加のユーザー定義のセキュリティーグループがコントロールプレーンのポートに割り当てられるようになり、セキュリティーグループルールがコントロールプレーンノードに正しく適用されるようになりました。(BZ#1899853)

- 以前のバージョンでは、別のセキュリティーグループをソースとするデフォルトの AWS セキュリティーグループのルールにより、クラスターを破棄する際に、インストールプログラムがその他のセキュリティーグループを削除することができませんでした。これにより、クラスターの破棄プロセスが完了せず、AWS リソースが残されたままになりました。デフォルトのセ

キュリティーグループからルールが削除され、他のセキュリティーグループの削除のブロックが解除されました。これにより、すべての AWS リソースをクラスターから削除されるようになりました。(BZ#1903277)

- Red Hat OpenStack Platform (RHOSP) 検証に欠落しているガードが空のサブネット ID を持つサブネットの一覧を取得し、一部の RHOSP 以外のクラウドが予期しない値を返す可能性がありました。予期しないエラーコードにより検証に失敗し、OpenShift Container Platform が RHOSP 以外のクラウドにインストールできませんでした。今回のバグ修正により、欠落していたガードが空のサブネット ID に対して追加され、適切な検証が可能になりました。(BZ#1906517)

- 以前のバージョンでは、VMware vSphere へ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の参照ロードバランサーは単純な TCP チェック用に設定され、ヘルスチェックは api サーバーの正常性を考慮しませんでした。この設定により、API サーバーが再起動されるたびに API 要求が失敗することがありました。ヘルスチェックは **/readyz** エンドポイントに対して API サーバーの正常性をチェックし、参照 API ロードバランサーが API サーバーの再起動時に要求を正常に処理するようになりました。(BZ#1836017)

- 以前のバージョンでは、インストールプログラムを使用する際に CTRL+C を押しても、プログラムは常に中断されず、常に予想通りに終了する訳ではありませんでした。インストールプログラムを使用して CTRL+C を押すと、プログラムは常に中断し、終了します。BZ#1855351)

- 以前のバージョンでは、サービスプリンシパルの期限が切れた時など、無効な認証情報を使用して Azure のクラスターの削除を試行し、デバッグログを表示しない場合に、クラスターは削除されない場合も削除されているものとして表示されました。クラスターを削除しないことのほかに、ローカルに保存されたクラスターメタデータが削除され、**openshift-install destroy cluster** をコマンドを再度実行してもクラスターを削除できませんでした。無効な Azure 認証情報の使用時にクラスターの削除を試行する場合に、インストールプログラムはエラーを出して終了し、認証情報を更新してから再試行できるようになりました。(BZ#1866925)

- 以前のバージョンでは、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ベアメタルのインストール方法の **install-config.yaml** ファイルは **clusterProvisioningIP** 名ではなく **provisioningHostIP** 名を誤って使用しました。これにより、ドキュメントと YAML ファイルで使用される実際のフィールド名との間に差異が生じました。**provisioningHostIP** フィールドが非推奨となり、**clusterProvisioningIP** が優先して使用されることになり、差異がなくなりました。(BZ#1868748)

- 以前のバージョンでは、インストールプログラムは Ignition 設定ファイルの期限切れの証明書の有無をチェックしませんでした。期限切れの証明書が原因で、説明なしにインストールが失敗していました。インストールプログラムは、期限切れの証明書の有無をチェックし、証明書の期限が切れている場合に警告を出力するようになりました。(BZ#1870728)

kube-apiserver

- 以前のバージョンでは、**preserveUnknownFields** フィールドは **v1beta1** CRD で **true** に設定され、**oc explain** で CRD フィールドについての説明がなくてもエラーは出されませんでした。検証条件が追加され、**preserveUnknownFields** フィールドが **false** に設定されていない **v1beta** CRD のステータスに **spec.preserveUnknownFields: Invalid value: true: must be false** のエラーが表示されます。(BZ#1848358)

- 以前のバージョンでは、IBM Cloud クラスターの OpenShift Container Platform では、**LocalStorageCapacityIsolation** 機能ゲートはデフォルトで無効にされていました。無効にされている場合、一時ストレージ要求または制限を設定すると、Pod がスケジュール対象外になります。今回の修正によりコードが変更され、**LocalStorageCapacityIsolation** 機能ゲートが無効になっている場合に、一時ストレージ要求または制限は無視され、Pod を予想通りにスケジュールできるようになりました。(BZ#1886294)

Red Hat OpenShift Logging

今回のリリースにより、**Cluster Logging** は **Red Hat OpenShift Logging** バージョン 5.0 になりました。詳細は、『Red Hat OpenShift Logging 5.0 リリースノート 』を参照してください。

Machine Config Operator

- 以前のリリースでは、Red Hat OpenStack Platform (RHOSP) にデプロイして、ホスト名と共に HTTP プロキシーを使用する場合、インストールプロセスがコンテナーイメージのプルに失敗し、エラーメッセージ **unable to pull image** がレポートされる可能性がありました。今回のバグ修正により、プロキシーが環境変数で設定される方法が修正され、ノードがリモートレジストリーからコンテナーイメージをプルできるようになりました。(BZ#1873556)

- 以前のバージョンでは、アップグレード時に、以前のリリースの Machine Config Controller (MCC) は新規の Machine Config Operator (MCO) からの設定変更に応答する可能性がありました。MMC は次に別の変更を導入し、これにより、アップグレードプロセスで不要な再起動が生じました。今回のバグ修正により、MCC が新規 MCO からの設定変更に応答しなくなり、不要な再起動を回避できるようになりました。(BZ#1879099)

- 以前のバージョンでは、CoreDNS 分散クエリーの転送プラグインが、設定されたすべての DNS サーバーに対してランダムにクエリーを実行していました。CoreDNS は機能しない DNS サーバーにクエリーするため、名前解決は断続的に失敗しました。今回のバグ修正により、クエリーが応答する最初の DNS サーバーに送信されるように、順次ポリシーを使用するよう転送プラグインが設定されました。(BZ#1882209)

- 以前のバージョンでは、Machine Config Operator は **multi-user.target.wants** ディレクトリーからの有効にされた systemd ターゲットユニットのみを読み込みました。そのため、**multi-user.target.wats** ディレクトリーをターゲットにしないユニットはこのディレクトリーをターゲットとするように変更されました。今回の修正により、systemd で事前に設定されるファイルを使用して MCO で事前設定されたファイルを作成できるように MCO が変更されました。これにより、すべての systemd サービスが予想通りに有効および無効にされます。(BZ#1885365)

- 以前のバージョンでは、クラスターを OVN-Kubernetes デフォルト Container Network Interface (CNI) に移行する際に、事前に設定された Linux ボンディングインターフェースのボンディングオプションは無視されました。そのため、ボンディングは指定されるモードではなく、ラウンドロビンを使用して設定され、ボンディングが機能しない可能性がありました。ovs-configuration.service (configure-ovs.sh) が変更され、Linux ボンディング上の以前のボンディングオプションは **ovs-if-phys0** Network Manager 接続にコピーされます。これにより、すべてのボンディングは最初に設定されるように機能するはずです。(BZ#1899350)

- OpenShift Container Platform 4.6 では、BFQ (Budget Fair Queueing) Linux I/O スケジューラーを使用するように変更が加えられました。そのため、etcd の fsync I/O レイテンシーが引き上げられました。今回の修正により、I/O スケジューラーを使用しないように設定された NVMe デバイスを除き、I/O スケジューラーが mq-deadline スケジューラーを使用するように変更されました。Red Hat Enterprise Linux CoreOS (RHCOS) の更新では、BFQ スケジューラーは引き続き使用されます。その結果、レイテンシーが許容レベルに短縮されました。(BZ#1899600)

Web コンソール（Administrator パースペクティブ）

- 以前のバージョンでは、依存関係の問題により、OpenShift Container Platform Web コンソールで **YAML Editor** の永続的なアンマウントおよび再マウントが生じました。そのため、YAML エディターは数秒ごとに YAML ファイルの上部にジャンプしました。今回の修正により、依存関係についてのデフォルトのパラメーター値が削除されました。その結果、**YAML** エディターは予想通りに動作するようになりました。(BZ#1903164)

- 以前のバージョンでは、OpenShift Container Platform Web コンソールの Operator の説明のリンクがサンドボックス iframe でレンダリングされ、これによりその iframe 内の java スクリプトが無効になりました。そのため、ユーザーがリンクをクリックすると、サンドボックスの制限が新規タブによって継承されるため、JavaScript はリンクされたページを実行しませんでした。このリンクは、 **allow-popups-to-escape-sandbox** パラメーターを Operator の説明の iframe サンドボックスの属性に追加することで修正され、新規タブはサンドボックスの外部で開くことができます。その結果、Operator の説明からのリンクが開か、通常通りに実行されるようになりました。(BZ#1905416)

- 以前のバージョンでは、OpenShift Container Platform Web コンソールのスケーリング Pod 機能は **scale** サブリソースを使用せず、デプロイメント設定に **patch** 動詞のないカスタムロールおよびデプロイメントは Web コンソールの Pod をスケーリングできませんでした。今回の修正によりコードが変更され、スケーリング Pod 機能で **scale** サブリソースを使用するようになりました。その結果、ユーザーは **patch** 動詞を追加せずに Web コンソールで Pod をスケーリングできます。(BZ#1911307)

- 以前のバージョンでは、**fieldDependency** 記述が同一の名前を持つコントロールフィールドを使用するスキーマプロパティーに適用される OpenShift Container Platform Web コンソールでカスタムリソースを作成すると、**getJSONSchemaPropertySortWeight** ヘルパー関数が無限に再帰しました。これにより、**DynamicForm** コンポーネントが例外をスローし、Web ブラウザーがクラッシュする可能性がありました。今回の修正により、**getJSONSchemaPropertySortWeight** 関数が変更され、現在のパスを追跡し、パス全体を使用してフィールド名のみではなく依存関係を判別できるようになりました。その結果、**DynamicForm** コンポーネントは上記の条件下で例外をスローしなくなりました。(BZ#1913969)

- 以前のバージョンでは、**SamplesTBRInaccessibleOnBoot** アラートの説明には「bootstrapped」という用語の誤字が含まれていました。アラートの説明の内容が正しくなりました。(BZ#1914723)

- 以前のバージョンでは、CPU およびメモリーの **specDescriptor** フィールドにより、YAML エディターで空の文字列が追加されました。これらのフィールドは YAML エディターに空の文字列を追加しなくなりました。(BZ#1797766)

- 以前のバージョンでは、**Subscription** および **CSV** オブジェクトは Operator のインストール時に **Installed Operators** ページに表示されました。この重複は修正され、一致する **CSV** オブジェクトがすでに存在する場合、 **Subscription** Operator が **Installed Operators** ページに表示されなくなりました。(BZ#1854567)

- 以前のバージョンでは、ビルドが 1 時間前に開始された場合に、空のリソース使用状況チャートが **Build details** ページに表示されましたが、デフォルトは最後の 1 時間のみを表示するよう設定されていました。**Build details** ページの使用状況チャートには、ビルドの実行時間についてのデータが表示されるようになりました。(BZ#1856351)

- 以前のバージョンでは、OpenAPI 定義は初回のページの読み込み時にのみ更新されました。OpenAPI 定義は 5 分間隔、およびモデルが API からフェッチされるたびに更新されるようになりました。OpenAPI 定義は、ページの更新がなくても最新の状態を維持します。(BZ#1856354)

- 本リリースでは、クラスターモニタリングのドキュメントへの破損したリンクが修正されています。(BZ#1856803)

- 以前のバージョンでは、、**utm_source** パラメーターは Red Hat Marketplace URL にありませんでした。本リリースでは、**utm_source** パラメーターが属性についての Red Hat Marketplace URL に追加されました。(BZ#1874901)

- 以前のバージョンでは、**Escape** キーを使用しても、プロジェクトの選択ドロップダウンを閉じることができませんでした。**Escape** キーのハンドラーが更新され、ユーザーはプロジェクト選択ドロップダウンを終了し、閉じることができるようになりました。(BZ#1874968)

- 以前のバージョンでは、スケジュールステータスに使用されるフォントの色はアクセシビリティーに準拠するものではありませんでした。フォントとフォントの色が更新され、使用しやすくなりました。スケジュールで無効にされたノードは黄色の警告アイコン (感嘆符アイコン) で表示されます。(BZ#1875516)

- 以前のバージョンでは、一部の API 呼び出しのパッチのパスは正しくありませんでした。これにより、仕様記述子フィールドがリソースプロパティーを更新しませんでした。本リリースでは、記述子からパッチパスをビルドするロジックが更新されました。(BZ#1876701)

- 以前のバージョンでは、**Unschedulable** ステータスフィールドは **True** に設定されている場合にのみ表示されました。本リリースでは、ステータス情報をより明確に表示するために、新たな UX デザインが実装されました。(BZ#1878301)

- 以前のバージョンでは、同じ namespace の別のサブスクリプションに手動の承認ストラテジーがある場合に、自動承認ストラテジーが設定されたサブスクリプションは手動の承認ストラテジーを持つかのように動作しました。本リリースでは、手動承認ストラテジーを持つサブスクリプションによって、namespace のすべてのサブスクリプションが手動で動作することをユーザーに通知するよう更新が加えられました。(BZ#1882653)

- 以前のバージョンでは、手動インストール計画が複数の Operator に影響する可能性がありました。ただし UI では、実際に影響を与える場合でもこれについて明確に示唆せず、承認を要求する UI が表示されました。そのため、ユーザーは複数の Operator のインストール計画を承認しても、UI ではそのことが明確に示唆されないことがありました。本リリースでは、UI には手動の承認計画で影響を受けるすべての Operator が一覧表示され、インストールされる Operator を明確に示されます。(BZ#1882660)

- 以前のバージョンでは、namespace 作成モーダルから重複する namepsace を作成すると、拒否エラーが生じました。本リリースでは、プロジェクトを作成する際のエラーハンドラーが追加され、重複プロジェクトを作成しても拒否エラーが生じなくなりました。(BZ#1883563)

- 以前のバージョンでは、Prometheus swagger 定義には解決できない **$ref** プロパティーが含まれていたため、Prometheus オペランドの作成フォームでランタイムエラーが発生しました。**definitions** プロパティーが、**definitionFor** ヘルパー関数で返されるスキーマに追加され、 **$ref** が解決され、ランタイムエラーが発生しなくなりました (BZ#1884613)。

- 以前のバージョンでは、ユーザーは、インストールステータスページが表示されるまで、必要なリソースがバックグラウンドで読み込まれるのを待機する必要がありました。インストールステータスページは更新され、ユーザーの Operator のインストール時にすぐに表示されるようになりました。(BZ#1884664)

- 以前のリリースでは、iOS は自己署名証明書を使用したセキュアな Websocket 経由で接続する機能をサポートしないため、コンソールに白い画面が表示されました。自己署名証明書のある Websocket が正常に実行されない場合は、接続が https にフォールバックし、コンソールが正しく読み込まれるようになりました。(BZ#1885343)

- 以前のバージョンでは、ユーザーが Web コンソールで新規のロールバインディングを作成する際に、システムロールは存在しませんでした。システムロールはロール名のドロップダウンに表示されるようになり、ユーザーは新規ロールバインディングの作成時にシステムロールを選択できるようになりました。(BZ#1886154)

- 以前のバージョンでは、ターミナルではすべての Pod が Linux Pod であると仮定し、Windows Pod を考慮しませんでした。そのため、ターミナルは sh コマンドにデフォルト設定される際に Windows Pod を使用すると機能しませんでした。ターミナルは Pod のタイプを検出し、必要

に応じてコマンドを変更するようになりました。(BZ#1886524)

- 以前のバージョンでは、新規プロビジョナー名には **kubernetes.io/** プレフィックスが含まれないため、ユーザーは web-console から PVC を aws-ebs-csi-driver(gp2-csi) で作成する際に RWX および RWO アクセスモードを選択できました。追加のプロビジョナーが AccessMode マッピングに追加され、web-console から aws-ebs-csi-driver(gp2-csi) で PVC を作成する場合に RWX および RWO アクセスモードは利用できなくなりました。(BZ#1887380)

- 以前のバージョンでは、アクティブな namespace を維持するロジックでは、現在アクティブな namespace の削除は考慮されませんでした。そのため、UI で最近削除された namespace は現在アクティブな namespace として設定されたままになる可能性がありました。今回のリリースより、アクティブな namespace のロジックが更新され、現行のブラウザーセッションでユーザーが現在アクティブな namespace を削除する際に、デフォルトで「All namespaces」に設定されるようになりました。ユーザーが現在アクティブな namespace を削除すると、同じブラウザーセッションでアクティブな namespace は「All Namespaces」に自動的に更新されるようになりました。(BZ#1887465)

- 以前のバージョンでは、v0.1.1 のコンソールベンダーの 'runc' モジュールに潜在的なセキュリティー上の問題が含まれていたため、frog xray は 'runc' に潜在的な脆弱性があるものとしてフラグを付けていました。'runc' モジュールは修正を含む v1.0.0-rc8 バージョンに固定されました。これには修正が含まれ、'runc' の依存関係には潜在的な脆弱性があるものとしてのフラグが付けられなくなりました。(BZ#1887864)

- 以前のバージョンでは、CSV および PackageManifest は最新バージョンだけではなく、提供されたすべての API バージョンを一覧表示したため、CSV および PackageManifest ページには重複 API が表示される可能性がありました。API を取得するためのロジックが更新され、提供される各 API の最新バージョンのみが表示されるようになりました。(BZ#1888150)

- 以前のバージョンでは、Install Operand Form の記述が「SynchMarkdownView」コンポーネントに欠落していたため、マークダウンでフォーマットされませんでした。Install Operand Form がマークダウンでフォーマットされ、Install Operand Form の記述が正しくフォーマットされるようになりました (BZ#1888036)。

- 以前のバージョンでは、、**fieldDependency specDescriptor** は同位 (sibling) 以外の依存関係に対応するように設計されておらず、テストされませんでした。そのため、同位 (sibling) 以外の依存関係の場合あに、想定通りに動作することが保証されませんでした。今回の更新により、同位 (sibling) 以外の依存関係が予想通りに機能するようにロジックが修正されました。(BZ#1890180)

- 以前のバージョンでは、ローカルの **ensureKind** 関数 が null の **data** 引数を適切に処理しない場合に例外がスローされました。今回の更新により、**data** 引数の使用する際に null の合体 (coalescence) が追加され、例外がスローされなくなり、null **data** 引数の正常な処理が可能になりました。(BZ#1892198)

- 以前のバージョンでは、TLS シークレットはコンソールで編集できませんでした。今回の更新により、コンソールで TLS シークレットを更新できるように **type** フィールドが追加されました。(BZ#1893351)

- 今回の更新により、Web コンソールに正しくないファイルシステムの容量および使用データが表示される問題が修正されました。(BZ#1893601)

- 以前のバージョンでは、Web コンソールは Operator Lifecycle Manager (OLM) Operator のメトリクスを収集するために正しくないサービスアカウントの Prometheus Operator にパーミッションを誤って付与していました。コンソールは prometheus-k8s サービスアカウントにパーミッションを正しく付与し、メトリクスを収集できるようになりました。(BZ#1893724)

- 以前のバージョンでは、コンソール Pod の **TopologyKey** は **kubernetes.io/hostname** に設定

され、これにより、更新およびゾーンの停止時に可用性の問題が生じました。今回の更新により、**TopologyKey** が **topology.kubernetes.io/zone** に設定され、更新およびゾーンの停止時の可用性が改善されました。(BZ#1894216)

- 以前のバージョンでは、namespace に **status** ブロックがない OperatorGroup は、OperatorHub から新規 Operator をインストールする際に Web コンソールでランタイムエラーを発生させる可能性がありました。この問題は解決されています。(BZ#1895372)

- 以前のバージョンでは、CRD のモデルが存在しない場合、コンソールは Provided API 一覧からカスタムリソース定義 (CRD) をフィルターしました。そのため、Details タブには初回インストール時に Provided API カードが表示されず、これにより、Operator が API を提供していないというように表示されました。今回の更新により、API カードからフィルターが削除され、モデルが存在しない場合にそれらが表示されるようになりました。その結果、Provisiond API カードとそれらの対応するタブは常に一致するようになり、モデルが利用可能ではない場合に UI に空の状態が表示されなくなりました。(BZ#1897354)

- lodash **startCase** 関数が記述子フィールドのオペランドに適用されることがありました。そのため、フィールドラベルは Start Case としてフォーマットされ、記述子の **displayName** プロパティーを上書きしました。今回の更新により、記述子の **displayName** が指定されていない場合にのみ、**startCase** が適用され、オペランドフォームに **displayName** が適切に表示されるようになりました。(BZ#1898532)

- 以前のバージョンでは、**react-jsonschema-form** は null に明示的に設定された配列タイプのスキーマを適切に処理しませんでした。DynamicForm コンポーネントに渡されるフォームデータに null に設定された配列タイプのプロパティーが含まれる場合、ランタイム例外が発生しました。今回の更新により、配列フィールドに null チェックが追加され、このシナリオで例外がスローされなくなりました。(BZ#1901531)

モニタリング

- 以前のバージョンでは、**prometheus-adapter** は OpenAPI 仕様を実装しませんでした。そのため、API サーバーは、Prometheus アダプターがクラスターにデプロイされる間に OpenAPI が存在しないことを示すメッセージを、60 秒ごとにログに記録しました。さらに、**KubeAPIErrorsHigh** アラートはログのエラーによって実行される可能性がありました。今回の修正により、OpenAPI 仕様が **prometheus-adapter** に導入され、OpenShift Container Platform の他のコア API リソースに準拠するようになりました。(BZ#1819053)

- 以前のバージョンでは、SCC (Security Context Constraints) を昇格する特定のシナリオで、Prometheus のステートフルセットのデプロイメントが失敗しました。**nonroot** SCC がモニタリング用のステートフルセットのデプロイメントに使用されるようになりました。今回の修正により、Alertmanager、Prometheus、および Thanos Ruler のすべてのモニタリングのステートフルセットのデプロイメントについて、以下の Kubernetes セキュリティーコンテキスト設定が必要になります。

```
securityContext:
  fsGroup: 65534 1
  runAsNonRoot: true
  runAsUser: 65534 2
```

1. ファイルシステムグループ ID は、**nobody** ユーザーの ID **65534** に設定されます。kubelet は Pod の起動時にグループ ID を再帰的に設定します。Pod のボリュームパーミッションおよび所有権変更ポリシーの設定についての詳細は、Kubernetes ドキュメントを参照してください。

2. ステートフルセットのモニタリングデプロイメントはすべて、**nobody** ユーザーの ID **65534** で実行されます。

(BZ#1868976)

- 以前のバージョンでは、ハイパーバイザーが別の仮想プロセッサーを提供する間に仮想 CPU が実際の CPU を待機する時間である CPU Steal Time が報告される CPU 消費のメトリクスックに影響を及ぼしました。その結果、CPU 使用率はノードの CPU 数よりも大きくなる可能性がありました。今回のリリースより、CPU 消費を報告するメトリクスは CPU Steal Time を考慮しなくなり、報告される CPU 使用率は実際の CPU の使用状況を反映するようになりました。(BZ#1878766)

- 以前のバージョンでは、権限昇格したパーミッションのない認証要求は、ユーザー定義プロジェクトの Prometheus の **/api/v1/query** および **/api/v1/query_range** エンドポイントにアクセスできました。そのため、通常のサービスアカウントのトークンにアクセスできるユーザーは、任意のモニターされるターゲットからメトリクスを読み取れる可能性がありました。**kube-rbac-proxy** は、**/metrics** エンドポイントのみへの要求を許可するように設定されるました。**/metrics** エンドポイントのクラスター全体のパーミッションのない認証要求は、**api/v1/query** および **/api/v1/query_range** エンドポイントへのクエリーに対応して HTTP 404 ステータスコードを受信します。(BZ#1913386)

ネットワーク

- デフォルトゲートウェイを検出する **ovn-kube** のコードでは、マルチパス環境が考慮されませんでした。そのため、Kubernetes ノードはデフォルトゲートウェイを見つけることができず、起動に失敗しました。マルチパスが存在する場合に、最初に利用可能なゲートウェイを考慮するようロジックが変更されました。OVN-Kubernetes は、マルチパスおよび複数のデフォルトゲートウェイを使用する環境で機能するようになりました。(BZ#1914250)

- クラスターをデュアルスタックモードでデプロイする場合、OVN-Kubernetes は信頼できない情報源を使用していました。
  OVN-Kubernetes マスターノードは初期同期を実行し、OVN および Kubernetes システムのデータベースの同期を保ちます。この問題により、OVN-Kubernetes の起動時に競合状態が生じ、一部の Kubernetes サービスに到達不可能になりました。ブートストラップのロジックでは、これらのサービスが孤立していると見なされるとこれらを削除しました。

  今回のバグ修正により、Kubernetes が信頼できる情報源 (source of truth) として使用されるようになりました。OVN-Kubernetes が正しく起動し、起動時に OVN と Kubernetes の両方の同期を維持するようになりました。(BZ#1915295)

- Cluster Network Operator (CNO) 設定オブジェクトに **additionalNetworks** スタンザを指定して追加のネットワークを作成する場合、CNO は作成される NetworkAttachmentDefinition オブジェクトのライフサイクルを管理します。ただし、**additionalNetworks** スタンザから追加のネットワークを除外するように CNO 設定が更新されてもオブジェクトは削除されませんでした。本リリースでは、CNO は追加のネットワークに関連するすべてのオブジェクトを削除するようになりました。(BZ#1755586)

- OVN-Kubernetes クラスターネットワークプロバイダーの場合、egress IP アドレスが設定され、egress IP アドレスをホストするノードのいずれかが到達不能になる場合、到達不能なノードに割り当てられる egress IP アドレスは他のノードに再度割り当てられませんでした。本リリースでは、egress IP アドレスをホストするノードが到達不能であるも、egress IP アドレスは別のノードに割り当てられます。(BZ#1877273)

- OVN-Kubernetes クラスターネットワークプロバイダーの場合、**br-ex** ブリッジのルートの優先順位は、クラスターのインストール後に追加されるセカンダリーネットワークインターフェースのデフォルトルートによって置き換えられる可能性があります。セカンダリーデバイスのデフォルトルートがノードの br-ex ブリッジよりも優先される場合、クラスターネットワークは機能しなくなります。本リリースでは、**br-ex** ブリッジのデフォルトルートを置き換えることはできません。(BZ#1880259)

- 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、Red Hat Enterprise Linux (RHEL) 7 ワーカーノードをクラスターに追加する際に、新規ワーカーノードはクラスターネットワークに接続できませんでした。本リリースでは、RHEL ワーカーノードを正常に追加できるようになりました。(BZ#1882667)

- 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、VLAN またはボンディングされたネットワークデバイスをノード上のデフォルトゲートウェイとして使用することができませんでした。本リリースでは、OVN-Kubernetes はこれらのネットワークデバイスと連携するようになりました。(BZ#1884628)

- Kuryr 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、ホストネットワークを使用する Pod 用に不要な Neutron ポートが作成されました。本リリースでは、Neutron ポートはホストネットワーク Pod 用に作成されなくなりました。(BZ#1886871)

- 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、**br-ex** ブリッジは **veth<N>** などの他のインターフェースの割り当てをサポートせず、ブリッジに追加されるインターフェースが正常に機能しませんでした。本リリースでは、新しいインターフェースを **br-ex** インターフェースに割り当てることができ、正常に機能するようになりました。(BZ#1887456)

- 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、ExternalIP アドレスが設定されていると、その IP アドレスを使用するように設定されていないクラスター内のノードは、externalIP に送信されるトラフィックをルーティングしませんでした。クラスターのすべてのノードが ExternalIP に必要なルートで設定されるようになりました。(BZ#1890270)

- OpenShift SDN 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、namespace とネットワーク namespace が削除される順序は無視できませんでした。Namespace オブジェクトに関連付けられた NetNamespace オブジェクトが最初に削除される場合、ネットワーク namespace を再度作成できませんでした。本リリースでは、namespace およびその関連付けられたネットワークの namespace は任意の順序で削除できるようになりました。(BZ#1892376)

- OpenShift SDN 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、以前のバージョンでは、ネットワークプロバイダーは **unable to allocate netid 1** というメッセージをログに記録しました。このメッセージは、NETID が **10** 未満の場合は安全性に問題がないため、本リリースでは OpenShift SDN が NETID が **10** 未満の場合にこのメッセージを生成しなくなりました。(BZ#1897073)

- クラスターが OVN-Kubernetes クラスターネットワークプロバイダーを使用している場合、すべてのインバウンド ICMPv6 はノードと OVN の両方に誤って送信されました。本リリースでは、ICMPv6 Neighbor Advertisement および Route Advertisement のみがホストと OVN の両方に送信されます。その結果、クラスター内のノードに送信された ping により、重複した応答が出されなくなりました。(BZ#1897641)

- 以前のバージョンでは、ノードが多数あるクラスターでは、過剰なマルチキャスト DNS (mDNS) トラフィックが生成されました。その結果、ネットワークスイッチがオーバーフローする可能性がありました。本リリースでは、mDNS クエリーを 1 秒ごとに 1 回に制限しています。

- 以前のバージョンでは、IPv6、Whereabouts CNI プラグイン、および指定の除外されたサブネット範囲を使用する追加のネットワークの割り当てを作成すると、除外されたサブネット範囲が無視されました。今回のバグ修正により、サブネット範囲を除外できるようにプラグインが修正されました。(BZ#1900835)

- 以前のバージョンでは、特定の状況では、Pod は Multus のエラー状態により終了しませんでした。Multus のログには、問題が発生した場合に **failed to destroy network for pod sandbox**

というメッセージが含まれます。今回のバグ修正により、Multus が削除されたキャッシュファイルを容認し、Pod が終了できるようになりました。(BZ#1900835)

- 以前のバージョンでは、ネットワークポリシーで OpenShift SDN ネットワークプロバイダーを使用する場合、ネットワークポリシーを使用しない namespace であっても、Pod でネットワーク接続の問題が発生する可能性がありました。今回のバグ修正により、ネットワークポリシーを実装する基礎となる Open vSwitch (OVS) フローが有効になりました。(BZ#1914284)

- 以前のバージョンでは、OVN-Kubernetes ネットワークプロバイダーを使用し、複数の Pod を使用して外部ゲートウェイとして機能させる場合に、Pod をスケールダウンすると、namespace の他の Pod がトラフィックを残りの外部ゲートウェイにルーティングすることができませんでした。トラフィックはノードのデフォルトゲートウェイにルーティングされました。今回のバグ修正により、Pod は残りの外部ゲートウェイへのトラフィックのルーティングを継続するようになりました。(BZ#1917605)

ノード

- 以前のバージョンでは、Pod またはコンテナーの作成要求に時間がかかりすぎると、負荷がかかったクラスターはタイムアウトする可能性がありました。CRI-O がリソースの作成中の場合でも、kubelet はそのリソースの再要求を試行します。これにより、要求は **name is reserved** エラーを出して失敗します。CRI-O が元の要求を終了した後に、要求がタイムアウトしたことを認識し、失敗した Pod/コンテナーをクリーンアップし、プロセスを開始します。その結果、Pod およびコンテナーの作成は停止し、複数の **name is reserved** エラーが kubelet によって報告されます。これにより、すでにオーバーロードされたノードがさらにオーバーロードされます。今回の修正により CRI-O が変更され、システムの負荷が原因でタイムアウトした Pod またはコンテナー作成の進捗が保持されるようになりました。さらに CRI-O は kubelet からの新規の要求を停止するため、**name is reserved** エラーの発生が少なくなります。その結果、クラスターに負荷がかかる場合に、CRI-O は kubelet を表示し、クラスターへの負荷を軽減します。ノードの全体の負荷が減り、Kubelet および CRI-O はより迅速に調整されます。(BZ#1785399)

- 以前のバージョンでは、ボリュームのディープディレクトリーにより、SELinux の再ラベル時間が長くなりました。そのため、コンテナー作成要求はタイムアウトし、kubelet がそのリソースの再要求を試行し、**error reserving ctr name** または **Kubelet may be retrying requests that are timing out in CRI-O due to system load** エラーが生じました。今回の修正により CRI-O が変更され、システムの負荷が原因でタイムアウトした Pod またはコンテナー作成の進捗が保持されるようになりました。そのため、コンテナーの要求を時間内に満たすことができます。(BZ#1806000)

- 以前のバージョンでは、CRI-O は、ホストポートマッピングの管理に IPv4 iptables のみを使用していました。したがって、IPv6 では、ホストポートは機能しません。今回の修正により、IPv6 ホストポートをサポートするように CRI-O が変更されました。その結果、IPv6 を使用するホストポートは予想通りに機能します。(BZ#1872128)

- 以前のバージョンでは、HTTP/2 トランスポートにはタイムアウトロジックを提供する接続に正しいオプションが割り当てられませんでした。これにより、VMWare ネットワークインターフェース (およびその他のシナリオ) がが数秒間にわたって応答しなくなり、接続が警告なしに失敗しました。そのため、接続が滞り、これによりノードの停止していても検出されない、古い接続を使用した API 呼び出しの失敗などの他の関連する障害が発生しました。今回の修正により、適切なタイムアウトが追加されました。その結果、システム内の HTTP/2 接続の信頼性が高くなり、副次的な影響が軽減されます。(BZ#1873114)

- 以前のバージョンでは、Topology Manager のエンドツーエンドテスト (**openshift-tests run-test**) では、Machine Config Daemon (MCD) が各ワーカーノードで実行されている必要がありました。これは、Red Hat Enterprise Linux CoreOS (RHCOS) ノードにデプロイされるノードの場合に該当し、Red Hat Enterprise Linux (RHEL) にデプロイされるノードの場合には該当しません。そのため、RHEL にデプロイされたクラスターに対して実行する場合、Topology

Manager のエンドツーエンドテストは検出漏れ (false-negative) で失敗しました。今回の修正により、テストが変更され、MCD が検出されないノードを省略できるようになりました。その結果、検出漏れ (false-negative) を招く障害が報告されなくなりました。(BZ#1887509)

- 以前のバージョンでは、ステータスが欠落している場合に Kubelet は移行を適切に処理しませんでした。そのため、一部の終了した Pod は再起動されませんでした。今回の修正により、**failed** というコンテナーのステータスが追加され、必要に応じてコンテナーを再起動できるようになりました。その結果、kubelet Pod の処理によって無効な状態の移行が生じなくなりました。(BZ#1888041)

- 以前のバージョンでは、**cAdvisor** からのマシンメトリクスは Kubernetes 1.19 以降の場合に欠落していました。今回の修正により、**CAdvisor** マシンメトリクスを適切に収集できるようにコードが変更されました。その結果、マシンメトリクスが表示されるようになりました。(BZ#1913096)

- 以前のバージョンでは、Horizontal Pod Autoscaler (HPA) は、init コンテナーを持つ Pod などの不完全なメトリクスを持つ Pod を無視していました。そのため、init コンテナーを持つ Pod はスケーリングされませんでした。今回の修正により、Prometheus アダプターが init コンテナーの完全なメトリクスを送信するようになりました。その結果、HPA は init コンテナーを持つ Pod をスケーリングできます。(BZ#1867477)

- 以前のバージョンでは、Vertical Pod Autoscaler (VPA) にはデプロイメント設定のモニターするためのアクセスがありませんでした。そのため、VPA はデプロイメント設定のワークロードをスケーリングできませんでした。今回の修正により、VPA に適切なパーミッションが追加され、デプロイメント設定をモニターできるようになりました。その結果、VPA はデプロイメント設定のワークロードをスケーリングできます。(BZ#1885213)

Node Tuning Operator

- 無効な Tuned プロファイルが作成されると、**openshift-tuned** supervisor プロセスは今後のプロファイルの更新を無視し、更新されたプロファイルの適用に失敗する可能性があります。今回のバグ修正により、Tuned プロファイルアプリケーションの成否などの状態についての情報が保持されるようになりました。**openshift-tuned** は、新規の有効なプロファイルを受信する際にプロファイルアプリケーションの障害から回復できるようになりました。(BZ#1919970)

oauth-proxy

- 以前のバージョンでは、認証チェックの失敗についてのレガシーのロギングがありました。oauth-proxy の背後にあるサービスへの要求により、行がプロキシーログに書き込まれる可能性があり、これにより、ログが一杯になりました。今回の修正により、プロキシーから不要なログの行が削除されました。プロキシーではログのスパムが発生しなくなりました。(BZ#1879878)

- 以前のバージョンでは、**oauth-proxy** コマンドで正しくないオプションの組み合わせが指定されると、無効なオプションの処理により nil 逆参照 (nil dereference) が生じました。これにより、使用メッセージの最後にセグメンテーションの障害スタックトレースが出力されました。オプションの処理が改善され、正しくないオプションの組み合わせが指定されている場合に nil 逆参照が発生しなくなりました。正しくないオプションを指定すると、スタックの追跡なしで使用メッセージが出力されます。(BZ#1884565)

oc

- 以前のバージョンでは、ロギングライブラリーの変更により、ログレベルが 2 という低いレベルで goroutine スタックトレースが出力され、デバッグがより困難になりました。goroutine スタックトレースのログレベルが引き上げられ、ログレベル 6 以上でのみ出力されるようになりました。(BZ#1867518)

- 以前のバージョンでは、同じユーザー名を使用して OpenShift CLI (**oc**)で複数クラスターにログインすると、毎回それぞれのクラスターにログインする必要がありました。ユーザー名が同じ場合でも一意になるように、コンテキスト名が適切に更新されました。ログイン後にコンテキストを切り替えると、再度ログインする必要がなくなりました。(BZ#1868384)

- 以前のバージョンでは、**oc adm release mirror**を使用してリリースがディスクにミラーリングされる場合に、マニフェストファイル名にはアーキテクチャーの拡張 (例: **-x86_64**) が含まれませんでした。これにより、タグ名が競合しない場合でも、複数のアーキテクチャーを同じリポジトリーにミラーリングすることはできませんでした。ファイル名に適切なアーキテクチャーの拡張が含まれるようになり、タグ名の競合を防げるようになりました。(BZ#1878972)

- 以前のバージョンでは、イメージ検証オブジェクトが適切に設定されず、これにより、イメージの検証時に OpenShift CLI (**oc**) が nil ポインター例外を出して失敗する可能性がありました。イメージ検証オブジェクトが適切に設定され、イメージの検証時に OpenShift CLI (**oc**) は、nil ポインター例外を出して失敗しなくなりました。(BZ#1885170)

- 以前のバージョンでは、**oc adm verify-image-signature** を使用してイメージ署名を検証する際に正しくないユーザー名が使用され、イメージ署名の検証に失敗しました。イメージ署名を検証し、イメージ署名の検証が予想通りに機能する場合に、適切なユーザー名が使用されるようになりました。(BZ#1890671)

- 以前のバージョンでは、バージョン情報を提供するメタデータはビルドプロセス中に生成されず、OpenShift CLI (**oc**) の Windows バイナリーに存在しませんでした。適切な Windows バージョン情報が生成され、Windows バイナリーで利用可能になりました。(BZ#1891555)

- 以前のバージョンでは、ルート条件についての nil チェックがないと、ルートの記述時に OpenShift CLI (**oc**) でクラッシュが発生する可能性がありました。nil チェックが追加され、ルートの記述が適切に機能するようになりました。(BZ#1893645)

- 以前のバージョンでは、OpenShift CLI (**oc**) にはクライアントスロットリングについての低い制限が設定され、API 検出に到達する要求はクライアントコードによって制限されました。クライアントのスロットリング制限が引き上げられ、クライアント側のスロットリングが表示される頻繁が低くなりました。(BZ#1899575)

- 以前のバージョンでは、**oc debug** コマンドの変更時に init コンテナーのサポートが失われ、init コンテナーのデバッグを行うことができませんでした。init コンテナーのサポートが **oc debug** コマンドに追加され、init コンテナーのデバッグが可能になりました。(BZ#1909289)

OLM

- Marketplace Operator は、**marketplace-operator** Pod が正常に終了するたびにその提供するサービスが低下することを報告するように作成されました。このレポートは通常のクラスターアップグレード時に発生しました。これにより、通常のアップグレード時に Pod が動作が低下したものとして報告されるため、混乱が生じました。Marketplace Operator は、正常に終了し、Telemeter クライアントが degraded のフラグを付けない場合は低下したことを示す報告をしなくなりました。(BZ#1838352)

- 以前のバージョンでは、Operator のアップグレード時に、Operator Lifecycle Manager (OLM) はアップグレードの完了前に既存のクラスターサービスバージョン (CSV) を削除しました。これにより、新規 CSV が「Pending」状態のままになりました。今回のバグ修正により OLM が更新され、サービスアカウントの所有権がチェックされ、新規 CSV について新規サービスアカウントが作成されるようになりました。その結果、新規 CSV が「Succeeded」の状態に正常に移行するまで既存の CSV が削除されなくなりました。(BZ#1857877)

- 以前のバージョンでは、Operator Lifecycle Manager (OLM) は存在しないチャネルを指定する **Subscription** オブジェクトを受け入れました。サブスクリプションは正常であると表示され、関連するエラーメッセージが表示されないため、ユーザーに混乱を招きました。今回のバグ修

正により OLM が更新され、このシナリオでは **Subscription** オブジェクトが失敗するようになりました。クラスター管理者は、以下の例のように、依存関係の解決の失敗情報について **default** namespace のイベントを確認できます。

```
$ oc get event -n default
```

出力例

```
LAST SEEN   TYPE      REASON           OBJECT                  MESSAGE
6m22s       Warning   ResolutionFailed   namespace/my-namespace    constraints not satisfiable: my-operator is mandatory, my-operator has a dependency without any candidates to satisfy it
```

(BZ#1873030)

- 以前のバージョンでは、Operator Lifecycle Manager (OLM) での受付 Webhook 設定のサポートは、API サーバーのデプロイ時に使用される CA 証明書生成コードを再利用していました。このコードで使用されるマウントディレクトリーは、証明書情報を以下の場所に配置します。

  - **/apiserver.local.config/certificates/apiserver.crt**
  - **/apiserver.local.config/certificates/apiserver.key**

  ただし、Kubebuilder または Operator SDK を使用してビルドされる受付 Webhook は、CA 証明書が以下の場所にマウントされることを予想します。

  - **/tmp/k8s-webhook-server/serving-certs/tls.cert**
  - **/tmp/k8s-webhook-server/serving-certs/tls.key**

  この不一致により、Webhook の実行が失敗しました。今回のバグ修正により、OLM が更新され、Kubebuilder または Operator SDK でビルドされる Webhook によって予想されるデフォルトの場所に Webhook CA 証明書がマウントされるようになりました。その結果、Kubebuilder または Operator SDK でビルドされた Webhook を OLM でデプロイできるようになりました。(BZ#1879248)

- API サービス、変換 Webhook、または受付 Webhook を使用して Operator をデプロイする場合、Operator Lifecycle Manager (OLM) は既存のリソースから CA を取得し、CA ハッシュアノテーションを算出する必要があります。このアノテーションは、OLM がデプロイメントが正常にインストールされていることを確認するために使用するデプロイメントハッシュに影響を与えます。現時点で、OLM は変換 Webhook から CA を取得しないため、無効なデプロイメントハッシュが発生し、これにより OLM はクラスターサービスバージョン (CSV) の再インストールを試行します。
  CSV が変換 Webhook を定義するものの、API サービスまたは受付 Webhook が含まれていない場合、CSV は「Pending」、「ReadyToInstall」、および「Installing」フェーズを無限に繰り返します。今回のバグ修正により OLM が既存の変換 Webhook を使用して CA の値を取得できるように更新され、デプロイメントハッシュを正しく計算されるようになりました。その結果、OLM は API サービスまたは受付 Webhook なしで変換 Webhook を定義する CSV をインストールできるようになりました。(BZ#1885398)

- 以前のバージョンでは、**opm** コマンドの **semver-skippatch** モードでは、リリース前のバージョンが無視され、後のパッチバージョンのあるバンドルのみが有効な置き換えとして許可されました。同じパッチバージョンであるが、後のリリース前のバージョンを持つバンドルは、置き換え用として許可されませんでした。今回のバグ修正により、**semver-skippatch** チェッ

クをベースをパッチバージョンのみでなく、セマンティクスバージョン全体とするように **opm** コマンドが更新されました。その結果、後のリリース前のバージョンが **semver-skippatch** モードに対して有効になりました。(BZ#1889721)

- 以前のバージョンでは、Marketplace Operator はクラスターのアップグレード時に古いサービスをクリーンアップせず、Operator Lifecycle Manager (OLM) はサービスを検証せずに古いサービスを受け入れました。そのため、古いサービスはトラフィックを、古いコンテンツが含まれるカタログソース Pod に転送しました。今回のバグ修正により OLM がサービスに仕様ハッシュ情報を追加し、ハッシュ情報を比較してサービスに正しい仕様が含まれることをチェックするように更新されました。OLM はサービスが古い場合に削除し、再作成します。その結果、サービス仕様はトラフィックを正しいカタログソース Pod に転送するようになりました。(BZ#1891995)

- Operator を非接続レジストリーにミラーリングした後に、関連するバンドルイメージがないために Operator のインストールが失敗する可能性がありました。この問題は、バンドルイメージが **index.db** データベースに存在しないために生じました。今回のバグ修正により、**opm** コマンドが更新され、バンドルイメージがデータベースの **related_images** テーブルに置かれるようになりました。(BZ#1895367)

- 以前のバージョンでは、Operator の作成者は、**1** から **65535** の範囲外で設定されたコンテナーのポートを持つ Webhook を定義するクラスターサービスバージョン (CSV) を作成できました。そのため、検証の失敗により **ValidatingWebhookConfiguration** または **MutatingWebhookConfiguration** オブジェクトを作成できませんでした。正常にインストールされることのない CSV が作成される可能性がありました。CSV のカスタムリソース定義 (CRD) 検証に、**webhookDescription ContainerPort** フィールドの適切な最小および最大値が含まれるようになりました。コンテナーポートが定義されていない場合、デフォルトで **443** に設定されるようになりました。無効なコンテナーポートを持つ CSV は CSV の作成前に検証に失敗するようになりました。(BZ#1891898)

- いずれのチャネルエントリーでも参照されない標準 Operator イメージバンドルは **opm index prune** 操作後もそのまま残りました。これにより、予期しないインデックスイメージがミラーリングされました。標準イメージバンドルは、インデックスがプルーニングされる際に削除され、Operator カタログが後にミラーリングされる際に予期しないイメージが含まれなくなりました。(BZ#1904297)

- 以前のバージョンでは、Operator の更新により、Operator Pod が新規サービスアカウントの作成前にデプロイされる可能性がありました。Pod は既存のサービスアカウントを使用してデプロイでき、パーミッションが不十分な場合に起動に失敗する可能性がありました。クラスターサービスバージョン (CSV) が **Pending** から **Installing** 状態に移行する前に新規サービスアカウントが存在することを確認するためのチェックが追加されました。新規サービスアカウントが存在しない場合、CSV は **Pending** 状態のままとなり、デプロイメントは更新されません。(BZ#1905299)

- 以前のバージョンでは、Operator Lifecycle Manager (OLM) が **ClusterServiceVersion** (CSV) オブジェクトを複数のターゲット namespace にコピーする際に、コピーした CSV の **.status.lastUpdateTime** フィールドは現在の時間に設定されました。現在の時間が元の CSV の最後の更新時間よりも後の時間である場合、コピーされる CSV が元の CSV に一致しない同期の競合状態がトリガーされました。これは、多くの namespace がクラスターに存在する場合に発生する可能性が高くなりました。元の **.status.lastUpdateTime** タイムスタンプがコピーされた CSV に保持され、同期の競合状態は **.status.lastUpdateTime** の値の差異によってトリガーされなくなりました。(BZ#1905599)

- 以前のバージョンでは、**ClusterServiceVersion** (CSV) オブジェクトの **StrategyDetailsDeployment** オブジェクトで定義される Pod テンプレートには、CSV で定義されたものと一致しない Pod アノテーションが含まれる可能性がありました。Operator Lifecycle Manager (OLM) は、CSV のアノテーションが CSV の一部としてデプロイされる Pod に存在することが予想されたため、Operator のインストールに失敗しまし

た。**StrategyDetailsDeployment** オブジェクトで定義される Pod テンプレートのアノテーションは CSV で定義されるもので上書きされるようになりました。OLM は、アノテーションが Pod テンプレートで定義されたものと競合する CSV のデプロイに失敗しなくなりました。(BZ#1907381)

- **openshift-marketplace** namespace のデフォルトのカタログソースが OperatorHub API で無効にされる場合、そのデフォルトと同じ名前でカスタムカタログソースを作成できます。以前のバージョンでは、デフォルトのカタログソースと同じ名前を持つカスタムカタログソースは、Marketplace の再起動時に Marketplace Operator によって削除されました。アノテーションが Marketplace Operator によって作成されるデフォルトのカタログソースに追加されました。Operator は、Marketplace の再起動時にアノテーションを含むカタログソースのみを削除するようになりました。デフォルトカタログソースと同じ名前で作成されたカスタムカタログソースは削除されません。(BZ#1908431)

- 以前のバージョンでは、**oc adm catalog mirror** コマンドは、namespace がない Operator インデックスイメージの適切なマッピングを生成しませんでした。また、**--filter-by-os** オプションは、マニフェスト一覧全体をフィルターしました。これにより、カタログでフィルターされたイメージへの無効な参照が生じました。namespace のないインデックスイメージが正しくマッピングされ、**--index-filter-by-os** オプションが追加され、プルおよび展開されるインデックスイメージのみをフィルターできるようになりました。**oc adm catalog mirror** コマンドは、namespace のないインデックスイメージの有効なマッピングを生成し、**--index-filter-by-os** オプションでフィルターされたイメージへの有効な参照を作成できるようになりました。(BZ#1908565)

- 以前のバージョンでは、Operator はクラスターサービスバージョン (CSV) 置き換えチェーンで **skipRange** を指定し、これにより、Operator Lifecycle Manager (OLM) が Operator をそれ自体に対して更新する可能性がありました。この無限ループにより、CPU の使用率が上昇しました。CSV の置き換えチェーンが更新され、Operator が無効な **skipRange** がある場合も無限ループに陥ることがなくなりました。(BZ#1916021)

- 以前のバージョンでは、クラスターサービスバージョン (CSV) 調整ループの **csv.status.LastUpdateTime** 時間の比較は、常に **false** の結果を返しました。これにより、Operator Lifecycle Manager (OLM) Operator は CSV オブジェクトを継続的に更新し、別の調整イベントをトリガーしました。時間の比較が改善され、ステータスが変更されない場合に CSV が更新されなくなりました。(BZ#1917537)

- デフォルトの 15 分の再同期期間よりも長い 15 分の倍数のポーリング間隔が設定されたカタログ更新 Pod は、Catalog Operator によって継続的に調整されます。これは、次のポーリング時間に達するまで継続され、これにより CPU 負荷が増大しました。調整の再キューイングのロジックが改善され、継続的な調整と関連する CPU 負荷の増大が発生しなくなりました。(BZ#1920526)

- 以前のバージョンでは、Operator サブスクリプション作成の試行時に一致する Operator が見つからない場合に、解決の失敗イベントに一覧表示される制約に内部で使用される用語が含まれました。サブスクリプション制約の文字列は、ユーザーの視点での解決失敗の理由を説明するものではありませんでした。制約の文字列はより分かりやすくなりました。(BZ#1921954)

openshift-apiserver

- 以前のバージョンでは、**deploymentconfigs/<name>/instantiate** サブリソースをターゲットにする要求は **no kind "DeploymentConfig" is registered for version apps.openshift.io/** を出して失敗しました。**DeploymentConfig** の正しいバージョンが設定され、これらの要求は失敗しなくなりました。(BZ#1867380)

Operator SDK

- 以前のバージョンでは、すべての **operator-sdk** サブコマンドが、**PROJECT** がディレクトリー

である場合でも **PROJECT** ファイルの読み取りを試行しました。その結果、**PROJECT** ファイルを要求しないサブコマンドが失敗しました。**PROJECT** ファイルを要求しないサブコマンドは、この読み取りを試行せず、無効な **PROJECT** ファイルが存在する場合でも正常に実行されるようになりました。(BZ#1873007)

- 以前のバージョンでは、**operator-sdk cleanup** コマンドを実行すると、**operator-sdk run bundle** コマンドでデプロイされた Operator はクリーンアップされませんでした。その代わりにエラーメッセージが表示され、Operator はクリーンアップされませんでした。**operator-sdk cleanup** コマンドが更新され、**run bundle** でデプロイされた Operator は **cleanup** コマンドを使用してクリーンアップできるようになりました。(BZ#1883422)

Performance Addon Operator

- 以前のバージョンでは、must-gather ロジックの誤った待機時間により、ログ収集が早く終了しました。この問題によって、タイミングによっては、ログ収集操作が途中で中断されました。これにより、ログ収集が部分的になりました。これは、must-gather ロジックに正しい待機時間を追加して修正されています。(BZ#1906355)

- 以前のバージョンでは、must-gather はすべてのノードでバインドされていない量の kubelet ログを収集していました。この問題により、過剰な量のデータが転送および収集されましたが、これにはユーザーにとっての実際の利点はありませんでした。
この問題は、収集される量を最後の 8 時間にバインドし、kubelet ログをワーカーノードでのみ収集し、コントロールプレーンノードでは収集しないようにすることで修正されています。(BZ#1918691)

- 以前のバージョンでは、マシン設定プールのパフォーマンスが低下すると、パフォーマンスプロファイルは正確なマシン設定プールの状態を表示するように更新されませんでした。パフォーマンスプロファイルノードセレクターまたはマシン設定プールセレクターは関連するマシン設定プールを適切に監視し、動作が低下したマシン設定プールは正しいステータスを反映するようになりました。(BZ#1903820)

RHCOS

- 以前のバージョンでは、RHCOS のインストール時に追加の Azure ディスクを設定すると、Azure ディスクの **udev** ルールが RHCOS initramfs に欠落するために失敗しました。インストール時に追加のディスクが正しく設定されるように、必要な **udev** ルールが追加されました。(BZ#1756173)

- 以前のリリースでは、**rhcos-growpart.service** はベストプラクティスではない方法で使用されていました。**rhcos-growpart.service** はインストール時に Ignition でディスクを設定することが優先されるために削除されました。RHCOS の初回インストール後にディスク設定を変更するには、必要なディスク設定の変更でシステムを再プロビジョニングする必要があります。(BZ#1851103)

- 以前のバージョンでは、Machine Config Operator は **rpm-ostree cleanup -p** の実行時に rpm-ostree の変更のロールバックを試行し、「System transaction in progress」エラーが発生しました。今回の修正により、D-Bus 処理に関連する rpm-ostree コードが改善され、エラーが発生しなくなりました。(BZ#1865839)

- 以前は、RHEL 8.2 の KVM では ppc64le または s390x での NVME エミュレーションのサポートはなく、NVME エミュレーションを使用する **kola --basic-qemu-scenarios** は失敗しました。ppc64le および s390x の NVME エミュレーションのテストが無効にされ、テストが正常に実行されるようになりました。(BZ#1866445)

- 以前のバージョンでは、Ignition は、DHCP サーバーの DHCP クエリーへの応答に時間がかかり過ぎる場合に、ネットワーク経由でリモート設定をフェッチできませんでした。
NetworkManager が DHCP の応答の待機を停止し、ネットワークが initramfs で設定されない

ためです。NetworkManager の新規バージョンでは、タイムアウトと再試行回数を増やすためにカーネルパラメーターとして **rd.net.timeout.dhcp=xyz** および **rd.net.dhcp.retry=xyz** オプションが設定されている場合にこれらを認識し、遅延する DHCP 応答に対応するようにこれらのオプションを設定できるようになりました。(BZ#1877740)

- 以前のバージョンでは、カーネルコマンドラインの複数の **nameserver=** エントリーが複数の NetworkManager 接続プロファイルを作成するために、正しくないネットワーク設定が作成されました。RHCOS の NetworkManager の新しいバージョンは複数の **nameserver=** エントリーを正しく処理し、複数の **nameserver=** エントリーが指定される場合にネットワーク設定が適切に生成されるようになりました。(BZ#1882781)

- 以前のバージョンでは、スタックをオーバーフローする再帰的呼び出しが原因で、ノードプロセスでセグメンテーション障害が生じました。このロジックエラーが修正され、セグメンテーション障害が発生しなくなりました。(BZ#1884739)

- 以前のバージョンでは、ネットワーク関連のサービスユニットは厳密に順序付けられていませんでした。つまり、 **-copy-network** を使用してコピーされたネットワーク設定がインストール済みシステムへの初回の再起動時に有効にならないことがありました。関連するサービスユニットの順序が修正され、それらが最初の再起動時に常に有効になるようになりました。(BZ#1895979)

- 以前のバージョンでは、**coreos-installer** コマンドが fdasd を呼び出して s390x 上の有効な DASD ラベルの有無をチェックする際に、udev が DASD デバイスを再度プローブし、これにより udev が依然としてデバイスにアクセス中であるために DASD のフォーマットに失敗しました。DASD ラベルのチェック後に、**coreos-installer** は udev が DASD の処理を完了するまで待機し、DASD フォーマットが正常に実行されるようになりました。(BZ#1900699)

- 以前のバージョンでは、DHCP を使用する場合に NetworkManager の接続設定のクエリーおよび修正を実行する際に混乱が生じました。すべてのインターフェースに一致する単一の NetworkManager 接続がデフォルトで作成されるためです。DHCP を使用する際に、NetworkManager がデフォルトで各インターフェースに個別の接続を作成するようになり、ユーザーエクスペリエンスが改善されました。(BZ#1901517)

- 以前のバージョンでは、実際のルートに切り替える前に initrd のネットワークインターフェースを適切に停止できないと、VLAN インターフェースへの静的 IP 割り当てが実際のルートで正常にアクティブにならない可能性がありました。今回の修正により、initrd でネットワークインターフェースが停止する方法が変更され、VLAN インターフェースへの静的 IP 割り当てが実際のルートで正常にアクティベートされるようになりました。(BZ#1902584)

- 以前のバージョンでは、RHCOS を DHCP 操作に dhclient を使用するように設定している場合に、システムでは DHCP アドレスを適切に取得できませんでした。initramfs で NetworkManager の使用への切り替えが行われると dhclient バイナリーが RHCOS から削除されるためです。dhsclient バイナリーは RHCOS に組み込まれ、RHCOS システムが dhclient を使用して DHCP 操作を正常に実行できるようになりました。(BZ#1908462)

- 以前のバージョンでは、iSCSI イニシエーター名を再生成するサービスユニットが初回起動時にのみ機能するため、アップグレードされたノードは一意の生成されるイニシエーター名を受信しませんでした。今回の修正により、サービスユニットが毎回のブート時に実行されるようになり、アップグレードされたノードが生成されたイニシエーター名を受信できるようになりました (すでに存在しない場合)。(BZ#1908830)

- 以前のバージョンでは、**/etc/mke2fs.conf** が存在しない場合に **mkfs.ext4** が失敗するため、Ignition で ext4 ファイルシステムを作成できませんでした。今回の修正により、**/etc/mke2fs.conf** が initramfs に追加され、Ignition が ext4 ファイルシステムを正常に作成できるようになりました。(BZ#1916382)

ルーティング

- 以前のバージョンでは、**haproxy.router.openshift.io/timeout** アノテーションを 25 日を超える値を使用してルートに設定することができました。25 日を超える値により、Ingress コントローラーが失敗しました。今回のバグ修正により、タイムアウトの上限が 25 日に設定されます。(BZ#1861383)

- 以前のバージョンでは、DNS がプロビジョニングされていないか、または必要なロードバランサーが準備状態にない場合でも、Ingress コントローラーは Available のステータスを報告していました。今回のバグ修正により、Ingress Operator に検証が追加され、Ingress コントローラーが利用可能になる前に DNS がプロビジョニングされ、必要な場合はロードバランサーが準備状態にあることを確認できるようになりました。(BZ#1870373)

- 以前のバージョンでは、誤字エラーを入力して、Ingress コントローラーのデフォルト証明書を存在しないシークレットに設定することができました。今回のバグ修正により、デフォルトの証明書を変更する前にシークレットが存在することを確認する検証が追加されました。(BZ#1887441)

- 以前のバージョンでは、63 文字を超える長さの名前を持つルートを作成できました。ただし、ルートの作成後に検証は失敗しました。今回のバグ修正により、ルートの作成時の検証が追加されました。(BZ#1896977)

ストレージ

- 以前のバージョンでは、受付プラグインは適切に設定されていない場合でもフェイルオーバードメインおよびリージョンラベルを追加し、静的にプロビジョニングされた永続ボリューム (PV) を使用する Pod が設定に空のリージョンを持つ OpenStack クラスターでの起動に失敗しました。今回の修正により、有効なリージョンおよび障害ドメインが含まれる場合にのみテーブルが PV に追加され、静的にプロビジョニングされた PV を使用する Pod は、空のリージョンまたは障害ドメインで設定された OpenStack クラスターの動的にプロビジョニングされる PV と同じ動作をするようになりました。(BZ#1877681)

- 以前のバージョンでは、**LocalVolumeDiscoveryResult** オブジェクトが Web コンソールに表示され、これらを手動で定義できる可能性があることを暗示しました。今回の修正により、**LocalVolumeDiscoveryResult** タイプに内部オブジェクトのフラグが付けられ、これは Web コンソールに表示されなくなりました。ローカルディスクを表示するには、**Compute → Nodes → Select Nodes → Disks** の順に移動します。(BZ#1886973)

- 以前のバージョンでは、認証情報を必要とするスナップショットの作成時に、**VolumeSnapshotClass** CRD がすでに削除されている場合にスナップショットの削除を強制的に実行できませんでした。今回のリリースより、**VolumeSnapshotClass** CRD が存在するかどうかに依存せずに、認証情報が **VolumeSnapshotContent** CRD から取得されるようになり、これらの認証情報を含むシークレットが継続的に存在する場合に、認証情報を使用するボリュームスナップショットおよびボリュームスナップショットのコンテンツを削除できるようになりました。(BZ#1893739)

- 以前のバージョンでは、Kubernetes FibreChannel (FC) ボリュームプラグインは削除前にマルチパスデバイスを適切にフラッシュしませんでした。また、稀なケースとして、マルチパス FC デバイスのファイルシステムは Pod の破棄時に破損しました。Kubernetes は、ファイルシステムの破損を防ぐために FC マルチパスデバイスを削除する前にデータをフラッシュするようになりました。(BZ#1903346)

スケーリング

- 以前のバージョンでは、ハイパースレッディングを設定する **nosmt** 追加カーネル引数については、OpenShift Container Platform で使用する方法について文書化されていませんでした。ハイパースレッディングを無効にするには、ハードウェアおよびトポロジーに適したパフォーマンスプロファイルを作成し、**nosmt** を追加のカーネル引数として設定します。

詳細は、低レイテンシーおよびリアルタイムのアプリケーションのハイパースレッディングについて参照してください。

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
- **GA**: 一般公開機能
- **-**: 利用不可の機能

表1.2 テクノロジープレビュートラッカー

機能	OCP 4.5	OCP 4.6	OCP 4.7
Precision Time Protocol (PTP)	TP	TP	TP
oc CLI プラグイン	TP	TP	TP
Descheduler	TP	TP	GA
OVN-Kubernetes Pod ネットワークプロバイダー	TP	GA	GA
Prometheus に基づく HPA カスタムメトリクスアダプター	TP	TP	TP
メモリー使用率のための HPA	TP	TP	GA
サービスバインディング	TP	TP	TP
ログ転送	TP	GA	GA
ユーザー定義プロジェクトのモニタリング	TP	GA	GA
Cinder での raw ブロック	TP	TP	TP
CSI ボリュームスナップショット	TP	TP	GA
CSI ボリュームのクローン作成	TP	GA	GA
CSI ボリューム拡張	TP	TP	TP
vSphere Problem Detector Operator	-	-	GA

機能	OCP 4.5	OCP 4.6	OCP 4.7
CSI GCP PD Driver Operator	-	-	TP
CSI OpenStack Cinder Driver Operator	-	-	TP
CSI AWS EBS Driver Operator	TP	TP	TP
Red Hat Virtualization (oVirt) CSI ドライバー Operator	-	GA	GA
CSI インラインの一時ボリューム	TP	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
OpenShift Pipeline	TP	TP	GA
OpenShift GitOps	-	TP	GA
Vertical Pod Autoscaler	TP	TP	TP
Operator API	TP	GA	GA
カーネルモジュールのノードへの追加	TP	TP	TP
egress ルーター CNI プラグイン	-	-	TP
スケジューラーのプロファイル	-	-	TP
プリエンプションを実行しない優先順位クラス	-	-	TP
Kubernetes NMState Operator	-	-	TP
支援付きインストーラー	-	-	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 4.7 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、またはこれを引き続き許可することができます。特定の必要がなければ、認証されていないアクセスを無効にすることが推奨されます。認証されていないアクセスを引き続き許可する場合は、それに伴ってリスクが増大することに注意してください。

警告

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

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

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

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

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

(BZ#1821771)

- 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で vSphere 上の仮想マシンの電源をオンにすると、ノードのスケールアッププロセスは予想通りに機能しない可能性があります。ハイパーバイザー設定の既知の問題により、ハイパーバイザー内にマシンが作成されますが、電源がオンになりません。マシンセットをスケールアップした後にノードが **Provisioning** 状態のままである場合、vSphere インスタンス自体で仮想マシンのステータスを調査できます。VMware コマンド **govc tasks** および **govc events** を使用して、仮想マシンのステータスを判別します。以下のようなエラーメッセージがあるかどうかを確認します。

```
[Invalid memory setting: memory reservation (sched.mem.min) should be equal to
memsize(8192). ]
```

この VMware KBase の記事にある手順に従って、問題の解決を試行できます。詳細は、Red Hat ナレッジベースのソリューションの「[UPI vSphere] Node scale-up doesn't work as expected」を参照してください。(BZ#1918383)

- **x86_64** アーキテクチャーを使用する VMware でクラスターを実行し、**platform: none** フィールドが **install-config.yaml** ファイルに設定されていると、OpenShift Container Platform クラスターバージョン 4.7 の新規インストール、またはクラスターバージョン 4.6 からバージョン 4.7 へのアップグレードに失敗する可能性があります。この失敗は、クラスターが仮想ハードウェアバージョン 14 以上で設定された仮想マシン (VM) を使用する場合に発生します。回避策として、仮想ハードウェアのバージョン 13 を使用するように仮想マシンを設定できます。VMware Cloud (VMC) にデプロイされるクラスターでは、仮想ハードウェアバージョン 14 以上の問題は発生しません。(BZ#1941714)

- Prometheus の割り当てられた PVC を使用してクラスターモニタリングを実行している場合、OpenShift Container Platform 4.7 へのアップグレード時に OOM による強制終了が生じる可能性があります。永続ストレージが Prometheus 用に使用される場合、Prometheus のメモリー使用量はクラスターのアップグレード時、およびアップグレードの完了後の数時間で 2 倍になります。OOM による強制終了の問題を回避するには、ワーカーノードで、アップグレード前に利用可能なメモリーのサイズを 2 倍にできるようにします。(BZ#1925061)

- Pod をすぐに起動および停止すると、Pod が **Terminating** 状態のままになる可能性があります。回避策として、以下のコマンドを実行して停止状態の Pod を削除する必要があります。

```
$ oc delete --force -n <project_name> <pod_name>
```

  この問題は OpenShift Container Platform の今後のリリースで修正されます。(BZ#1929463)

- RHCOS リアルタイム (RT) カーネルは、現時点ではコンピュートノードでのみサポートされており、コントロールプレーンノードではサポートされていません。コンパクトなクラスターは、OpenShift Container Platform 4.7 の RT カーネルではサポートされていません。(BZ#1887007)

- 現時点で、現在の OpenShift Container Platform の制限により、AWS C2S シークレットリージョンにインストールされたクラスターで、テクノロジープレビュー機能である AWS Secure Token Service (STS) を使用することはできません。これは OpenShift Container Platform の今後のリリースで修正されます。(BZ#1927157)

- Red Hat が推奨する CloudFormation テンプレート をベースに独自のインフラストラクチャーを使用して AWS C2S Secret Region にクラスターをインストールしようとしても、インストール時のブートストラップノードの作成に関する問題が原因でこれを実行することはできません。(BZ#1924080)

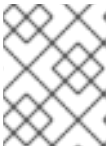
- Performance Addon Operator を 4.6 から 4.7 にアップグレードすると、エラーを出して失敗します。

```
"Warning  TooManyOperatorGroups  11m   operator-lifecycle-manager  csv created in namespace with multiple operatorgroups, can't pick one automatically"
```

  アップグレードする前に、「以前に特定の namespace にインストールされている場合の Performance Addon Operator のアップグレード」に説明されている手順に従います。

  (BZ#1913826)

- サポートされる NIC で SR-IOV の変更を有効にするには、再起動が必要になる場合があります。現時点で SR-IOV は準備状態になると再起動を実行します。この再起動が Machine Config ポリシーの変更と同時に起こると、ノードは不確定 (undermined) の状態になる可能性があります。Machine Config Operator は、更新されたポリシーが適用されていなくても適用されたと仮定します。



注記

この競合状態は、ノードを MCP および SR-IOV 変更を含む Machine Config Pool に追加すると生じる可能性もあります。

この問題を回避するには、MCO および SR-IOV の変更を必要とする新規ノードを順番に完了する必要があります。最初にすべての MCO 設定を適用し、ノードが解決するのを待機します。次に、SR-IOV 設定を適用します。

新規ノードが SR-IOV を含む Machine Config Pool に追加される場合は、Machine Config Pool から SR-IOV ポリシーを削除してから新規ワーカーを追加することで、この問題を回避できます。次に、SR-IOV ポリシーを再度適用します。

(BZ#1921321)

- **stalld** サービスはカーネルのバグをトリガーするために、ノードのフリーズが生じます。この問題を回避するには、Performance Addon Operator はデフォルトで **stalld** を無効にします。この修正は、DPDK ベースのワークロードに関連するレイテンシーに影響しますが、カーネルのバグ (BZ#1912118) が修正される場合に機能が復元されます。

- **ruby-kafka-1.1.0** および **fluent-plugin-kafka-0.13.1** gem を持つ Fluentd Pod には Apache Kafka バージョン 0.10.1.0 との互換性はありません。詳細は、Red Hat OpenShift Logging 5.0 リリースノートの「既知の問題」を参照してください。

- PTP (Precision Time Protocol) の障害が、アダプターカードの Mellanox MT27800 ファミリー [ConnectX-5] で確認されます。**ptp4l** ログでは、クロックの同期を妨げるエラーが確認されています。
このようなエラーにより、NIC ハードウェアクロックのリセットが必要となるため、通常のシステムクロック更新よりも大規模な更新が必要になります。この問題の根本的な原因は不明であり、現時点で回避策はありません。

  (BZ#1913279)

- 以前のバージョンでは、OpenStack SDK のバグにより、サーバーグループ **OSP16** を要求する際に失敗が生じました。そのため、コントロールプレーンサーバーの作成タスクの実行時に UPI Playbook の **control-plane.yaml** が失敗します。一時的な回避策として、OpenStack SDK を更新するためのホットフィックスを要求することができます。これにより、bastion ホストの OpenStack SDK が更新され、少なくとも **python-openstacksdk-0.36.4-1.20201113235938.el8ost** に対して UPI Ansible タスクを実行できるようになります。このホットフィックスにより、Playbook が正常に実行されるようになりました。(BZ#1891816)

- 最新の Dell ファームウェア (04.40.00.00)ノードを使用してベアメタルへの IPI インストールを試みると、デプロイが行われず、エラーがステータスに表示されます。これは、eHTML5 を Virtual Console Plugin として使用する Dell Firmware (4.40.00.00) によって生じます。
この問題を回避するには、Virtual Console Plugin を HTML5 に変更し、デプロイメントを再度実行します。ノードが正常にデプロイされるはずです。詳細は、仮想メディアを使用してインストールするためにファームウェア要件について参照してください。

  (BZ#1915828)

- ブートストラップ時に Kuryr を使用する RHOSP のクラスターのインストールは以下のメッセージを出してタイムアウトします。

```
INFO Waiting up to 20m0s for the Kubernetes API at https://api.ostest.shiftstack.com:6443...
INFO API v1.20.0+ba45583 up
INFO Waiting up to 30m0s for bootstrapping to complete...
```

```
ERROR Attempted to gather ClusterOperator status after wait failure: listing ClusterOperator
objects: Get
"https://api.ostest.shiftstack.com:6443/apis/config.openshift.io/v1/clusteroperators": dial tcp
10.46.44.166:6443: connect: connection refused
INFO Use the following commands to gather logs from the cluster
INFO openshift-install gather bootstrap --help
FATAL failed to wait for bootstrapping to complete: timed out waiting for the condition
```

タイムアウトは、Kuryr がクラスターのノードの RHOSP Networking サービス (neutron) サブネットを検出する方法の変更によって生じます。

回避策として、インストールドキュメントの「Kubernetes マニフェストおよび Ignition 設定ファイルの作成」セクションで説明されているコントロールプレーンマシンのマニフェストは削除しないでください。以下のコマンドを実行するように指示される場合:

```
$ rm -f openshift/99_openshift-cluster-api_master-machines-*.yaml openshift/99_openshift-
cluster-api_worker-machineset-*.yaml
```

代わりに以下のコマンドを実行します。

```
$ rm -f openshift/99_openshift-cluster-api_worker-machineset-*.yaml
```

(BZ#1927244)

- OpenShift Container Platform 4.3 および 4.4 では、ユーザーが複数のタブでコンソールを開いている場合、**Developer** パースペクティブの一部のサイドバーのリンクがプロジェクトに直接リンクされず、選択されたプロジェクトで予期しない変化が生じます。この問題は、今後のリリースで解決される予定です。(BZ#1839101)

- OpenShift Container Platform 4.5 では、スケーリングパーミッションを持つユーザーは、デプロイメントまたはデプロイメント設定の編集権限がない場合、コンソールを使用してデプロイメントまたはデプロイメント設定をスケーリングできません。この問題は、今後のリリースで解決される予定です。(BZ#1886888)

- OpenShift Container Platform 4.5 では、**Developer** パースペクティブに最小限のデータがあるか、またはデータがない場合、大半のモニタリングチャートまたはグラフ (CPU 消費、メモリー使用量、および帯域幅) には -1 から 1 の範囲が表示されます。ただし、これらの値はいずれもゼロ未満の値にすることはできません。この問題は、今後のリリースで解決される予定です。(BZ#1904106)

- 現時点で、Web コンソールのクイックスタートカードの前提条件は、一覧ではなく段落で表示されます。この問題は、今後のリリースで解決される予定です。(BZ#1905147)

- 現時点で、**Search Page** で、**Pipeline** リソーステーブルは **Name** フィルターの適用または削除の直後に更新されません。ただし、ページを更新するか、または **Pipelines** セクションを閉じるか、または展開する場合に、**Name** フィルターが適用されます。**Name** フィルターを削除すると同じ動作が確認されます。この問題は、今後のリリースで解決される予定です。(BZ#1901207)

- Operator SDK CLI ツールは macOS での実行をサポートしますが、現時点で macOS バイナリーは OpenShift ミラーサイトにありません。macOS バイナリーは今後の更新に追加されます。(BZ#1930357)

- 現時点で、IPsec が有効にされているクラスターで、Red Hat Enterprise Linux (RHEL) 7.9 ノードは Red Hat Enterprise Linux CoreOS (RHCOS) ノードと通信できません。(BZ#1925925)

- すべての HTTP トラフィックを HTTPS にリダイレクトする管理者によってプロビジョニングされる外部ロードバランサーを使用してデフォルトの Ingress Controller を公開するクラスターがある場合、4.6 から 4.7 へのアップグレードプロセスで Edge Termination を使用するように新規のクリアテキストの Ingress Canary ルートにパッチを適用する必要があります。

  patch コマンドの例

  ```
  $ oc patch route/canary -n openshift-ingress-canary -p '{"spec":{"tls":
  {"termination":"edge","insecureEdgeTerminationPolicy":"Redirect"}}}'
  ```

  (BZ#1932401)

- openswitch ("net: openvswitch: reorder masks array based on usage") コードへの更新により、openvswitch et/openvswitch/flow_table::flow_lookup がプリエンプション可能な (移行可能な) セクションの CPU ごとのデータにアクセスし、リアルタイムのカーネルパニックが発生します。その結果、kernel-rt は不安定になり、低レイテンシーのアプリケーションに影響します。これが修正されるまで、OpenShift Container Platform 4.7 にアップグレードしないことが推奨されます。

  (BZ#1918456)

- SR-IOV デバイスプラグインでは、ノード上の VFIO デバイスをリソースとして公開することを許可しません。これにより、Intel デバイスで DPDK ワークロードがブロックされます。
  この問題が修正されるまで、SR-IOV をお使いのお客様におかれましては OpenShift Container Platform 4.7 にアップグレードしないことをお勧めします。

  (BZ#1930469)

- OpenShift Container Platform 4.7 では、Operator インフラストラクチャーコードに追加される **ConfigInformers** オブジェクトは正常に起動しません。そのため、**ConfigObserver** オブジェクトはキャッシュの同期に失敗します。これが生じると、oVirt CSI ドライバー Operator は数分後にシャットダウンし、これにより継続的に再起動が繰り返されます。回避策として、以下の手順を実行できます。

  1. oVirt CSI Operator でプロジェクトをクラスターに切り替えます。

     ```
     $ oc project openshift-cluster-csi-drivers
     ```

  2. **warning: restart** メッセージの有無を確認します。

     ```
     $ oc status
     ```

  3. 警告がない場合は、以下のコマンドを入力します。

     ```
     $ oc get pods
     ```

  これにより、oVirt CSI ドライバー Operator は継続的に再起動しなくなります。(BZ#1929777)

- **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)

- OVN-Kubernetes ネットワークプロバイダーは、**NodePort** タイプサービスおよび **LoadBalancer** タイプサービスの **externalTrafficPolicy** 機能をサポートしていません。**service.spec.externalTrafficPolicy** フィールドは、サービスのトラフィックをノードロー

カルまたはクラスター全体のエンドポイントにルーティングするかどうかを決定します。現在、このようなトラフィックはデフォルトでクラスター全体のエンドポイントにルーティングされており、トラフィックをノードローカルエンドポイントに制限する方法はありません。この問題は、今後のリリースで解決される予定です。(**BZ#1903408**)

- 現在、Kubernetes ポートの衝突の問題により、Pod が再デプロイされた後でも、Pod 間の通信が機能しなくなる可能性があります。詳細および回避策については、Red Hat ナレッジベースソリューションの「Port collisions between pod and cluster IPs on OpenShift 4 with OVN-Kubernetes」を参照してください。(**BZ#1939676**、**BZ#1939045**)

- OpenShift Container Platform 4.7 では、Pod の制限および要求が Web コンソールに表示されません。この機能は、モニタリングに重大な変更を導入せずに、本リリースで実装することはできません。この機能は OpenShift Container Platform 4.8 リリースで修正されています。詳細は、Red Hat ナレッジベースソリューションの OpenShift Container Platform 4.7 コンソールで CPU およびメモリー使用量のチャートに要求または制限行が表示されなくなりました (BZ**#1975147**)。

1.9. エラータの非同期更新

OpenShift Container Platform 4.7 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 4.7 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することができます。エラータの通知を有効にすると、登録している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 4.7 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 4.7.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については、詳細についてその後のサブセクションで説明します。

重要

OpenShift Container Platform のいずれのリリースについても、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. RHEA-2020:5633 - OpenShift Container Platform 4.7.0 イメージのリリース、バグ修正およびセキュリティー更新

発行日: 2021-02-24

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.0 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2020:5633 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-2020:5634 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.0 コンテナーイメージの一覧

1.9.2. RHBA-2021:0678 - OpenShift Container Platform 4.7.1 バグ修正の更新

発行日: 2021-03-08

OpenShift Container Platform リリース 4.7.1 が公開されました。この更新に含まれるバグ修正は、RHBA-2021:0678 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-2021:0677 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.1 コンテナーイメージの一覧

1.9.2.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.3. RHBA-2021:0749 - OpenShift Container Platform 4.7.2 バグ修正の更新

発行日: 2021-03-15

OpenShift Container Platform リリース 4.7.2 が公開されました。この更新に含まれるバグ修正は、RHBA-2021:0749 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-2021:0746 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.2 コンテナーイメージの一覧

1.9.3.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.4. RHBA-2021:0821 - OpenShift Container Platform 4.7.3 バグ修正の更新

発行日: 2021-03-22

OpenShift Container Platform リリース 4.7.3 が公開されました。この更新に含まれるバグ修正は、RHBA-2021:0821 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-2021:0822 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.3 コンテナーイメージの一覧

1.9.4.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.5. RHSA-2021:0957 - OpenShift Container Platform 4.7.4 バグ修正およびセキュリティー更新

発行日: 2021-03-29

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.4 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2021:0957 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-2021:0958 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.4 コンテナーイメージの一覧

1.9.5.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.6. RHSA-2021:1005 - OpenShift Container Platform 4.7.5 バグ修正およびセキュリティー更新

発行日: 2021-04-05

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.5 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2021:1005 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-2021:1006 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.5 コンテナーイメージの一覧

1.9.6.1. 機能

1.9.6.1.1. AWS の VMC へのクラスターのインストール

OpenShift Container Platform クラスターは、クラスターを VMware Cloud (VMC) on AWS にデプロイして VMware vSphere インフラストラクチャーにインストールできます。詳細は、クラスターの VMC へのデプロイについてのドキュメントを参照してください。

1.9.6.1.2. メモリーおよびアップタイムのメタデータの Insights Operator アーカイブへの追加

今回の更新により、**uptime** および **memory alloc** メタデータが Insights Operator アーカイブに追加され、小規模なメモリーリークが適切に調査できるようになりました。詳細は、**BZ#1935605** を参照してください。

1.9.6.1.3. SAP ライセンス管理の強化

今回の更新により、以下のコマンドを使用してライセンス管理 Pod で失敗を検出できるようになりました。

```
# oc logs deploy/license-management-l4rvh
```

出力例

```
Found 2 pods, using pod/license-management-l4rvh-74595f8c9b-flgz9
+ iptables -D PREROUTING -t nat -j VSYSTEM-AGENT-PREROUTING
+ true
+ iptables -F VSYSTEM-AGENT-PREROUTING -t nat
+ true
+ iptables -X VSYSTEM-AGENT-PREROUTING -t nat
+ true
+ iptables -N VSYSTEM-AGENT-PREROUTING -t nat
iptables v1.6.2: can't initialize iptables table `nat': Permission denied
```

結果が **Permission denied** を返す場合は、iptables または kernal のアップグレードが必要になる場合があります。詳細は、BZ#1939061 を参照してください。

1.9.6.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.7. RHBA-2021:1075 - OpenShift Container Platform 4.7.6 バグ修正の更新

発行日: 2021-04-12

OpenShift Container Platform リリース 4.7.6 が公開されました。この更新に含まれるバグ修正は RHBA-2021:1075 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。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.6 コンテナーイメージの一覧

1.9.7.1. バグ修正

- 以前のバージョンでは、**Topology** ページの読み込み時にエラーが発生していました。今回のリリースにより、この問題は解決され、**Topology** ページが正常に読み込まれるようになりました。(BZ#1940437)

- 4.6 から 4.7 にアップグレードする場合、vsphere-hostname サービスで設定したホスト名はノードのインストール時にのみ適用されました。アップグレード前にホスト名が静的に設定されていない場合には、ホスト名が失われている可能性があります。今回の更新により、vsphere-hostname サービスのノードのインストール時のみの実行を許可する条件が削除されました。その結果、vsphere-hostname はアップグレード時に失われなくなりました。(BZ#1943143)

- 以前のバージョンでは、BZ#1936587 はグローバル CoreDNS キャッシュの最大 TTL を 900 秒に設定しました。そのため、アップストリームリゾルバーから受信される NXDOMAIN レコードが 900 秒間キャッシュされました。今回の更新により、最大 30 秒間、ネガティブな DNS 応答レコードが明示的にキャッシュされるようになりました。その結果、NXDOMAINs レコードの解決は 900 秒間キャッシュされなくなりました。(BZ#1943826)

- 以前のバージョンでは、**growpart** スクリプトは、インプレースの LUKS rootfs ファイルの再プロビジョニングを **requiring growing** と見なしませんでした。そのため、インプレース LUKs 暗号化を有効にするマシンが作成する rootfs ファイルを小さすぎる結果になりました。今回の更新により、**growpart** スクリプト (現在は **ignition-ostree-growfs**) はインプレース LUKS rootfs ファイルの再プロビジョニングを **requiring growing** と見なすようになりました。その結果、インプレース LUKs 暗号化を有効にするマシンは、利用可能なすべてのディスク領域を消費する rootfs ファイルを作成します。(BZ#1941760)

- 以前のバージョンでは、LUKS などの rootfs の再プロビジョニングが有効な場合に、**prjquota** カーネル引数がドロップされました。そのため、OpenShift Container Platform のディスク領域のクォータ管理機能が中断しました。今回の更新により、rootfs が再プロビジョニングされている場合でも、**prjquota** カーネル引数が保持されるようになりました。その結果、rootfs マウントオプションに依存する OpenShift Container Platform 機能が機能するようになりました。(BZ#1940966)

1.9.7.2. 機能

1.9.7.2.1. BareMetal Operator の機能拡張

今回の更新により、BareMetal Operator に新機能が追加され、異なる再起動モードを使用できるようになりました。これにより、クライアントが修復目的でシステムの電源を迅速にオフにし、ノードに障害が発生した場合にワークロードを可能な限り迅速に復元できるパスが提供されます。詳細は、BZ#1936407 を参照してください。

1.9.7.2.2. クラスター API プロバイダー BareMetal (CAPBM) の機能拡張

今回の更新により、クラスター API プロバイダーの BareMetal (CAPBM) に新機能が追加され、修復時にハード電源オフを要求するようになりました。今回の機能拡張により、BareMetal Operator に加えられた最近の変更を利用して、ハードリブートおよびソフトリブートモードをサポートするようになりました。その結果、修復が必要な場合に CAPBM がハードリブートを要求し、BareMetal Operator が発行するデフォルトのソフト電源オフを回避します。詳細は、BZ#1936844 を参照してください。

1.9.7.3. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.8. RHBA-2021:1149 - OpenShift Container Platform 4.7.7 バグ修正およびセキュリティー更新

発行日: 2021-04-20

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.7 が利用可能になりました。この更新に含まれるバグ修正は RHBA-2021:1149 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-2021:1150 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.7 コンテナーイメージの一覧

1.9.8.1. バグ修正

- 以前のバージョンでは、また不明な理由により、kubelet はノードに誤った IP アドレスを登録

する可能性がありました。その結果、ノードは再起動されるまで **NotReady** 状態になります。systemd マネージャーの設定は環境変数として有効な IP アドレスで再読み込みされるようになりました。つまり、kubelet が誤った IP アドレスを登録することによりノードが **NotReady** 状態になることはなくなりました。(BZ#1944394)

- 以前のバージョンでは、CVE-2021-3344 が修正された後に、ビルドはノードにエンタイトルメントキーを自動的にマウントしませんでした。この修正により、Pod の **/run/secrets** ディレクトリーからビルドコンテナーにコピーされるデータの量が最小限に抑えられ、**/run/secrets/etc-pki-entitlements** ファイルが省略されました。この修正により、OpenShift ホストまたはノードにエンタイトルメント証明書が保存されると、エンタイトルメントが適用されたビルドがシームレスに機能しませんでした。
  OpenShift ビルドイメージおよび関連付けられた Pod は、エンタイトルメント関連のすべてのファイルを **/run/secrets** からビルドコンテナーにマウントするようになりました。エンタイトルメントが適用されたビルドは OpenShift ホスト/ノードに保存されている証明書を取得できません。OpenShift Container Platform ビルドを Red Hat Enterprise Linux CoreOS (RHCOS) ノードで実行する際に、**level=warning msg="Path \"/run/secrets/etc-pki-entitlement\" from \"/etc/containers/mounts.conf\" doesn't exist, skipping** などの警告メッセージを無視できることに注意してください。

  (BZ#1945692)

1.9.8.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.9. RHSA-2021:1225 - OpenShift Container Platform 4.7.8 バグ修正およびセキュリティー更新

発行日: 2021-04-26

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.8 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2021:1225 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-2021:1226 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.8 コンテナーイメージの一覧

1.9.9.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.10. RHBA-2021:1365 - OpenShift Container Platform 4.7.9 バグ修正およびセキュリティー更新

発行日: 2021-05-04

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.9 が利用可能になりました。この更新に含まれるバグ修正は RHBA-2021:1365 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-2021:1366 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.9 コンテナーイメージの一覧

1.9.10.1. バグ修正

- 以前のバージョンでは、Cluster Samples Operator は監視するオブジェクトのコントローラーのキャッシュに変更を加える可能性がありました。これにより、Kubernetes がコントローラーキャッシュを管理する際にエラーが生じました。今回の更新により、Cluster Samples Operator がコントローラーキャッシュの情報を使用する方法が修正されました。そのため、Cluster Samples Operator はコントローラーキャッシュを変更してもエラーが生じなくなりました。(BZ#1950808)

1.9.10.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.11. RHBA-2021:1550 - OpenShift Container Platform 4.7.11 バグ修正およびセキュリティー更新

発行日: 2021-05-19

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.11 が利用可能になりました。この更新に含まれるバグ修正は、RHBA-2021:1550 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-2021:1551 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.11 コンテナーイメージの一覧

1.9.11.1. 機能

1.9.11.1.1. AWS 内部レジストリーの拡張機能

今回の更新により、ユーザーはインストール時に Amazon Web Services (AWS) 内部レジストリーにカスタムバケットタグを入力できるようになりました。これにより、ユーザーは OpenShift Container Platform によって作成されるオブジェクトを簡単に特定できます。

1.9.11.1.2. vSphere クラスターの拡張機能

今回の更新により、vSphere クラスターで **vsphere_node_hw_version_total** メトリクスを収集する新機能が追加されました。この情報を収集すると、ユーザーは **vsphere_node_hw_version_total** メトリクスに基づいて新規のヘルスチェックを作成できます。その結果、このメトリクスは Insights Operator の **config/metrics** ファイルに表示されるようになりました。詳細は、BZ#1955476 を参照してください。

1.9.11.1.3. Insights Operator の拡張機能

今回のリリースにより、Insights Operator は関連のある Pod、または正常でない Operator と同じ namespace にある Pod からログを収集するようになりました。詳細は、BZ#1953579 を参照してください。

1.9.11.1.4. AWS でのクラスターの既存 IAM ロールの使用

install-config.yaml ファイルに **compute.platform.aws.iamRole** および **controlPlane.platform.aws.iamRole** フィールドを設定して、マシンインスタンスプロファイルに既存の AWS アイデンティティーアクセス管理 (IAM) ロールを定義できるようになりました。これにより、命名スキームに一致させ、AWS にインストールされたクラスターの IAM ロール用に事前に定義されたパーミッション境界を含めることができます。

1.9.11.1.5. AWS での既存の Route53 ホストプライベートゾーンの使用

install-config.yaml ファイルに **platform.aws.hostedZone** フィールドを設定して、クラスターの既存の Route 53 プライベートホストゾーンを定義できるようになりました。独自の VPC を指定する場合も、既存のホストゾーンのみを使用できます。

1.9.11.1.6. 新規の OAuth トークン形式の情報提供アラート

OpenShift Container Platform の今後のリリースでは、SHA-256 プレフィックスが含まれない OAuth トークンは使用されず、作成できなくなります。今回のリリースにより、情報提供アラートは、プレフィックスのない OAuth トークンが含まれるクラスターの管理者に対し、予定される動作の変更について通知します。詳細は、BZ#1949941 を参照してください。

1.9.11.2. バグ修正

- 以前のバージョンでは、ユーザーにリソースの作成パーミッションがあるものの、編集パーミッションがない場合、Web コンソールの YAML エディターは読み取り専用モードに誤って設定されました。エディターのコンテンツは、リソースの作成アクセスのあるユーザーが編集できるようになりました。(BZ#1942027)

- 以前のバージョンでは、CCO デプロイメントが正常ではない場合に、Cloud Credential Operator (CCO) および Cluster Version Operator (CVO) の両方が報告しました。これにより、問題がある場合に 2 つのレポートが作成されました。今回のリリースにより、CCO はデプロイメントが正常ではない場合に報告しなくなりました。(BZ#1948702)

- 以前のバージョンでは、namespace は Machine Config Operator **relatedObjects** リソースになく、そのために一部のオンプレミスサービスのログは **must-gather** で収集されませんでした。今回のリリースにより、必要な namespace が Machine Config Operator **relatedObjects** リソースに追加され、オンプレミスサービスのログは **must-gather** で収集されるようになりました。(BZ#1950498)

- 以前のバージョンでは、kubelet は、とくにノードの再起動時にシークレットおよび設定マップの多数の監視要求を開くことで、API サーバーに影響を与えることがありました。今回のリリースにより、kubelet の監視要求の数が減り、API サーバーの負荷を軽減できるようになりました。(BZ#1951815)

- 以前のバージョンでは、Web コンソールはほとんどの場合に 12 時間形式で時間を表示し、24 時間形式で表示する場合もありました。また、過去の 1 年を上回る日数について年が表示されませんでした。今回のリリースにより、日付と時間が一貫性のある方法でフォーマットされ、ユーザーのロケールと言語設定と一致するようになり、過去の 1 年を上回る日数について年が表示されるようになりました。(BZ#1952209)

- 以前のバージョンでは、クラスターのアップストリームリゾルバーは、UDP 経由で 512 バイトを超える DNS 応答を返しました。そのため、CoreDNS がエラー **SERVFAIL** を返し、さまざまなエラーメッセージをログに記録することがありました。これらのエラーにより、クライアントが TCP での再試行を強制されることがあります。今回のリリースにより、CoreDNS **bufsize** プラグインは UDP バッファーサイズ 1232 バイトで有効にされ、CoreDNS は UDP で大規模な

DNS 応答を処理する際にエラー **SERVFAIL** を返したり、ランタイムエラーを表示する可能性が低くなりました。この変更により、UDP パケットの断片化が生じる可能性も低くなります。(BZ#1953097)

- 以前のバージョンでは、デフォルトの Google Cloud Platform (GCP) イメージは古く、新しい Ignition バージョンをサポートしない 4.6 リリースからのバージョンを参照していました。そのため、新規マシンがデフォルトの GCP イメージの使用時に起動できませんでした。今回の更新により、GCP イメージがリリースバージョンに一致するように修正され、新規マシンがデフォルトイメージで適切に起動されるようになりました。(BZ#1954610)

- 以前のバージョンでは、devfile をインポートする際に、環境変数、ポートおよび制限の設定を提供する **buildguidanceimage-placeholder** コンテナーは無視されました。そのため、プレースホルダーイメージを取得できず、ユーザーのコンテナーには追加の設定が欠落しているために、新規デプロイメントには起動できない 2 つ目のコンテナーが含まれました。今回のリリースにより、**buildguidanceimage-placeholder** コンテナーが新規デプロイメントから削除され、環境変数、ポート、および制限の設定がユーザーコンテナーに追加され、devfile が正常にインポートされるようになりました。(BZ#1956313)

- 以前のバージョンでは、Keepalived が強制的に再起動されると仮想 IP (VIP) アドレスが適切にクリーンアップされませんでした。そのため、VIP アドレスが複数のノードに表示される可能性があり、これにより VIP の背後でサービスへの接続に問題が発生しました。今回のリリースにより、Keepalived を起動する前に設定された VIP アドレスの削除が検証され、VIP アドレスが複数のノードに表示されなくなりました。(BZ#1957015)

1.9.11.3. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.12. RHSA-2021:1561 - OpenShift Container Platform 4.7.12 バグ修正およびセキュリティー更新

発行日: 2021-05-24

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.12 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2021:1561 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-2021:1562 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.12 コンテナーイメージの一覧

1.9.12.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.13. RHSA-2021:2121 - OpenShift Container Platform 4.7.13 バグ修正およびセキュリティー更新

発行日: 2021-05-31

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.13 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2021:2121 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-2021:2122 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.13 コンテナーイメージの一覧

1.9.13.1. バグ修正

- 以前のリリースでは、**é** などのアクセント文字が含まれるファイル名を使用して **oc start-build foo --from-dir=. --wait --follow** コマンドを実行すると、ビルドが失敗し、**error: unable to extract binary build input, must be a zip, tar, or gzipped tar, or specified as a file: exit status 1** のエラーが表示されました。今回の更新にでは、アクセント文字を使用してファイルを作成しても、ビルドが正常に完了するようになりました。(BZ#1935165)

1.9.13.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.14. RHSA-2021:2286 - OpenShift Container Platform 4.7.16 バグ修正およびセキュリティー更新

発行日: 2021-06-15

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.16 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2021:2286 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-2021:2287 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.16 コンテナーイメージの一覧

1.9.14.1. 特長

1.9.14.1.1. Insights Operator の拡張機能

今回の更新で、ユーザーは **virt_platform** メトリクスを収集できるようになりました。**virt_platform** メトリクスは、クラスターの仮想プラットフォームを判別するために Insights Operator のルールに必要です。この情報は、**config/metric** ファイルの Insights Operator アーカイブに保存されます。(BZ#1960645)

1.9.14.2. バグ修正

- 以前のバージョンでは、CoreDNS プラグインを使用すると、クエリーがローカルサーバーで応答されない場合にクエリーを転送できませんでした。そのため、クラスタードメインの DNS 名のクエリーは不正に失敗していました。今回の更新で、クエリーを正しく転送する CoreDNS プラグインへの変更が、クラスタードメインの有効なクエリーがすべて正常に機能するようになりました。(BZ#1962288)

- 以前のバグ修正中に、Pod ログのダウンロードリンクが、空のダウンロード属性を持つ標準の HTML アンカー要素に変更されました。その結果、ダウンロードファイルはデフォルトのファ

イル名形式を失いました。この更新により、アンカー要素のダウンロード属性にファイル名が追加され、Pod ログのダウンロード時に **<pod-name>-<container-name>.log** 形式のデフォルトのファイル名が使用されるようになりました。(BZ#1951210)

- 以前のバージョンでは、**vsphere-problem-detector** が OpenShift Container Platform 4.7 に新たに導入されたため、正常に動作させるには有効な vSphere 認証情報が必要でした。そのため、有効な vSphere 認証情報がない OpenShift Container Platform クラスターは **Degraded** とマークされました。今回の更新により、**vsphere-problem-detector** を使用してもクラスターは **Degraded** としてマークされず、代わりにアラートが発生して、そのまま実行されるようになりました。(BZ#1959546)

- 今回の更新で、Web コンソールの **Administration → Cluster Settings → Global Configuration** ページで設定リソースに対して不要な HTTP 要求が生じる問題を修正しています。(BZ#1960686)

- 以前のバージョンでは、Amazon Web Services コンソールの S3 レベルのバケットタグは、Operator の同期サイクルで上書きされました。そのため、ユーザー指定のタグがバケットからなくなることがありました。今回の更新により、ユーザータグは上書きされず、ユーザーが **spec.storage.managementState** を **Managed** に設定されている場合に常にバケットに設定されるようになりました。(BZ#1957308)

- 以前のバージョンでは、1 つ以上のコントロールプレーンノードに 2 つ目の内部 IP アドレスが追加されました。そのため、etcd メンバーシップの変更によってノードの etcd 提供証明書が再生成されないことがあり、etcd Operator のパフォーマンスは IP アドレスの変更の検出後に低下していました。今回の更新により、etcd Operator は新規ノードおよび既存ノードの IP アドレスの変更を区別し、Operator は既存ノードへの変更に対して証明書を提供するようになりました。その結果、IP アドレスをコントロールプレーンノードに追加すると、Operator のパフォーマンスが低下しなくなりました。(BZ#1954121)

- 以前のバージョンでは、マシン設定プール名のサフィックスをサポートしない設定が複数含まれている場合に OpenShift Container Platform 4.6.25 からアップグレードすると、Machine Config Operator (MCO) が同じ設定の重複するマシン設定を生成しました。その結果、アップグレードに失敗していました。今回の更新により、以前の重複マシン設定が消去され、OpenShift Container Platform 4.6.25 から 4.7.16 への適切なアップグレードが可能になりました。(BZ#1964568)

1.9.14.3. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.15. RHBA-2021:2502 - OpenShift Container Platform 4.7.18 バグ修正の更新

発行日: 2021-06-28

OpenShift Container Platform リリース 4.7.18 が公開されました。この更新に含まれるバグ修正は RHBA-2021:2502 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-2021:2503 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.18 コンテナーイメージの一覧

1.9.15.1. 特長

1.9.15.1.1. ストラテジーごとのビルド数の新しい Telemetry メトリクス

今回の更新では、Telemetry には新規の **openshift:build_by_strategy:sum** 測定メトリクスが含まれており、このメトリクスは、ストラテジータイプごとのビルド数を Telemeter クライアントに送信します。このメトリクスにより、サイト信頼性エンジニア (SRE) と製品マネージャーは、OpenShift Container Platform クラスターで実行されるビルドの種類を可視化できます。(BZ#1969963)

1.9.15.2. バグ修正

- 以前のバージョンでは、空の文字列 ('') がデフォルト値として指定されたパラメーターを使用してパイプラインを作成した場合に、OpenShift Container Platform Web コンソールのフィールドでは空の文字列を使用できませんでした。現在のリリースではこの問題は修正されています。現在は、'' は、**parameters** セクションで有効なデフォルトプロパティーとしてサポートされています。(BZ#1966275)

- 以前のバージョンでは、Cluster Version Operator は **ClusterOperator** リソースのパフォーマンスが 10 分間低下すると、**ClusterOperatorDegraded** アラートを報告していました。また、このアラートは通常より早く、インストール時にリソースの作成途中に発信されました。今回の更新により、期間が 10 分から 30 分に変更され、**ClusterOperatorDegraded** アラートが途中で発生することなく、十分な時間を提供することで、インストールが進行するようになりました。(BZ#1957991)

- vSphere にインストールする場合、ブートストラップマシンは **/etc/resolv.conf** ファイルのネームサーバーを正しく更新しないことがありました。その結果、ブートストラップマシンは一時的なコントロールプレーンにアクセスできず、インストールは失敗しました。この修正には、更新する適切な行の検索の信頼性を高める変更が含まれています。ブートストラップマネージャーが一時的なコントロールプレーンにアクセスできるようになったため、正常にインストールすることができます。(BZ#1967355)

- この更新の前は、Pipeline **ServiceAccount** は、プライベート Git リポジトリーの git import フロー中に作成されたシークレットを使用していなかったため、これらの Pipeline は失敗していました。この更新では、シークレットと Pipeline **ServiceAccount** にアノテーションを追加することで、問題を修正しています。プライベート Git リポジトリーの Pipeline が正しく実行されるようになりました。(BZ#1970485)

- 以前のバージョンでは、Google Cloud Load Balancer のヘルスチェックによりクラスターホストの以前の **conntrack** エントリーが残り、Google Cloud Load Balancer を使用した API サーバートラフィックにネットワークの中断が発生していました。今回の修正により、ヘルスチェックトラフィックがホストをループしなくなり、API サーバーへのネットワークが中断しなくなりました。(BZ#1949348)

- 以前のバージョンでは、Web コンソールの **Topology** ビューで Knative サービスを視覚化すると、ビルドステータスとリポジトリー情報が誤った場所に表示されました。今回の更新により、UI に渡されるデータが調整され、正しい情報のみが表示されるようになりました。(BZ#1954962)

- 以前のバージョンでは、Google Cloud Platform パーミッションが事前定義された **CredentialsRequest** カスタムリソースは、事前定義されたすべてのパーミッションを使用しない GCP プロジェクトに適用されると拒否されました。今回の修正により、Cloud Credentials Operator は許可されたパーミッションのテスト一覧を定期的に取得するようになり、**CredentialsRequest** カスタムリソースはパーミッションチェックに失敗しなくなりました。(BZ#1958983)

- BZ#1953097 の修正は、一部の DNS リゾルバーが最大 512 バイトしかを処理できない場合でも、バッファーサイズ 1232 バイトで CoreDNS **bufsize** プラグインを有効化しました。その結果、一部の DNS リゾルバーは DNS Operator からメッセージを受信できませんでした。今回の

修正により、バッファーサイズが 512 バイトに設定され、DNS リゾルバーは予想通りにメッセージを受信できるようになりました。(BZ#1967766)

- 以前のバージョンでは、Red Hat Enterprise Linux イメージを抽出する時に拡張ファイル属性の設定に root 権限が必要でした。そのため、通常のユーザーの場合には **oc image extract** が失敗していました。今回の更新により、OpenShift CLI (**oc**) はユーザーパーミッションをチェックし、拡張属性を root ユーザーだけに設定するようになりました。**oc image extract** コマンドは、root および通常のユーザーの両方で正常に機能します。(BZ#1969928)

1.9.15.3. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.16. RHBA-2021:2554 - OpenShift Container Platform 4.7.19 バグ修正およびセキュリティー更新

発行日: 2021-07-06

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.19 が利用可能になりました。この更新に含まれるバグ修正は RHBA-2021:2554 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-2021:2555 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.19 コンテナーイメージの一覧

1.9.16.1. バグ修正

- 以前のバージョンでは、ローカルクラスターサーバーで応答できない場合にCoreDNS プラグインにより、クエリーは転送されませんでした。状況によっては、これが原因でクラスター内の DNS 名のクエリーが失敗することがありました。今回の修正により、プラグインがすべてのクエリーを正しく転送できるものに変更になりました。(BZ#1962288)

- 今回の更新以前は、**kubeconfig** ファイルからのオプションで、別のプロジェクトに切り替える時にコピーされないものがありました。**exec** プラグインを使用してプロキシーを使用した認証を行い、クラスターにアクセスした場合に、その認証情報が失われる可能性があります。今回の更新により、必要な情報がすべてコピーされ、ユーザーはプロジェクトの切り替え後にプロキシーを継続して使用できるようになりました。(BZ#1963784)

- 以前は、イメージミラーリング中に作成された承認ヘッダーが、一部のレジストリーのヘッダーサイズ制限を超える可能性がありました。これにより、ミラーリング操作中にエラーが発生します。現在は、**oc adm catalog mirror** コマンドの **--skip-multiple-scopes** オプションが **true** に設定され、承認ヘッダーがヘッダーサイズの制限を超えないようになりました。(BZ#1976284)

1.9.16.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.17. RHBA-2021:2762 - OpenShift Container Platform 4.7.21 バグ修正およびセキュリティー更新

発行日: 2021-07-26

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.21 が利用可能になりました。この更新に含まれるバグ修正は RHBA-2021:2762 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-2021:2763 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.21 コンテナーイメージの一覧

1.9.17.1. 特長

1.9.17.1.1. Amazon Web Services SDK の更新

今回の更新により、**aws-sdk-go** は v1.38.35 に組み込まれ、新しい Amazon Web Services (AWS) リージョンをサポートするようになりました。この機能により、**image-registry** Pod がクラッシュするリスクなしに、新規クラスターを未知なリージョンにインストールできます。詳細は、**BZ#1977159** を参照してください。

1.9.17.2. バグ修正

- 以前のバージョンでは、Keepalived 設定が正しくないと、間違ったシステムに VIP が配置される場合があり、正しいシステムに戻れませんでした。今回の更新では、VIP が正しいシステムに配置されるように、Keepalived の誤った設定が削除されました。(**BZ#1971864**)

- 以前のリリースでは、プロキシーが設定された状態で Baremetal IPI がデプロイされると、内部の **machine-os** イメージのダウンロードはプロキシーを介して送信されました。これによりイメージが破損し、ダウンロードできなくなりました。この更新により、内部イメージトラフィックが **no_proxy** に修正され、イメージのダウンロードでプロキシーが使用されなくなります。(**BZ#1972291**)

1.9.17.3. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.18. RHBA-2021:2903 - OpenShift Container Platform 4.7.22 バグ修正の更新

発行日: 2021-08-03

OpenShift Container Platform リリース 4.7.22 が公開されました。この更新に含まれるバグ修正は RHBA-2021:2903 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-2021:2904 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.22 コンテナーイメージの一覧

1.9.18.1. 特長

1.9.18.1.1. Amazon Web Services (AWS) リージョンのサポート

今回の更新では、Amazon Web Services (AWS) **ap-northeast-3** リージョンへのインストールがサポートされるようになりました。詳細は、BZ#1942706 を参照してください。

1.9.18.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.19. RHSA-2021:2977 - OpenShift Container Platform 4.7.23 バグ修正およびセキュリティー更新

発行日: 2021-08-10

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.23 が利用可能になりました。この更新に含まれるバグ修正は、RHSA-2021:2977 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-2021:2979 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.23 コンテナーイメージの一覧

1.9.19.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.20. RHBA-2021:3032 - OpenShift Container Platform 4.7.24 バグ修正の更新

発行日: 2021-08-17

OpenShift Container Platform リリース 4.7.24 が公開されました。この更新に含まれるバグ修正は、RHBA-2021:3032 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-2021:3033 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.24 コンテナーイメージの一覧

1.9.20.1. バグ修正

- 以前のバージョンでは、インストールプログラムは、**noProxy** でスペースが入力できるので、順番になっていない **noProxy** の値が作成されていました。今回の更新で、インプットに含まれるスペースが削除され、値が適切に並び替えられました。(BZ#1954595)
- 以前のバージョンでは、OVN-Kubernetes は複数の **ipBlocks** で一部の NetworkPolicies を処理していたので、すべての IP アドレスに到達できませんでした。今回の更新では、**ipBlocks** が複数ある Kubernetes NetworkPolicies から Open Virtual Network (OVN) ACL が適切に生成されるようになりました。(BZ#1967132)
- 以前のバージョンでは、**spec.tolerations** のカスタム容認は **spec.nodeSelector** が設定されている場合にのみ適用されていました。今回の更新では、**spec.tolerations** が設定されている場合に、Operator はカスタム容認 (Toleration) を使用するようになりました。(BZ#1988388)

1.9.20.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.21. RHSA-2021:3262 - OpenShift Container Platform 4.7.28 バグ修正およびセキュリティー更新

発行日: 2021-09-01

OpenShift Container Platform リリース 4.7.28 が公開されました。この更新に含まれるバグ修正は、RHSA-2021:3262 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-2021:3263 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.28 コンテナーイメージの一覧

1.9.21.1. バグ修正

- 以前のバージョンでは、クラスターの **Insights status** を選択した場合に、Insights ウィジェットは、問題が何も発見されなかったと表示しませんでした。その結果、情報が何も含まれない、空白のウィジェットが表示されていました。今回の更新で、クラスターの **Insights status** を選択した場合に、問題が 0 件であったケースにその旨の情報が追加されます。その結果、クラスターが正常の場合に、ウィジェットには **Total Issues = 0** というチャートと、OpenShift Cluster Manager へのリンクが提供されます。(BZ#1986724)

- 以前のバージョンでは、BZ#1932452 のバックポートにより、ironic への導入に失敗した場合に **baremetal-operator** がプロビジョニングされた登録エラーを報告できました。そのため、**cluster-baremetal-operator** には、クラスターにインストールされている **BareMetalHost** カスタムリソース定義 (CRD) の別のコピーが含まれていました。ホストステータスの新しい値を保存すると、エラーが発生しました。今回の更新により、CRD の変更がバックポートされ、エラーが発生しなくなりました。(BZ#1976924)

- 以前のバージョンでは、**logs** コマンドに、クライアント設定がありませんでした。その結果、**oc logs** はパイプラインビルドでは機能しませんでした。今回の更新で、**logs** コマンドのクライアント設定が修正されました。その結果、**oc logs** はパイプラインビルドと連携するようになりました。(BZ#1974264)

- 以前のバージョンでは、無効なイメージストリームまたは未解決のイメージでデプロイメントが作成された場合には、デプロイメントコントローラーと API サーバーの **imagepolicy** プラグインの間の状態が一致しませんでした。そのため、レプリカセットの数が無限に発生し、etcd クォータの上限に到達してしまう可能性がありました。これが原因で、OpenShift Container Platform クラスター全体がクラッシュする可能性がありました。今回の更新により、API サーバーの **imagepolicy** プラグインの機能を減らしました。そのため、デプロイメントでは、不整合なイメージストリームは解決されません。(BZ#1981775)

1.9.21.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.22. RHSA-2021:3303 - OpenShift Container Platform 4.7.29 バグ修正およびセキュリティー更新

発行日: 2021-09-07

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.29 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-2021:3303 アドバイザリーに一覧表示されます。この更新に含まれる RPM パッケージは RHBA-2021:3304 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.29 コンテナーイメージの一覧

1.9.22.1. バグ修正

- OpenShift Container Platform 4.5 の OVN-Kubernetes で使用されるアドレスセットの命名規則が OpenShift Container Platform 4.6 で変更されたにも拘らず、アップグレードの一部として、既存のアドレスセットから新規命名規則への移行は処理されませんでした。ingress または egress セクションの namespace セレクターの条件を使用してバージョン 4.5 で作成されたネットワークポリシーは、この namespace 内の Pod IP アドレスの最新の情報に更新されていない以前のアドレスセットに依存していました。これらのポリシーは 4.6 以降のリリースでは正しく機能せず、予期しないトラフィックを許可または拒否する可能性があります。
  以前のバージョンでは、回避策はこれらのポリシーを削除し、再作成する必要がありました。
  今回のリリースにより、命名規則が古いアドレスセットが削除され、以前のアドレスセットを参照するポリシー ACL が OVN-Kubernetes のアップグレード時に新規命名規則に従ったアドレスセットを参照するように更新されました。バージョン 4.5 で作成した影響を受けるネットワークポリシーは、アップグレード後に再度機能するようになります。(**BZ#1976242**)

1.9.22.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.23. RHBA-2021:3422 - OpenShift Container Platform 4.7.30 バグ修正の更新

発行日: 2021-09-15

OpenShift Container Platform リリース 4.7.30 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-2021:3422 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-2021:3421 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.30 コンテナーイメージの一覧

1.9.23.1. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.24. RHBA-2021:3510 - OpenShift Container Platform 4.7.31 バグ修正の更新

発行日: 2021-09-21

OpenShift Container Platform リリース 4.7.31 が公開されました。この更新に含まれるバグ修正は RHBA-2021:3510 アドバイザリーに一覧表示されます。この更新に含まれる RPM パッケージは RHBA-2021:3509 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.31 コンテナーイメージの一覧

1.9.24.1. 特長

1.9.24.1.1. クラスタに対する新しい最小ストレージ要件

OpenShift Container Platformのクラスタをインストールするために必要な最小ストレージが、120GBから100GBに減少しました。このアップデートは、サポート対応のすべてのプラットフォームに適用されます。

1.9.24.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.25. RHBA-2021:3636 - OpenShift Container Platform 4.7.32 バグ修正およびセキュリティー更新

発行日： 2021-09-28

セキュリティー更新を含む OpenShift Container Platform リリース 4.7.32 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 -2021:3636 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-2021:3635 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.32 コンテナーイメージの一覧

1.9.25.1. 特長

- Kubernetes v1.20.10 が公開されました。詳細は、v1.20.10、v1.20.9、v1.20.8、v1.2 0.7、v1.20.6、v1.20.6、v1.2 0.5、v1.20.4、 v1.20.3、v1.20.2、v1.20.1、v1.20.0 の changelog を参照してください。

1.9.25.2. バグ修正

- 以前のバージョンでは、プロキシーとカスタム CA 証明書の組み合わせで RHOSP にデプロイされる場合、クラスターは完全に機能しませんでした。これは、プロキシー設定がないカスタム CA 証明書を使用して RHOSP エンドポイントへの HTTP トランスポート接続が原因でした。今回の更新で、カスタム CA 証明書に接続する際に、HTTP トランスポートへのプロキシー設定が使用されるようになりました。(**BZ#2000551**)

1.9.25.3. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

1.9.26. RHBA-2021:3686 - OpenShift Container Platform 4.7.33 バグ修正の更新

発行日： 2021-10-12

OpenShift Container Platform リリース 4.7.33 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 -2021:3686 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-2021:3685 アドバイザリーで提供されています。

このアドバイザリーでは、このリリースのすべてのコンテナーイメージに関する説明は除外されています。このリリースのコンテナーイメージに関する情報については、以下の記事を参照してください。

OpenShift Container Platform 4.7.33 コンテナーイメージの一覧

1.9.26.1. バグ修正

- 以前のバージョンでは、ハンドラー Pod の誤った容認により、それらがテイントを持つノードにデプロイされませんでした。今回の更新により、正しい容認が ハンドラー Pod に設定され、それらの容認はすべてのノードにデプロイされるようになりました。(BZ#1970127)

- 以前のバージョンでは、**NetworkManager-wait-online.service** が早い段階でタイムアウトし、**coreos-installer** が **Ignition** 設定をフェッチする前に接続を確立できませんでした。今回の更新で、**NetworkManager-wait-online.service** タイムアウトがデフォルトのアップストリーム値に引き上げられ、**Ignition** 設定の取得に失敗しなくなりました。(BZ#1983774)

- 以前のバージョンでは、チェックされていないインデックス操作 **--max-components** 引数がありました。今回の更新により、コンポーネントが範囲外のインデックスの値を要求しないようにチェックが実装されました。(BZ#2004194)

1.9.26.2. アップグレード

既存の OpenShift Container Platform 4.7 クラスターをこの最新リリースにアップグレードする方法については、CLI の使用によるクラスターの更新について参照してください。

第2章 OPENSHIFT CONTAINER PLATFORM のバージョン管理ポリシー

OpenShift Container Platform では、サポートされているすべての API の厳密な後方互換対応を保証しています。 ただし、アルファ API (通知なしに変更される可能性がある) およびベータ API (後方互換性の対応なしに変更されることがある) は例外となります。

Red Hat では OpenShift Container Platform 4.0 を公的にリリースせず、バージョン 3.11 の後に OpenShift Container Platform 4.1 を直接リリースしました。

OpenShift Container Platform のバージョンは、マスターとノードホストの間で一致している必要があります。ただし、クラスターのアップグレード時にバージョンが一時的に一致しなくなる場合を除きます。たとえば、4.7 クラスターではすべてのマスターは 4.7 で、すべてのノードが 4.7 である必要があります。以前のバージョンの **oc** をインストールしている場合、これを使用して OpenShift Container Platform 4.7 のすべてのコマンドを実行することはできません。新規バージョンの **oc** をダウンロードし、インストールする必要があります。

セキュリティーとは関連性のない理由で API が変更された場合には、古いバージョンの **oc** が更新されるように 2 つ以上のマイナーリリース (例: 4.1、4.2、4.3) 間での更新が行われます。新機能を使用するには新規バージョンの **oc** が必要になる可能性があります。4.3 サーバーにはバージョン 4.2 の **oc**で使用できない機能が追加されている場合や、バージョン 4.3 の **oc** には 4.2 サーバーでサポートされていない追加機能が含まれる場合があります。

表2.1 互換性に関する表

	X.Y (**oc** クライアント)	X.Y+N[a] (**oc** クライアント)
X.Y (サーバー)	1	3
X.Y+N[a] (サーバー)	2	1

[a] ここで、N は 1 よりも大きい数値です。

1 完全に互換性がある。

2 **oc** クライアントはサーバー機能にアクセスできない場合があります。

3 **oc** クライアントでは、アクセスされるサーバーと互換性のないオプションや機能を提供する可能性があります。