OpenShift Container Platform 4.5

リリースノート

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

Last Updated: 2023-05-22

OpenShift Container Platform 4.5 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

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Release_notes.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

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 4.5 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

Red Hat OpenShift Container Platform (RHBA-2020:2409) をご利用いただけるようになりました。本リリースでは、CRI-O ランタイムで Kubernetes 1.18 を使用します。以下では、OpenShift Container Platform 4.5 に関連する新機能、変更点および既知の問題について説明します。

Red Hat は OpenShift Container Platform 4.5.0 を GA バージョンとしてリリースせず、OpenShift Container Platform 4.5.1 を GA バージョンとしてリリースしています。

OpenShift Container Platform 4.5 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 4.5 は、RHEL バージョン 7.7 または 7.8、および Red Hat Enterprise Linux CoreOS (RHCOS) 4.5 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 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 RHEL バージョン 7.7 以降のいずれかを使用できます。

重要

RHEL 7 バージョン 7.7 以降のみがコンピュートマシンでサポートされるため、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 4.5 のリリースでは、バージョン 4.2 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. 新機能および機能拡張

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

1.2.1. インストールおよびアップグレード

1.2.1.1. インストーラーでプロビジョニングされるインフラストラクチャーを使用した vSphere へのクラスターのインストール

OpenShift Container Platform 4.5 では、インストーラーでプロビジョニングされるインフラストラクチャーを使用して vSphere にクラスターをインストールするためのサポートが導入されました。

1.2.1.2. ユーザーによってプロビジョニングされるインフラストラクチャーおよび共有 VPC を使用した GCP へのクラスターのインストール

OpenShift Container Platform 4.5 では、ユーザーによってプロビジョニングされるインフラストラクチャーおよび共有 VPC を使用して Google Cloud Platform (GCP) にクラスターをインストールするためのサポートが導入されました。

1.2.1.3. 3 ノードのベアメタルデプロイメント

ワーカーなしで OpenShift Container Platform に 3 ノードクラスターをインストールし、実行できます。これにより、デプロイメント、開発、テストに使用するための小規模なリソース効率の高いクラスターが提供されます。

以前のバージョンではテクノロジープレビューでしたが、この機能は OpenShift Container Platform 4.5 で完全にサポートされるようになりました。

詳細は、Running a three-node cluster を参照してください。

1.2.1.4. ネットワークが制限された環境のクラスターのアップグレードにおける改善

Cluster Version Operator (CVO) は、ネットワークが制限されたクラスターのアップグレードプロセスで、イメージ署名がクラスターの設定マップとして利用可能であるかどうかについてリリースイメージを検証できるようになりました。これにより、ネットワークが制限された環境でのアップグレード時に **--force** フラグを使用する必要がなくなりました。

この改善されたアップグレードワークフローは、強化された **oc adm release mirror** コマンドで実行されます。以下のアクションが実行されます。

- ミラーリングプロセスでリリースからイメージ署名をプルします。
- 署名設定マップを接続されたクラスターに直接適用します。

1.2.1.5. Azure プライベート DNS ゾーンの移行

Azure プライベート DNS ゾーンの移行に新規の **openshift-install migrate** コマンドが利用できるようになりました。インストーラーでプロビジョニングされるインフラストラクチャーを使用する Azure に OpenShift Container Platform バージョン 4.2 または 4.3 クラスターをインストールしている場合、クラスターはレガシーのプライベート DNS ゾーンを使用する可能性があります。その場合、これを新しいタイプのプライベート DNS ゾーンに移行する必要があります。

1.2.1.6. install-config.yaml でサポートされるフィールドについてのビルドインヘルプ

各リソースの短い説明を含め、サポートされている **install-config.yaml** ファイルのバージョンのすべてのフィールドを一覧表示する新規の **openshift-install explain** コマンドを利用できます。また、これは必須フィールドの詳細も提供し、デフォルト値を指定します。**explain** コマンドを使用すると、**install-config.yaml** ファイルの作成またはカスタマイズ時に設定オプションを常に検索する必要が少なくなります。

1.2.1.7. KMS キーを使用した EBS インスタンスボリュームの暗号化

KMS キーを定義して、EBS インスタンスボリュームを暗号化できるようになりました。これは、AWS へのデプロイ時に明示的なコンプライアンスおよびセキュリティー上のガイドラインがある場合に役立

ちます。KMS キーは、オプションの **kmsKeyARN** フィールドを設定して **install-config.yaml** ファイルに設定できます。以下は例になります。

```
apiVersion: v1
baseDomain: example.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    aws:
      rootVolume:
        kmsKeyARN: arn:aws:kms:us-east-2:563456982459:key/4f5265b4-16f7-xxxx-xxxx-
xxxxxxxxxxxx
...
```

キーが指定されていない場合、その特定リージョンのアカウントのデフォルト KMS キーが使用されます。

1.2.1.8. AWS に複数の CIDR を持つ既存 VPC へのインストール

AWS に複数の CIDR を持つ VPC に OpenShift Container Platform をインストールできるようになりました。これにより、マシンネットワークのセカンダリー CIDR を選択できます。VPC がインストーラーによってプロビジョニングされる場合、複数の CIDR を作成したり、サブネット間のルーティングを設定したりしません。複数の CIDR を持つ既存 VPC へのインストールは、ユーザーによってプロビジョニングされるインフラストラクチャーおよび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インストールワークフローでサポートされています。

1.2.1.9. カスタムドメイン名の AWS Virtual Private Cloud (VPC) DHCP オプションセットへの追加

カスタムドメイン名が AWS Virtual Private Cloud (VPC) DHCP オプションセットに追加できるようになりました。これにより、カスタム DHCP オプションが使用される場合に、新規ノードの証明書署名要求 (CSR) の承認が有効になります。

1.2.1.10. Ironic による IPv6 を使用したベアメタルホストのプロビジョニング

UEFI ネットワークスタックを使用した IPv6 プロビジョニングに必要なバイナリーが Ironic に導入されました。Ironic により IPv6 を使用してベアメタルホストをプロビジョニングできるようになりました。**snpnoly.efi** ブートローダーの実行プログラムおよび互換性のある iPXE バイナリーが **tftpboot** ディレクトリーに含まれるようになりました。

1.2.1.11. RHOSP 上のクラスターのカスタムネットワークおよびサブネット

OpenShift Container Platform 4.5 では、既存のネットワークおよびサブネットに依存する Red Hat OpenStack Platform (RHOSP) にクラスターをインストールするためのサポートが導入されました。

1.2.1.12. RHOSP 上のクラスターの追加ネットワーク

OpenShift Container Platform 4.5 では、RHOSP で実行されるクラスターでの複数のネットワークのサポートが導入されました。これらのネットワークは、インストール時にコントロールプレーンおよびコンピュートマシンの両方に指定できます。

1.2.1.13. Kuryr を使用するクラスターについての RHOSP ロードバランサーのアップグレードエクスペリエンスが強化される

Kuryr を使用するクラスターでは、13 から 16 にアップグレードされた RHOSP クラスターの Octavia 負荷分散サービスのサポートが改善されました。たとえば、これらのクラスターは Octavia OVN プロバイダードライバーをサポートするようになりました。

詳細は、Octavia OVN ドライバー について参照してください。

1.2.1.14. RPM パッケージをインストールする際に、複数のバージョンスキームが許可される

RPM パッケージをインストールする際に、OpenShift Container Platform では 3 つの値で表示されるバージョンスキームと 2 つの値で表示されるバージョンスキームの両方を使用できるようになりました。3 つの値で設定されるバージョンスキームは **x.y.z** 形式に従いますが、2 つの値で設定されるバージョンスキームは **x.y** 形式に従います。いずれかのスキームを使用するパッケージをインストールすることができます。詳細は、BZ#1826213 を参照してください。

1.2.1.15. デバッグ情報に SSH 設定が不要になる

ブートストラップホストからのデバッグ情報の収集に SSH 設定は必要なくなりました。詳細は、BZ#1811453 を参照してください。

1.2.1.16. マスターノードに有効なホスト名を付けることが可能になる

マスターノードには、有効なホスト名を付けることができます。詳細は、BZ#1804944 を参照してください。

1.2.1.17. Octavia OVN プロバイダードライバーが以前の RHOSP バージョンでサポートされる

RHOSP が Octavia OVN プロバイダードライバーをサポートする前にデプロイされていた OpenShift Container Platform クラスターがこのドライバーを使用できるようになりました。詳細は、BZ#1847181 を参照してください。

1.2.1.18. Octavia OVN プロバイダードライバーが同じポートのリスナーをサポートする

ovn-octavia ドライバーが、複数のプロトコルについて同じポートのリスナーをサポートするようになりました。以前のバージョンでは、これは **ovn-octavia** ドライバーでサポートされていませんでしたが、現在はサポートされており、これをブロックする必要はありません。つまり、**ovn-octavia** を使用する際に、たとえば DNS サービスが TCP プロトコルと UDP プロトコルの両方でポート 53 を公開することができます。詳細は、BZ#1846452 を参照してください。

1.2.2. セキュリティー

1.2.2.1. ネットワークが制限されたインストールでの oauth-proxy イメージストリームの使用

oauth-proxy イメージは、**oauth-proxy** イメージストリームを使用して、ネットワークが制限されたインストールの外部コンポーネントで使用できるようになりました。

1.2.3. イメージ

1.2.3.1. ファイルへの/からのリリースイメージのミラーリング

レジストリーからファイル、およびファイルからレジストリーにリリースイメージをミラーリングできるようになりました。

1.2.3.2. リリースイメージ署名のミラーリング

oc adm release mirror コマンドを拡張して、 Cluster Version Operator がミラーリングされたリリースを検証するために使用できる、リリースイメージ署名が含まれる設定マップマニフェストが作成され、適用されていました。

1.2.4. マシン API

1.2.4.1. AWS マシンセットによるスポットインスタンスのサポート

AWS マシンセットがスポットインスタンスをサポートするようになりました。これにより、オンデマンドのインスタンスよりもコストを節約できるようにマシンをスポットインスタンスとしてデプロイするマシンセットを作成できます。マシンセット YAML ファイルの **providerSpec** フィールドに以下の行を追加し、スポットインスタンスを設定できます。

```
providerSpec:
  value:
    spotMarketOptions: {}
```

1.2.4.2. マシンの最小数 0 への自動スケーリング

マシン Autoscaler のレプリカの最小数を **0** に設定できるようになりました。これにより、ゼロマシンとワークロードで必要とされるリソースに基づく必要なマシンとマシン数の間でスケーリングでき、Autoscaler のコスト効率が向上します。

詳細は、**MachineAutoscaler** リソース定義 について参照してください。

1.2.4.3. 空のセレクターを持つ MachineHealthCheck リソースがすべてのマシンを監視

空の **selector** フィールドを含む **MachineHealthCheck** リソースはすべてのマシンを監視するようになりました。

MachineHealthCheck リソースの **selector** フィールドについての詳細は、サンプル **MachineHealthCheck** リソース について参照してください。

1.2.4.4. oc explain の使用によるマシンおよびマシンセットフィールドの記述

完全な OpenAPI スキーマがマシンおよびマシンセットカスタムリソースに提供されるようになりました。**oc explain** コマンドは、マシンおよびマシンセット API リソースに含まれるフィールドの説明を提供するようになりました。

1.2.5. ノード

1.2.5.1. 新しい Descheduler ストラテジーが利用可能になりました (テクノロジープレビュー)

Descheduler では、**RemovePodsHavingTooManyRestarts** ストラテジーを設定できるようになりました。このストラテジーにより、再起動が多すぎる Pod がノードから削除されるようになります。同様に、Descheduler Operator は詳細なアップストリームの Descheduler ストラテジー名をサポートし、追加の 1 対 1 の設定が可能になりました。

詳細は、Descheduler ストラテジー を参照してください。

1.2.5.2. Vertical Pod Autoscaler Operator (テクノロジープレビュー)

OpenShift Container Platform 4.5 では、VPA (Vertical Pod Autoscaler Operator) が導入されました。VPA は、Pod 内のコンテナーの履歴および現在の CPU とメモリーリソースを自動的に確認し、確認された使用についての値に基づいてリソース制限および要求を更新できます。個別のカスタムリソース (CR) を作成して、VPA に対して **Deployment**、 **Deployment Config**、**StatefulSet**、**Job**、**DaemonSet**、 **ReplicaSet**、または **ReplicationController** などのなどのワークロードオブジェクトに関連付けられたすべての Pod を更新するように指示することができます。VPA は、Pod に最適な CPU およびメモリーの使用状況を理解するのに役立ち、Pod のライフサイクルを通じて Pod のリソースを自動的に維持します。

1.2.5.3. RHOSP での非アフィニティーコントロールプレーンノードのスケジューリング

RHOSP デプロイメントで別の物理ホストが利用可能な場合には、コントロールプレーンノードはそれらすべてに対してスケジュールされます。

1.2.6. クラスターモニターリング

1.2.6.1. 独自のサービスの監視 (テクノロジープレビュー)

以下の改善により、独自のサービスのモニターリングをさらに強化できるようになりました。

- 独自のサービスのメトリクスとクラスターメトリクスの統合が可能になります。
- ユーザー namespace でのサービスのメトリクスを記録およびアラートルールで使用できます。
- Alertmanager API のマルチテナンシーサポートを追加します。
- ユーザーの記録およびアラートルールをデプロイする機能が追加され、高い可用性で使用できるようになりました。
- Thanos Querier を使用して Thanos Stores をインストロスペクトする機能が追加されました。
- Web コンソールの単一ビューで、すべてのサービスのメトリクスにアクセスできます。

詳細は、独自のサービスのモニターリング を参照してください。

1.2.7. クラスターロギング

1.2.7.1. Elasticsearch のバージョンアップグレード

OpenShift Container Platform 4.5 のクラスターロギングは Elasticsearch 6.8.1 をデフォルトのログストアとして使用するようになりました。

新規 Elasticsearch バージョンでは、新しい Elasticsearch データモデルが導入されました。新規のデータモデルでは、タイプ (インフラストラクチャーおよびアプリケーション) およびプロジェクトでデータがインデックス化されなくなりました。データはタイプ別にのみインデックス化されます。

- OpenShift Container Platform 4.4 の **project-** インデックスで以前に使用されていたアプリケーションログは、**app-** で始まるインデックスのセットで使用されます。
- **.operations-** インデックスで以前に使用されたインフラストラクチャーログは、**infra-** インデックスで使用されるようになりました。

- 監査ログは **audit-** インデックスに保存されます。

新規データモデルにより、更新により、既存のカスタム Kibana インデックスパターンおよびビジュアライゼーションは新規バージョンに移行しません。更新後、Kibana インデックスパターンおよびビジュアライゼーションを、新規インデックスに一致させるように再作成する必要があります。

Elasticsearch 6.x には、新規セキュリティープラグイン、Open Distro for Elasticsearch も含まれます。Open Distro for Elasticsearch は、データのセキュリティーを維持するために設計された包括的な高度なセキュリティー機能のセットを提供します。

1.2.7.2. 新規の Elasticsearch ログ保持機能

新規のインデックス管理機能は、インデックスを維持するために Elasticsearch ロールオーバー機能に依存します。クラスターから削除されるまでのデータの保持期間を設定できます。インデックス管理機能は Curator に置き換わります。OpenShift Container Platform 4.5 で、Curator は OpenShift Container Platform 4.5 より前の Elasticsearch インデックス形式のデータを削除しますが、これは今後のリリースでは削除されます。

1.2.7.3. Web コンソールの Kibana リンクが移動する

Kibana を起動するリンクが **Monitoring** メニューから OpenShift Container Platform コンソールの上部にある **Application Launcher** に移動しました。

1.2.8. Web コンソール

1.2.8.1. OperatorHub の Operator の新規インフラストラクチャー機能フィルター

OperatorHub の インフラストラクチャー機能 で Operator をフィルターできるようになりました。たとえば、非接続環境で機能する Operator を表示するには、**Disconnected** を選択します。

1.2.8.2. Developer パースペクティブ

Developer パースペクティブを使用して以下を実行できるようになりました。

- 関連する説明およびドキュメントを使用して、**Developer Catalog** での Helm チャートのインストールについて情報に基づく決定を行います。
- Helm リリースをアンインストールし、アップグレードし、ロールバックします。
- 動的な Knative イベントソースを作成し、削除します。
- 仮想マシンをデプロイし、それらのマシンでアプリケーションを起動するか、または仮想マシンを削除します。
- Git Webhook、Trigger、および Workspace を提供し、プライベート git リポジトリーの認証情報を管理し、OpenShift Pipeline の改善されたログを使用してトラブルシューティングを実行します。
- アプリケーションのデプロイメント時またはデプロイメント後にヘルスチェックを追加します。
- 効率的にナビゲートし、頻繁に検索される項目を追加します。

1.2.8.3. クラスターダッシュボードからアラートを設定するための単純化された手順

Web コンソールのクラスターダッシュボードに表示される **AlertManagerReceiversNotConfigured** アラートについては、新規の **Configure** リンクを利用できます。このリンクは Alertmanager 設定ページに移動します。これにより、アラートの設定に必要なステップが少なくなります。詳細は、BZ#1826489 を参照してください。

1.2.9. スケーリング

1.2.9.1. クラスターの最大数

OpenShift Container Platform 4.5 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。

1.2.10. ネットワーク

1.2.10.1. OpenShift SDN デフォルトの CNI ネットワークプロバイダーからの移行 (テクノロジープレビュー)

OVN-Kubernetes デフォルト Container Network Interface (CNI) ネットワークプロバイダーを OpenShift SDN のデフォルト CNI ネットワークプロバイダーから移行できるようになりました。

詳細は、OpenShift SDN デフォルト CNI ネットワークプロバイダーからの移行 を参照してください。

1.2.10.2. Ingress コントローラーの拡張機能

OpenShift Container Platform 4.5 には、以下の 2 つの重要な Ingress コントローラーの拡張機能が導入されました。

- Ingress コントローラーのアクセスログを有効にできます。
- Ingress コントローラーでワイルドカードルートポリシーを指定 できます。

1.2.10.3. HAProxy がバージョン 2.0.14 にアップグレード

Ingress コントローラーに使用される HAProxy がバージョン 2.0.13 から 2.0.14 にアップグレードされました。このアップグレードにより、ルーターの再読み込みのパフォーマンスが向上します。ルーターの再読み込みの最適化は、数千のルートを持つクラスターの場合に最も利点があります。

1.2.10.4. HTTP/2 Ingress サポート

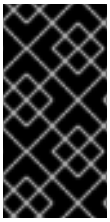
HAProxy で、透過的なエンドツーエンドの HTTP/2 接続を有効にできるようになりました。この機能により、アプリケーションの所有者は、単一接続、ヘッダー圧縮、バイナリーストリームなどの HTTP/2 プロトコル機能を利用できます。

個別の Ingress コントローラーまたはクラスター全体について、HAProxy で HTTP/2 接続を有効にすることができます。詳細は、HTTP/2 Ingress 接続 について参照してください。

クライアントから HAProxy への接続について HTTP/2 の使用を有効にするために、ルートはカスタム証明書を指定する必要があります。デフォルトの証明書を使用するルートは HTTP/2 を使用することができません。この制限は、クライアントが同じ証明書を使用する複数の異なるルートに接続を再使用するなどの、接続の結合 (coalescing) の問題を回避するために必要です。

HAProxy からアプリケーション Pod への接続は、re-encrypt ルートのみに HTTP/2 を使用でき、edge

termination ルートまたは非セキュアなルートには使用しません。この制限は、HAProxy が TLS 拡張である Application-Level Protocol Negotiation (ALPN) を使用してバックエンドで HTTP/2 の使用をネゴシエートするという事実によるものです。そのため、エンドツーエンドの HTTP/2 はパススルーおよび re-encrypt 使用できますが、非セキュアなルートまたは edge termination ルートでは使用できません。



重要

HTTP/2 プロトコルを使用する接続を WebSocket プロトコルにアップグレードすることはできません。WebSocket 接続を許可するための設計されたバックエンドアプリケーションがある場合、接続で HTTP/2 プロトコルの使用をネゴシエートすることを許可できません。さもないと WebSocket 接続は失敗します。

1.2.11. 開発者のエクスペリエンス

1.2.11.1. oc new-app で Deployment リソースが生成される

oc new-app コマンドは、デフォルトで **DeploymentConfig** リソースではなく、**Deployment** リソースを生成するようになりました。**DeploymentConfig** リソースを作成する場合は、**oc new-app** の呼び出し時に **--as-deployment-config** フラグを渡すことができます。詳細は、**Deployment および DeploymentConfig について** を参照してください。

1.2.11.2. イメージレジストリー CRD でのノードアフィニティースケジューラーのサポート

ノードアフィニティースケジューラーは、インフラストラクチャーノードが存在しない場合でもイメージレジストリーのデプロイメントが完了するようにサポートされるようになりました。ノードアフィニティースケジューラーは手動で設定する必要があります。

詳細は、ノードのアフィニティールールを使用したノード上での Pod 配置の制御 を参照してください。

1.2.11.3. カスタム S3 エンドポイントの仮想ホストバケット

仮想ホストバケットは、クラスターを新規または非表示の AWS リージョンにデプロイするためにサポートされるようになりました。

1.2.11.4. ビルドおよびイメージストリームのインポート時のノードのプル認証情報

ビルドおよびイメージストリームのインポートは、プルシークレットが明示的に設定されていない場合にクラスターをインストールするために使用されるプルシークレットを自動的に使用します。開発者は、このプルシークレットをそれらの namespace にコピーする必要はありません。

1.2.12. バックアップおよび復元

1.2.12.1. クラスターの正常なシャットダウンおよび再起動

OpenShift Container Platform 4.5 クラスターを正常にシャットダウンし、再起動できるようになりました。メンテナーンスの目的で、またはリソースコストの節約のためにクラスターを一時的にシャットダウンする必要がある場合があります。

詳細は、クラスターの正常なシャットダウン について参照してください。

1.2.13. 障害復旧

1.2.13.1. コントロールプレーンの証明書の自動リカバリー

OpenShift Container Platform 4.4.8 の初回導入時より、OpenShift Container Platform はコントロールプレーン証明書の期限切れの状態から自動的にリカバリーできるようになりました。例外として、kubelet 証明書を回復するために保留状態の **node-bootstrapper** 証明書署名要求 (CSR) を手動で承認する必要があります。

詳細は、Recovering from expired control plane certificates を参照してください。

1.2.14. ストレージ

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

Container Storage Interface (CSI) を使用して、AWS Elastic Block Store (EBS) 永続ストレージのプロビジョニングに必要な CSI ドライバーをデプロイできるようになりました。この Operator はテクノロジープレビュー機能です。詳細は、AWS Elastic Block Store CSI ドライバー Operator を参照してください。

1.2.14.2. OpenStack Manila CSI ドライバー Operator を使用した永続ストレージ

CSI を使用して、OpenStack Manila 共有ファイルシステムサービスの 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 ドライバー Operator を参照してください。

1.2.14.3. CSI インライン一時ストレージを使用した永続ストレージ (テクノロジープレビュー)

CSI を使用して、永続ボリュームではなく、Pod 仕様にボリュームを直接指定できるようになりました。この機能はテクノロジープレビューであり、CSI ドライバーを使用する場合にデフォルトで利用できます。詳細は、CSI インラインの一時ボリューム を参照してください。

1.2.14.4. CSI ボリュームのクローン作成を使用した永続ストレージ

CSI を使用したボリュームのクローン作成 (以前はテクノロジープレビュー) は OpenShift Container Platform 4.5 で完全にサポートされるようになりました。詳細は、CSI ボリュームのクローン作成 を参照してください。

1.2.14.5. 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。

1.2.15. Operator

1.2.15.1. Operator および opm CLI ツールをパッケージ化する Bundle Format

Operator の Bundle Format は、OpenShift Container Platform 4.5 以降サポートされている Operator Framework によって導入された新しいパッケージ形式です。スケーラビリティーを向上させ、アップストリームユーザーがより効果的に独自のカタログをホストできるようにするために、Bundle Format 仕様は Operator メタデータのディストリビューションを単純化します。

注記

レガシーの Package Manifest Format は OpenShift Container Platform 4.5 で非推奨となっていますが、これは引き続きサポートされ、現在 Red Hat が提供する Operator は Package Manifest Format を使用して提供されています。

Operator バンドルは Operator の単一バージョンを表し、Operator SDK を使用してスキャフォールディングできます。オンディスクの バンドルマニフェスト は、Kubernetes マニフェストおよび Operator メタデータを保存する実行不可能なコンテナーイメージである バンドルイメージ としてコンテナー化され、提供されます。次に、バンドルイメージの保存および配布は、**podman**、**docker**、および Quay などのコンテナーレジストリーを使用して管理されます。

Bundle Format についての詳細は、パッケージ形式 について参照してください。

新規の **opm** CLI ツールも Bundle Format と共に導入されます。**opm** CLI を使用して、repository に相当するインデックスと呼ばれるバンドルの一覧から Operator のカタログを作成し、維持することができます。結果として、インデックスイメージ というコンテナーイメージをコンテナーレジストリーに保存し、その後にクラスターにインストールできます。

インデックスには、コンテナーイメージの実行時に提供される組み込まれた API を使用してクエリーできる、Operator マニフェストコンテンツへのポインターのデータベースが含まれます。OpenShift Container Platform では、OLM はインデックスイメージを **CatalogSource** オブジェクトで参照し、これをカタログとして使用できます。これにより、クラスター上にインストールされた Operator への頻度の高い更新を可能にするためにイメージを一定の間隔でポーリングできます。

opm の使用方法についての詳細は、カスタムカタログの管理 について参照してください。

1.2.15.2. Operator Lifecycle Manager での v1 CRD サポート

Operator Lifecycle Manager (OLM) は、Operator をカタログにロードし、それらをクラスターでデプロイする際に v1 カスタムリソース定義 (CRD) を使用する Operator をサポートするようになりました。以前のバージョンでは、OLM は v1beta1 CRD のみをサポートしていましたが、OLM は v1 および v1beta1 CRD を同じ方法で管理できるようになりました。

この機能をサポートするために、OLM は既存の CRD ストレージバージョンがアップグレードされた CRD に欠落することがなく、データ損失の可能性を回避することで CRD のアップグレードをより安全に行うようになりました。

1.2.15.3. etcd メンバーのステータス条件の報告

etcd クラスター Operator は etcd メンバーのステータス条件を報告するようになりました。

1.2.15.4. OLM での受付 Webhook のサポート

検証用および変更用の受付 Webhook により、リソースがオブジェクトストアに保存され、Operator コントローラーによって処理される前に、Operator の作成者はリソースのインターセプト、変更、許可、および拒否を実行することができます。Operator Lifecycle Manager (OLM) は、Operator と共に提供される際にこれらの Webhook のライフサイクルを管理できます。

詳細は、Operator Lifecycle Manager での受付 Webhook の管理 を参照してください。

1.2.15.5. openshift-config namespace から追加された設定マップの設定

設定マップの設定が Insights Operator を使用して **openshift-config** namespace から追加されるようになりました。これにより、証明書がクラスターの認証局に使用されるかどうかを確認し、**openshift-config** namespace から他のクラスター関連の設定を収集できます。

1.2.15.6. 読み取り専用 Operator API (テクノロジープレビュー)

新規 Operator API が読み取り専用モードでテクノロジープレビューとして利用可能になりました。以前のバージョンでは、Operator Lifecycle Manager (OLM) を使用した Operator のインストールでは、クラスター管理者が **CatalogSource**、 **Subscription**、 **ClusterServiceVersion**、および **InstallPlan** オブジェクトを含む複数の API を認識している必要がありました。この単一 Operator API リソースは、OpenShift Container Platform クラスターで Operator のライフサイクルを検出し、管理するためのよりシンプルなエクスペリエンスを実現するための最初のステップになります。

現時点では、CLI でのみ利用可能であり、有効にするにはいくつかの手順を実行する必要があります。この機能プレビューではファーストクラスの API オブジェクトとして Operator と対話します。クラスター管理者は、**oc get operator** コマンドなどを使用し、この API を読み取り専用モードで使用して以前にインストールされた Operator を検出できます。

このテクノロジープレビュー機能を有効にするには、以下を実行します。

手順

1. OLM の Cluster Version Operator (CVO) 管理 を無効にします。

```
$ oc patch clusterversion version \
    --type=merge -p \
    '{
       "spec":{
         "overrides":[
           {
             "kind":"Deployment",
             "name":"olm-operator",
             "namespace":"openshift-operator-lifecycle-manager",
             "unmanaged":true,
             "group":"apps/v1"
           }
         ]
       }
    }'
```

2. **OperatorLifecycleManagerV2=true** 機能ゲートを OLM Operator に追加します。

   a. OLM Operator のデプロイメントを編集します。

   ```
   $ oc -n openshift-operator-lifecycle-manager \
       edit deployment olm-operator
   ```

   b. 以下のフラグをデプロイメントの **args** セクションに追加します。

   ```
   ...
       spec:
         containers:
         - args:
   ```

```
...
      - --feature-gates
      - OperatorLifecycleManagerV2=true
```

c. 変更を保存します。

3. まだインストールしていない場合は、通常の OperatorHub メソッドを使用して Operator をインストールします。この例では、プロジェクト **test-project** にインストールされた etcd Operator を使用します。

4. インストールされた etcd Operator の新規 Operator リソースを作成します。

a. 以下をファイルに保存します。

etcd-test-op.yaml ファイル

```
apiVersion: operators.coreos.com/v2alpha1
kind: Operator
metadata:
  name: etcd-test
```

b. リソースを作成します。

```
$ oc create -f etcd-test-op.yaml
```

5. インストールされた Operator の新規 API へのオプトインを可能にするには、**operators.coreos.com/etcd-test** ラベルを Operator に関連する以下のオブジェクトに適用します。

- **Subscription**
- **InstallPlan**
- **ClusterServiceVersion**
- Operator によって所有される CRD

注記

今後のリリースでは、これらのオブジェクトには **Subscription** オブジェクトを使用して CSV がインストールされている Operator についてのラベルが自動的に付けられます。

以下は例になります。

```
$ oc label sub etcd operators.coreos.com/etcd-test="" -n test-project
$ oc label ip install-6c5mr operators.coreos.com/etcd-test="" -n test-project
$ oc label csv etcdoperator.v0.9.4 operators.coreos.com/etcd-test="" -n test-project
$ oc label crd etcdclusters.etcd.database.coreos.com operators.coreos.com/etcd-test=""
$ oc label crd etcdbackups.etcd.database.coreos.com operators.coreos.com/etcd-test=""
$ oc label crd etcdrestores.etcd.database.coreos.com operators.coreos.com/etcd-test=""
```

6. Operator が新規 API にオプトインしていることを確認します。

a. すべての **operators** リソースを一覧表示します。

```
$ oc get operators

NAME        AGE
etcd-test   17m
```

b. Operator の詳細を検査し、ラベルを付けたオブジェクトが表示されていることを確認します。

```
$ oc describe operators etcd-test
```

```
Name:         etcd-test
Namespace:
Labels:       <none>
Annotations:  <none>
API Version:  operators.coreos.com/v2alpha1
Kind:         Operator
Metadata:
  Creation Timestamp:  2020-07-02T05:51:17Z
  Generation:          1
  Resource Version:    37727
  Self Link:           /apis/operators.coreos.com/v2alpha1/operators/etcd-test
  UID:                 6a441a4d-75fe-4224-a611-7b6c83716909
Status:
  Components:
    Label Selector:
      Match Expressions:
        Key:       operators.coreos.com/etcd-test
        Operator:  Exists
    Refs:
      API Version:  apiextensions.k8s.io/v1
      Conditions:
        Last Transition Time:  2020-07-02T05:50:40Z
        Message:               no conflicts found
        Reason:                NoConflicts
        Status:                True
        Type:                  NamesAccepted
        Last Transition Time:  2020-07-02T05:50:41Z
        Message:               the initial names have been accepted
        Reason:                InitialNamesAccepted
        Status:                True
        Type:                  Established
      Kind:                    CustomResourceDefinition
      Name:                    etcdclusters.etcd.database.coreos.com 1
...
      API Version:             operators.coreos.com/v1alpha1
      Conditions:
        Last Transition Time:  2020-07-02T05:50:39Z
        Message:               all available catalogsources are healthy
        Reason:                AllCatalogSourcesHealthy
        Status:                False
        Type:                  CatalogSourcesUnhealthy
      Kind:                    Subscription
      Name:                    etcd 2
```

```
    Namespace:            test-project
...
    API Version:          operators.coreos.com/v1alpha1
    Conditions:
      Last Transition Time:  2020-07-02T05:50:43Z
      Last Update Time:      2020-07-02T05:50:43Z
      Status:                True
      Type:                  Installed
    Kind:                  InstallPlan
    Name:                  install-mhzm8 (3)
    Namespace:             test-project
...
    Kind:                  ClusterServiceVersion
    Name:                  etcdoperator.v0.9.4 (4)
    Namespace:             test-project
Events:                    <none>
```

1. いずれかの CRD
2. **Subscription** オブジェクト。
3. **InstallPlan** オブジェクト。
4. CSV。

1.2.15.7. メータリングのアップグレードおよびクラスター全体のプロキシー設定を反映するためのサポート

メータリング Operator を 4.2 から 4.4、4.5 にアップグレードできるようになりました。以前のバージョンでは、現行のメータリングのインストールをアンインストールしてから、メータリング Operator の新規バージョンを再インストールする必要がありました。詳細は、メータリングのアップグレード を参照してください。

今回の更新により、クラスター全体のプロキシー設定のサポートが利用可能になりました。さらに、アップストリームリポジトリーは operator-framework 組織から kube-reporting に移行しました。

1.2.16. OpenShift Virtualization

1.2.16.1. OpenShift Container Platform 4.5 での OpenShift Virtualization のサポート

Red Hat OpenShift Virtualization は OpenShift Container Platform 4.5 で実行するためにサポートされます。以前のバージョンで Container-native Virtualization として知られていた OpenShift Virtualization は、従来の仮想マシンをコンテナーと共に実行される OpenShift Container Platform に組み込み、それらをネイティブ Kubernetes オブジェクトとして管理することを可能にします。

1.3. 主な技術上の変更点

OpenShift Container Platform 4.5 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 SDK v0.17.2
OpenShift Container Platform 4.5 では Operator SDK v0.17.2 をサポートし、主に以下のような技術的な変更点が加えられています。

- **--crd-version** フラグが **new**、**add api**、 **add crd**、および **generate crds** コマンドに追加され、ユーザーが **v1** CRD にオプトインできるようになりました。デフォルト設定は **v1beta1** です。

Ansible ベースの Operator の拡張機能には、以下が含まれます。

- Ansible ベースの Operator 監視ファイルの相対 Ansible ロールおよび Playbook パスのサポート。
- Operator ログへのイベント統計出力。

Helm ベースの Operator の拡張機能には、以下が含まれます。

- Prometheus メトリクスのサポート。

terminationGracePeriod パラメーターのサポート
OpenShift Container Platform は、CRI-O コンテナーランタイムで **terminationGracePeriodSeconds** パラメーターを適切にサポートするようになりました。

API サーバーの正常性プローブの **/readyz** 設定
ユーザーによってプロビジョニングされるインフラストラクチャーを使用するすべての OpenShift Container Platform 4.5 クラスターは、API サーバーのヘルスチェックに **/readyz** エンドポイントを使用し、サポートされている状態を維持できるように設定される必要があります。OpenShift Container Platform 4.5 よりも前のバージョンにインストールされたユーザーによってプロビジョニングされるインフラストラクチャーを使用するクラスターは、**/readyz** を使用するように再度設定する必要があります。

/readyz を設定せずにユーザーによってプロビジョニングされるインフラストラクチャーを使用するクラスターでは、API サーバーの再起動時に API が停止する可能性があります。API サーバーは、設定の変更、証明書の更新またはコントロールプレーンマシンの再起動などのイベント後に再起動できます。ロードバランサーは、API サーバーが **/readyz** エンドポイントをオフにしてからプールから API サーバーインスタンスを削除するまで最大 30 秒かかるように設定する必要があります。この時間内に、エラーが返されるか、または正常な状態になるかによって **/readyz** エンドポイントを削除したり、追加したりする必要があります。readiness チェックでは 5 秒または 10 秒ごとにプローブすることが推奨されます。この場合、2 回連続して要求が正常に実行されると正常な状態となり、3 回連続して要求が失敗すると、正常でない状態になります。

詳細は、ご使用のクラウドプロバイダー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インストールについてのドキュメントでネットワークトポロジーの要件を確認してください。

OpenShift Container Platform リリースのバイナリー**sha256sum.txt.sig** ファイルの名前が変更される
OpenShift Container Platform リリースに含まれる **sha256sum.txt.sig** ファイルの名前が **sha256sum.txt.gpg** に変更されました。このバイナリーファイルには、各インストーラーおよびクライアントバイナリーのハッシュが含まれており、これらはバイナリーの整合性を確認するために使用されます。

バイナリーファイルの名前を変更すると、GPG が **sha256sum.txt** を正しく検証できるようになりますが、これは、命名の競合により実行できませんでした。

1.4. 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 4.5 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 4.3	OCP 4.4	OCP 4.5
サービスカタログ	DEP	DEP	REM
テンプレートサービスブローカー	DEP	DEP	REM
OpenShift Ansible Service Broker	DEP	REM	REM
OperatorSource	DEP	DEP	DEP
CatalogSourceConfig	DEP	DEP	REM
Operator Framework のパッケージマニフェスト形式	GA	DEP	DEP
v1beta1 CRD	GA	GA	DEP
AWS EFS の外部プロビジョナー (テクノロジープレビュー)	REM	REM	REM

1.4.1. 非推奨の機能

1.4.1.1. Jenkins Pipeline ビルドストラテジー

Jenkins Pipeline ビルドストラテジーが非推奨になりました。代わりに Jenkins または OpenShift Pipeline で Jenkinsfile を直接使用してください。

1.4.1.2. v1beta1 CRD

カスタムリソース定義 (CRD) の **apiextensions.k8s.io/v1beta1** API バージョンが非推奨になりました。これは今後の OpenShift Container Platform リリースで削除されます。

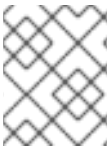
関連する詳細情報については、Operator Lifecycle Manager での v1 CRD サポート を参照してください。

1.4.1.3. カスタムラベルが使用されなくなる

flavor.template.kubevirt.io/Custom ラベルはカスタムフレーバーを特定するために使用されなくなりました。

1.4.1.4. OperatorSource および CatalogSourceConfig オブジェクトブロッククラスターのアップグレード

OperatorSource および **CatalogSourceConfig** オブジェクトは複数の OpenShift Container Platform リリースで非推奨になりました。OpenShift Container Platform 4.4 以降、クラスターにカスタム **OperatorSource** または **CatalogSourceConfig** オブジェクトがある場合、**marketplace** クラスター Operator は **Upgradeable=false** 条件を設定し、**Warning** アラートを発行します。つまり、オブジェクトが依然としてインストールされている場合は、OpenShift Container Platform 4.5 へのアップグレードはブロックされます。



注記

OpenShift Container Platform 4.4 z-stream リリースへのアップグレードは、この状態で引き続き許可されます。

OpenShift Container Platform 4.5 では、**OperatorSource** オブジェクトは依然として非推奨であり、デフォルトの **OperatorSource** オブジェクトを使用するためにのみ存在します。ただし、**CatalogSourceConfig** オブジェクトは削除されるようになりました。

アラートをクリアし、OpenShift Container Platform 4.5 へのクラスターのアップグレードを可能にするために **OperatorSource** および **CatalogSourceConfig** を **CatalogSource** オブジェクトの直接の使用に変換する方法については、OpenShift Container Platform 4.4 リリースノート を参照してください。

1.4.1.5. Ignition 設定仕様 v2

v2 Ignition 設定仕様について、新規 OpenShift Container Platform 4.6 インストールの一部として新規ノードをデプロイする際の使用が非推奨になりました。v2 Ignition 設定仕様は、マシン設定について引き続きサポートされます。

新規クラスターをデプロイするためにカスタム Ignition v2 仕様設定を作成している場合、新規 OpenShift Container Platform 4.6 クラスターのインストール時にこれらを仕様 v3 に変換する必要があります。Ignition Config Converter ツール を使用して変換プロセスを完了する必要があります。通常、v2 は v3 に直接変換できます。特定のエッジケースでは、出力を変更して仕様 v2 で想定される明示的な設定の詳細を行う必要がある場合があります。

1.4.2. 削除された機能

1.4.2.1. OpenShift CLI コマンドおよびフラグが削除される

以下の **oc** コマンドおよびフラグが関係します。

- **oc policy can-i** コマンドは OpenShift Container Platform 3.9 で非推奨となり、削除されています。代わりに **oc auth can-i** を使用する必要があります。
- **oc new-app** および **oc new-build** コマンドに以前使用されていた **--image** フラグは OpenShift Container Platform 3.2 で非推奨となり、削除されています。代わりに、これらのコマンドで **--image-stream** フラグを使用する必要があります。

- **oc set volumes** コマンドで以前使用されていた **--list** フラグは OpenShift Container Platform 3.3 で非推奨となり、削除されています。**oc set volumes** は、フラグなしにボリュームを一覧表示します。
- **oc process** コマンドで以前使用されていた **-t** フラグは OpenShift Container Platform 3.11 で非推奨となり、削除されています。代わりにこのコマンドで **--template** フラグを使用する必要があります。
- **oc process** コマンドで以前使用されていた **--output-version** フラグは OpenShift Container Platform 3.11 で非推奨となり、削除されています。このフラグはすでに無視されています。
- **oc set deployment-hook** コマンドで以前使用されていた **-v** フラグは OpenShift Container Platform 3.11 で非推奨となり、削除されています。代わりにこのコマンドで **--volumes** フラグを使用する必要があります。
- **oc status** コマンドで以前使用されていた **-v** および **--verbose** フラグは OpenShift Container Platform 3.11 で非推奨となり、削除されています。代わりにこのコマンドで **--suggest** フラグを使用する必要があります。

1.4.2.2. oc run OpenShift CLI コマンドが Pod の使用に制限される

oc run コマンドは、Pod を使用する場合にのみ使用できるようになりました。他のリソースを作成するには、代わりに **oc create** コマンドを使用します。

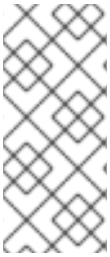
1.4.2.3. サービスカタログ、テンプレートサービスブローカー、およびそれらの Operator

重要

サービスカタログは OpenShift Container Platform 4 ではデフォルトでインストールされませんが、インストールされている場合は OpenShift Container Platform 4.5 へのアップグレードがブロックされるようになりました。

OpenShift Container Platform 4.2 以降ではサービスカタログ、テンプレートサービスブローカー、Ansible Service Broker およびそれらに関連付けられた Operator が非推奨になりました。Ansible Service Broker Operator および関連する API および APB を含む Ansible Service Broker は OpenShift Container Platform 4.4 で削除されています。

サービスカタログ、テンプレートサービスブローカー、およびそれらの関連付けられた Operator は、関連する **.servicecatalog.k8s.io/v1beta1** API を含め、OpenShift Container Platform 4.5 で削除されています。



注記

テンプレートは依然として OpenShift Container Platform 4.5 で利用できますが、テンプレートサービスブローカーで処理されなくなりました。デフォルトで、Samples Operator は、Red Hat Enterprise Linux (RHEL) ベースの OpenShift Container Platform イメージストリームおよびテンプレートを処理します。詳細は、Samples Operator の設定 を参照してください。

service-catalog-controller-manager および **service-catalog-apiserver** クラスター Operator は 4.4 で **Upgradeable=false** に設定されていました。これは、これらがインストールされている場合に、この場合ではバージョン 4.5 などの次のマイナーバージョンへのアップグレードがブロックされることを意味します。ただし、4.4.z などの z-stream リリースへのアップグレードはこの場合も引き続き許可されます。

サービスカタログおよびテンプレートサービスブローカーが 4.4 で有効にされている場合 (とくに管理状態が **Managed** に設定されている場合)、Web コンソールは、これらの機能が依然として有効にされていることをクラスター管理者に警告します。以下のアラートは、4.4 クラスターの **Monitoring** → **Alerting** ページから表示でき、これらには **Warning** の重大度が設定されます。

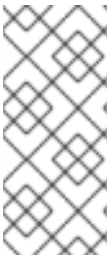
- **ServiceCatalogAPIServerEnabled**
- **ServiceCatalogControllerManagerEnabled**
- **TemplateServiceBrokerEnabled**

これらが依然として 4.4 クラスターで有効にされている場合、クラスター管理者は、OpenShift Container Platform 4.4 ドキュメントの Uninstalling Service Catalog および Uninstalling Template Service Broker を参照し、これをアンインストールできます。その後 4.5 へのアップグレードが許可されます。

4.5 では、クラスターのアップグレードプロセスで実行される新規の **openshift-service-catalog-removed** namespace にジョブのペアが作成されます。これらの動作は、サービスカタログの管理状態によって異なります。

- **Removed**: ジョブは以下のサービスカタログ項目を削除します。
  - Operator
  - namespace
  - カスタムリソース (CR)
  - **ClusterRole** オブジェクト
  - **ClusterRoleBinding** オブジェクト
- **Unmanaged**: ジョブは削除を省略し、何も実行しません。
- **Managed**: ジョブはエラーをログで報告します。アップグレードがブロックされているため、この状態が発生することはほとんどありません。ジョブは他のアクションは実行しません。

ジョブおよび **openshift-service-catalog-removed** namespace は今後の OpenShift Container Platform リリースで削除されます。



注記

OpenShift Container Platform 4.5 の時点で、すべての Red Hat が提供するサービスブローカーが削除されています。ユーザーによってインストールされるその他のブローカーがアップグレードプロセスで削除されることはありません。これにより、ブローカーを使用してデプロイされている可能性のあるサービスを削除することを防ぐことができます。ユーザーはこれらのブローカーを手動で削除する必要があります。

1.4.2.4. CatalogSourceConfig オブジェクトの削除

CatalogSourceConfig オブジェクトが削除されるようになりました。詳細は、**OperatorSource および CatalogSourceConfig オブジェクトブロッククラスターのアップグレード** について参照してください。

1.4.2.5. 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/dotnet/dotnet-30-rhel7:3.0
registry.redhat.io/dotnet/dotnet-30-runtime-rhel7:3.0
registry.redhat.io/openjdk/openjdk-11-rhel8:1.1
registry.redhat.io/rhoar-nodejs-tech-preview/rhoar-nodejs-10-webapp
registry.redhat.io/rhscl/mongodb-32-rhel7
registry.redhat.io/rhscl/python-35-rhel7
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.5.1
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.5.0
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.5.1
registry.redhat.io/rhdm-7-tech-preview/rhdm-optaweb-employee-rostering-rhel8:7.5.0
registry.redhat.io/rhdm-7-tech-preview/rhdm-optaweb-employee-rostering-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.5.1
registry.redhat.io/rhscl/ruby-23-rhel7
```

1.4.2.6. 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。

1.5. バグ修正

apiserver-auth

- 以前のバージョンでは、**oc login** は HTTP 要求を実行して、リモートログインサーバーへの接続に使用する CA バンドルを判別していました。これにより、ログインに成功しても、ログインを試行するたびに OAuth サーバーログに **remote error: tls: bad certificate** エラーが生成されました。サーバー証明書チェーンはセキュアでない TLS ハンドシェイクから取得されるため、正しい CA バンドルが選択され、OAuth サーバーはログインの試行時に正しくない証明書についてのエラーをログに記録しなくなりました。(BZ#1819688)

- 以前のバージョンでは、OAuth サーバー Pod のセキュリティーコンテキストが不完全なために、デフォルト動作を元に戻すカスタム SCC (Security Context Constraints) を取得すると、Pod がクラッシュループする可能性があります。OAuth サーバー Pod のセキュリティーコンテキストが変更され、カスタム SCC は OAuth サーバー Pod の実行を阻止しなくなりました。(BZ#1824800)

- 以前のバージョンでは、Cluster Authentication Operator はすべての OIDC アイデンティティープロバイダーのチャレンジ認証フローを常に無効にしていました。つまり、**oc login** でのログインは成功しませんでした。OIDC アイデンティティープロバイダーが設定されていると、Cluster Authentication Operator は Resource Owner Password Credentials の付与を許可するかどうかを確認し、存在する場合にチャレンジベースのログインを許可するようになりました。Resource Owner Password Credentials 認証付与を許可する OIDC アイデンティティープロバイダーの **oc login** を使用してログインできるようになりました。(BZ#1727983)

- 以前のバージョンでは、Cluster Authentication Operator は OAuth サーバーへの接続を適切に

閉じませんでした。そのため、接続がドロップされるよりも速く開かれると、OAuth サーバーへのトラフィック量が増大しました。接続が適切に閉じられ、Cluster Authentication Operator の独自ペイロードのサービスのレベルが低下することはなくなりました。(BZ#1826341)

- 以前のバージョンでは、設定時に **kube-apiserver** に到達する際にエラーが生じると、**oauth-proxy** コンテナーはエラーを出して終了しました。これにより、**kube-apiserver** およびコントローラーの安定性や速さが十分でない場合、複数のコンテナーが再起動しました。**kube-apiserver** に対するチェックの複数の試行が **oauth-proxy** コンテナーの起動時に許可されるようになりました。これにより、基礎となるインフラストラクチャーに障害が実際にある場合にのみコンテナーが失敗するようになりました。(BZ#1779388)

ベアメタルハードウェアのプロビジョニング

- IPv4 ネットワークの使用時に UEFI ブートプロセスは **ipxe.efi** バイナリーを使用するため、ブートプロセスではネットワークデバイスが見つからないことを報告していました。このため、PXE (Preboot eXecution Environment) は **No network devices** を出してマシンを起動します。**dnsmasq.conf** ファイルが、IPv4 ネットワークの **snponly.efi** バイナリーを使用するように更新されました。PXE で起動するマシンは、ネットワーク接続があるため、UEFI ネットワークドライバーを使用し、デプロイできます。(BZ#1830161)

- インストール時にクラスターにネットワークの問題がある場合 (イメージの低速なダウンロードなど)、インストールは失敗する可能性があります。この問題に対処するために、PXE ブートは再試行を組み込むように変更され、ベアメタルプロビジョナーとプロビジョニングされるノード間の通信における再試行のネットワークの最大数が引き上げられました。インストーラーは低速なネットワーク条件を処理できるようになります。(BZ#1822763)

ビルド

- ビルドを開始する前に、OpenShift Container Platform ビルダーは提供された **Dockerfile** を解析し、ビルドに使用する修正バージョンの再構築を行いました。このプロセスには、ラベルを追加し、**FROM** 命令で名前が付けられたイメージの置き換えを処理することが含まれました。生成される **Dockerfile** は **ENV** および **LABEL** 命令を常に正しく再構築する訳ではありませんでした。生成される **Dockerfile** には、元の **Dockerfile** には含まれない **=** 文字が含まれる場合がありました。これにより、ビルドが構文エラーを出して失敗しました。変更した **Dockerfile** を生成する際に、**ENV** および **LABEL** 命令の元のテキストがそのまま使用されることにより、問題が修正されました。(BZ#1821858)

- 以前のバージョンでは、ビルド Pod init コンテナーで失敗が生じた場合に、エラーログの最後の数行がビルドに割り当てられませんでした。そのため、誤った形式の Git URL などの init コンテナーでのビルドエラーを診断するのが困難でした。ビルドコントローラーは更新され、Init コンテナーで失敗が生じる際にエラーログがビルドに割り当てられるようになりました。ビルドの障害を診断しやすくなりました。(BZ#1809862)

- 以前のバージョンでは、イメージのインポートの失敗または無効な **Dockerfiles** によって生じるビルドの失敗は、一般的なビルドエラーとしてのみ分類されました。このような問題を診断するには、デフォルト以外のビルドのロギングレベルが必要でした。イメージのインポートの失敗および無効な **Dockerfiles** については、新たな失敗の理由が導入されました。イメージのインポートの失敗や無効な **Dockerfiles** に関連するビルドの失敗が、ビルドオブジェクトのステータス内で特定できるようになりました。(BZ#1809861)

- 以前のバージョンでは、ビルドラベルの生成および検証には完全な Kubernetes 検証ルーチンが含まれていませんでした。特定の有効なビルド設定名を持つビルドは、無効なビルドラベルの値が作成されるめに失敗しました。ビルドコントローラーおよびビルド API サーバーは、完全な Kubernetes 検証ルーチンを使用して、追加されたビルドラベルがラベルの基準を満たすようになりました。有効なビルド設定名を持つビルドにより、有効なビルドラベルの値が作成されます。(BZ#1777337)

- 以前のバージョンでは、Buildah は、変数内に含まれる値を解析するのではなく、**Dockerfiles** の変数を文字通り解釈していました。そのため、**Dockerfiles** に変数が含まれる場合にビルドは失敗しました。Buildah が **Dockerfile** 変数を拡張するように更新されました。Buildah は、コンテナーイメージのビルド時に **Dockerfile** 環境変数の値を解析するようになりました。(BZ#1810174)

- **RunOnceDuration** 受付プラグインが OpenShift 4 で無効にされている場合、**activeDeadlineSeconds** の値は Pod のビルドに自動的に適用されませんでした。**activeDeadlineSeconds** が nil に設定された Pod は、 **NotTerminating** スコープを含むリソースクォータに一致します。そのため、ビルド Pod はクォータの制限により、**NotTerminating** スコープが定義されたリソースクォータを持つ namespace で起動に失敗しました。ビルドコントローラーは、Pod をビルドするために適切なデフォルトの **activeDeadlineSeconds** 値を適用するようになりました。ビルド Pod は **NotTerminating** スコープを含むリソースクォータを持つ namespace で適切に処理されるようになりました。(BZ#1829447)

クラウドコンピュート

- クラスター Autoscaler は、ノードおよびマシンオブジェクトでのプロバイダー ID が完全に一致することを予想します。以前のバージョンでは、マシン設定に大文字と小文字が混在するリソースグループ名が含まれる場合、クラスター Autoscaler は一致するものが見つからないためにマシンを 15 分後に終了させていました。リソースグループ名はサニタイズされ、すべての文字が小文字に設定されるようになりました。今回のリリースより、大文字と小文字の組み合わせを使用してリソースグループ名を入力しても、一致するプロバイダー ID が正しく特定されるようになりました。(BZ#1837341)

- 以前のバージョンでは、マシンおよびマシン設定仕様内の **metadata** フィールドは、マシンセットの作成または更新時に検証されませんでした。無効なメタデータによってアンマーシャリングのエラーが生じ、コントローラーがオブジェクトを処理できなくなりました。**metadata** フィールドは、マシンセットの作成および更新時に検証され、無効なエントリーがエラーを返すようになりました。無効なメタデータはマシンセットの作成前に識別され、後続のオブジェクト処理エラーの発生を防げるようになりました。(BZ#1702089)

- スケールダウンの操作時に、マシンセットの最後のマシンには削除 (deletion) アノテーションが含まれることがあります。このマシンは、削除前に最小のマシンセットのサイズに達すると Autoscaler によって削除されません。以前のバージョンでは、最後のマシンの削除アノテーションはスケールダウン後に削除されませんでした。スケールダウン後にマシンのアノテーションのマークを解除する方法を変更する修正が導入されました。このアノテーションはマシンセットの最後のマシンで永続化しなくなりました。(BZ#1820410)

- 以前のバージョンでは、ワーカーノードに割り当てられる AWS Identity and Access Management (IAM) ロールには、マウント時に Amazon Elastic Block Store (EBS) ボリュームを復号化するために AWS Key Management Service (KMS) キーにアクセスできる十分なパーミッションがありませんでした。そのため、Amazon Elastic Compute Cloud (EC2) インスタンスは受け入れられましたが、それらはルートドライブからの読み取りを実行できないために起動に失敗しました。カスタマーマネージドキーで KMS で暗号化された EBS ボリュームを復号化できるように、EC2 インスタンスについての必要なパーミッションが付与されました。EBS ボリュームの暗号化にカスタマーマネージドキーを使用する場合、インスタンスが正常に起動するのに必要なパーミッションを持つようになりました。(BZ#1815219)

- マシンセット仕様の **replicas** フィールドは nil に設定できます。以前のバージョンでは、Autoscaler がマシンセット内のレプリカ数を判別できない場合、自動スケーリング操作は実行されませんでした。**replicas** フィールドが設定されていない場合、Autoscaler はマシンセットに応じて観察されるレプリカの最後の数に基づいてスケーリングの決定を行うようになりました。Autoscaling の操作は、マシン設定仕様の **replicas** フィールドが nil に設定されている場合でも、マシンセットコントローラーがレプリカ数を **MachineSet.Status.Replicas** に対して同期していることを前提としてそのまま実行できるようになりました。(BZ#1820654)

- 以前のバージョンでは、Autoscaler は、既存ノードの削除が完了していなくても、**DeleteNodes** への呼び出しごとにノードグループのサイズを 1 つ減らしていました。これにより、クラスターのノード数が必要な最小数未満になりました。ノードのマシンにすでに削除タイムスタンプがある場合、ノードグループのサイズはさらに縮小されなくなりました。これにより、Autoscaler が **DeleteNodes** を呼び出す際に、ノード数を必要な容量未満に減らすことがなくなりました。(BZ#1804738)

Cloud Credential Operator

- Cloud Credential Operator (CCO) は、元のクラスターが OpenShift Container Platform 4.1 でインストールされている場合にクラッシュループする可能性がありました。CCO は、**CredentialsRequest** オブジェクトにあるパーミッション要求を調整できませんでした。今回のバグ修正により、CCO では **Infrastructure** フィールドの一部が利用可能であることを前提としなくなりました。これにより、CCO は元々 OCP 4.1 でインストールされていたクラスターと連携できます。(BZ#1813343)

- Cloud Credential Operator (CCO) は SCC (Security Context Constraints) をバイパスしなくなりました。以前のバージョンでは、CCO は CCO がタスクを実行する上で必要のない余分のパーミッションで実行されていました。今回の機能拡張により、CCO についての SCC のバイパスが不必要に行われなくなりました。(BZ#1806892)

クラスターバージョン Operator

- Cluster Version Operator (CVO) には競合状態があり、この場合にタイムアウトした更新の調整サイクルが成功した更新と見なされていました。これは、Operator でリリースイメージ署名の取得の試行がタイムアウトしたネットワークが制限されたクラスターについてのみ生じました。このバグにより、CVO が shuffled-manifest 調整モードに入りました。このモードでは、コンポーネントが処理できない順序でマニフェストが適用されるとクラスターが破損する可能性がありました。CVO はタイムアウトした更新を失敗として処理するようになろ。更新が正常に実行される前に調整モードに入らなくなりました。(BZ#1843526)

- 更新時のデプロイメントのロールアウトの失敗のログは CVO ログにのみに記録され、一般的なエラーメッセージのみが **ClusterVersion** オブジェクトに報告されました。この一般的なエラーメッセージにより、CVO ログを確認しない限り、ユーザーおよびチームがエラーをデバッグすることが困難になりました。今回のバグ修正により CVO が更新され、ロールアウトの根本的なエラーが **ClusterVersion** オブジェクトに公開されるようになりました。その結果、アップグレード時のデプロイメントのロールアウトをデバッグすることが容易になりました。(BZ#1768260)

コンソール kubevirt プラグイン

- 今回のリリースでは、仮想マシンが無効なバスタイプまたは推奨されていないバスタイプでディスクを使用するように設定されている場合、作成される仮想マシンの **Disks** タブにはディスクインターフェイスの警告が表示されます。(BZ#1803780)

- 以前のバージョンでは、すべての **DataVolume** オブジェクトは VM Disk インポートとして分類されました。この正しくない分類により、仮想マシンへの所有者の参照のない **DataVolume** オブジェクトについての **Activity** カードが非表示になりました。今回のリリースにより、仮想マシンの所有者参照のある **DataVolume** オブジェクトのみが VM Disk インポートとして分類され、仮想マシンへの所有者の参照を持たない **DataVolume** オブジェクトについての **Activity** カードが表示されるようになりました。(BZ#1815138)

- 以前のバージョンでは、**DataVolume** オブジェクトおよびそれらの関連付けられた永続ボリューム要求 (PVC) は仮想マシンディスクの削除時に削除されませんでした。これらのオブジェクトは仮想マシンの削除時にのみ削除され、仮想マシンの削除時に **DataVolume** オブジェクトを保持するオプションはありませんでした。今回のリリースにより、ユーザーは仮想マシ

ンディスクまたは仮想マシンを削除する際に **DataVolume** オブジェクトおよび PVC を保持するか、または削除することを選択できます。これは CD-ROM モーダルを使用して削除されたディスクについては適用されません。(BZ#1820192)

- 以前のリリースでは、インベントリー内のディスク数は、ディスク一覧のディスク数と一致しませんでした。インベントリービューが更新され、CD-ROM およびディスクが別々に表示されるようになりました。(BZ#1803677)

- 以前のバージョンでは、仮想マシンウィザードで使用するデフォルトの YAML で仮想マシンを作成することはできませんでした。これは、デフォルトの YAML 仮想マシンテンプレートに仮想マシンウィザードで必要な値が含まれていないためです。今回のリリースにより、デフォルトの YAML 仮想マシンテンプレートに必要な値すべてが含まれるようになりました。(BZ#1793962)

- 以前のバージョンでは、失敗した仮想マシンの移行が成功したと報告されていました。仮想マシンの移行時に、Web コンソールでは、仮想マシンの移行に失敗するとそれを正しく報告するようになりました。(BZ#1806974)

- 以前のバージョンでは、仮想マシンウィザードは正しい形式で **cloud-init** 設定を生成しなかったために、これが仮想マシンに適用されませんでした。今回のリリースにより、ウィザードによって生成された形式が修正され、仮想マシンウィザードで提供される **cloud-init** 設定が仮想マシンに適用されるようになりました。(BZ#1821024)

- 以前のバージョンでは、仮想マシンテンプレートのソケットは仮想マシンウィザードで作成された最終的な仮想マシンに反映されなかったために、仮想マシンの作成後に vCPU の数が 2 倍になりました。今回のリリースにより、仮想マシンテンプレートのソケット、コアおよびスレッドは、仮想マシンの作成時に反映され、vCPU の正確な数が出されるようになりました。(BZ#1810372)

- 仮想マシンテンプレート一覧についての URL の変更により、ユーザーは仮想マシンテンプレートの削除後に誤ったページにリダイレクトされていました。今回のリリースで URL が修正されました。(BZ#1810379)

- 以前のバージョンでは、実行中の仮想マシンが削除されると、関連付けられた VMI が **VM error** のステータスで仮想マシン一覧に表示されました。今回のリリースにより、削除済みの関連付けられた仮想マシンのある古くなった VMI が一覧表示されなくなりました。(BZ#1803666)

- 以前のバージョンでは、ディスクのインポートプロセスでは、仮想マシンのインポートリソースのみが予想されていました。そのため、仮想マシンテンプレートまたは VMI からのインポート用の仮想マシンリソースリンクは、存在しない仮想マシンを参照していました。今回のリリースにより、インポートプロセスで、インポートリソースと正しいリソースへのリンクである仮想マシンテンプレートおよび VMI を認識できるようになりました。(BZ#1840661)

- 今回のリリースにより、仮想マシンディスクのインポートプロセスが **NaN%** のプロセス値を報告しなくなりました。(BZ#1836801)

- 以前のバージョンでは、仮想マシンウィザードは、一般的なテンプレートで指定されるインターフェイスを使用する代わりに、仮想マシンルートディスクのデフォルトインターフェイスとして **virtIO** を使用していました。しかし、**virtIO** インターフェイスはすべてのオペレーティングシステムと互換性がありません。今回のリリースにより、オペレーティングシステムの適切なデフォルトインターフェイスが、使用される一般的なテンプレートに基づいて選択されるようになりました。(BZ#1803132)

Console Metal3 プラグイン

- 以前のバージョンでは、Web コンソールの **Powering on/off** メッセージとベアメタルホストリンク間にはスペースがありませんでした。メッセージが適切に読み取られるようにスペースが追加されました。(BZ#1819614)

- 以前のリリースでは、ベアメタルのインストールでは、一部のノードが利用できない場合に、**Bare Metal Host Details** ページが読み込まれませんでした。**Bare Metal Host Details** ページにはゼロ (0) Pod が表示されるようになりました。(BZ#1827490)

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、**Topology** ビューで Knative サービスに関連付けられた Pod またはリソースの一覧を表示することは容易ではありませんでした。今回のバグ修正により、Knative サービスを選択すると、サイドバーに Pod の一覧とログを表示するリンクが表示されるようになりました。(BZ#1801752)

- **Monitoring** ビューの **metrics** タブにある PromQL エディターを使用して既存のクエリーを編集すると、カーソルは行の最後に移動します。今回のバグ修正により、PromQL エディターが予想通りに機能するようになりました。(BZ#1806114)

- Knative イメージの場合、**Add → From Git** オプションで、 **Routing** の **Advanced Options** は事前にフェッチされたコンテナーポートのオプションを提供しません。また、ポートのデフォルト値 **8080** を更新せずにサービスを作成した場合には、リビジョンは表示されません。今回のバグ修正により、ユーザーはドロップダウンリストを使用して利用可能なポートオプションを選択するか、または別のポートを使用する必要がある場合は入力でき、リビジョンは予想通りに表示できるようになりました。(BZ#1806552)

- 以前のバージョンでは、イメージを取得できなかったため、CLI を使用して作成された Knative サービスはコンソールを使用して編集できませんでした。編集中に関連付けられたイメージストリームが見つからない場合には、YAML ファイルでコンテナーイメージについてユーザーが指定した値が使用されるようになりました。これにより、CLI を使用してサービスを作成した場合でも、ユーザーはコンソールを使用してサービスを編集できます。(BZ#1806994)

- **Topology** ビューで、Knative サービスの外部イメージレジストリーでイメージ名を編集しても新規リビジョンは作成されませんでした。今回のバグ修正により、サービスの名前が変更されると、サービスの新規リビジョンが作成されます。(BZ#1807868)

- **Add → Container Image** オプションを使用してから、**Image stream tag from internal registry** を選択した場合、**ImageStreams** ドロップダウンリストには、**OpenShift** namespace からイメージをデプロイするオプションは一覧表示されませんでした。ただし、CLI からそれらにアクセスすることができました。今回のバグ修正により、すべてのユーザーがコンソールおよび CLI を使用して **OpenShift** namespace のイメージにアクセスできるようになりました。(BZ#1822112)

- 以前のバージョンでは、**Pipeline Builder** では、存在していない Task を参照している Pipeline を編集すると、画面全体が白くなりました。今回の修正により、アクションが必要であることを示すアイコンが表示され、Task 参照を簡単に更新できるドロップダウンリストが表示されるようになりました。(BZ#1839883)

- **Pipelines Details** ページで、**Parameters** および **Resources** タブの既存のフィールドを変更する際に、新規の変更が検出されても **Save** ボタンが無効にされていました。検証基準が変更され、変更を送信できるように **Save** ボタンが有効になります。(BZ#1804852)

- **Add → From Git** オプションで、OpenShift Pipelines Operator によって提供される Pipeline テンプレートは **Deployment** または **Knative Services** リソースオプションが選択されている場合に失敗します。今回のバグ修正により、リソースタイプとランタイムを使用して Pipeline テンプレートを判別するサポートが追加され、リソース固有の Pipeline テンプレートが提供されるようになりました。(BZ#1796185)

- Pipeline が **Pipeline Builder** を使用して作成され、array タイプの Task パラメーターが使用されると、Pipeline は起動しませんでした。今回のバグ修正により、array および string タイプのパラメーターの両方がサポートされるようになりました。(BZ#1813707)

- **Topology** ビューで、namespace に Operator によってサポートされるサービスがある場合に、アプリケーションによるノードのフィルターを実行するとエラーが返されました。今回のバグ修正により、選択されたアプリケーショングループに基づいて Operator がサポートするサービスノードをフィルターに掛けるロジックが追加されました。(BZ#1810532)

- **Developer Catalog** には、**Clear All Filters** オプションを選択するまでカタログの結果が表示されませんでした。今回のバグ修正により、すべてのカタログ項目がデフォルトで表示されるようになり、すべてのフィルターをクリアする必要がなくなりました。(BZ#1835548)

- 以前のバージョンでは、ユーザーは **knative** サービスの環境変数を追加できませんでした。そのため、**envVariables** が必要になるアプリケーションには予想通りに機能できない場合があります。今回のリリースより、環境変数についてのサポートが追加されました。(BZ#1839114)

- Developer Console **Navigation** メニューが利用できるようになり、最新の UX デザインに合わせて調整されました。(BZ#1801278)

- **Developer** パースペクティブの **Monitoring** タブに **Time Range** および **Refresh Interval** ドロップメニューが追加されました。(BZ#1807210)

- **Start Pipeline** モーダルには Pipeline リソースが必要でしたが、Pipeline リソースは namespace に作成されませんでした。ユーザーにはフィールドの上に無効の、および空のドロップダウンが表示され、フィールドのコンテキストの一部が失われました。今回のバグ修正により、**Create Pipeline Resource** から、**Start Pipeline** モーダルでのコンテキスト情報がユーザーに提供されるようになりました。ユーザーは、namespace に Pipeline リソースが作成されていない場合に、Start モーダルから Pipeline を開始しやすくなりました。(BZ#1826526)

- レイアウトのパディングがないため、タイトルが **Close** ボタン上に表示されました。テキストが **Close** ボタンの上に置かれると、クリックすることが困難になります。レイアウトが修正され、タイトルが 閉じる ボタン上に表示されないように修正され、ボタンはマウスクリックで常にアクセスできるようになりました。(BZ#1796516)

- Pipeline Builder は、空の文字列 ('') のデフォルト値をデフォルトなしとして誤って解釈していました。Operator で提供される一部のタスクでは、これをデフォルトにする必要があり、デフォルトなしの機能で問題が生じました。デフォルトプロパティーの有無を確認し、値が有効であることを前提としないでください。今回のリリースより、OpenShift Pipeline Operator が有効なデフォルト値として認識するすべての値が考慮されるようになりました。(BZ#1829567)

- Pipeline Builder は **Task**/**ClusterTask** 定義を読み取り、すべてのパラメーターのタイプが **string** であると誤って仮定していました。**array** タイプの **Task** パラメーターが出ると、array を string にキャストし、これを表示するため、タイプが失われました。また、**Task** パラメーターへの値を **string** として生成するため、**Task** への接続が中断しました。**array** タイプが web コンソールでサポートされ、タイプが適切に再調整されるようになりました。どちらのタイプも管理することで、Pipeline Builder は予想通りに機能できるようになりました。(BZ#1813707)

- Pipeline ページは他のページとの整合性がありません。**Create Pipeline** ボタンは常に有効にされており、プロジェクトが利用できない場合に考慮されませんでした。**Create Pipeline** ボタンは、Getting Started ガイドが有効にされている場合に削除されるようになりました。(BZ#1792693)

- **Dashboard & Metrics** タブのメトリクスのクエリーが設計文書で更新されました。クエリーに関して同期するために必要なコード。クエリーが更新され、メトリクスクエリーとそれらのラベルの順序が設計と同期するようになりました。(BZ#1806518)

- タイル説明変数は、CSV 記述で追加された CRD 記述に誤って設定されました。これにより、タイルの説明の正しい内容が表示されませんでした。タイルの説明は元の値に戻り、追加された値がそれ自体の変数に移されました。(BZ#1814639)

- **eventSources** API グループは、最新のサポートされている API グループ **sources.knative.dev** に更新されました。今回の更新により、新規の API グループによって生成されたソースが Web コンソールの **Topology** ビューで認識されるようになりました。(BZ#1836805)

- Red Hat OpenShift Serverless 1 の Serverless Operator バージョン 1.7.1 のリリースにより、Operator は一般的に利用可能になりました。Web コンソールの **Developer** パースペクティブの Tech Preview バッジが削除されました。(BZ#1827042)

DNS

- 以前のバージョンでは、CoreDNS メトリクスは、クラスター内の非セキュアなチャネルで公開されていました。CoreDNS メトリクスエンドポイントをセキュアにし、セキュアなチャネル上で CoreDNS メトリクスを公開するために適切な TLS コンポーネントおよび **kube-rbac-proxy** サイドカーが追加されました。(BZ#1809197)

- 以前のバージョンでは、任意のテイントをノードに追加すると、DNS Operator のオペランドに関連する問題が発生する可能性がありました。DNS Operator のオペランドは、ノードに追加されるテイントを許容するようになりました。オペランドは、すべての Linux ノードホストの **/etc/hosts** で実行され、これを更新します。オペランドが初期化中のノードで起動する場合に、**Missing CNI default network**イベントが観察される可能性がありますが、このエラーは一時的であり、無視することができます。(BZ#1813479)

- 以前のバージョンでは、マスターノードに特定の DNS 名を持たせる際に依存関係を考慮する必要がありました。任意の有効なホスト名をマスターノードに使用できるようになりました。(BZ#1807234)

- 以前のバージョンでは、**dnses.operator.openshift.io/default** オブジェクトが存在するものの、それに対応する DaemonSet が利用不可の場合、 **clusteroperators/dns** は、**Available** 状態を、正しくない **NoDNS** の理由と **No DNS resource exists** メッセージと共に報告していました。同じ条件下で、正しい理由とメッセージが表示されるようになりました。(BZ#1835725)

etcd

- 以前のバージョンでは、etcd ピア証明書には IPv6 localhost アドレスが含まれず、**https://[::1]:2379** メッセージでの接続に失敗していました。今回のバグ修正により、**::1** がピア証明書のホストの 1 つとして含まれます。繰り返し失敗する **https://[::1]:2379** を使用した接続の試行は表示されなくなりました。(BZ#1810997)

- 以前のバージョンでは、CVO は設定マップの証明書を 10 分ごとに上書きしていました。これにより、多くのオーバーヘッドが発生し、これによりクラスターのパフォーマンスと安定性にマイナスの影響が及びました。証明書は設定マップに 1 回限り作成されるようになり、パフォーマンスおよび安定性が向上します。(BZ#1819472)

- 以前のバージョンでは、クラスター etcd Operator のヘルスステータスのレポートは容易に理解できるものではありませんでした。これはログメッセージングの設定が不適切に行われていたために生じ、これにより、クラスターのステータスが不確実になりました。これは、etcd のステータスについての適切なログメッセージおよびイベントを作成するために別の機能を使用して Operator ステータスを適切に分析することで修正されています。すべてのマスターノードでの etcd Pod のステータスがより分かりやすくなりました。(BZ#1821286)

- 以前のバージョンでは、TLS 証明書の署名が、3 年について署名されると文書で記載されていても、10 年について誤って署名されていました。証明書は 3 年についてのみ署名されるようになりました。(BZ#1837594)

- gRPC-go 1.23.0 には、クライアント側のロードバランサーのバグがありました。このバグによりデッドロックが生じる可能性がありました。gRPC-go はバージョン 1.23.1 にアップグレードされ、バグは修正されています。(BZ#1823993)

- すべての Pod を停止した後、復元プロセスは **etcd**、**api-server**、**api-scheduler**、および **controller-manager** のみを再起動します。ネットワーク Pod を再起動しませんでした。そのため、kubelet は通信できず、ベアメタルクラスターを起動できませんでした。復元サービスは再起動できない Pod を停止しなくなりました。クラスターは復元プロセスの実行後に起動します。(BZ#1835146)

Etcd Operator

- 以前のバージョンでは、etcd 仕様にプロパティーがないため、**oc explain etcd** コマンドが仕様から参照されるプロパティーを誤って一覧表示していました。適用可能な CRD は、不足しているプロパティーを記述するように更新されました。**oc explain etcd** コマンドは etcd のプロパティーを完全に記述するようになりました。(BZ#1809282)

- Etcd Operator はヘルスチェックが適切に実行しないため、誤ったイベントレポートや誤解されるログメッセージが生成されました。ヘルスステータスは、改善されたメッセージングで正しく検出されるようになり、正確なヘルスステータスが提供されるようになりました。(BZ#1832986)

イメージ

- 以前のバージョンでは、nodeca デーモンは、レジストリーが **managed** に設定されている場合にのみ作成されていました。レジストリーが削除されると、nodeca デーモンは作成されません。今回のバグ修正により、nodeca デーモンが常に作成され、レジストリーが削除されても nodeca デーモンが作成されるようになりました。(BZ#1807471)

イメージレジストリー

- 以前のバージョンでは、適切なストレージ設定なしにレジストリー設定を削除した場合、ストレージ設定がないためにリソースは終了せず、Operator はストレージを認識しないためにストレージを削除できませんでした。今回のバグ修正により、ストレージ設定はオプションになり、これによりリソースを完了できるようになりました。(BZ#1798618)

- 以前のバージョンでは、イメージレジストリー Operator は、イメージレジストリーで作成されたリソースに **nodeSelector** ラベルを設定しませんでした。そのため、実行できるノードリソースが指定されないための問題が発生する可能性が生じ、レジストリーがサポート対象外のプラットフォームで実行される可能性がありました。今回のバグ修正により、不足しているラベルが作成されるリソースに追加されるようになりました。作成されたリソースでラベルを確認できるようになりました。(BZ#1809005)

- 以前のバージョンでは、イメージを存在しない namespace にプッシュすると、イメージレジストリーは **500** のエラーコードを返していました。今回のバグ修正により、戻りコードが変更され、パーミッションがないことが示されるようになりました。イメージを存在しない namespace にプッシュすると、パーミッション拒否エラーが返されます。(BZ#1804160)

- Azure インフラストラクチャー名は、生成される Azure コンテナーおよびストレージアカウントに使用されます。そのため、Azure インフラストラクチャー名に大文字が含まれる場合、コンテナーは正常に作成されますが、ストレージアカウントの作成は失敗しました。今回のバグ

修正により、コンテナー名の作成ロジックが無効な文字を破棄するように調整され、イメージレジストリーを名前に無効な文字が含まれるインフラストラクチャーにデプロイできるようになりました。(BZ#1827807)

- GCP ストレージと共に空でないイメージレジストリーを削除する際に、イメージレジストリーホスト名はイメージ設定ファイルから削除されませんでした。これにより、新規イメージレジストリーを作成することができませんでした。イメージレジストリーの削除時に、イメージ設定ファイルからイメージレジストリーホスト名を削除できるようにコードが変更されました。この結果として、イメージレジストリーを予想通りに削除し、作成することができます。(BZ#1827075)

- イメージレジストリーはバケットの削除前にバケットからオブジェクトを削除していなかったため、イメージと共にバケットを削除できませんでした。コードは、バケットを削除する前にイメージを削除するように変更されました。空でないバケットを予想通りに削除することができます。(BZ#1827075)

- イメージレジストリーのイメージは yum キャッシュをクリアしていないため、イメージサイズが大きくなる可能性があります。イメージレジストリー **Dockerfile** は、**yum clean all** コマンドを組み込むように変更されました。イメージのサイズはさらに小さくなります。(BZ#1804493)

- イメージプルーニングのカスタムリソースの **keepYoungerThan** パラメーターはナノ秒を使用し、より長い時間を使用するように設定することはできません。ナノ秒は、イメージプルーナーで使用するのに適切な期間ではありません。新規パラメーターが、イメージプルーニングカスタムリソースの **keepYoungerThan** パラメーターを置き換え、上書きする **keepYoungerThanDuration** に追加されました。(BZ#1835004)

- イメージレジストリー Operator は、ユーザーが Operator を **Removed** 状態に切り換える際にストレージのステータスを適切にクリーンアップしませんでした。その結果、ユーザーが Operator を **Managed** に戻すと、Operator は新規ストレージ Pod を作成できませんでした。Operator はストレージステータスを適切にクリーンアップするように変更され、Operator は新規ストレージ Pod を作成できるようになりました。(BZ#1785534)

- イメージレジストリー Operator はログを取り除かないため、ログに適切でないメッセージが表示される可能性がありました。ログを取り除き、これらの不適切なメッセージを削除するようにコードが変更されました。ログに適切な情報が表示されるようになりました。(BZ#1797840)

- デフォルトのイメージレジストリー Operator はゼロ (0) レプリカで設定されているため、値を手動で変更しない限り、問題が発生する可能性がありました。Operator は 1 でインストールするように更新されました。(BZ#1811846)

- クラスターのインストール時に使用されるレジストリーの認証情報は、特定の namespace で利用できず、ユーザーは新規の認証情報を作成する必要がありました。レジストリーの認証情報がインストール時に提供されている場合、ユーザーはこれらの認証情報を使用してイメージをインポートできるようにコードが変更されました。(BZ#1816534)

- イメージレジストリー Operator は 1 つの Pod でのみインストールされているため、要件を満たしませんでした。Operator は高可用性の確保のために 2 つの Pod と共にインストールできるようになりました。(BZ#1810317)

インストーラー

- Azure プラットフォームでは、Pod のボリュームマウントを作成するために **cifs-utils** パッケージが必要になります。今回のリリースにより、OpenShift Container Platform のインストール時に RHEL 7 ホスト用にインストールされるパッケージに **cifs-utils** が含まれます。(BZ#1827982)

- コントロールプレーン証明書の期限切れの状態からのリカバリー時に、クラスターはポート 7443 のリカバリー API サーバーに接続できません。これは、リカバリー API サーバーのポートが OpenStack、oVirt、ベアメタル、および vSphere に使用される HAProxy ポートと競合するためです。これにより、**Unable to connect to the server: x509: certificate signed by unknown authority** エラーが生じます。HAProxy はポート 9443 でリッスンするようになり、リカバリー API サーバーはポート 7443 を使用して期限切れのコントロールプレーン証明書のリカバリープロセスを容易にします。(BZ#1821720)

- 以前のリリースでは、RHOSP インストーラーは、トラフィックの発信元を許可するために **remote_group_id** を使用してセキュリティーグループを作成していました。セキュリティールールで **remote_group_id** を使用すると、OVS エージェントによる多くの計算をトリガーしてフローを生成するため非効率なプロセスが生じました。このプロセスでは、フローの生成に割り当てられた期間が超過することがありました。このような場合、すでに負荷がかかっている環境ではとくに、マスターノードはワーカーノードと通信できず、デプロイメントに失敗します。**remote_group_id** ではなく、トラフィックの発信元をホワイトリスト化するための IP 接頭辞が使用されるようになりました。これにより、Neutron リソースの負荷が軽減され、タイムアウトの発生回数が減ります。(BZ#1825286)

- 以前のバージョンでは、Red Hat Virtualization (RHV) に OpenShift Container Platform クラスターを作成する前に、インストールプログラムでは、ユーザーは仮想マシンテンプレートを手動で作成する必要がありました。これは、インストールプログラムが RHV バージョン 4.3.9 で以下の要件を満たしていないためです。

  - インストールプログラムは ignition を仮想マシンに渡す必要があります。
  - テンプレートは、その OS タイプを Red Hat CoreOS (RHCOS) として指定する必要があります。

  インストールプログラムは、RHCOS を OS タイプとして指定するテンプレートを作成し、Ignition を仮想マシンに渡します。ユーザーが仮想マシンテンプレートを作成する必要がなくなりました。(BZ#1821151)

- 以前のリリースでは、ベアメタルインストーラーでプロビジョニングされるインフラストラクチャークラスターで API-VIP と INGRESS-VIP アドレスの両方にフェイルオーバーを提供する Keepalive プロセスは、ローカルコンポーネントのステータスを監視してデプロイメントが IPV6 アドレスを使用しても VIP を所有するノードを判別するスクリプトで IPV4 ローカルアドレスを使用しました。このため、IPv6 デプロイメントでは、Keepalived が正しくないコンポーネントのステータスを受信することがありました。Keepalived スクリプトは localhost を使用しており、V4 デプロイメントでは 127.0.0.1 に、V6 デプロイメントでは ::1 に解決されるため、常に正しいローカル IP アドレスを使用します。(BZ#1800969)

- 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を使用するベアメタルクラスターで、VIP は常に正常なロードバランサーでコントロールプレーンマシンにフェイルオーバーする訳ではありませんでした。そのため、ローカルロードバランサーが正常ではなく、OpenShift Container Platform API が ~10 秒間到達できない場合でも、コントロールプレーンマシンは API-VIP IP アドレスを引き続き所有します。API-VIP スクリプトの Keepalived チェックはセルフホスト型のロードバランサーの正常性を監視し、API-VIP は実行中のロードバランサーでコントロールプレーンノードにフェイルオーバーし、OpenShift Container Platform API のサービスダウンタイムの発生を防ぐようになりました。(BZ#1835974)

- 以前のバージョンでは、インストールプログラムは **machineCIDR** と **provisioningNetworkCIDR** 範囲の重複の有無を明示的に確認しませんでした。その結果、重複するネットワーク範囲が不明確な場合にエラーメッセージが表示されました。インストールプログラムはこれらのネットワーク範囲の重複を明示的にチェックし、重複がある場合には明確なエラーメッセージを表示するようになりました。(BZ#1813422)

- コントロールプレーンの Operator はブートストラッププロセスの完了前に起動できるので、ベアメタルのプロビジョニングインフラストラクチャーがブートストラップとコントロールプレーンの両方で同時にアクティブになる可能性があります。以前のバージョンでは、プロビジョニングインフラストラクチャーの両方がコンピュートマシンをプロビジョニングし、マシンすべてが同じインフラストラクチャーを使用する訳ではありませんでした。ブートストラップのプロビジョニングインフラストラクチャーはコントロールプレーンマシンのみをプロビジョニングするようになり、両方のプロビジョニングインフラストラクチャーを同時にオンラインにすることができます。(BZ#1800746)

- 以前のバージョンでは、IPv6 のブートストラップノードへの DHCP トラフィックをブロックする際に誤ったポート番号が使用されていました。このため、コントロールプレーンマシンがブートストラップノードから DHCP リースを誤って取得した場合に競合状態が生じました。正しいポートが DHCPv6 についてブロックされ、コントロールプレーンマシンはクラスターで実行されるベアメタルインフラストラクチャーからのみプロビジョニングされるようになりました (BZ#1809691)。

- 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を使用するベアメタルクラスターの場合、VRRP を使用して OpenShift Container Platform クラスターの仮想 IP アドレスを管理することは、複数のクラスターを実行する場合に仮想ルーター ID がブロードキャストドメインですでに使用されている可能性があることを意味しました。このため、ノードにはすでに使用中の仮想 IP アドレスが割り当てられる可能性があります。ツールを使用して、クラスターをデプロイする前に、選択したクラスター名に使用される仮想ルーター ID を確認できるようになりました。(BZ#1821667)

- OpenShift Container Platform version 4.1 クラスターは **infrastructure.status.infraPlatform** パラメーターを使用しませんでした。そのため、Operator は元はバージョン 4.1 をインストールしたクラスターの古いフィールドをチェックして使用する必要があり、これにより、アップグレード時にエラーが生じました。移行コントローラーはクラスターで利用可能な情報を使用して、アップグレード時にすべてのクラスターの新規フィールドを設定し、Operator がすべての新規パラメーターを使用し、アップグレードエラーを減らすことができるようになりました。(BZ#1814332)

- クラスターのリソースの取得に使用される AWS API の前に削除されたリソースへの反応が非常に遅くなるため、削除されたホストゾーンの削除を試み、クラスターを複数回破棄しようとすると失敗が生じました。このため、destroy コマンドは、AWS API がホストされたゾーンをそれらの応答から削除するまでループしました。インストールプログラムは、ホストされるゾーンの **notfound** エラーを省略し、destroy コマンドがより速く実行されます。(BZ#1817201)

- 以前のバージョンでは、ブートストラップサーバーのエンドポイントは、外部ロードバランサーを通過する **api** エンドポイントを使用していました。このため、別のポートを開いて RHEL ノードをクラスターに追加する必要がありました。ブートストラップサーバーのエンドポイントは内部の **api-int** エンドポイントを使用するようになり、外部ロードバランサーで別のポートを開く必要がなくなりました。(BZ#1792822)

- 以前のリリースでは、ベアメタルクラスターの場合、ノード DNS 解決をサポートするために、ノードの **/etc/resolv.conf** ファイルは、ノードのコントロールプレーンの IP アドレスをノードの **/etc/resolv.conf** ファイルに追加してインフラストラクチャー CoreDNS のローカルインスタンスを参照しました。そのため、ホストの **/etc/resolv.conf** ファイルに 3 つのネームサーバーがすでに一覧表示されている場合、Pod は nameserver limits was exceeded アラートを生成していました。最初の 3 つのネームサーバーのみが生成される **/etc/resolv.conf** ファイルに含まれるようになり、アラートが Pod によって生成されなくなりました。(BZ#1825909)

- 以前のリリースでは、**ipxe.efi** ファイルが実行中の ironic コンテナーに存在しないため、**ipxe.efi** が必要な場合に起動 UEFI が失敗しました。**ipxe.efi** ファイルがランタイム時に **/shared** ディレクトリーにコピーされ、UEFI ブートは影響を受けなくなりました。(BZ#1810071)

- 以前のバージョンでは、AWS からの速度制限により、クラスターのレコードを作成できませんでした。インストールプログラムは指数関数的バックオフを使用して待機タイムアウトを長くすることができ、速度制限による失敗数が少なくなりました。(BZ#1766691)

- 以前のバージョンでは、AWS からの速度制限により、クラスターのゾーンの取得に失敗する場合があり、これによってクラスターのインストールが実行できなくなりました。インストールプログラムは指数関数的バックオフを使用して待機タイムアウトを長くすることができ、速度制限による失敗数が少なくなりました。(BZ#1779312)

- 以前のバージョンでは、インストールプログラムが設定ファイルへの相対パスを判別する際にシンボリックリンクをチェックしないため、インストールプログラムがシンボリックリンクから実行される場合に、インストールは失敗します。インストールプログラムはシンボリックリンクの有無を確認し、シンボリックリンクを指定したディレクトリーからインストールプログラムを実行できます。(BZ#1767066)

- 以前のバージョンでは、インストールプログラムが使用する AWS Terraform プロバイダーにより S3 バケットでの競合状態が生じ、クラスターのインストールは以下のエラーを出して失敗することがありました。

  > When applying changes to module.bootstrap.aws_s3_bucket.ignition, provider level=error msg="\"aws\" produced an unexpected new value for was present, but now absent.

  インストールプログラムは異なる AWS Terraform プロバイダーコードを使用します。これは、S3 の最終的な一貫性を確実に処理し、インストーラーでプロビジョニングされた AWS クラスターのインストールがエラーで失敗しなくなりました。(BZ#1745196)

- 以前のバージョンでは、CoreDNS forward プラグインはデフォルトでランダムサーバー選択ポリシーを使用していました。そのため、複数の外部 DNS リゾルバーが指定されている場合に、クラスターは OpenStack API ホスト名の解決に失敗していました。プラグインは、指定された順序で DNS サーバーを使用できるようになりました。(BZ#1809611)

- OpenShift Container Platform をインストールできる RHOSP クラウド間にはパフォーマンスの変動性があるため、インストール時間は異なります。その結果、インストールが成功する前にインストーラーがタイムアウトする可能性があります。回避策として、インストーラーが失敗について示唆した後にクラスターのステータスを確認します。クラスターは正常である可能性があります。(BZ#1819746)

- RHOSP では、コントロールプレーンおよびコンピュートノードは、IP アドレスを優先するネームサーバーとして **/etc/resolv.conf** ファイルに挿入します。その結果、ファイルにすでに 3 つのネームサーバーがあるホストは、ネームサーバーの制限についての警告を生成しました。/etc/resolve.conf の最初の 3 つのネームサーバーのみが保持されるようになりました。この場合、Pod はネームサーバーの警告を生成しなくなりました。(BZ#1791008)

- 以前のリリースでは、トランクポートのない RHOSP クラウドは、インストーラーが失敗として誤って解釈したエラーを返す可能性がありました。その結果、クラスターの破棄がタイムアウト前にループする可能性がありました。今回の更新により、インストーラーがエラーを正しく解釈し、トランクポートをサポートしないクラウドでのクラスターの正常な破棄が可能になりました。(BZ#1814593)

- 名前を共有する RHOSP リソースは削除できません。以前のバージョンでは、名前を共有するセキュリティーグループが存在する場合には、Ansible Playbook を使用するクラスターの破棄が RHOSP クラウドで失敗しました。**down-security-groups.yaml** Playbook はクラスターを破棄する際に名前の代わりにグループ ID を使用できるようになりました。Playbook が正常に終了すると、すべてのセキュリティーグループが削除されます。(BZ#1841072)

- 一部の RHOSP 環境では、仮想マシンが一時ディスクで起動できないようにするポリシーが実

行される可能性があります。そのため、ブートストラップマシンが一時ディスクから起動しようとすると、クラスターのインストールが失敗しました。ブートストラップマシンはコントロールプレーンのマシンプールからの **rootVolume** 設定に従い、仮想マシンが一時ディスクで起動できない環境でクラスターのインストールを正常に実行できるようになりました。(BZ#1820434)

- 以前のバージョンでは、RHOSP で実行されるクラスターでの Floating IP アドレス (FIP) の関連付けの前に、前提条件の Terraform の手順が常に実行される訳ではありませんでした。そのため、競合状態が生じ、インストールが失敗する可能性がありました。Thereaform の手順は FIP の関連付けの前に常に実行されるようになりました。(BZ#1846297)

- RHOSP 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スクリプトは一部の Ansible バージョンと互換性がないため、インストールは失敗しました。このスクリプトは、より幅広い互換性を確保できるように更新されました。これで、Ansible のバージョンに関係なくインストールは正常に実行されるようになります。(BZ#1810916)

- 現時点で、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 は、クラスターの有効期間に作成される Cinder ボリュームを削除しません。そのため、破棄されるクラスターは Cinder ボリュームをリークします。回避策として、クラスターの破棄後に Cinder ボリュームを手動で削除します。(BZ#1814651)

- 以前のバージョンでは、RHOSP のクラスターは、認証局 (CA) ファイルバンドルでこれに渡されたすべての証明書を処理しませんでした。そのため、クラスターはデフォルト以外の信頼される認証局によって署名された中間証明書でインストールできませんでした。CA ファイルは分割され、個別に処理されるようになりました。これにより、デフォルト以外の信頼できる認証局によって署名された中間証明書を使用するインストールが可能になりました。(BZ#1809780)

kube-apiserver

- 以前のバージョンでは、一部のユーザーは、アップストリームのバグが Kubernetes 1.14 および 1.16 コンポーネントの組み合わせを使用するクラスターの実行を妨げていたために、4.2 から 4.3 にアップグレードできませんでした。今回の修正には、アップグレード時に OpenShift Container Platform 4.3 が OpenShift Container Platform 4.2 と互換性を持つように、アップストリームからのマージが含まれるようになりました。(BZ#1816302)

- 以前のバージョンでは、Operator の新規バージョンの作成時に、ロックがリリースされるまでに数分かかる可能性があり、リーダーの選択の設定は、Operator がシャットダウンする UNIX シグナルを受信する際にロックを解除しないため、新規バージョンの Operator が継続する可能性がありました。今回の修正により、Operator のロールアウト時間は、コントロールプレーン Operator が正常に終了する期間を確保し、起動時にロックがリリースされるまで待機する必要がないため、大幅に改善されました。(BZ#1775224)

- 以前のバージョンでは、アップグレード時に OpenShift Container Platform API サーバーは、ノード上のルートが誤って設定されたためにトラフィックを提供できなくても、GCP ロードバランサーに再び追加されることがありました。これは、ノードと GCP ロードバランサー間の競合状態が原因で生じました。これは、ルート設定を iptables に移動し、ローカルトラフィックと非ローカルトラフィックを区別することで修正されています。ローカル以外のトラフィックは常に受け入れられるようになりました。API サーバーのアップグレード時に、接続は正常に終了し、新しい接続は実行中の API サーバーに対してのみ負荷分散されるようになりました。(BZ#1802534)

kube-scheduler

- 以前のバージョンでは、Descheduler はノードチェックループの初期段階で Pod が **NodeAffinity** ストラテジーでエビクトできるかどうかを判別するため、特定のノードに適合するためにエビクト可能であった Pod はエビクトされない可能性がありました。ノードチェック

ループのブレーク条件が修正され、エビクトの可能性を確認する際にすべてのノードが考慮されるようになりました。(BZ#1820253)

ロギング

- 以前のバージョンでは、Fluentd バッファーキューは制限されず、大量の受信ログにより、ノードのファイルシステムが一杯になり、クラッシュする可能性がありました。その結果として、アプリケーションはスケジュール変更されます。この種のクラッシュを防ぐために、Fluentd バッファーキューは出力ごとに固定した量のチャンクに制限されるようになりました (デフォルト: **32**)。(BZ#1780698)

- IPv6 ベアメタルのデプロイメントでは、Elasticsearch はクラスター IPv6 アドレスではなく IPv4 ループバックアドレスにバインドされました。その結果、Elasticsearch クラスターは起動できませんでした。Elasticsearch のバインディングおよび公開ホストを設定するために Downward API が変更されました。Elasticsearch はネットワークインターフェイスにバインドでき、予想通りに起動します。(BZ#1811867)

- クラスターロギングのクラスターロギングバージョン (CSV) は、一部のクラスターロギングコンポーネントのステータスを取得するために誤ったパスを使用していたため、ステータスは報告されませんでした。そのため、クラスターロギングは適切に機能しませんでした。パスは修正され、クラスターロギングが予想通りに機能するようになりました。(BZ#1840888)

- Elasticsearch Operator は 4 つ以上の Elasticsearch ノードが設定された場合に 2 つ目のデプロイメントを作成するため、Cluster Logging Operator は Elasticsearch ノードの正確な数を読み取りませんでした。そのため、クラスターロギングのカスタムリソースは、1 つのデプロイメントに関連するノードの数を常に報告しました。Cluster Logging Operator は Elasticsearch ノードの数を正しく計算するために変更されました。(BZ#1732698)

Machine Config Operator

- ワーカーノードで利用可能な複数のネットワークにより、CRI-O のコントロールプレーンでアドレスを選択することは容易ではありません。これにより、CRI-O はコントロールプレーン以外のインターフェイスにバインドされることがよくあります。今回のバグ修正により、CRI-O systemd サービスが適切なインターフェイスを選択し、CRI-O サービスを設定するサービスに依存するようになりました。これにより、CRI-O は予想通りにコントロールプレーンのアドレスにバインドされます。(BZ#1808018)

- 以前のバージョンでは、IPv6 ベアメタルデプロイメントで OperatorHub をネットワークが制限された環境用に設定する場合、DHCP で提供される名前がなしに OpenShift Container Platform (OCP) ノードで複数のインターフェイスが起動することがありました。これにより、マルチキャスト DNS 公開サービスがデフォルトの **localhost** 名で開始されました。今回のバグ修正により、Machine Config Operator はデフォルト以外の名前のみを設定し、それらが利用可能になるまで待機するようになりました。これにより、正しいホスト名がマルチキャスト DNS に公開されます。(BZ#1810333)

- Ingress 仮想 IP 管理設定は、パスワードに固定の文字列を使用していました。別個のクラスターの 2 つの VRRP keepalived インスタンスが同じ仮想ルーター ID を持つ場合、それらのインスタンスは同じパスワードを持ち、それらは単一の仮想ルーターに属する可能性がありました。今回のバグ修正により、クラスターの設定に応じてパスワードが変更されるようになりました。その結果、異なるクラスターの Ingress 仮想 IP が異なるパスワードを持つようになりました。(BZ#1803232)

- 以前のバージョンでは、コントロールプレーン IP を検出し、Kubelet および CRI-O の設定を実行する systemd サービスは、コントロールプレーン IP を設定する前に実行でき、これにより、**nodeip-configuration** 'Failed to find suitable node ip' という Kubelet および CRI-O の失敗メッセージが表示されました。システムはインターフェイスにコントロールプレーン IP が設定されるまで再試行するようになりました。(BZ#1819484)

- 以前のバージョンでは、CoreDNS が **/etc/resolv.conf** ファイルのサーバー一覧の DNS 要求を転送する際に、ファイルが変更されていると、その変更は CoreDNS Corefile に反映されませんでした。今回の修正により、Coredns-monitor Pod では CoreDNS の転送一覧が **/etc/resolv.conf** と同期し、サーバーの一覧がファイルに表示されることが検証されています。(BZ#1790819)

- 以前のバージョンでは、keepalived が使用するインターフェイスがブリッジ接続されている場合、ユーザーがインターフェイスをボンドまたはブリッジに動的に配置することが可能でした。これにより、keepalived が動作を再開できなくなり、仮想 IP 管理が中断する可能性がありました。今回の修正により、モニターインターフェイスが変更され、keepalived を再読み込みするようになり、新しい設定および仮想 IP 管理を読み取り、中断を最小限に抑えて動作するようになりました。(BZ#1751978)

- 一部のルートには **expires** フィールドが含まれるため、IPv6 (**non_virtual_ip** スクリプト) はルートを処理できませんでした。その結果、**non_virtual_ip** で設定される必要のあるサービスが失敗します。**non_virtual_ip** スクリプトが更新されています。ルートが解析され、サービスが正しく設定されます。(BZ#1817236

Web コンソール (Administrator パースペクティブ)

- モニターリングメトリクスクエリーページの Prometheus リンクがないために、コンソールの開始時に無効なモニターリングフラグが設定されました。適切なフラグが設定され、Prometheus モニターリングがメトリクスクエリーページで利用可能になりました。(BZ#1811481)

- ユーザーがサポートされない namespace へのインストールを試行する場合、ユーザーにとって Operator グループでサポートされるインストールモードが明確ではないため、フォームが送信されませんでした。サポートされる Operator のインストールモードについてアラートが追加されました。アラートは、選択された namespace をインストール Operator で使用できる理由を明確に示します。(BZ#1821407)

- **Machine Health Checks** および **Machine Config** は視覚的に区分けされておらず、ユーザーに混乱が生じさせました。明確化を図るために、分割バーが **Machine Health Checks** と **Machine Config** の間に追加されました。(BZ#1817879)

- 反応コンポーネントのプロパティーがないため、ブラウザーのコンソールにエラーメッセージが表示されます。反応コンポーネントにプロパティーが追加され、エラーメッセージは出されなくなりました。(BZ#1800769)

- 複数のアラートレシーバーは同じ名前で作成できます。同じ名前の付いたアラートのいずれかが削除されると、すべてが削除されます。**Create Receiver** フォームで、名前がすでに存在する場合にユーザーにエラーメッセージと共にプロンプトが出され、**Create** ボタンが無効になります。ユーザーは、同じ名前を持つ 2 つのレシーバーを作成できません。(BZ#1805133)

- PVC はアルファベット順で並べ替えられていましたが、現在は数値順に並べ替えられます。(BZ#1806875)

- サービスはアルファベット順に一覧表示され、**oc** は最初のオプションではありませんでした。**oc** オプションが一覧の先頭に追加されるようになりました。(BZ#1802429)

- アラートが Silenced 状態に変更された後も、**Status** カードと通知ドロワーはサイレンスにされているアラートを引き続き表示しました。ダッシュボードおよび通知ドロワーにはサイレンスのアラートが表示されなくなりました。(BZ#1802034)

- アラートが Silenced 状態に変更された後も、**Status** カードと通知ドロワーはサイレンスにされているアラートを引き続き表示しました。ダッシュボードおよび通知ドロワーにはサイレンスのアラートが表示されなくなりました。(BZ#1808059)

- ソートは列のデータに基づいておらず、誤ってソートされました。データは正しいオペランドのステータス値でソートされるようになりました。(BZ#1812076)

- ステータス記述子パスは、Donut チャート内で割り当てられた領域よりも長くなります。非常に長いステータス記述子パスは左右両側でクリッピングされ、値を不明確になる場合がありました。ステータス記述子のパスはドーナツグラフの下に置かれ、これを必要に応じてラップし、1 行に複数のステータス記述子を許可できるようになりました。長い値を持つステータス記述子パスが完全に表示され、ステータス記述子をすべて表示するために必要なスクロールが少なくなります。(BZ#1823870)

- Web コンソールには、バージョンが更新チャネルに表示されない場合に **Error Retrieving** の正しくない更新ステータスが表示されました。バージョンが利用可能であると示唆されても、実際には利用できないことがありました。バージョンが更新チャネルに表示されない場合に、Web コンソールに **Version not found** が表示されるように更新されました。(BZ#1819892)

- インストールされた Operator の一覧は **Name** 列でのみソート可能であり、ユーザーのソートオプションを制限します。ユーザーは name 列以外でも一覧をソートできるようになりました。(BZ#1797931)

- Pod の詳細ページには条件が含まれませんでした。条件がないと、Pod のステータスを把握することが困難でした。Pod の詳細ページに条件セクションが用意され、これにより Pod のステータスをより簡単に判別できるようになりました。(BZ#1804869)

- クエリーのブラウザーの結果はハードコーディングされたソートでレンダリングされました。ハードコーディングされたソートはクエリーで指定されたソートを上書きし、要求された結果とは異なる結果がレンダリングされる可能性があります。ハードコーディングされたソートが削除され、クエリーに指定されたソートが保持されるようになりました。(BZ#1808394)

- 以前のバージョンでは、ts-loader が正しくない **tsconfig.json** を使用するために Web コンソールの特定のページでランタイムエラーが生じることがありました。ts-loader の問題が解決され、すべての Web コンソールページが適切に読み込まれるようになりました。(BZ#1811886)

- Web コンソールの **Developer** パースペクティブから **Advanced → Project Details → Inventory** セクションに移動する場合、**DeploymentConfig** オブジェクトは一覧表示されませんでした。**DeploymentConfig** オブジェクトは追跡され、ダッシュボードの **Inventory** セクションに含まれるようになりました。(BZ#1825228)

- 以前のバージョンでは、ユーザー名に **#** などの特殊文字が含まれる場合に、Web コンソールにユーザーの詳細は表示されませんでした。Web コンソールには、ユーザー名の特殊文字に関係なくユーザーの詳細が表示されるようになりました。(BZ#1835460)

- 以前のバージョンでは、オブジェクトが YAML エディターで編集されると、必要な **metadata** フィールドが存在するかどうかを確認できませんでした。オブジェクトが保存される際にフィールドが見つからない場合は、エラーがブラウザーの JavaScript コンソールに記録されましたが、フィードバックは表示されませんでした。必要な **metadata** フィールドがない場合、Web コンソールには使用可能なエラーメッセージが表示されるようになりました。(BZ#1787503)

- 以前のバージョンでは、フォームビューを使用してオブジェクトを編集する際に、オブジェクトの YAML エディターに切り替えてもすべての既存データが同期されませんでした。すべてのデータがフォームビューと YAML エディター間で正しく同期されるようになりました。(BZ#1796539)

- 以前のバージョンでは、Tab キーで移動すると、通知ドロワーがトリガーされ、拡張される可能性がありました。今回のバグ修正により、UI 要素を使用してタブ入力しても通知ドロワーがトリガーされなくなりました。(BZ#1810568)

- 以前のバージョンでは、カスタムリソース定義 (CRD) の既存のインスタンスを一覧表示する際に、一覧にデータを設定するために正しくない API が使用されていました。正しい API を一覧でデータを設定するために使用できます。(BZ#1819028)

- **Operators → Installed Operators** ページで、選択した Operator で利用可能なカスタムリソース (CR) 一覧を表示する際に、**Version** 列に値 **Unknown** が表示されます。CR にはバージョン情報がないため、このフィールドは UI から削除されました。(BZ#1829052)

- 以前のバージョンでは、**Create Operator Subscription** フォームの入力時に、**Update Channel** フィールドが変更されると、サブスクリプションのターゲット namespace は誤ってリセットされ、フォームは送信されませんでした。**Update Channel** を調整する際に、ターゲット namespace の値が保持され、フォームが正常に送信されるようになりました。(BZ#1798851)

- 以前のバージョンでは、メトリクス **openshift_console_operator_build_info** は適切に公開されませんでした。今回のバグ修正により、メトリクスは Prometheus で利用可能になりました。(BZ#1806787)

- 以前のバージョンでは、Administration パースペクティブでは、サイドパネルが表示される **Workloads** タブを表示すると、通知ドロワーが、これを拡張するとサイドパネルの下で非表示になりました。今回のバグ修正により、CSS **z-index** が調整され、通知ドロワーが表示されるようになりました。(BZ#1813052)

- 以前のバージョンでは、Web コンソールで OperatorHub はクラスター管理者のみに表示されていました。今回の更新により、Web コンソールで、OperatorHub が **aggregate-olm-view** および **aggregate-olm-edit** クラスターロールバインディングが割り当てられたユーザーに表示されるようになりました。(BZ#1819938)

- 以前のバージョンでは、Web コンソールの **Administrator** パースペクティブの **Home → Events** ページで、複数のノードイベントについてノード名が表示されませんでした。今回の更新により、すべてのイベントが対応するノードに正しくリンクされるようになりました。(BZ#1809813)

- 以前のバージョンでは、Web コンソールの **Administrator** パースペクティブの **Home → Overview** メニュー項目は、namespace を一覧表示できず、クラスターメトリクスを表示するパーミッションを持つユーザーには非表示にされました。今回の更新により、クラスターメトリクスを閲覧する権限を持つすべてのユーザーに対して **Overview** ナビゲーションアイテムが表示されるようになりました。(BZ#1811757)

- 以前のバージョンでは、**Installed Operators** ページの OperatorHub で、インストールされた Operator の追加の API を表示するリンクでは正しいタブが開かれませんでした。今回の更新により、**Provided APIs** の下にある **View x more** リンクがインストールされた Operator の **Details** タグに移動されるようになりました。(BZ#1824254)

- 以前のバージョンでは、OperatorHub でコンテナーの背景のオーバーフローはモバイルビューで非表示にされませんでした。今回の更新によりグレーの背景が修正され、オーバーフローが非表示になりました。(BZ#1809812)

- 以前のバージョンでは、**fieldDependency specDescriptor** が予想通りに機能しませんでした。そのため、Control Field は Dependent Field の可視性を制御しませんでした。Dependent Field の可視性は、Control Field によって正常に有効または無効にされるようになりました。(BZ#1826074)

- 以前のバージョンでは、デフォルトの CA 証明書がコンソール Pod 内で使用されていました。今回のバグ修正により、設定マップが存在する場合に、コンソールを **default-ingress-cert** 設定マップを使用するように設定でき、存在しない場合には、コンソールが代わりにデフォルト

の CA 証明書を設定するようになりました。これにより、Ingress コントローラーが作成するルートへのアクセスを検証するために、(利用可能な場合は) デフォルトの Ingress 証明書を使用できます。(BZ#1824934)

- 以前のバージョンでは、新規の Alert Receiver の作成時に、Web コンソールはルーティングラベルが必要であることを示唆しませんでした。ルーティングラベルが必要であることを視覚的に示すインジケーターとして、赤いアスタリスクが追加されました。(BZ#1803614)

- 以前のバージョンでは、Web コンソールの **ClusterRole** の詳細ページの **Role Bindings** タブに、同じ名前を持つ namespace を使用したロールのバインディングが表示されていました。このタブには **ClusterRole** のバインディングのみが表示されるようになりました。(BZ#1624328)

- 以前のバージョンでは、OLM Operator のマークダウンテーブルは、コンテンツが多数ある場合に適切にレンダリングされませんでした。Web コンソールは、これらのテーブルの表示を改善し、必要な場合に水平スクロールバーを追加しました。(BZ#1831315)

- 以前のバージョンでは、Web コンソールですべての PVC をチェックする場合、PVC が属するストレージクラスを区別することは容易ではありませんでした。PVC ストレージクラスの列が Web コンソールに追加されたので、PVC のストレージクラス情報を見つけることがより簡単になりました。(BZ#1800459)

- 以前のバージョンでは、コンソールの **Compute → Machine Config Pools → Create Machine Config Pool** ボタンを使用して新規 MachineConfigPool を作成すると、ノードの一致しない MachineConfigPool が生成されました。これは、一致するノードを選択するために **spec.machineSelector** キーを使用するテンプレートによって生じました。ただし、このキーは API によって認識されません。ノードを選択する正しいキーは **spec.nodeSelector** です。ノードを選択するためのキーは更新され、Web コンソールに適切なノードに一致する Machine Selector が表示されるようになりました。(BZ#1813369)

- 以前のバージョンでは、CLI ダウンロードがアルファベット順で一覧表示されるため、**oc** は CLI ダウンロードページで最初に一覧表示されませんでした。**oc** は OpenShift Container Platform の主な CLI であるため、これは CLI ダウンロードページの上部に一覧表示されるようになりました。(BZ#1824934)

- 以前のバージョンでは、**Explorer** ビューで、**Access Review** タブがこれらのタブを表示するパーミッションを持たないユーザーに表示されていました。この許可のないユーザーにはエラーメッセージとタブの祭よ見込みを試行する指示が表示されましたが、再試行しても結果は変わりませんでした。今回のリリースにより、**Access Review** タブは、タブの内容を表示するパーミッションを持たないユーザーに表示されなくなりました。(BZ#1786251)

- 以前のリリースでは、**Cluster Utilization** カードビューと上位コンシューマーのポップオーバービューのメモリー消費データはメモリー使用量の計算に異なる方法を使用していたため、これらのデータに一貫性がありませんでした。今回のリリースにより、2 つのビューが同じ方法を使用してメモリー使用量を計算するため、それらが提供するデータに一貫性があります。(BZ#1812096)

- 以前のバージョンでは、ユーザーは単一のアラートレシーバーに 2 つのルーティングラベルを作成できました。2 つのルーティングラベルが同じキーを持つ場合、一覧ページには最も新しく作成されたラベルのみが表示されました。ただし、ルーティングラベルの 1 つが正規表現を使用している場合、Details ページでは、これらが 2 つの異なるルーティングラベルとして区別されます。今回のリリースにより、ユーザーは単一のアラートレシーバーに 2 つのルーティングラベルを作成できなくなりました。(BZ#1804049)

- 今回のリリースにより、Web コンソールが使用するライブラリーが更新され、一部のビューのパフォーマンスおよび表示に関連する問題が解決されました。(BZ#1796658)

- マストヘッドの選択リンクには、ターゲット宛先が含まれる OnClick ハンドラーと共に href の値 # が含まれました。そのため、それらのリンクには新規タブで開くオプションがありますが、# は意図されるターゲット宛先ではなく、ダッシュボードに対して解決されます。今回のリリースより、# の href のあるリンクがボタン要素に対して更新され、**Open Link In New Tab** オプションが利用できなくなりました。**Open Link In New Tab**オプションを持つリンクには、正しい URL が表示されます。(BZ#1703757)

モニターリング

- 以前のバージョンでは、Prometheus PVC 名に関連するメタデータを誤って処理すると、バージョン 4.4.0-4.4.8 間のアップグレードが失敗する可能性がありました。メトリクスデータを保持し、アップグレードを完了できるように、データが古い物理ボリュームから新しい物理ボリュームにコピーされるようになりました。(BZ#1832124)

- 以前のバージョンでは、Thanos Querier はマスターノードとワーカーノードの両方でスケジュールできましたが、これはワーカーノードでのみスケジュールされることが意図されていました。Thanos Querier のマスターノードでのスケジュールを許可する容認が削除され、Thanos Querier はワーカーノードのみにデプロイされるようになりました。(BZ#1812834)

- 以前のバージョンでは、Prometheus 記録ルールの評価は失敗することがあり、ルールから生成されるメトリクスがなくなることがありました。記録ルールは修正されました。(BZ#1802941)

- 以前のバージョンでは、データの統計的スムーズ化により、CPU の使用率で正しくない結果が表示されました。CPU の使用量を計算する方法が更新され、**oc adm top** の結果が Linux **top** ユーティリティーと同様になります。(BZ#1812004)

- 以前のバージョンでは、**cluster-monitoring-config** マップは無効であり、クラスターモニターリング Operator はデフォルト設定を使用するようデフォルト設定されるため、クラスターモニターリングへののカスタム設定が失われました。クラスターモニターリング Operator が **cluster-monitoring-config** 設定マップをデコードできない場合、デフォルト設定を使用せず、代わりにアラート警告が出されるようになりました。(BZ#1807430)

ネットワーク

- Kube-proxy メトリクス実装への変更により、一部のメトリクスは Kubernetes 1.17 のリベース時に非表示になりました。今回のバグ修正により、メトリクスが SDN で公開される方法が変更され、それらが非表示にされなくなりました。(BZ#1811739)

- 以前のバージョンでは、インストーラーで **machineNetwork** が導入されると、Cluster Network Operator はこれを **proxy.status.noProxy** に追加するように変更されませんでした。今回のバグ修正により、**proxy.status.noProxy** は **machineNetwork** を含む予想されるフィールドを含むように設定されました。(BZ#1797894)

- 以前のバージョンでは、ノードは自己 IP を誤って検出し、これにより割り当てられた egress IP を所有することができませんでした。今回のバグ修正により、Kubernetes API からノード IP が割り当てられるようになりました。(BZ#1802557)

- コードの変更により、サードパーティーのプラグインのステータスの設定が意図せず停止しました。つまり、Cluster Network Operator のステータスでこれが機能していると示唆されることはありませんでした。今回のバグ修正により、サードパーティーのプラグインが使用されている場合にステータスを設定するコードが追加されました。サードパーティープラグインが使用されている場合に Cluster Network Operator がステータスを正しく報告するようになりました。(BZ#1807611)

- 以前のバージョンでは、Kuryr ブートストラップの Cluster Network Operator には、非推奨となったセキュリティーグループルールが新規ルールで置き換えられる際に、それらを削除する

ロジックがありませんでした。OpenShift Container Platform のアップグレードでは、古いセキュリティーグループルールがセキュリティーグループに残されました。つまり、4.3 から 4.4 にアップグレードされた環境では、セキュリティーを強化するための措置は行われませんでした。今回のバグ修正により、Cluster Network Operator は古いセキュリティーグループルールを削除し、セキュリティーグループルールが 4.3 から 4.4 のアップグレードで削除され、Pod がホスト仮想マシンへの制限されたアクセスを正しく取得できるようになりました。(BZ#1832305)

- 以前のバージョンでは、トラフィックをブロックするネットワークポリシーを実行するために、そのポリシーに一致するサービスには、トラフィックをブロックするこれに対応するロードバランサーが必要でした。Octavia を ACL を使用し、ロードバランサーリスナーで admin 状態を作動してこれを提供しました。そのため、OpenShift Container Platform エンドポイントの Kuryr アノテーションでのセキュリティーグループと Pod に実際に設定されたセキュリティーグループの不一致により、一部のロードバランサーがネットワークポリシーの更新の対象として考慮され、トラフィックが admin 状態が無効にされた状態でブロックされました。今回のバグ修正により、エンドポイントについての Kuryr アノテーションのセキュリティーグループフィールドは、選択された Pod の既存のセキュリティーグループに一致します。ネットワークポリシーがブロックしていない場合には、すべてのロードバランサーリスナーの admin 状態が有効されるようになりました。(BZ#1824258)

- 以前のバージョンでは、iptables にはロックの問題がありました。Pod が起動に失敗し、**oc describe pod** コマンドで以下のテキストを含むイベントが表示されることが稀にありました。Failed create pod sandbox ... could not set up pod iptables rules: Another app is currently holding the xtables lock 今回のバグ修正により、**-w** はコードの関連する部分で iptables に渡され、iptables はロックを待機し、誤って失敗しなくなりました。(BZ#1810505)

- 以前のバージョンでは、ノードの削除時にノードの chassis レコードは south-bound データベースから削除されませんでした。古くなった chassis レコードにより、削除されない古い chassis の論理フローが生じました。今回のバグ修正により、ノードの同期メカニズムが **ovnkube-master** に追加され、削除されたノードの chassis レコードが消去されるようになりました。これで、south-bound データベースの削除されたノードに対応する古くなった chassis レコードまたは論理フローがなくなりました。(BZ#1809747)

- etcd の実行速度が遅いと、**openshift-sdn** では競合状態により namespace の作成イベントが失敗する可能性がありました。これにより、その namespace の Pod に接続がなくなる場合がありました。今回のバグ修正により、競合状態が削除されました。その結果、Pod は最終的に接続されるようになります。(BZ#1825355)

ノード

- 以前のバージョンでは、**kubepods.slice** メモリー cgroup は最大限度から予約分を差し引いた値に設定されませんでした。これにより、ノードがメモリー不足のエラーでオーバーロードし、ワークロードをエビクトできませんでした。**kubepods.slice** メモリー予約が適切に設定されるようになりました。(BZ#1800319)

- 以前のバージョンでは、デバイスのデバイスマッパーにはメトリクスがないため、システムがルートデバイスのデバイスマッパーを使用している場合にメトリクスを利用できませんでした。cadvisor は修正され、デバイスマッパーがルートデバイスに使用されるかどうかにかかわらず、メトリクスが利用可能になりました。(BZ#1849269)

Node Tuning Operator

- Node Tuning Operator には、BZ#1702724 および BZ#1774645 に関連する tuned デーモンの動作に対応する修正が同梱されていませんでした。そのため、ユーザーによって無効なプロファイルが指定されると、オペランドの機能のサービス拒否 (Denial of Service、DoS) が発生

しました。また、プロファイルを訂正してもオペランドの機能は復元されませんでした。これは、前述のバグ修正を適用することで修正され、tuned デーモンが修正された新規プロファイルを処理し、設定できるようになりました。(BZ#1823941)

- 以前のバージョンでは、チューニングされた Pod はホストから **/etc/sysctl.{conf,d/}** をマウントしませんでした。これにより、ホストが提供する設定が tuned プロファイルでオーバーライドされることが可能になりました。**/etc/sysctl.{conf,d/}** がチューニングされる Pod のホストからマウントされるようになり、これにより、tuned プロファイルが **/etc/sysctl.{conf,d/}** のホスト sysctl 設定をオーバーライドしなくなりました。(BZ#1825322)

oc

- 以前のバージョンでは、プリンターフラグが適切に接続されず、**oc adm group sync** コマンドには出力オプションがありませんでした。フラグが正しく接続されるようになり、すべての出力オプションが正しく機能するようになりました。(BZ#1828194)

- 以前のバージョンでは、結果をフォーマットする関数にはハードコーディングされたサイズが設定され、配列がハードコーディングされた制限よりも少ない値で一杯になるとパニックが生じました。LDAP エントリーの数は、実際の配列の容量に基づいて制限され、関数がその結果が正しくフォーマットするようになりました。(BZ#1806876)

- 以前のバージョンでは、**oc image mirror** コマンドは、**--dir** オプションを上書きするはずの場合でも、**--from-dir** オプションのみが指定される場合にエラーを出しました。**--from-dir** が **--dir** を適切に上書きし、コマンドが正常に実行されるようになりました。(BZ#1807807)

- 以前のバージョンでは、**oc adm release** コマンドのヘルプの例が正しく表示されませんでした。それらは更新され、適切に表示されるようになりました。(BZ#1810310)

OLM

- Operator Lifecycle Manager (OLM) によってインストールされたカスタムリソースには、適用元の **InstallPlan** オブジェクトに **OwnerReference** オブジェクトが付与されます。**InstallPlan** オブジェクトを削除すると、適用されたカスタムリソースが削除されます。今回のバグ修正により、OLM がカスタムリソースの **OwnerReference** オブジェクトをインストールに使用された CSV を参照するように更新されました。これにより、**InstallPlan** を削除しても、適用されたカスタムリソースは削除されなくなりました。(BZ#1808113)

- 以前のバージョンでは、ガベージコレクションのリソースイベントキューが正しく設定されませんでした。そのため、Operator のアンインストール時に Operator Lifecycle Manager (OLM) によって管理される Operator 用に生成されるクラスタースコープのリソースがクリーンアップされませんでした。今回のバグ修正により、OLM が更新され、ガベージコレクションのキューが任意の namespace を参照する所有者ラベルについてヒットされるように再設定されました。その結果、OLM によって管理される Operator 用に生成されるクラスタースコープのリソースが Operator のアンインストール時に適切にクリーンアップされるようになりました。(BZ#1834136)

- グループ (group)、バージョン (version)、および種類 (kind) (GVK) が直前のバージョンの Operator 以降変更されていない必須の API を提供する Operator がアップグレードされており、API に依存する Operator が **spec.Replaces** の代わりに **skipRange** を使用する場合、Operator Lifecycle Manager (OLM) は正しい **replaces** フィールドでアップグレードされた CSV を生成できません。具体的には、OLM は以下を実行します。

  1. 新規 Operator を生成に追加し、これが提供する API に **present** のマークを付けます。

  2. 生成から古い Operator を削除し、(新規バージョンの Operator で提供されている場合でも) これが提供する API に **absent** のマークを付けます。

3. 欠落している **API** の解決を試行し、新規バージョンの Operator を **spec.Replaces** フィールドが設定されていないコピーで上書きします。
   これにより、特定の Operator の新規バージョンへのアップグレードが失敗しました。今回のバグ修正により OLM が更新され、新規 Operator を生成に追加する前に古い Operator が現行の生成から削除されるようになりました。その結果、アップグレードは予想通りに成功します。(BZ#1818788)

- 無効な **CatalogSource** 設定により、nil-pointer の例外およびパニックが発生していました。**catalog-operator** Pod は、無効な **CatalogSource** オブジェクトが調整されるたびにクラッシュしていました。今回のバグ修正により、ランタイムの nil チェックおよび **CatalogSource** オブジェクトの検証が追加されました。その結果、無効な **CatalogSource** オブジェクトに代表的な条件が指定され、**catalog-operator** Pod がクラッシュしなくなりました。(BZ#1817833)

- Operator Lifecycle Manager (OLM) を使用すると、ユーザーは **Subscription** オブジェクトの **subscriptionConfig** フィールドを使用してボリュームおよび volumeMount を指定できます。この機能を使用することで、**ClusterServiceVersion** リソース (CSV) に定義される **Deployment** リソースを更新できます。OLM ではそのキャッシュに CSV 用の **Subscription** オブジェクトが作成されず、CSV は、**Subscription** オブジェクトにボリュームまたはボリュームマウントが定義された **Deployment** リソースを作成せずに installing phase (インストールフェーズ) に置かれることがありました。その後 OLM は、計算された **Deployment** リソースのハッシュが **Deployment** リソースの実際の **Deployment** ハッシュと一致しないため、CSV を Succeeded phase (成功フェーズ) に移動できませんでした。このエラーは、OLM が installing phase (インストールフェーズ) で **Deployment** リソースを更新したり、再作成したりしないために解決されず、このエラーは OLM が CSV を再同期してから 5 分が経過するまで残りました。その結果、OLM は CSV のインストール時に遅延することがありました。今回のバグ修正により、OLM が CSV のインストール時に **Deployment** リソースのハッシュエラーが生じると、OLM が **Deployment** リソースを再作成します。その結果、OLM が誤った **Deployment** リソースのハッシュにより遅延しなくなりました。(BZ#1826443)

- 以前のバージョンでは、Operator Lifecycle Manager (OLM) は単一の **Deployment** リソースで複数の **APIService** リソースの実行を想定せず、OLM によって作成された最後の **APIService** リソースに関連付けられた CA のみをマウントしていました。これにより、OLM は単一の **Deployment** リソースで複数の **APIService** リソースを実行できませんでした。今回のバグ修正により、OLM が単一 **Deployment** リソース上のすべての **APIService** リソースに同じ CA を使用できるように更新されました。その結果、OLM は単一 **Deployment** リソースで複数の **APIService** リソースを実行できるようになりました。(BZ#1805412)

- 以前のバージョンでは、Operator Lifecycle Manager (OLM) は、設定スキーマの導入時に v1alpha2 バージョンの **OperatorGroup** カスタムリース定義 (CRD) を正しく非推奨にしませんでした。このため、v1alpha2 **OperatorGroup** CRD はサポートされなくなり、それらを作成できませんでした。今回のバグ修正により v1alpha2 **OperatorGroup** CRD が再導入され、その結果として OLM は v1alpha2 **OperatorGroup** CRD を再度サポートするようになりました。(BZ#1798051)

- 以前に解決された **InstallPlan** オブジェクトに同等のマニフェストのセットが含まれなくなると、新たに確定的でない方法で解決された依存関係のセットの適用がトリガーされました。複数の有効な Operator の依存関係のセットが存在する場合、同等の異なる解決が既存のセットに適用されることがありました。今回のバグ修正により、**generation** フィールドが **InstallPlan** オブジェクト API のステータスに追加され、解決されるたびに増分し、最新のステータスの生成により **InstallPlan** オブジェクトのみが適用されるようになりました。その結果、所定の時間に Operator の依存関係の 1 つのセットのみがクラスターに存在することになります。(BZ#1784024)

- **OperatorHub** タイプの定義には、Kubernetes クライアントの生成に必要な追加の **+genclient** マーカーのコメントがありませんでした。そのため、生成されたクライアントが

openshift/client-go 設定クライアントでは利用できませんでした。今回のバグ修正により、欠落していた **+genclient** マーカーのコメントが **OperatorHub** 設定タイプに追加され、結果として生成されるクライアントが予想通りに利用可能な状態になりました。(BZ#1816483)

openshift-apiserver

- 以前のバージョンでは、アップグレード時に OpenShift API サーバーがクライアントで利用できなくなり、失敗が発生していました。OpenShift API サーバーは、アップグレード時も引き続きクライアントで利用可能になりました。(BZ#1791162)

openshift-controller-manager

- 以前のバージョンでは、OpenShift Container Platform 内部レジストリーのプルシークレットの作成に使用されるクライアントには低いレート制限が設定されていました。多数の namespace が短時間に作成された場合には、イメージレジストリーのプルシークレットが作成されるまでに時間がかかりました。クライアントのレート制限が引き上げられたため、内部レジストリーのプルシークレットはトラフィック量が多い場合でも迅速に作成されるようになりました。(BZ#1785023)

- 以前のバージョンでは、**workqueue_depth** などのメトリクスは Prometheus メトリクスで利用不可能でした。今回のバグ修正により、欠落していたメトリクスが利用可能になりました。(BZ#1825324)

- **openshift-controller-manager** Pod が失敗しても、終了メッセージは出されませんでした。Pod が終了すると、終了メッセージが表示されるようになりました。(BZ#1804432)

- 以前のバージョンでは、メトリクスは OpenShift Container Platform コントロールプレーンについて適切に登録されませんでした。今回のバグ修正により、コントロールプレーンのメトリクスが利用可能になりました。(BZ#1809699)

- 以前のバージョンでは、関連付けられたトークンが削除されると、内部レジストリーのプルシークレットが孤立した状態になりました。今回のバグ修正により、プルシークレットとトークン間に参照が作成され、関連付けられたトークンが削除されてもプルシークレットが孤立しなくなりました。(BZ#1765294)

- 以前のバージョンでは、OpenShift Container Platform がグローバルプロキシーで設定されている場合、プロキシーは外部イメージレジストリーへの接続時に使用されませんでした。外部レジストリーからイメージをプルする際に、OpenShift Container Platform はクラスター全体のプロキシー設定を使用するようになりました。(BZ#1805168)

- 以前のリリースでは、デプロイメントのローリング更新時に、コントローラーが長時間使用できなくなる可能性がありました。今回のバグ修正により、デプロイメントの Pod の終了時に、コントローラーがリースをプロアクティブにリリースできるようにすることで遅延が最小限に抑えられます。(BZ#1809719)

- 以前のバージョンでは、**openshift-controller-manager-operator** は、昇格した SELinux 権限へのアクセスを使用して実行される可能性がありました。今回のバグ修正により、適切な SCC (Security Context Constraints) が適用されるようになりました。(BZ#1806913)

- 以前のバージョンでは、アップグレード時に **openshift-controller-manager** は Operator がアップグレードされ、利用可能であることを誤って報告していました。Operator が正常に更新されると、Operator はこれを正常に報告するようになりました。(BZ#1804434)

- インストールまたはアップグレード時に、**openshift-controller-manager** は進捗の状態を適切に報告しませんでした。その結果、インストールまたはアップグレードが失敗する可能性があります。Operator はインストールまたはアップグレードが正常に実行されると、その進捗を正しく報告するようになりました。(BZ#1814446)

- 以前のバージョンでは、**image-resolve-plugin** は、**alpha.image.policy.openshift.io/resolve-names** アノテーションがリソースの作成後に追加された場合にイメージを解決しませんでした。**image-resolve-plugin** は修正され、 **alpha.image.policy.openshift.io/resolve-names** アノテーションがリソースの作成後に追加されてもイメージを解決するようになりました。(BZ#1805155)

- 以前のバージョンでは、IPv6 クラスターを使用する場合に、コントローラーマネージャー Operator はそのメトリクスを公開しませんでした。そのため、メトリクスが適切に収集されず、これにより、ユーザーにはパフォーマンスデータをグラフ化したり、クエリーする方法がありませんでした。コントローラーマネージャー Operator は IPv6 インターフェイスに適切にバインドされ、メトリクスは適切に収集され、ユーザーに表示されるようになりました。(BZ#1813233)

ルーティング

- 以前のバージョンでは、サービ出力ドバランサーに Azure マスターノードを含めることができませんでした。このため、ワーカーノードがマスターノードでもあるコンパクトなクラスターで Ingress の機能が中断しました。Azure は、ノードのネットワークインターフェイスカード (NIC) を単一ロードバランサーに関連付けることを常に許可します。今回の更新により、インストーラーは **LoadBalancer** タイプの API とサービスの両方に使用される統一されたロードバランサーとネットワークセキュリティーグループを作成するように変更されました。サービ出力ドバランサーには Azure のマスターノードを含めることができ、Ingress はコンパクトなクラスターでも機能するようになりました。(BZ#1794839)

- 以前のバージョンでは、openshift-router はシークレットが無効な場合に、デフォルトの証明書シークレットコンテンツの監視を設定しませんでした。起動時に、openshift-router は、ルーター Pod が起動するために必要なシークレットが無効な場合、そのシークレットの読み取りに失敗しました。そのため、ユーザーは無効なシークレットを更新し、現在のルーター Pod を削除する必要がありました。今回の更新により、ルーターは、ルーター Pod を削除せずにデフォルトの証明書シークレットの変更の有無を監視するようになりました。シークレットが無効な場合、ルーターはデフォルトのルーター証明書を使用し、これを提供します。シークレットが有効である場合、ルーターはそのシークレットからデフォルトの証明書を提供します。(BZ#1820400)

- 以前のバージョンでは、AWS China リージョンで実行される場合に Ingress Operator は DNS の設定に失敗しました。今回の更新により、Ingress Operator は AWS China リージョンで実行されるタイミングを検出し、Route 53 API エンドポイントで DNS を設定できるようになりました。(BZ#1805224)

- 以前のバージョンでは、Ingress Operator は Azure および Google Cloud Provider (GCP) で管理される DNS レコードに対する upsert 操作を継続的に実行しました。今回の更新により、Ingress Operator は、レコードがすでに公開されており、コントローラーがレコードに対して最後に upsert 操作を実行してからレコードや DNS ゾーン設定が変更されていない場合に、DNS レコードに対する upsert 操作を防ぎます。Ingress Operator によるクラウドプロバイダー API への呼び出し回数が減り、これにより **openshift-ingress** namespace での クラウドプロバイダーのレート制限 イベントの発生を防ぐことができる可能性があります。さらに、Ingress Operator ログには **upserted DNS record** ログメッセージの数が少なくなります。(BZ#1809354)

- 以前のバージョンでは、ingress-to-route コントローラーは、Kubernetes 1.18 で非推奨となった **extensions/v1beta1** API グループからの ingresses リソースを使用していました。今回の更新により、ingress-to-route コントローラーは **networking.k8s.io/v1beta1** API グループからの ingresses リソースを使用するようになりました。(BZ#1801415)

- 以前のバージョンでは、ルーターは、競合するルートが検出されると、アクティブではないルートをプロモートしませんでした。ルートが検出されると、ルーターはすべての非アクティブなルートを再処理し、削除されたルートと競合しなくなったルートをアクティブにするよう

になりました。(BZ#1821095)

- 以前のバージョンでは、タイプ **LoadBalancer** のサービスまたは **LoadBalancerService** エンドポイント公開ストラテジータイプの Ingress コントローラーが削除されると、サービスはそのまま存在し、**pending** 状態になりました。サービスコントローラーは OpenShift Container Platform 3.10 で変更され、**LoadBalancer** 以外のサービスが作成または削除される際に不要な **GetLoadBalancer** クラウドプロバイダー API 呼び出しを防ぐように変更されました。Kubernetes 1.15 の後続の変更により、これらの不要な API 呼び出しは別の方法で不可能にされました。その結果、これらの 2 つの変更の相互作用により、タイプ **LoadBalancer** のサービスについてのサービスコントローラーのクリーンアップロジックに障害が生じました。今回の更新により、OpenShift Container Platform 3.10 で追加された変更が削除されました。**LoadBalancer** タイプのサービスおよび **LoadBalancerService** タイプの Ingress コントローラーを削除できるようになりました。(BZ#1798282)

- 以前のバージョンでは、エンドポイント公開ストラテジーにロードバランサーの管理が含まれていない場合に、Ingress Operator によって不明確な **LoadBalancerManager** の状況条件の理由が設定されました。**IngressController** リソース が **LoadBalancerService** 以外のエンドポイント公開ストラテジータイプを使用するように設定される場合、Ingress Operator は Ingress コントローラーのロードバランサーを管理しません。今回の更新により、**LoadBalancerManager** の状況条件には、Operator が Ingress コントローラーのロードバランサーを管理しない理由がより明確に示されるようになりました。メッセージには、**unsupported** または **does not support** などのフレーズが使用されなくなりました。(BZ#1826113)

- 以前のバージョンでは、標準以外の **proto-version** パラメーターを持つ Forwarded HTTP ヘッダーは、Ingress コントローラーが HTTP 要求をアプリケーションに転送する際に追加されました。そのため、Forwarded ヘッダーは標準に準拠しておらず、アプリケーションがヘッダー値を解析しようとする際に問題が生じる可能性がありました。今回の更新により、Forwarded ヘッダーが標準に準拠し、Ingress コントローラーは Forwarded ヘッダーに **proto-version** パラメーターを指定しなくなりました。(BZ#1803001)

- 以前のバージョンでは、アクティブなセッション数を表示する Prometheus カウンターはルーターの再起動後も保持され、無限に増加していました。今回の更新により、**haproxy_frontend_current_session** および **haproxy_server_current_session** はアクティブなセッション数を正確に示すようになりました。このカウンターの値は、ルーターの再起動時にリセットされるようになりました。(BZ#1832539)

- ルート経由で公開されるサービスのバッキング Pod が利用不可である場合 (クラッシュループ、削除などによる)、ルーターは **503** エラーを出して応答します。以前のリリースでは、そのルートの **haproxy_server_http_responses_total** メトリクスは利用可能でなくなっていたため、そのルートでのモニターリングは実行できませんでした。今回の更新により、すべてのバックエンドメトリクスが報告され、ユーザーは Pod が起動しないタイミングを追跡できるようになりました。(BZ#1835845)

サンプル

- 以前のバージョンの Samples Operator はサンプルコンテンツが s390x および ppc64le アーキテクチャーで利用可能にされていない場合でも、それらのアーキテクチャーで削除されず、ブートストラップが正常に実行されませんでした。これにより、サンプルコンテンツが実際には利用可能ではないのにこれがあることが予想されたため、s390x および ppc64le アーキテクチャーでのクラスターのアップグレードが失敗しました。Samples Operator に必要なサンプルコンテンツが含まれていない場合でも、そのアップグレードが強制的に実行されるようになりました。これにより、s390x および ppc64le アーキテクチャーで利用できないサンプルコンテンツによって生じるクラスターのアップグレードの障害が修正されました。(BZ#1835112)

- 以前のバージョンの OpenShift Container Platform リリースで利用可能なイメージストリームのサンプルが後続のリリースで削除された場合、その後続のリリースへのアップグレード時

に、削除されたイメージストリームが完了までにイメージストリームのインポートが必要であるとして誤って追跡される可能性がありました。しかし、イメージストリームのインポートは発生しないため、サンプルはアップグレードを完了済みとして報告しませんでした。これにより、クラスターのアップグレードが失敗しました。Samples Operator は、アップグレードが予定されるリリースではなく、以前のリリースに存在するイメージストリームの追跡を無視できるように更新されました。イメージストリームはリリース間で削除されるようになり、アップグレード時に Samples Operator が失敗しなくなりました。(BZ#1811143)

- 以前のバージョンでは、Samples Operator は削除済みとしてブートストラップされる際に、無効な設定や欠落しているイメージプルシークレットについてのアラートを送信していました。これにより、無効な設定および欠落しているイメージプルシークレットについての誤解を生じさせるアラートがユーザーに送信されました。Samples Operator が削除されている場合、これによってこれらのアラートが送信されるはずがないためです。Samples Operator は、それが削除済みの状態でブートストラップが実行される際にサンプルのインポートに関連するアラートを送信しないように更新されました。(BZ#1813175)

- 以前のバージョンでは、以前のリリースで利用可能であり、その後のリリースで削除されたテンプレートのサンプルには、needing updates (要更新) というマークが付けられる場合がありました。テンプレートの更新を試みると、さまざまなエラーと失敗ステータスが出されました。これらのテンプレートは、削除後に更新を受信しないように更新されました。そのため、削除されたサンプルテンプレートはエラーや障害を生成しません。(BZ#1828065)

ストレージ

- 以前のバージョンでは、ボリュームは、適切なアベイラビリティーゾーンのサポートなしに作成された特定の Azure リージョンでのプロビジョニングに失敗する可能性がありました。今回の修正により、すべての Azure リージョンでボリュームのプロビジョニングを有効にするために、アベイラビリティーゾーンのサポートがプロビジョニング時に検出されるようになりました。(BZ#1828174)

- 以前のバージョンでは、namespace は **VolumeSnapshotClass** が関連付けられた **VolumeSnapshot** リソースの前に削除される場合に **Terminating** のままになり、**VolumeSnapshot** オブジェクトはクラスターに残りました。この場合、関連付けられたリソースを削除することができなくなるためです。今回の修正により、**VolumeSnapshot** 機能は、関連する **VolumeSnapshotClass** リソースがすでに削除されているかどうかを検査するようになり、対応する **VolumeSnapshotClass** が存在しない場合も **VolumeSnapshot** リソースが正常に削除されるようになりました。(BZ#1808123)

- 以前のバージョンでは、**VolumeSnapshotContents** リソースが nil の場合に CSI スナップショットコントローラーがクラッシュする可能性がありました。システムは、**VolumeSnapshotContent** リソースの使用前にこれが nil であるかどうかを確認します。(BZ#1814280)

- 以前のバージョンでは、ローカルストレージ Operator をアップグレードする際に、**LocalVolume** リソースも変更されない限り、関連付けられたディスクメーカーおよびプロビジョナー Pod はどちらも古くなっている可能性があります。今回の修正により、デーモンセットのハッシュがアノテーションに含まれるようになりました。ハッシュが一致しない場合、Pod はデプロイされ、ローカルストレージ Operator の更新時にディスクメーカーおよびプロビジョナー Pod が正常に更新されるようになりました。(BZ#1822213)

- 以前のバージョンでは、**oc get volumesnapshot** はリソースの名前および作成時間のみを表示し、ステータスは表示されませんでした。今回の修正により、**oc get volumesnapshot** には、関連付けられた **VolumeSnapshotContent** リソース、 **VolumeSnapshot** リソースソース、その他関連情報などの追加の詳細情報が含まれるようになりました。(BZ#1800437)

- 以前のバージョンでは、**oc get volumesnapshotclass** はリソースの名前および作成時間のみを表示し、削除ポリシーまたはドライバー情報を表示しませんでした。今回の修正により、**oc**

get volumesnapshotclass に、関連付けられた CSI ドライバーおよび削除ポリシーなどの追加の詳細情報が含まれるようになりました。(BZ#1800470)

- 以前のバージョンでは、**oc get volumesnapshotcontent** はリソースの名前および作成時間のみを表示し、追加の詳細情報を表示しませんでした。今回の修正により、 **oc get volumesnapshotcontent** には、関連付けられた **VolumeSnapshot** リソース、**VolumeSnapshotClass** リソース、その他関連情報などの追加の詳細情報が含まれるようになりました。(BZ#1800477)

1.6. 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 4.3	OCP 4.4	OCP 4.5
Precision Time Protocol (PTP)	TP	TP	TP
oc CLI プラグイン	TP	TP	TP
experimental-qos-reserved	TP	TP	TP
Pod Unidler	TP	TP	GA
一時ストレージの制限/要求	TP	TP	TP
Descheduler	-	TP	TP
Podman	TP	TP	TP
PID Namespace のコントロール共有	TP	TP	GA
OVN-Kubernetes Pod ネットワークプロバイダー	TP	TP	TP
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	TP

機能	OCP 4.3	OCP 4.4	OCP 4.5
マシンのヘルスチェック	TP	GA	GA
3 ノードのベアメタルデプロイメント	TP	TP	GA
Helm CLI	TP	GA	GA
サービスバインディング	TP	TP	TP
ログ転送	TP	TP	TP
ユーザーワークロードの監視	TP	TP	TP
OpenShift Serverless	TP	GA	GA
コンピュートノードトポロジーマネージャー	TP	TP	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
CSI ボリュームのクローン作成	-	TP	GA
CSI ボリューム拡張	TP	TP	TP
CSI AWS EBS Driver Operator	-	-	TP
OpenStack Manila CSI ドライバー Operator	-	-	GA
CSI インラインの一時ボリューム	-	-	TP
OpenShift Pipeline	-	TP	TP
Vertical Pod Autoscaler	-	-	TP
Operator API	-	-	TP
OpenShift Virtualization	TP	TP	GA

1.7. 既知の問題

- 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)

- 内部 Elasticsearch インスタンスが永続ボリューム要求 (PVC) を使用する場合、PVC には **logging-cluster:elasticsearch** ラベルが含まれる必要があります。ラベルがない場合、アップグレード時にガベージコレクションプロセスではそれらの PVC が削除され、Elasticsearch Operator は新規 PVC を作成します。バージョン 4.4.30 より前の OpenShift Container Platform バージョンから更新する場合は、ラベルを Elasticsearch PVC に手動で追加する必要があります。OpenShift Container Platform 4.4.30 以降では、Elasticsearch Operator はラベルを PVC に自動的に追加します。

- 新規 OpenShift Container Platform z-stream リリースにアップグレードする場合、ノードがアップグレードされると API サーバーへの接続が中断され、API 要求が失敗する可能性があります。(BZ#1845411)

- 新規 OpenShift Container Platform z-stream リリースにアップグレードする場合、ルーター Pod が更新されているためにルーターへの接続が中断される可能性があります。アップグレードの期間中、一部のアプリケーションには常に到達できなくなる可能性があります。(BZ#1809665)

- デフォルトの CNI ネットワークプロバイダーを OVN-Kubernetes に設定して新規の OpenShift Container Platform リリースにアップグレードする場合、アップグレードは失敗し、クラスターは使用不可能な状態のままになります。(BZ#1854175)

- イメージレジストリーのプルスルーの **ImageContentSourcePolicy** はまだサポートされていないため、イメージストリームでプルスルーポリシーが有効にされている場合、デプロイメント Pod はダイジェスト ID を使用してイメージをミラーリングできません。この場合、**ImagePullBackOff** エラーが表示されます。(BZ#1787112)

- ユーザーによってプロビジョニングされるインフラストラクチャーを使用する RHOSP でのクラスターの実行中に RHEL ワーカーを使用して拡張すると、Ingress ポートの VIP が RHEL ワーカーにある場合にすべてのルートにアクセスできなくなります。回避策として、ルーター Pod を RHCOS ノードに再スケジュールし、Ingress VIP を RHCOS ノードに移行する必要があります。これを実行するには、アップグレード前に **node.openshift.io/os_id: rhcos** ラベルを Ingress コントローラーに追加します。

```
$ oc -n openshift-ingress-operator edit ingresscontroller/default -o yaml
spec:
  nodePlacement:
    nodeSelector:
      matchLabels:
        kubernetes.io/os: linux
        node-role.kubernetes.io/worker: ""
        node.openshift.io/os_id: rhcos
```

(BZ#1848945)

- Che Workspace Operator は、**Workspace** カスタムリソースの代わりに **DevWorkspace** カス

タムリソースを使用するように更新されました。ただし、OpenShift Web ターミナルは引き続き **Workspace** カスタムリソースを使用します。このため、OpenShift Web ターミナルは最新バージョンの Che Workspace Operator で機能しなくなります。(BZ#1846969)

- **basic-user** は、**Developer** パースペクティブの **Monitoring** ビューで **Dashboard** および **Metrics** タブを表示できません。(BZ#1846409)

- **Topology** ビューで Knative サービスを右クリックすると、コンテキストメニューで **Edit Application Grouping** オプションが 2 度表示されます。(BZ#1849107)

- Special Resources Operator (SRO) は OpenShift Container Platform 4.5 に正常にデプロイできません。このため、クラスターに必要な NVIDIA ドライバーが GPU リソースを必要とするワークロードを実行することができません。また、この既知の問題があるために Topology Manager 機能は GPU リソースでテストすることができませんでした。(BZ#1847805)

- Web コンソールには、SLIRP バインディングで仮想マシンの vNIC を作成するオプションが含まれますが、これはサポートされていません。このオプションの使用を試みると、仮想マシンが起動に失敗します。このオプションは選択しないでください。(BZ#1828744)

- ノード内で OpenShift SDN のデフォルト CNI ネットワークプロバイダーを使用する Pod がネットワーク通信を失い、Pod がクラッシュする可能性が生じる問題があります。これは、クラスターのアップグレード時に発生することがあります。回避策として、Pod を削除して再作成できます。(BZ#1855118)

- マスターノードでカスタムプールがサポートされないという既知の問題があります。コマンド **oc label node** は新規カスタムロールをターゲットマスターノードに適用しますが、Machine Config Operator はカスタムプールに固有の変更を適用しません。これによりエラーが生じ、エラーは Machine Config Controller Pod ログに表示されます。コントロールプレーンノードの安定した状態を維持するための推奨される回避策として、マスターで複数のロールを適用しないことが推奨されます。(BZ#1797687)

- クラスターのロギングパフォーマンスは、OpenShift Container Platform の以前のバージョンと比較すると低下します。これについては調査が行われており、OpenShift Container Platform の今後のリリースで更新されます。(BZ#1833486)

- ボリュームに多数のファイルが含まれる場合、システムがボリュームをマウントできないというメッセージが表示される可能性があります。これは、Pod が **FSGroup SecurityContext** で設定されるボリュームをマウントする場合に発生する可能性があります。ファイルの GID 所有権がボリューム上のすべてのファイルについて再帰的に更新される必要があるためです。ユーザーは Pod が多数のファイルを持つボリュームを使用しており、**FSGroup SecurityContext** 設定の場合に起動にかなり時間がかかる可能性があることを予想する必要があります。(BZ#1515907)

- プローブが頻繁に発生する Pod を実行すると、共通プロセス (common process) の数がすぐに増大する可能性があります。共通プロセス (common process) は親 (CRI-O) から切り離されるプログラムであり、コンテナーランタイムの実行に使用されます。プローブが頻繁に発生すると、systemd はその新規の子すべてを取得できず、一部の共通プロセス (common process) がゾンビ (zombie) 状態になる可能性があります。(BZ#1852064)

- Microsoft Azure では、4.4 から 4.5 にアップグレードする際に、Ingress Operator はトークンの更新エラーにより DNSRecord を確認できない場合があります。Ingress Operator を再起動すると、この問題は解決されます。(BZ#1854383)

- 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 Azure で OpenShift Container Platform を実行する場合、**oc** コマンドが TLS ハンドシェイクのタイムアウトエラーで断続的に失敗するという既知の問題があります。(BZ#1851549)

- 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 VMware vSphere インスタンス上のクラスターの場合、ブートストラップワーカーは失敗します。デフォルトのリソースプールは複数のインスタンスに解決します。(BZ#1852545)

- OpenShift Container Platform クラスターのインストール時に Machine Config Operator (MCO) のパフォーマンスが低下する問題があります。これは、ブートストラップのプロセス時にマシン設定の順序付けの問題によって生じます。回避策として、カスタムマシン設定ファイルに **99-** ではなく、**98-** の異なる優先順位の接頭辞を付ける必要があります。(BZ#1826150)

- HTTPS プロキシーを通過する git clone 操作は失敗します。非 TLS (HTTP) プロキシーは問題なく使用できます。(BZ#1750650)

- ソース URI が **git://** または **ssh://** スキームを使用する場合、git clone 操作はプロキシーの背後で実行されているビルドで失敗します。(BZ#1751738)

- s390x および ppc64le アーキテクチャーについて、強制的な再起動または電源が切れた後にノードがワークロードで利用できない状態になる問題が確認されました。ノードを強制的に再起動したり、ノードの電源を切らないようにしてください。
  強制的な再起動または電源オフを回避できず、再起動後または電源オフ後のノードがワークロードで利用不可になる場合、以下を実行してください。

  1. ノードに対して SSH を実行します。
  2. CRI-O および kubelet サービスを停止します。
  3. **rm -rf /var/lib/containers** コマンドを実行します。
  4. CRI-O および kubelet サービスを再起動します。
     (BZ#1858411)

- AWS アカウントが、グローバル条件を使用してすべてのアクションを拒否するか、または特定のパーミッションを要求する AWS 組織サービスコントロールポリシー (SCP) を使用するように設定されている場合、OpenShift Container Platform AWS のインストールは、提供される認証情報にインストールに必要なパーミッションが含まれる場合でも失敗します。
  この問題に対する回避策 が OpenShift Container Platform 4.5.8 で導入されました。
  (BZ#1829101)

- 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 4.5 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)

- **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)

1.8. エラータの非同期更新

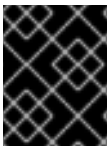
OpenShift Container Platform 4.5 のセキュリティー、バグ修正、拡張機能の更新は、Red Hat Network 経由で非同期エラータとして発表されます。OpenShift Container Platform 4.5 のすべてのエラータは Red Hat カスタマーポータルから入手 できます。非同期エラータについては、OpenShift Container Platform ライフサイクル を参照してください。

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 4.5 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 4.5.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。

1.8.1. RHBA-2020:2409 - OpenShift Container Platform 4.5 イメージリリースおよびバグ修正アドバイザリー

発行日: 2020-07-13

OpenShift Container Platform リリース 4.5 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-2020:2409 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-2020:2408 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 4.5.1 コンテナーイメージの一覧

1.8.2. RHSA-2020:2412 - Moderate (中程度): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-07-13

コンテナーイメージの更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:2412 アドバイザリーに記載されています。

1.8.3. RHSA-2020:2413 - Moderate (中程度): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-07-13

パッケージの更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:2413 アドバイザリーに記載されています。

1.8.4. RHBA-2020:2909 - OpenShift Container Platform 4.5.2 バグ修正の更新

発行日: 2020-07-16

OpenShift Container Platform リリース 4.5.2 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-2020:2909 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-2020:2908 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 4.5.2 コンテナーイメージの一覧

1.8.4.1. バグ修正

- OpenShift Container Platform 4.5.1 へのアップグレードは Secure Boot が設定されたノードで失敗します。Secure Boot で設定されたクラスターの場合、コントロールプレーンとコンピュートマシン設定プールの両方からの 1 つのノードが再起動に失敗し、これにより Machine Config Operator (MCO) のパフォーマンスが低下します。その後、クラスターはアップグレードに失敗しました。本リリースではこの問題はありません。(BZ#1856501)

1.8.5. RHBA-2020:2956 - OpenShift Container Platform 4.5.3 バグ修正の更新

発行日: 2020-07-22

OpenShift Container Platform リリース 4.5.3 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-2020:2956 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-2020:2955 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 4.5.3 コンテナーイメージの一覧

1.8.5.1. バグ修正

- 以前のバージョンでは、強制的な再起動または電源オフの後にノードがワークロードで利用できなくなる問題がありました。これは修正されています。(BZ#1857224)

- 以前のバージョンでは、Web コンソールでは、パッケージで宣言された最初のチャネルからのアイコンを返して、OperatorHub に表示される Operator アイコンを選択していました。これにより、表示されるアイコンがパッケージに公開される最新のアイコンとは異なる場合がありました。これは、デフォルトのチャネルからアイコンを選択することにより修正され、最新のアイコンが表示されるようになりました。(BZ#1844588)

- 以前のバージョンでは、OpenShift Container Platform ビルドで使用されるコンテナーイメージ署名ポリシーにはローカルイメージの設定が含まれていませんでした。特定のレジストリーからのイメージのみを許可する場合、ローカルイメージの使用が許可されていないため、ビルドの **postCommit** スクリプトは失敗していました。コンテナーイメージ署名ポリシーが更新され、ローカルストレージ層を直接参照するイメージが常に許可されるようになりました。ビルドに **postCommit** フックが含まれる場合、ビルドが正常に実行されるようになりました。(BZ#1849173)

1.8.6. RHBA-2020:3028 - OpenShift Container Platform 4.5.4 バグ修正の更新

発行日: 2020-07-30

OpenShift Container Platform リリース 4.5.4 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:3028 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-2020:3027 および RHEA-2020:3208 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 4.5.4 コンテナーイメージの一覧

1.8.6.1. 機能

1.8.6.1.1. IBM Z および LinuxONE

本リリースでは、IBM Z および LinuxONE は OpenShift Container Platform 4.5 と互換性があります。インストール手順については、IBM Z および LinuxONE 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。

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。
  - OpenShift Virtualization
  - ログ転送
  - Precision Time Protocol (PTP) ハードウェア
  - CSI ボリュームスナップショット
  - OpenShift Pipeline
- 以下の OpenShift Container Platform 機能はサポートされていません。
  - Red Hat OpenShift Service Mesh
  - OpenShift Do (odo)
  - CodeReady Container (CRC)
  - OpenShift Container Platform Metering
  - Multus CNI プラグイン
  - OpenShift Container Platform アップグレードの段階的ロールアウト
  - 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イス (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

- 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のタイプは Filesystem: NFS である必要があります。
- これらの機能は 4.5 の場合に IBM Z での OpenShift Container Platform に利用できますが、x86 での OpenShift Container Platform 4.5 には利用できません。
    - IBM System Z 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)。

1.8.6.1.2. IBM Power Systems

本リリースでは、IBM Power Systems は OpenShift Container Platform 4.5 と互換性があります。IBM Power 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 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。

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

- IBM Power Systems 向けの OpenShift Container Platform には、以下のテクノロジープレビュー機能が含まれていません。
    - Container-native virtualization (CNV)
    - OpenShift Serverless
- 以下の OpenShift Container Platform 機能はサポートされていません。
    - Red Hat OpenShift Service Mesh
    - OpenShift Do (odo)
    - CodeReady Container (CRC)
    - Tekton をベースとする OpenShift Pipeline
    - OpenShift Container Platform Metering
    - SR-IOV CNI プラグイン
- 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** モードである必要があります。
- ネットワークは、Red Hat OpenShift SDN で DHCP または静的アドレス指定のいずれかを使用する必要があります。

サポートされる機能

- 現時点で、3 つの Operator がサポートされています。
    - Cluster-Logging-Operator
    - Cluster-NDF-Operator
    - Elastic Search-Operator

1.8.6.2. バグ修正

- 以前のバージョンでは、オペランド一覧のオペランドのアクションメニューは、メニューが開かれた直後に閉じられました。この動作は、**Installed Operators → Operator Details** ページで Operator が提供する API のタブをクリックする際に確認されました。このメニューは正常に機能し、ユーザーの対話なしに閉じられることはなくなりました。(BZ#1842717)

- 以前のバージョンでは、Web コンソールで OperatorHub カタログをフィルターする際に、一部の Operator アイコンはユーザーがページ上でスクロールダウンするまで表示されませんでした。今回のリリースにより、フィルターが適用されるとアイコンがすぐに表示されます。(BZ#1844503)

- 以前のバージョンでは、Web コンソールの **Resource Quota Details** ページのクォータ測定チャートは幅がゼロで表示されませんでした。この問題は本リリースでは解決されています。(BZ#1845125)

- 以前のバージョンでは、**EtcdRestores** ページの **Create EtcdRestore** をクリックすると、Web コンソールの応答が停止しました。今回のリリースにより、**Create EtcdRestore** フォームビューのワークフローが正しく読み込まれるようになりました。(BZ#1847277)

- 以前のバージョンでは、OpenShift Serverless Operator の **Create Knative Serving** フォームビューワークフローで、数字のみが許可されるはずの一部のフィールドで数字以外の文字も許可されていました。この問題は本リリースでは解決されています。(BZ#1847283)

- 以前のバージョンでは、Manila CSI ドライバー Operator について **Create ManilaDriver** フォームビューワークフローで **Create** をクリックしても、Web コンソールで **ManilaDriver** インスタンスや応答が作成されませんでした。この問題は本リリースでは解決されています。(BZ#1853274)

1.8.6.3. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.7. RHSA-2020:3207 - Moderate (中程度): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-07-30

jenkins-2-plugins の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3207 アドバイザリーに記載されています。

1.8.8. RHBA-2020:3188 - OpenShift Container Platform 4.5.5 バグ修正の更新

発行日: 2020-08-10

OpenShift Container Platform release 4.5.5 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-2020:3188 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-2020:3189 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 4.5.5 コンテナーイメージの一覧

1.8.8.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.9. RHBA-2020:3330 - OpenShift Container Platform 4.5.6 バグ修正の更新

発行日: 2020-08-17

OpenShift Container Platform release 4.5.6 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:3330 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-2020:3331 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 4.5.6 コンテナーイメージの一覧

1.8.9.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.10. RHSA-2020:3453 - Important (重要): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-08-17

jenkins-2-plugins および **python-rsa** の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3453 アドバイザリーに記載されています。

1.8.11. RHBA-2020:3436 - OpenShift Container Platform 4.5.7 バグ修正の更新

発行日: 2020-08-24

OpenShift Container Platform release 4.5.7 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:3436 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-2020:3437 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 4.5.7 コンテナーイメージの一覧

1.8.11.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.12. RHSA-2020:3519 - Important (重要): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-08-24

jenkins および **openshift** の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3519 アドバイザリーに記載されています。

1.8.13. RHSA-2020:3520 - Moderate (中程度): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-08-24

openshift-enterprise-hyperkube-container の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3520 アドバイザリーに記載されています。

1.8.14. RHBA-2020:3510 - OpenShift Container Platform 4.5.8 バグ修正の更新

発行日: 2020-09-08

OpenShift Container Platform リリース 4.5.8 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:3510 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-2020:3511 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 4.5.8 コンテナーイメージの一覧

1.8.14.1. 機能

1.8.14.1.1. ネットワークインターフェイスの **projectID** フィールドを追加

新規 **projectID** フィールドは、**.spec.template.spec.providerSpec.networkInterfaces** 下の **MachineSet** カスタムリソースで設定できるようになりました。このフィールドでは、マシンを共有 VPC で起動できます。

```
...
providerSpec:
  ...
  networkInterfaces:
    - network: <infrastructureID>-network
      subnetwork: <infrastructureID>-<role>-subnet
      projectID: <projectID>
...
```

詳細は、BZ#1868751 を参照してください。

1.8.14.1.2. 正しくない **AWS** パーミッションの検証をバイパスするために **credentialsMode** パラメーターを追加

AWS インストールの場合、OpenShift Container Platform はパーミッションを検証する際に AWS ポリシーシミュレーター API に依存します。AWS アカウントが AWS 組織サービス制御ポリシー (SCP) を使用するように設定されている場合、パーミッションは SCP で設定されるポリシーに対してチェックされます。SCP にグローバル条件を使用してすべてのアクションを拒否するか、または特定のパーミッションを要求するポリシーが含まれる場合、ポリシーシミュレーター API はパーミッションを適切に検証しません。たとえば、**us-east-1** および **us-west-2** を除くすべてのリージョン用、または **role-xyz** を除くすべてのロール用の条件のあるポリシーにより、AWS API は未検出 (false negative) を返します。

パーミッションを検証できない場合、提供される認証情報に OpenShift Container Platform をインストールするのに必要なパーミッションがある場合でも、OpenShift Container Platform AWS のインストールに失敗します。

今回のリリースにより、**credentialsMode** パラメーターの値を **install-config.yaml** 設定ファイルに設定して、ポリシーシミュレーターのパーミッションチェックをバイパスできます。

サンプル install-config.yaml 設定ファイル

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Mint (1)
compute:
- architecture: amd64
  hyperthreading: Enabled
...
```

(1) この行は、**credentialsMode** パラメーターを **Mint** に設定するために追加されます。

credentialsMode の値を設定すると、SCP を使用するよう設定された AWS アカウントのパーミッションチェックがバイパスされ、インストールを続行できます。このチェックを省略する場合、指定する認証情報に指定されたモードに必要なパーミッションがあることを確認します。

credentialsMode の値は、Cloud Credential Operator (CCO) の動作を以下のように変更します。

- **Mint**: CCO は提供される管理レベルのクラウド認証情報を使用してインストーラーを実行します。インストール後に認証情報が削除されない場合、これは保存され、クラスター内の **CredentialsRequest** カスタムリソースを処理し、特定の必要なパーミッションを持つそれぞれの新規ユーザーを作成するために CCO によって使用されます。

- **Passthrough**: CCO は、インストーラーを実行してインストールを実行するのに十分なパーミッションを含む、提供される管理者以外のクラウド認証情報を使用します。インストールされている OpenShift Container Platform のバージョンの **CredentialsRequest** で指定されるパーミッションを見つける方法についての詳細は、Manually creating IAM for AWS を参照してください。

1.8.14.2. バグ修正

- 以前のバージョンでは、断続的な API サーバーエラーが Samples Operator 設定オブジェクトの **SamplesExists** 状態ではなく、**ImageChangesInProgress** 状態について報告されました。API サーバーがすべてのサンプルがインストールされていることを報告すると、Samples Operator は **ImageChangesInProgress** 状態に予期しないデータがあったため、**Progressing** 状態を **false** に切り替えることができませんでした。このため、アップグレードが未完了であると誤ってマークされました。今回のバグ修正により、**SamplesExists** 状態が更新され、API サーバーのエラーが報告されるようになりました。そのため、Samples Operator のアップグレード中に断続的な API サーバーエラーが発生した場合にアップグレードはブロックされなくなりました。(BZ#1857201)

- 以前のバージョンでは、**ironic-image** コンテナーの設定では、**idrac-redfish-virtual-media** ブートドライバーを有効にする設定が欠落していました。このため、ユーザーは Metal3 の **idrac-virtual-media** ブート URL を選択できませんでした。欠落していた **ironic-image** コンテナー設定が追加されるようになり、ユーザーは Metal3 の **idrac-virtual-media** URL を選択できるようになりました。(BZ#1859488)

- 以前のバージョンでは、Operand フォーム配列およびオブジェクトフィールドには、フォーム

でフィールドの説明を取得し、表示するロジックがありませんでした。そのため、配列またはオブジェクトタイプのフィールドの説明はレンダリングされませんでした。今回のバグ修正により、配列およびオブジェクトフィールドの説明が Operand 作成フォームで表示されるようになりました。(BZ#1861433)

- 以前のバージョンでは、Buildah はイメージのイメージアーキテクチャーおよび OS フィールドを削除していました。これにより、生成されるイメージがアーキテクチャーおよび OS を特定できないため、一般的なコンテナーツールが失敗していました。今回のバグ修正では、明示的にオーバーライドされない限り、Buildah がイメージおよびアーキテクチャーを上書きするのを防ぐようになりました。これにより、イメージにアーキテクチャーおよび OS フィールドが常に設定され、イメージの不一致についての警告が表示されなくなります。(BZ#1868401)

- 以前のバージョンでは、CoreDNS 1.6.6 の実行時に、断続的に無効なメモリーアドレスまたは nil ポインター逆参照エラーが発生し、Kuby API アクセスのタイムアウトが生じていました。これは、Endpoint Tombstones でエラーを正しく処理することで修正されるようになりました。CoreDNS は、断続的なパニックなしに意図されたとおりに動作するようになりました。(BZ#1869309)

- 以前のリリースでは、**BareMetalHost** オブジェクトのコントローラーは、最新のステータス更新のタイムスタンプを含め、ステータスデータをアノテーションにミラーリングしていました。これはクラスターで必要ではありませんでした。これにより、**BareMetalHost** オブジェクトが連続する流れ (continuous flux) のような状態に入り、影響を受ける **BareMetalHost** オブジェクトは、コントローラーが Kubernetes API に影響を与えるのを防ぐために調整においてより長いバックオフを受ける可能性がありました。問題を生じさせるアノテーションが書き込まれなくなり、問題が修正されます。(BZ#1851531)

- 以前のバージョンでは、Cluster Version Operator (CVO) は Pod 仕様の **shareProcessNamespace** パラメーターを同期しませんでした。これにより、レジストリー Operator は **shareProcessNamespace** 設定を更新しませんでした。CVO は **shareProcessNamespace**、**DNSPolicy**、および **TerminationGracePeriodSeconds** を同期し、レジストリー Operator の更新の問題を修正するようになりました。(BZ#1868478)

1.8.14.3. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.15. RHSA-2020:3578 - Moderate (中程度): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-09-08

cluster-network-operator-container、**cluster-version-operator-container**、**elasticsearch-operator-container**、**logging-kibana6-container**、および **ose-cluster-svcat-controller-manager-operator-container** の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3578 アドバイザリーに記載されています。

1.8.16. RHBA-2020:3618 - OpenShift Container Platform 4.5.9 バグ修正の更新

発行日: 2020-09-14

OpenShift Container Platform release 4.5.9 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:3618 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-2020:3619 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 4.5.9 コンテナーイメージの一覧

1.8.16.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.17. RHBA-2020:3719 - OpenShift Container Platform 4.5.11 バグ修正の更新

発行日: 2020-09-21

OpenShift Container Platform release 4.5.11 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-2020:3719 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-2020:3720 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 4.5.11 コンテナーイメージの一覧

1.8.17.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.18. RHSA-2020:3780 - Moderate (中程度): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-09-21

ose-cluster-svcat-apiserver-operator-container の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3780 アドバイザリーに記載されています。

1.8.19. RHBA-2020:3760 - OpenShift Container Platform 4.5.13 バグ修正の更新

発行日: 2020-09-30

OpenShift Container Platform リリース 4.5.13 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:3760 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-2020:3761 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 4.5.13 コンテナーイメージの一覧

1.8.19.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.20. RHSA-2020:3841 - Important (重要): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-09-30

jenkins の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3841 アドバイザリーに記載されています。

1.8.21. RHSA-2020:3842 - Moderate (中程度): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-09-30

openshift-enterprise-console-container の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:3842 アドバイザリーに記載されています。

1.8.22. RHBA-2020:3843 - OpenShift Container Platform 4.5.14 バグ修正の更新

発行日: 2020-10-12

OpenShift Container Platform リリース 4.5.14 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-2020:3843 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-2020:3844 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 4.5.14 コンテナーイメージの一覧

1.8.22.1. バグ修正

- 今回のリリースにより、各ロギングレベルの値は **imageregistry** API のロギングフィールドに記載されています。(BZ#1843244)
- 以前のバージョンでは、バージョンとデータベース間の不一致により、最新のイメージから Pod を復元する際に問題が発生することがありました。今回のリリースにより、Pod の設定 YAML ファイルがバックアップと共にコピーされ、不一致が生じなくなりました。(BZ#1877930)
- 以前のバージョンでは、Pod が無効なイメージ参照を参照する場合、プルーナージョブによりイメージレジストリー Operator が低下 (degraded) 状態になり、アップグレードがブロックされていました。アップグレードを可能にするには、ユーザーは問題を発生させた Pod を削除し、次回のプルーニングの発生を待機するか、プルーナージョブを一時停止する必要がありました。今回のリリースにより、プルーナージョブの失敗を示すメトリクスおよびアラートが追加され、プルーナーのステータスが Operator ステータスに影響しなくなりました。(BZ#1879176)
- 以前のバージョンでは、OpenShift Container Platform 4.5 ブランチの Cluster DNS Operator の Kubernetes の依存関係は更新されていませんでした。今回のリリースにより、Cluster DNS Operator の依存関係が Kubernetes 0.18.0-rc2 から v0.18.9 に更新されました。(BZ#1880311)
- 以前のバージョンでは、OpenShift Container Platform 4.5 ブランチの Cluster Ingress Operator の Kubernetes の依存関係は更新されませんでした。今回のリリースにより、Cluster Ingress Operator の依存関係が Kubernetes 0.18.3 から v0.18.9 に更新されるようになりました。(BZ#1880315)

- 以前のバージョンでは、Kubernetes API の監視 (watch) キャッシュはグローバルリビジョン (**etcd**) から初期化され、変更が加えられていない場合には定義されない期間そのまま残る可能性がありました。この動作により、クライアントが新しい RV を検出したサーバーからリソースバージョン (RV) を取得し、ネットワークエラーが原因で切断され、背後のサーバーに再接続され、Too large resource version エラーが発生する状態になることがありました。今回のリリースにより、リフレクターはこれらのエラーからリカバリーできるように修正され、サーバーから通知を取得するために **client-go** ライブラリーを使用する Operator のリカバリーが可能となり、エラーの受信時に進捗が見られるようになりました。
この問題は、 **cluster-kube-apiserver-operator (BZ#1880322) cluster-kube-storage-version-migrator-operator** (BZ#1880327) ** **cluster-openshift-apiserver-operator** (BZ#1880353) について解決されています。

- 以前のバージョンでは、Web コンソールは最新の OpenShift Pipelines Operator 1.1 と互換性がないため、新規パイプラインのトリガーは作成できませんでした。本リリースでは最新バージョンがサポートされ、パイプラインのトリガーの作成が可能になりました。(BZ#1880376)

- 以前のバージョンでは、Kubernetes のバグにより、API クライアントが TCP のリセットからのリカバリー後にすぐにリカバリーできませんでした。失われた接続が再度確立されると、クライアントログが Timeout: Too large resource version エラーで一杯になる発生する可能性があります。これにより、API サーバーへのクライアント接続を維持するコントローラーまたは Operator に問題が発生する可能性がありました。今回のリリースにより、Kubernetes バグの修正が Samples Operator に適用され、Operator はこのエラーメッセージループの影響を受けなくなりました。(BZ#1881068)

- 以前のバージョンでは、不必要な API VIP の移動が原因でクライアントの接続エラーが発生しました。今回のリリースにより、API VIP ヘルスチェックが移動回数を制限するようになり、エラーが少なくなりました。(BZ#1881147)

1.8.22.2. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.23. RHBA-2020:4228 - OpenShift Container Platform 4.5.15 バグ修正の更新

発行日: 2020-10-19

OpenShift Container Platform release 4.5.15 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-2020:4228 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-2020:4229 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 4.5.15 コンテナーイメージの一覧

1.8.23.1. バグ修正

- CSR の新しい API バージョンが OpenShift Container Platform の今後のバージョンで導入されました。そのため、アップグレード時に古いバージョンが証明書を承認したり、拒否したりすることができませんでした。今回のリリースにより、古いバージョンの **oc** の CSR のバージョンが許容されるようになり、今後のバージョンに対して **oc** 4.5 で証明書を拒否したり、承認したりすることができるようになりました。(**BZ#1860789**)

- ベアメタル環境では、**infra-dns** コンテナーは各ホストで実行され、ノード名の解決および他の内部 DNS レコードをサポートします。**NetworkManager** スクリプトは、**infra-dns** コンテナー

を参照するように、ホストの **/etc/resolv.conf** も更新します。さらに、Pod が作成されると、ホストから DNS 設定ファイル (**/etc/resolv.conf** ファイル) を受信します。
NetworkManager スクリプトがホストの **/etc/resolv.conf** ファイルを更新する前に HAProxy Pod が作成された場合、**api-int** 内部 DNS レコードが解決できないために Pod は繰り返し失敗する可能性があります。今回のバグ修正により、Machine Config Operator (MCO) が更新され、HAProxy Pod の **/etc/resolv.conf** ファイルがホストの **/etc/resolv.conf** ファイルと同じであることを確認できます。その結果、HAProxy Pod ではこれらのエラーが発生しなくなりました。(BZ#1862874)

- 以前のバージョンでは、コントロールプレーン kubelet に到達できず、Pod が実行中であった場合、そのノードで実行されているマシン API Pod は別のノードに再スケジュールされました。これにより、クラスター内のマシン API リソースを制御するために競争する複数のマシン API Pod が作成されました。これにより、過剰にインスタンスが作成され、マシン API コントローラーがインスタンスをリークする可能性が生じ、手動の介入が必要になる可能性がありました。今回のリリースにより、リーダーの選択がすべてのマシン API コントローラーに追加され、コントローラーの単一インスタンスのみがマシン API リソースを管理できるようになりました。コントローラーごとに 1 つのリーダーのみとなり、追加のインスタンスは作成されたり、リークされたりしなくなりました。(BZ#1864352)

- 以前のバージョンでは、編集 (edit) フローでリソース名が更新され、アプリケーションの編集ユーザーは Git リポジトリーを変更したり、アプリケーションを更新することができませんでした。今回の修正により、編集フローにある場合にアプリケーション名が更新されなくなり、編集フローのユーザーが Git リポジトリーを変更し、アプリケーションを更新できるようになりました。(BZ#1877290)

- 以前のバージョンでは、Kubernetes API の監視 (watch) キャッシュはグローバルリビジョン (**etcd**) から初期化され、変更が加えられていない場合には定義されない期間そのまま残る可能性がありました。この動作により、クライアントが新しい RV を検出したサーバーからリソースバージョン (RV) を取得し、ネットワークエラーが原因で切断され、背後のサーバーに再接続され、Too large resource version エラーが発生する状態になることがありました。今回のリリースにより、リフレクターは Too large resource version エラーからリカバリーできるように修正され、サーバーから通知を取得するために **client-go** ライブラリーを使用する Operator のリカバリーが可能となり、Too large resource version エラーの受信時に進捗が見られるようになりました。(BZ#1877346)

- 以前のバージョンでは、認証 Operator が **Accept: application/json** ヘッダーを無視した OpenID Connect Authentication (OIDC) サーバーから HTML ペイロードを受信すると、OIDC サーバーが、認証 Operator が JSON を予想するために解析に失敗したことを示す HTML ページを出して応答する可能性がありました。今回のリリースより、Operator はエラーを無視し、ヘッダーを無視する OIDC サーバーの CLI ログインを許可しなくなりました。(BZ#1879417)

- 以前のバージョンでは、イメージレジストリー Operator は Too large resource version エラーが出されると、クラスターからイベントを取得できませんでした。今回のリリースにより、**client-go** ライブラリーが更新され、Operator が Too large resource version エラーから回復できるようにリフレクターが修正されました。(BZ#1880314)

- Kubernetes ネットワークプロキシーは、ローカルトラフィックを検出するための複数のクラスター CIDR をサポートしません。複数の CIDR が OpenShift SDN で設定されている場合、Cluster Network Operator (CNO) は **KubeProxyConfiguration.clusterCIDR** フィールドを空の文字列に設定します。OpenShift Container Platform 4.4 以前では、空の値は無視されましたが、4.5 以降では空の値を渡すとエラーが生じます。その結果、4.4 から 4.5 にアップグレードした後に、 **sdn-config ConfigMap** が **clusterCIDR** フィールドに空の文字列を持つ場合、設定は解析できず、SDN Pod はクラッシュループに入ります。今回のリリースにより、空の値は無視され、複数の CIDR が設定される場合に SDN Pod がクラッシュしなくなりました。(BZ#1881830)

1.8.23.2. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.24. RHBA-2020:4268 - OpenShift Container Platform 4.5.16 バグ修正の更新

発行日: 2020-10-26

OpenShift Container Platform release 4.5.16 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-2020:4268 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-2020:4269 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 4.5.16 コンテナーイメージの一覧

1.8.24.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.25. RHSA-2020:4320 - Low (低): OpenShift Container Platform 4.5 セキュリティー更新

発行日: 2020-10-26

openshift4/ose-machine-config-operator の更新が OpenShift Container Platform 4.5 で利用可能になりました。更新の詳細については、RHSA-2020:4320 アドバイザリーに記載されています。

1.8.26. RHBA-2020:4325 - OpenShift Container Platform 4.5.17 バグ修正の更新

発行日: 2020-11-05

OpenShift Container Platform リリース 4.5.17 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-2020:4325 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-2020:4326 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 4.5.17 コンテナーイメージの一覧

1.8.26.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.27. RHBA-2020:4425 - OpenShift Container Platform 4.5.18 バグ修正の更新

発行日: 2020-11-10

OpenShift Container Platform リリース 4.5.18 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:4425 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-2020:4426 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 4.5.18 コンテナーイメージの一覧

1.8.27.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.28. RHBA-2020:5051 - OpenShift Container Platform 4.5.19 バグ修正の更新

発行日: 2020-11-17

OpenShift Container Platform release 4.5.19 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-2020:5051 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-2020:5052 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 4.5.19 コンテナーイメージの一覧

1.8.28.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.29. RHSA-2020:5118 - Moderate (中程度): OpenShift Container Platform 4.5.20 バグ修正およびセキュリティー更新

発行日: 2020-11-24

golang のセキュリティー更新を含む OpenShift Container Platform リリース 4.5.20 が公開されました。この更新に含まれるバグ修正の一覧は、RHSA-2020:5118 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-2020:5119 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 4.5.20 コンテナーイメージの一覧

1.8.29.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.30. RHSA-2020:5194 - Moderate (中程度): OpenShift Container Platform 4.5.21 バグ修正およびセキュリティー更新

発行日: 2020-12-01

openshift-enterprise-hyperkube のセキュリティー更新を含む OpenShift Container Platform リリース 4.5.21 が公開されました。この更新に含まれるバグ修正の一覧は、RHSA-2020:5194 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-2020:5193 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 4.5.21 コンテナーイメージの一覧

1.8.30.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.31. RHBA-2020:5051 - OpenShift Container Platform 4.5.22 バグ修正の更新

発行日: 2020-12-08

OpenShift Container Platform リリース 4.5.22 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:5250 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-2020:5251 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 4.5.22 コンテナーイメージの一覧

1.8.31.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.32. RHSA-2020:5359 - Moderate (中程度): OpenShift Container Platform 4.5.23 バグ修正およびセキュリティー更新

発行日: 2020-12-15

kubernetes のセキュリティー更新を含む OpenShift Container Platform リリース 4.5.23 が公開されました。この更新に含まれるバグ修正の一覧は、RHSA-2020:5359 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-2020:5356 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 4.5.23 コンテナーイメージの一覧

1.8.32.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.33. RHBA-2020:5468 - Moderate: OpenShift Container Platform 4.5.24 バグ修正の更新

発行日: 2020-12-21

OpenShift Container Platform リリース 4.5.24 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2020:5468 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-2020:5469 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 4.5.24 コンテナーイメージの一覧

1.8.33.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.34. RHBA-2021:0033: OpenShift Container Platform 4.5.27 バグ修正の更新

発行日: 2021-01-19

OpenShift Container Platform release 4.5.27 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-2021:0033 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-2021:0034 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 4.5.27 コンテナーイメージの一覧

1.8.34.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.35. RHBA-2021:0175 - OpenShift Container Platform 4.5.28 バグ修正の更新

発行日: 2021-01-26

OpenShift Container Platform release 4.5.28 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-2021:0175 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 4.5.28 コンテナーイメージの一覧

1.8.35.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.36. RHBA-2021:0231 - OpenShift Container Platform 4.5.30 バグ修正の更新

発行日: 2021-02-02

OpenShift Container Platform release 4.5.30 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-2021:0231 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-2021:0232 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 4.5.30 コンテナーイメージの一覧

1.8.36.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.37. RHSA-2021:0313: OpenShift Container Platform 4.5.31 バグ修正およびセキュリティー更新

発行日: 2021-02-09

OpenShift Container Platform release 4.5.31 が公開されました。この更新に含まれるバグ修正の一覧は、RHSA-2021:0313 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-2021:0314 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 4.5.31 コンテナーイメージの一覧

1.8.37.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.38. RHSA-2021:0428 - OpenShift Container Platform 4.5.33 バグ修正およびセキュリティー更新

発行日: 2021-03-03

OpenShift Container Platform リリース 4.5.33 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、RHSA-2021:0428 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-2021:0429 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 4.5.33 コンテナーイメージの一覧

1.8.38.1. 機能

1.8.38.1.1. Insights Operator の機能拡張

今回の更新により、Insights Operator が **MachineConfigPools** クラスターの情報を収集するようになりました。この情報は、トラブルシューティングに役立ちます。詳細は、**BZ#1887763** を参照してください。

1.8.38.2. バグ修正

- 以前のバージョンでは、OVN-kubernetes セキュリティールールが正しくないと、特定の受信接続がブロックされました。稀なケースですが、Pod への接続の試行は誤って失敗することもありました。今回の更新により、iptables が修正されて意図された接続をブロックされ、誤ったエラーが発生しなくなりました。(BZ#1921283)

- 以前のバージョンでは、Kubernetes API の監視 (watch) キャッシュはグローバルリビジョン (**etcd**) から初期化され、変更が加えられていない場合には定義されない期間そのまま残る可能性がありました。この動作により、クライアントが新しい RV を検出したサーバーからリソースバージョン (RV) を取得し、ネットワークエラーが原因で切断され、背後のサーバーに再接続され、**Timeout: Too large resource version** エラーが発生する状態になることがありました。今回のリリースにより、リフレクターはこれらのエラーからリカバリーできるように修正され、サーバーから通知を取得するために **client-go** ライブラリーを使用する Operator のリカバリーが可能となり、エラーの受信時に進捗が見られるようになりました。(BZ#1877346)

- 以前のバージョンでは、nil writer への書き込みを試みると、**invalid memory address** または **nil pointer dereference** エラーが生じる可能性がありました。writer の同じインスタンスを共有することで、**index out of range [43] with length 30 and recovered from err index > windowEnd** エラーが生じる可能性がありました。今回の更新により、kube-apiserver の **SerializeObject** 機能でのデータ競合が修正されました。(BZ#1879208)

- 以前のバージョンでは、メモリーからのレコードのプルーニング中に誤って配置された配列インデックスにより、メモリーが過剰に使用され、アーカイブから古いレポートを削除できなくなりました。今回の更新により、配列インデックスキーが変更され、プルーニングにより、メモリーを過剰に消費せずにレコードをメモリーから正常に削除できるようになりました。(BZ#1894243)

- 以前のバージョンでは、Red Hat Enterprise Linux CoreOS (RHCOS) は kernel-rt パッケージのステージリポジトリーの場所を使用していました。したがって、kernel-rt パッケージは vanilla カーネルパッケージと同期しませんでした。今回の更新により、RHCOS ビルド設定が実稼働リポジトリーの場所を使用するように変更され、kernel-rt パッケージが vanilla カーネルパッケージと適切に同期するようになりました。(BZ#1922262)

1.8.38.3. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.39. RHBA-2021:0714 - OpenShift Container Platform 4.5.34 バグ修正およびセキュリティー更新

発行日: 2021-03-10

OpenShift Container Platform リリース 4.5.34 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-2021:0714 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-2021:0713 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 4.5.34 コンテナーイメージの一覧

1.8.39.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.40. RHSA-2021:0785 - OpenShift Container Platform 4.5.35 バグ修正およびセキュリティー更新

発行日: 2021-03-17

OpenShift Container Platform リリース 4.5.35 が公開されました。この更新に含まれるバグ修正の一覧は、 RHSA-2021:0785 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-2021:0786 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 4.5.35 コンテナーイメージの一覧

1.8.40.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.41. RHBA-2021:0840 - OpenShift Container Platform 4.5.36 バグ修正の更新

発行日: 2021-03-24

OpenShift Container Platform リリース 4.5.36 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-2021:0840 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-2021:0841 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 4.5.36 コンテナーイメージの一覧

1.8.41.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.42. RHBA-2021:1015 - OpenShift Container Platform 4.5.37 バグ修正およびセキュリティー更新

発行日: 2021-04-12

OpenShift Container Platform リリース 4.5.37 が公開されました。この更新に含まれるバグ修正の一覧は、 RHBA-2021:1015 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-2021:1016 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 4.5.37 コンテナーイメージの一覧

1.8.42.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.43. RHBA-2021:1300 - OpenShift Container Platform 4.5.38 バグ修正の更新

発行日: 2021-04-28

OpenShift Container Platform release 4.5.38 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2021:1300 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-2021:1302 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 4.5.38 コンテナーイメージの一覧

1.8.43.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.44. RHBA-2021:1491 - OpenShift Container Platform 4.5.39 バグ修正の更新

発行日: 2021-05-13

OpenShift Container Platform リリース 4.5.39 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-2021:1491 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-2021:1492 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 4.5.39 container image list

1.8.44.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.45. RHBA-2021:2056 - OpenShift Container Platform 4.5.40 バグ修正およびセキュリティー更新

発行日: 2021-05-26

OpenShift Container Platform リリース 4.5.40 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA-2021:2056 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-2021:2057 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 4.5.40 container image list

1.8.45.1. アップグレード

既存の OpenShift Container Platform 4.5 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。

1.8.46. RHBA-2021:2430 - OpenShift Container Platform 4.5.41 バグ修正およびセキュリティー更新

発行日: 2021-06-30

OpenShift Container Platform リリース 4.5.41 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-2021:2430 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-2021:2431 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 4.5.41 container image list

1.8.46.1. アップグレード

既存の OpenShift Container Platform 4.5 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、4.5 クラスターではすべてのマスターは 4.5 で、すべてのノードが 4.5 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 4.5 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。