OpenShift Container Platform 4.9

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: 2022-01-15

OpenShift Container Platform 4.9 リリースノート

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

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

法律上の通知

概要

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

目次

第1章 OPENSHIFT CONTAINER PLATFORM 4.9 リリースノート

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

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

1.1. 本リリースについて

OpenShift Container Platform (RHSA-2021:3759) が公開されました。本リリースでは、CRI-O ランタイムで Kubernetes 1.22 を使用します。以下では、OpenShift Container Platform 4.9 に関連する新機能、変更点および既知の問題について説明します。

OpenShift Container Platform 4.9 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 4.9 は、Red Hat Enterprise Linux (RHEL) 7.9 および8.4ならびにRed Hat Enterprise Linux CoreOS (RHCOS) 4.9 でサポートされます。

コントロールプレーンには RHCOS マシンを使用する必要があり、コンピュートマシンには RHCOS または Red Hat Enterprise Linux (RHEL) 7.9 または8.4のいずれかを使用できます。

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

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

1.3. 新機能および改良された機能

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

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. インストール Ignition 設定は起動時に削除されます。

coreos-installer プログラムでインストールされるノードは、以前は **/boot/ignition/config.ign** ファイルにインストール Ignition 設定を保持していました。OpenShift Container Platform 4.9 のインストールイメージから、このファイルはノードのプロビジョニング時に削除されます。この変更は、以前の OpenShift Container Platform バージョンにインストールされたクラスターには影響を与えません。以前のブートイメージを使用するためです。

1.3.2. インストールおよびアップグレード

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

OpenShift Container Platform 4.9 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を使用して Azure Stack Hub 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。

デプロイメントプロセスを支援する Red Hat 提供の Azure Resource Manager (ARM) テンプレートのサンプルを組み込むか、または独自のテンプレートを作成することができます。他の方法を使用して必要なリソースを作成することもできます。ARM テンプレートはサンプルとしてのみ提供されます。

詳細は、Installing a cluster on Azure Stack Hub using ARM templates を参照してください。

1.3.2.2. クラスターを更新する前のマシンヘルスチェックの一時停止

アップグレードプロセスで、クラスター内のノードが一時的に利用できなくなる可能性があります。ワーカーノードの場合、マシンのヘルスチェックにより、このようなノードは正常ではないと識別され、それらが再起動される場合があります。このようなノードの再起動を回避するために、OpenShift Container Platform 4.9 では**cluster.x-k8s.io/paused=""**アノテーションが導入され、クラスターの更新前に**MachineHealthCheck**リソースを一時停止できます。

詳細は、Pausing a MachineHealthCheck resource を参照してください。

1.3.2.3. マシン CIDR 内の Azure サブネットサイズの拡大

Microsoft Azure の OpenShift Container Platform インストールプログラムは、マシン CIDR 内に可能な限り大きなサブネットを作成するようになりました。これにより、クラスターがマシン CIDR のサイズを、クラスター内のノード数に対応するように設定できます。

1.3.2.4. 中国での AWS リージョンのサポート

OpenShift Container Platform 4.9 では、中国の AWS リージョンのサポートが導入されました。**cn-north-1** (Beijing) および **cn-northwest-1**(Ningxia) リージョンに OpenShift Container Platform クラスターをインストールし、更新できるようになりました。

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

1.3.2.5. baremetal ネットワーク上の仮想メディアを使用したクラスターの拡張

OpenShift Container Platform 4.9 では、**baremetal** ネットワークで仮想メディアを使用して、**provisioning** ネットワークを使用してデプロイされるインストーラーでプロビジョニングされるクラスターを拡張することができます。**ProvisioningNetwork** 設定が **Managed** に設定されている場合、この機能を使用できます。この機能を使用するには、**provisioning** カスタムリソース(CR)で **virtualMediaViaExternalNetwork** 設定を **true** に設定する必要があります。また、API VIP アドレスを使用するようにマシンセットを編集する必要もあります。詳細は、Preparing to deploy with Virtual Media on the baremetal networkを参照してください。

1.3.2.6. OpenShift Container Platform 4.8 から 4.9 にアップグレードする際に、管理者の承認が必要

OpenShift Container Platform 4.9 は Kubernetes 1.22 を使用します。これにより、非推奨となった **v1beta1** APIs が大幅に 削除されました。

OpenShift Container Platform 4.8.14では、クラスターをOpenShift Container Platform 4.8から4.9にアップグレードする前に、管理者が手動で承認する必要があるという要件が導入されました。削除されたAPIが、クラスター上で実行されている、またはクラスターと対話しているワークロード、ツール、またはその他のコンポーネントによって引き続き使用されるOpenShift Container Platform 4.9にアップグレードした後の問題を防ぐ上で役立ちます。管理者は、削除する予定の使用中のAPIのクラスタを評価し、影響を受けるコンポーネントを移行して適切な新規APIバージョンを使用する必要があります。これが実行された後、管理者は管理者の承認を提供できます。

すべてのOpenShift Container Platform 4.8クラスターでは、OpenShift Container Platform 4.9にアップグレードする前に、この管理者の承認が必要になります。

詳細は、Preparing to update to OpenShift Container Platform 4.9 を参照してください。

1.3.2.7. PCIパススルーを使用するRHOSPデプロイメントへのインストールのサポート

OpenShift Container Platform 4.9では、PCI パススルー に依存するRed Hat OpenStack Platform (RHOSP) デプロイメントへのインストールがサポートされるようになりました。

1.3.2.8. etcd バージョン 3.4 から 3.5 へのアップグレード

OpenShift Container Platform 4.9 は etcd 3.5 をサポートします。クラスターをアップグレードする前に、有効な etcd バックアップが存在することを確認します。etcdバックアップは、アップグレードの失敗が発生した場合に、クラスターを復元できることを保証します。OpenShift Container Platform 4.9では、etcd のアップグレードは自動的に行われます。クラスターのバージョン 4.9 への移行状態によっては、etcd バックアップが利用可能である可能性があります。ただし、クラスターのアップグレードを開始する前に、バックアップが存在することを確認することが推奨されます。

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

OpenShift Container Platform 4.9 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 IBM Cloud® にクラスターをインストールするためのサポートが導入されました。手順は、以下の相違点で、ベアメタルのインストーラーでプロビジョニングされるインフラストラクチャーとほぼ同じです。

- IBM Cloud での OpenShift Container Platform 4.9 のインストーラーでプロビジョニングされるインストールには、**provisioning** ネットワーク、IPMI、および PXE ブートが必要です。Red Hat は、IBM Cloud での Redfish および仮想メディアを使用したデプロイメントをサポートしません。
- IBM Cloud でパブリックおよびプライベート VLAN を作成および設定する必要があります。
- インストールプロセスを開始する前に、IBM Cloud ノードが利用可能である必要があります。そのため、最初に IBM Cloud ノードを作成する必要があります。
- プロビジョナーノードを準備する必要があります。
- パブリック **baremetal** ネットワークに DHCP サーバーをインストールおよび設定する必要があります。
- 各ノードが IPMI を使用して BMC を参照できるように **install-config.yaml** ファイルを設定し、IPMI の権限レベルを **OPERATOR** に設定する必要があります。

詳細は、Deploying installer-provisioned clusters on IBM Cloud を参照してください。

1.3.2.10. インストーラーでプロビジョニングされるクラスターでの Fujitsu ハードウェアのサポートの改善

OpenShift Container Platform 4.9 は、インストーラーでプロビジョニングされるクラスターを Fujitsu ハードウェアにデプロイし、Fujite 統合 Remote Management Controller (iRMC)を使用する場合はワーカーノードの BIOS 設定サポートを追加します。詳細は、Configuring BIOS for worker node を参照してください。

1.3.3. Web コンソール

1.3.3.1. Node ページからのノードログへのアクセス

今回の更新により、管理者は **Node** ページからノードログにアクセスできるようになりました。ノードのログを確認するには、**Logs** タブをクリックして個別のログファイルとジャーナルログユニットを切り替えます。

1.3.3.2. ノードタイプ別のクラスター使用率のダウン

クラスターダッシュボードの **Cluster utilization** カードで、ノードタイプでフィルターできるようになりました。追加のノードタイプは作成時に一覧に表示されます。

1.3.3.3. ユーザー設定

今回の更新で、デフォルトのプロジェクト、パースペクティブ、トポロジービューなどの設定をカスタマイズするための **User Preferences** ページが追加されました。

1.3.3.4. プロジェクト一覧からのデフォルトプロジェクトを非表示に

今回の更新により、Web コンソールのマストヘッドで、**Projects** ドロップダウンから **default projects** を非表示にできるようになりました。検索およびフィルターの前に、**default projects** を表示に切り替えることができます。

1.3.3.5. Web コンソールでのユーザー設定の追加

今回の更新により、Web コンソールにユーザー設定を追加できるようになりました。ユーザーは、デフォルトのパースペクティブ、プロジェクト、トポロジー、およびその他の設定を選択できます。

1.3.3.6. Developer パースペクティブ

- Git リポジトリーを使用して devfile、Dockerfile、またはビルダーイメージをインポートして、デプロイメントをさらにカスタマイズできるようになりました。ファイルのインポートタイプを編集し、ファイルをインポートする別のストラテジーを選択することもできます。
- 開発者コンソールで、**Pipeline builder** の更新されたユーザーインターフェースを使用して、**Add task** および **Quick Search** を使用して、パイプラインにタスクを追加できるようになりました。この強化されたエクスペリエンスにより、ユーザーは **Tekton Hub** からタスクを追加できるようになりました。
- ビルド設定を編集するには、**Developer** パースペクティブの **Builds** ビューで **Edit BuildConfig** オプションを使用します。ユーザーは、**Form view** および **YAML view** を使用してビルド設定を編集できます。
- トポロジー **Graph view** のコンテキストメニューを使用してサービスを追加したり、Operator がサポートするサービスとの接続をプロジェクトに作成したりできます。

- トポロジー **Graph view** のコンテキストメニューで **+Add** アクションを使用すると、アプリケーショングループ内にサービスを追加したり、サービスを削除したりできます。
- **pipeline as code** の初期サポートは、OpenShift Pipelines Operator によって有効にされる **Pipelines Repository list** ビューで利用可能になりました。
- トポロジーの **Observe** ページの **Application Monitoring** セクションに、ユーザビリティーが強化されました。

1.3.4. IBM Z および LinuxONE

本リリースでは、IBM Z および LinuxONE は OpenShift Container Platform 4.9 と互換性があります。インストールは z/VM または RHEL KVM で実行できます。インストール手順については、以下のドキュメントを参照してください。

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

主な機能拡張
以下の新機能は、OpenShift Container Platform 4.9 の IBM Z および LinuxONE でサポートされます。

- Helm
- 複数ネットワークインターフェースのサポート
- サービスバインディング Operator

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

- 現時点で、以下の Operator がサポートされています。
  - Cluster Logging Operator
  - NFD Operator
  - OpenShift Elasticsearch Operator
  - Local Storage Operator
  - サービスバインディング Operator
- etcd に保存されるデータの暗号化
- マルチパス化
- iSCSI を使用した永続ストレージ
- ローカルボリュームを使用した永続ストレージ (Local Storage Operator)

- hostPath を使用した永続ストレージ
- ファイバーチャネルを使用した永続ストレージ
- Raw Block を使用した永続ストレージ
- OVN-Kubernetes
- 3 ノードクラスターのサポート
- SCSI ディスク上の z/VM Emulated FBA デバイス
- 4k FCP ブロックデバイス

これらの機能は、4.9 について IBM Z およびLinuxONEの OpenShift Container Platform にのみ利用できます。

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

制限
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。

- 以下の OpenShift Container Platform のテクノロジープレビュー機能はサポートされていません。
  - Precision Time Protocol (PTP) ハードウェア
- 以下の OpenShift Container Platform 機能はサポートされていません。
  - マシンヘルスチェックによる障害のあるマシンの自動修復
  - CodeReady Containers (CRC)
  - オーバーコミットの制御およびノード上のコンテナーの密度の管理
  - CSI ボリュームのクローン作成
  - CSI ボリュームスナップショット
  - FIPS 暗号
  - Multus CNI プラグイン
  - NVMe
  - OpenShift Metering
  - OpenShift Virtualization
  - OpenShift Container Platform のデプロイメント時の Tang モードのディスク暗号化
- ワーカーノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続共有ストレージは、NFS またはその他のサポートされるストレージプロトコルを使用してプロビジョニングする必要があります。

- 共有されていない永続ストレージは、iSCSI、FC、DASD、FCP または EDEV/FBA と共に LSO を使用するなど、ローカルストレージを使用してプロビジョニングする必要があります。

1.3.5. IBM Power Systems

本リリースでは、IBM Power Systems は OpenShift Container Platform 4.9 と互換性があります。インストール手順については、以下のドキュメントを参照してください。

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

主な機能拡張
以下の新機能は、OpenShift Container Platform 4.9 の IBM Power Systems でサポートされます。

- Helm
- Power10 のサポート
- 複数ネットワークインターフェースのサポート
- サービスバインディング Operator

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

- 現時点で、以下の Operator がサポートされています。
  - Cluster Logging Operator
  - NFD Operator
  - OpenShift Elasticsearch Operator
  - Local Storage Operator
  - SR-IOV ネットワーク Operator
  - サービスバインディング Operator
- マルチパス化
- iSCSI を使用した永続ストレージ
- ローカルボリュームを使用した永続ストレージ (Local Storage Operator)
- hostPath を使用した永続ストレージ
- ファイバーチャネルを使用した永続ストレージ
- Raw Block を使用した永続ストレージ
- OVN-Kubernetes
- 4K ディスクのサポート
- NVMe

- etcd に保存されるデータの暗号化
- 3 ノードクラスターのサポート
- Multus SR-IOV

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

- 以下の OpenShift Container Platform のテクノロジープレビュー機能はサポートされていません。
  - Precision Time Protocol (PTP) ハードウェア
- 以下の OpenShift Container Platform 機能はサポートされていません。
  - マシンヘルスチェックによる障害のあるマシンの自動修復
  - CodeReady Containers (CRC)
  - オーバーコミットの制御およびノード上のコンテナーの密度の管理
  - FIPS 暗号
  - OpenShift Metering
  - OpenShift Virtualization
  - OpenShift Container Platform のデプロイメント時の Tang モードのディスク暗号化
- ワーカーノードは Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。
- 永続ストレージは、ローカルボリューム、Network File System (NFS)、または Container Storage Interface (CSI) を使用する Filesystem タイプである必要があります。

1.3.6. セキュリティーおよびコンプライアンス

1.3.6.1. カスタムルールによる監査ログポリシーの設定

OpenShift Container Platform の監査ロギングレベルをきめ細かく制御できるようになりました。カスタムルールを使用して、異なるグループに異なる監査ポリシープロファイル（**Default**、**WriteRequestBodies**、**AllRequestBodies**、または **None**）を指定することができます。

詳細は、Configuring the audit log policy with custom rules を参照してください。

1.3.6.2. 監査ロギングの無効化

None 監査ポリシープロファイルを使用して OpenShift Container Platform の監査ロギングを無効にできるようになりました。

警告

問題のトラブルシューティング時に有用なデータが記録されないリスクを完全に理解していない限り、監査ロギングを無効にすることは推奨していません。監査ロギングを無効にしてサポートが必要な状況が生じた場合は、適切にトラブルシューティングを行うために監査ロギングを有効にし、問題を再現する必要がある場合があります。

詳細は、Disabling audit logging を参照してください。

1.3.6.3. OAuth サーバー URL のカスタマイズ

内部 OAuth サーバーの URL をカスタマイズすることができるようになりました。詳細は、Customizing the internal OAuth server URL を参照してください。

1.3.6.4. Network-Bound Disk Encryption (NBDE)

OpenShift Container Platform 4.9 では、NBDE を設定したシステムのメンテナンスを継続的に行う手順が追加されました。NBDEを使用すると、マシンの再起動時にパスワードを手動で入力しなくても、物理マシンおよび仮想マシン上のハードドライブのルートボリュームを暗号化できます。詳細は、About disk encryption technology を参照してください。

1.3.7. etcd

1.3.7.1. etcd 証明書の自動ローテーション

OpenShift Container Platform 4.9 では、etcd 証明書は自動的にローテーションされ、システムによって管理されます。

1.3.7.2. API サーバーの追加の TLS セキュリティープロファイル設定

Kubernetes API サーバー TLS セキュリティープロファイル設定も etcd で適用されるようになりました。

1.3.8. ネットワーキング

1.3.8.1. linuxptp サービスの強化

OpenShift Container Platform 4.9 では、PTP に以下の更新が導入されました。

- 新規 **ptp4lConf** フィールド
- **linuxptp** サービスを境界クロックとして設定する新しいオプション

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

1.3.8.2. PTP 高速イベント通知フレームワークを使用した PTP 高速イベントの監視

PTP イベントの高速イベント通知がベアメタルクラスターで利用可能になりました。PTP Operator

は、設定されたすべての PTP 対応ネットワークインターフェースのイベント通知を生成します。イベントは、同じノードで実行されているアプリケーションの REST API を介して利用できます。高速イベント通知は、AMQ Interconnect Operator によって提供される Advanced Message Queuing Protocol(AMQP)メッセージバスによって転送されます。

詳細は、About PTP and clock synchronization error events を参照してください。

1.3.8.3. OVN-Kubernetes クラスターネットワークプロバイダーの egress IP 機能によるノード全体での分散

OVN-Kubernetes の egress IP 機能は、namespace に複数の egress IP アドレスが割り当てられている場合、その指定された namespace のノード全体にほぼ均等にネットワークトラフィックを分散するようになりました。それぞれの IP アドレスは異なるノードに存在する必要があります。詳細は、OVN-Kubernetes のConfiguring egress IPs for a project を参照してください。

1.3.8.4. SR-IOV のコンテナー化された Data Plane Development Kit(DPDK)の一般提供

コンテナー化された Data Plane Development Kit(DPDK)が OpenShift Container Platform 4.9 で一般提供されるようになりました。詳細は、Using virtual functions (VFs) with DPDK and RDMA modes を参照してください。

1.3.8.5. Fast Datapath DPDK アプリケーションで vhost-net を使用するための SR-IOV サポート

SR-IOV は、Intel および Mellanox NIC 上の Fast Datapath DPDK アプリケーションで使用する vhost-net をサポートするようになりました。この機能は、**SriovNetworkNodePolicy** リソースを設定して有効にできます。詳細は、SR-IOV network node configuration object を参照してください。

1.3.8.6. 単一ノードクラスターの SR-IOV サポート

単一ノードクラスターは、SR-IOV ハードウェアおよび SR-IOV Network Operator をサポートします。SR-IOV ネットワークデバイスを設定すると、単一ノードが再起動するので、Operator の **disableDrain** フィールドを設定する必要があることに注意してください。詳細は、Configuring the SR-IOV Network Operator を参照してください。

1.3.8.7. SR-IOV でサポートされるハードウェア

OpenShift Container Platform 4.9 では、追加の Broadcom および Intel ハードウェアへのサポートが追加されました。

- Broadcom BCM57414 および BCM57508
- Intel E810-CQDA2、E810-XXVDA2、および E810-XXVDA4

詳細は、supported devices を参照してください。

1.3.8.8. MetalLB ロードバランサー

本リリースでは、MetalLB Operator が導入されました。MetalLB Operator のインストールおよび設定後に、MetalLB をデプロイして、ベアメタルクラスターのサービス用のネイティブロードバランサー実装を提供できます。ベアメタルのような他のオンプレミスインフラストラクチャーにもメリットがあります。

Operator はカスタムリソース **AddressPool** を導入します。MetalLB がサービスに割り当てることのできる IP アドレス範囲のアドレスプールを設定します。**LoadBalancer** タイプのサービスを追加する場合、MetalLB はプールから IP アドレスを割り当てます。

本リリースでは、Red Hat はレイヤー 2 モードでの MetalLB の使用のみをサポートします。

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

1.3.8.9. CNI VRF プラグインの一般提供

CNI VRF プラグインは以前は OpenShift Container Platform 4.7 のテクノロジープレビュー機能として導入されましたが、OpenShift Container Platform 4.9 では一般に利用可能となりました。

詳細は、Assigning a secondary network to a VRF を参照してください。

1.3.8.10. Ingress コントローラのタイムアウト設定パラメーター

このリリースでは、Ingress Controllerの **tuningOptions**パラメーター用に、6つのタイムアウト構成が導入されています。

- **clientTimeout** は、クライアント応答の待機中に接続が開かれる期間を指定します。
- **serverFinTimeout** は、接続を閉じるクライアントへの応答を待つ間、接続が開かれる期間を指定します。
- **serverTimeout** は、サーバーの応答を待機している間に接続が開かれる期間を指定します。
- **clientFinTimeout** は、クライアントの応答が接続を閉じるのを待機している間に接続が開かれる期間を指定します。
- **tlsInspectDelay** は、一致するルートを見つけるためにルーターがデータを保持する期間を指定します。
- **tunnelTimeout**は、トンネルがアイドル状態の間、WebSocket接続を含むトンネル接続が開いたままになる期間を指定します。

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

1.3.8.11. 相互 TLS 認証

spec.clientTLSを設定することにより、相互TLS（mTLS）認証を有効にするようにIngressコントローラーを設定できるようになりました。**clientTLS** フィールドは、クライアント証明書を検証するためのIngressコントローラーの設定を指定します。

詳細は、Configuring Mutual TLS Authentication を参照してください。

1.3.8.12. HAProxy エラーコードの応答ページのカスタマイズ

クラスター管理者は、503、404、または両方のエラーページのカスタムHTTPエラーコード応答ページを指定できます。

詳細は、Customizing HAProxy error code response pages を参照してください。

1.3.8.13. provisioningNetworkInterface 設定はオプションです。

OpenShift Container Platform 4.9では、インストーラーでプロビジョニングされたクラスター

の**provisioningNetworkInterface**設定はオプションになります。**provisioningNetworkInterface**設定は、**provisioning**ネットワークに使用される NIC 名を識別します。OpenShift Container Platform 4.9では、**install-config.yml**ファイルの**bootMACAddress**を代わりに指定できます。これにより、Ironicは**provisioning**ネットワークに接続されているNICのIPアドレスを識別し、これにバインドできます。プロビジョニングカスタムリソースの**provisioningInterface**設定を省略して、プロビジョニングカスタムリソースが代わりに**bootMACAddress**設定を使用するようにすることもできます。

1.3.8.14. DNS Operator managementState

OpenShift Container Platform 4.9では、DNS Operator **managementState**を変更できるようになりました。DNS Operator の **managementState** は、デフォルトで **Managed** に設定されます。これは、DNS Operator がそのリソースをアクティブに管理していることを意味します。これを **Unmanaged** に変更できます。つまり、DNS Operator がそのリソースを管理していないことを意味します。

以下は、DNS Operator **managementState** を変更するためのユースケースです。

- 開発者は、CoreDNS の問題が修正されているかどうかを確認するために、設定変更をテストする必要があります。**managementState**を**Unmanaged**に設定することにより、DNS Operatorによる変更の上書きを阻止することができます。
- クラスター管理者は、CoreDNSの問題を報告していますが、問題が修正されるまで回避策を適用する必要があります。DNS Operatorの**managementState**フィールドを**Unmanaged**に設定して、回避策を適用できます。

詳細は、Changing the DNS Operator managementStateを参照してください。

1.3.8.15. RHOSP上のクラスターのクラウドプロバイダーオプションとしてのロードバランサーの設定

RHOSPで実行されるクラスターの場合、クラウドプロバイダーのオプションとして、負荷分散用にOctaviaを設定できるようになりました。

詳細は、Setting cloud provider optionsを参照してください。

1.3.8.16. TLS 1.3 および Modern プロファイルのサポートの追加

今回のリリースにより、HAProxy に TLS 1.3 および **Modern** プロファイルの Ingress Controller のサポートが追加されました。

詳細は、Ingress Controller TLS security profiles を参照してください。

1.3.8.17. HTTP Strict Transport Security 要件用のグローバルアドミッションプラグイン

クラスター管理者は、**route.openshift.io/RequiredRouteAnnotations**と呼ばれるルーターのアドミッションプラグインを追加して、ドメインごとにHTTP Strict Transport Security（HSTS）検証を設定できます。クラスター管理者がこのプラグインを設定してHSTSを適用する場合、新しく作成されたルートは、準拠するHSTSポリシーで設定する必要があります。これは、**ingresses.config.openshift.io/cluster**と呼ばれるクラスターIngress設定のグローバル設定に対して検証されます。

詳細は、HTTP Strict Transport Securityを参照してください。

1.3.8.18. Ingress 空の要求ポリシー

OpenShift Container Platform 4.9 では、**logEmptyRequests** および **HTTPEmptyRequestsPolicy**フィールドを設定して、Ingress コントローラーが空の要求をログに記録または無視するように設定できます。

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

1.3.8.19. Web コンソールでのネットワークポリシーの作成

cluster-admin ロールで Web コンソールにログインすると、コンソールのフォームからクラスター内の任意の namespace に新しいネットワークポリシーを作成できるようになりました。以前のバージョンでは、これは YAML で直接実行することしかできませんでした。

1.3.9. ストレージ

1.3.9.1. AWS EBS CSI Driver Operator を使用した永続ストレージは一般に利用可能

OpenShift Container Platform は、AWS Elastic Block Store (EBS) の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。この機能は以前は OpenShift Container Platform 4.5 のテクノロジープレビュー機能として導入されましたが、OpenShift Container Platform 4.9 では一般に利用可能となり、デフォルトで有効にされます。

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

1.3.9.2. Azure Stack Hub CSI Driver Operator を使用した永続ストレージ (一般提供)

OpenShift Container Platform は、Azure Stack Hub StorageのCSI Driverを使用して PV をプロビジョニングできます。Azure Stack ポートフォリオの一部である Azure Stack Hub を使用すると、オンプレミス環境でアプリケーションを実行し、データセンターで Azure サービスを配信できます。このドライバーを管理する Azure Stack Hub CSI Driver Operator は 4.9 用となり、一般提供されます。

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

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

OpenShift Container Platform は、AWS Elastic File Service (EFS)のCSI Driverを使用して PV をプロビジョニングできます。このドライバーを管理する AWS EFS CSI Driver Operator はテクノロジープレビュー機能としてご利用いただけます。

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

1.3.9.4. CSI 自動移行のGCEのサポート（テクノロジープレビュー）

OpenShift Container Platform 4.8 以降では、in-tree ボリュームプラグインの同等の CSI ドライバーへの自動移行が、テクノロジープレビュー機能として利用可能になりました。この機能は、Google Compute Engine Persistent Disk (GCE PD) in-tree プラグインから Google Cloud Platform (GCP) Persistent Disk CSI ドライバーへの自動移行をサポートするようになりました。

詳細は、CSI Automatic Migration を参照してください。

1.3.9.5. CSI 自動移行のAzure Diskのサポート（テクノロジープレビュー）

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

詳細は、CSI Automatic Migration を参照してください。

1.3.9.6. VMWare vSphere CSI Driver Operator によるストレージポリシーの自動作成（テクノロジープレビュー）

vSphere CSI Operator Driver ストレージクラスが vSphere のストレージポリシーを使用するようになりました。OpenShift Container Platform は、クラウド設定で設定されるデータストアをターゲットにするストレージポリシーを自動的に作成します。

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

1.3.9.7. ローカルストレージ Operator に提供される新規メトリクス

OpenShift Container Platform 4.9 は、ローカルストレージ Operator の以下の新規メトリクスを提供します。

- **lso_discovery_disk_count**: 各ノードで検出されたデバイスの合計数
- **lso_lvset_provisioned_PV_count**: **LocalVolumeSet** オブジェクトによって作成される PV の合計数
- **lso_lvset_unmatched_disk_count**: 条件の不一致により、ローカルストレージ Operator がプロビジョニング用に選択しなかったディスクの合計数
- **lso_lvset_orphaned_symlink_count**: **LocalVolumeSet** オブジェクト基準に一致しなくなった PV のあるデバイスの数
- **lso_lv_orphaned_symlink_count**: **LocalVolume** オブジェクト基準に一致しなくなった PV のあるデバイスの数
- **lso_lv_provisioned_PV_count**: **LocalVolume**のプロビジョニングされた PV の合計数

詳細は、Persistent storage using local volumes を参照してください。

1.3.9.8. oVirt CSI ドライバーのサイズ変更機能が利用可能

OpenShift Container Platform 4.9 は、oVirt CSI ドライバーにサイズ変更機能を追加します。これにより、ユーザーは既存の永続ボリューム要求(PVC)のサイズを増やすことができます。この機能の前に、ユーザーはサイズが増加する新規 PVC を作成し、すべてのコンテンツを古い永続ボリューム(PV)から新規 PV に移動させる必要がありました。これにより、データが失われる可能性があります。ユーザーは既存の PVC を編集し、oVirt CSI ドライバーは基礎となる oVirt ディスクのサイズを調整できるようになりました。

1.3.10. レジストリー

1.3.10.1. イメージレジストリーは Azure Stack Hub インストールで Azure Blob Storage を使用します。

OpenShift Container Platform 4.9 では、統合イメージレジストリーは、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を使用して Microsoft Azure Stack Hub にインストールされたクラスターに Azure Blob Storage を使用します。

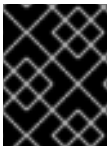
詳細は、Installing a cluster on Azure Stack Hub using ARM templates を参照してください。

1.3.11. Operator ライフサイクル

以下の新しい機能および機能拡張は、Operator Lifecycle Manager（OLM）を使用したOperatorの実行に関連しています。

1.3.11.1. Operator Lifecycle Manager が Kubernetes 1.22 にアップグレード

OpenShift Container Platform 4.9 以降、Operator Lifecycle Manager(OLM)は Kubernetes 1.22 をサポートします。その結果、多数の **v1beta1** APIが削除され**v1**に更新されています。削除された **v1beta1** API に依存する Operator は OpenShift Container Platform 4.9 では実行されません。クラスター管理者は、クラスターを OpenShift Container Platform 4.9 にアップグレードする前に、最新の チャネルにインストールされた Operatorをアップグレードする必要があります。



重要

Kubernetes 1.22 では、さまざまな特筆すべき変更が**CustomResorceDefinition** API の**v1**に加えられています。

1.3.11.2. ファイルベースのカタログ

ファイルベースのカタログは、Operator Lifecycle Manager(OLM)のカタログ形式の最新の反復になります。この形式は、プレーンテキストベース（JSONまたはYAML）であり、以前の形式の宣言的な設定の進化であり現在は非推奨の SQLite データベース形式であり、完全な下位互換性があります。この形式の目標は、Operatorのカタログ編集、構成可能性、および拡張性を有効にすることです。

ファイルベースのカタログ仕様の詳細は、Operator Framework packaging format を参照してください。

opm CLI を使用して、ファイルベースのカタログを作成する方法については、Managing custom catalogs を参照してください。

1.3.11.3. Single Node OpenShift の Operator Lifecycle Manager サポート

Operator Lifecycle Manager(OLM)が Single Node OpenShift(SNO)クラスターで利用でき、セルフサービスの Operator のインストールが可能になりました。

1.3.11.4. クラスタ管理者向けの強化されたエラーレポート

管理者は、このような問題を正常にデバッグするために、さまざまな低レベルAPI間の相互作用プロセスやOperator Lifecycle Manager（OLM）Podログへのアクセスを理解する必要がないため、OpenShift Container Platform4.9では、OLMに以下の拡張機能を導入し、よりわかりやすいエラーレポートとメッセージを管理者に提供します。

1.3.11.4.1. Operator グループのステータス条件の更新

以前は、namespaceに複数のOperatorグループが含まれていた場合、またはサービスアカウントが見つからなかった場合、Operatorグループのステータスはエラーを報告しませんでした。この機能拡張により、これらのシナリオでは、Operatorグループのステータス条件が更新され、エラーが報告されるようになりました。

1.3.11.4.2. インストール計画の失敗の理由の表示

このリリース以前は、インストールプランが失敗した場合、サブスクリプションの状態には失敗が発生した理由が記載されていませんでした。現在は、インストール計画が失敗すると、サブスクリプションのステータス状態は失敗の理由を示します。

1.3.11.4.3. サブスクリプションステータスでの解決競合の表示

依存関係の解決では、namespace内のすべてのコンポーネントが単一のユニットとして扱われるため、解決が失敗した場合、namespace上のすべてのサブスクリプションがエラーを示すようになりました。

1.3.11.5. カスタムカタログソースのイメージテンプレート

クラスターのアップグレードにより、Operatorのインストールがサポートされていない状態になったり、更新パスが継続されなかったりする可能性を回避するために、クラスターのアップグレードの一環として、Operatorカタログのインデックスイメージのバージョンを自動的に変更するように有効化することができます。

olm.catalogImageTemplate アノテーションをカタログイメージ名に設定し、イメージタグのテンプレートを作成する際に、1つ以上のKubernetesクラスターバージョン変数を使用します。

詳細は、Image template for custom catalog sources を参照してください。

1.3.12. Operator の開発

以下の新しい機能および拡張機能は、Operator SDK を使用した Operator の開発に関連しています。

1.3.12.1. 高可用性または単一ノードのクラスターの検出およびサポート

OpenShift Container Platformクラスターは、複数のノードを使用する高可用性（HA）モード、または単一ノードを使用する非HAモードで設定できます。Single Node OpenShift（SNO）とも呼ばれる単一ノードクラスターには、より慎重なリソース制約がある可能性があります。したがって、単一ノードクラスターにインストールされたOperatorがそれに応じて調整でき、正常に実行できることが重要です。

OpenShift Container Platformで提供されるクラスター高可用性モードAPIにアクセスすることにより、Operatorの作成者は、Operator SDKを使用して、Operatorがクラスターのインフラストラクチャートポロジー（HAモードまたは非HAモード）を検出できるようにすることができます。カスタム Operator ロジックは、検出されたクラスタートポロジーを使用して、Operator およびそれが管理するオペランドまたはワークロードの両方のリソース要件を、トポロジーに最も適したプロファイルに自動的に切り替えるように開発することができます。

詳細は、High-availability or single node cluster detection and support を参照してください。

1.3.12.2. ネットワークプロキシーの Operator サポート

Operator の作成者は、ネットワークプロキシーをサポートする Operator を開発できるようになりました。プロキシーをサポートする Operator は環境変数の Operator デプロイメントを検査し、必要なオペランドに変数を渡します。クラスター管理者は、Operator Lifecycle Manager (OLM)によって処理される環境変数のプロキシーサポートを設定します。詳細は、Go、Ansible、および Helm を使用して Operator を開発するための Operator SDK チュートリアルを参照してください。

1.3.12.3. Kubernetes 1.22 から削除された API のバンドルマニフェストの検証

bundle validate サブコマンドを使用して、テストの Operator Framework スイートを使用して Kubernetes 1.22 から削除された API のバンドルマニフェストを確認することができます。

以下は例になります。

```
$ operator-sdk bundle validate .<bundle_dir_or_image> \
  --select-optional suite=operatorframework \
  --optional-values=k8s-version=1.22
```

バンドルマニフェストに Kubernetes 1.22 から削除された API が含まれる場合は、このコマンドに警告メッセージが表示されます。警告メッセージは、移行する必要がある API および Kubernetes API 移行ガイドへのリンクを示します。

詳細は、table of beta APIs removed from Kubernetes 1.22 および Operator SDK CLI reference を参照してください。

1.3.13. ビルド

OpenShift Container Platform をビルドに使用する開発者として、この更新では、以下の新機能を使用できます。

- ビルドボリュームをマウントして、実行中のビルドに、アウトプットコンテナーイメージで永続化しない情報にアクセスできます。ビルドボリュームは、ビルド時にビルド環境や設定が必要なリポジトリーの認証情報などの機密情報をのみ提供できます。ビルドボリュームは、データが出力コンテナーイメージに保持されるビルド入力とは異なります。
- BuildConfig のステータスに記録される情報に基づいて、ビルドをトリガーするようにイメージの変更を設定できます。これにより、GitOps ワークフロー内のビルドで **ImageChange** トリガー を使用できます。

1.3.14. イメージ

1.3.14.1. レジストリーソースとしてのワイルドカードドメイン

本リリースでは、イメージレジストリー設定でレジストリーソースとしてワイルドカードドメインを使用するサポートが導入されました。***.example.com** などのワイルドカードドメインを使用して、各サブドメインを手動で入力しなくても、複数のサブドメインからイメージをプッシュおよびプルするようにクラスターを設定できます。詳細は、Image controller configuration parametersを参照してください。

1.3.15. マシン API

1.3.15.1. コンピュートマシン用のRed Hat Enterprise Linux(RHEL)8 のサポート

OpenShift Container Platform 4.9 以降、コンピュートマシンに Red Hat Enterprise Linux(RHEL)8.4 を使用できるようになりました。以前は、RHEL 8 はコンピュートマシン用にはサポートされませんでした。

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

1.3.16. ノード

1.3.16.1. スケジューラープロファイルの GA

スケジューラープロファイルを使用した Pod のスケジューリングが一般提供されました。これは、スケジューラーポリシーを設定する代わりに実行されます。以下のスケジューラープロファイルを利用できます。

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

詳細は、Scheduling pods using a scheduler profile を参照してください。

1.3.16.2. 新しい Descheduler プロファイルおよびカスタマイズ

以下の Descheduler プロファイルが利用可能になりました。

- **SoftTopologyAndDuplicates**: このプロファイルは **TopologyAndDuplicates** と同じです。ただし、**whenUnsatisfiable: ScheduleAnyway** など、ソフトトポロジー制約のある Pod もエビクションに考慮されます。
- **EvictPodsWithLocalStorage**: このプロファイルにより、ローカルストレージを持つ Pod がエビクションの対象となります。
- **EvictPodsWithPVC**: このプロファイルにより、永続ボリューム要求を持つ Pod がエビクションの対象となります。

LifecycleAndUtilization プロファイルの Pod ライフタイム値をカスタマイズすることもできます。

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

1.3.16.3. 同じレジストリーへの複数のログイン

Pod がプライベートレジストリーからイメージをプルできるように **docker/config.json**ファイルを設定する場合、同じレジストリ内の特定のリポジトリを一覧表示できるようになりました。各リポジトリには、そのレジストリパスに固有の認証情報が含まれています。以前は、特定のレジストリから1つのリポジトリしかリストできませんでした。特定の namespace でレジストリーを定義することもできるようになります。

1.3.16.4. ノードリソースのモニタリングの強化

ノード関連のメトリックスとアラートが強化され、ノードの安定性がいつ損なわれたかを早期に示すことができます。

1.3.16.5. Node Health Check Operator を使用したノードのヘルスチェックのデプロイ（テクノロジープレビュー）

Node Health Check Operator を使用して **NodeHealthCheck** コントローラーをデプロイできます。コントローラは、正常ではないノードを識別し、Poison PillOperatorを使用して、正常ではないノードを修正します。

1.3.17. Red Hat OpenShift Logging

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

1.3.18. モニタリング

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

1.3.18.1. モニタリングスタックコンポーネントおよび依存関係

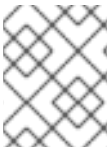
モニタリングスタックコンポーネントおよび依存関係のバージョンの更新には、以下が含まれます。

- Prometheus が 2.29.2 へ
- Prometheus Operator が 0.49.0 へ
- Prometheus アダプターが 0.9.0 へ
- Alertmanager が 0.22.2 へ
- Thanos が 0.22.0 へ

1.3.18.2. アラートルール

- 新規
  - **HighlyAvailableWorkloadIncorrectlySpread** は、可用性の高いモニタリングコンポーネントの 2 つのインスタンスが同じノード上で実行し、永続ボリュームが割り当てられている場合に潜在的な問題を通知します。
  - **NodeFileDescriptorLimit** は、ノードカーネルが利用可能なファイル記述子が不足するとアラートをトリガーします。警告レベルのアラートは 70% を超え、重大なレベルのアラートが 90% の使用量を超える場合に実行されます。
  - **PrometheusLabelLimitHit** は、ターゲットが定義されたラベルの制限を超えたかどうかを検出します。
  - **PrometheusTargetSyncFailure** は、Prometheus がターゲットの同期に失敗した場合に検出します。
  - すべての重要なアラートルールには、runbook を実行するためのリンクが含まれます。
- 改善
  - **AlertManagerReceiversNotConfigured** および **KubePodCrashLooping** には誤検出が少なくなりました。
  - **KubeCPUOvercommit** および **KubeMemoryOvercommit** は、不均一な環境でより堅牢になりました。
  - **NodeFilesystemAlmostOutOfSpace**アラートルールの**for**期間の設定が1時間から30分に変更され、ディスクの空き容量が少なくなったことをより迅速に検出できるようになりました。
  - **KubeDeploymentReplicasMismatch** が予想通りに実行されるようになりました。以前のバージョンでは、このアラートは実行されませんでした。
  - 以下のアラートには **namespace** ラベルが含まれるようになりました。
    - **AlertmanagerReceiversNotConfigured**

- **KubeClientErrors**
- **KubeCPUOvercommit**
- **KubeletDown**
- **KubeMemoryOvercommit**
- **MultipleContainersOOMKilled**
- **ThanosQueryGrpcClientErrorRate**
- **ThanosQueryGrpcServerErrorRate**
- **ThanosQueryHighDNSFailures**
- **ThanosQueryHttpRequestQueryErrorRateHigh**
- **ThanosQueryHttpRequestQueryRangeErrorRateHigh**
- **ThanosSidecarPrometheusDown**
- **Watchdog**



注記

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

1.3.18.3. Alertmanager

- プラットフォームおよびユーザー定義のプロジェクトモニタリングスタックの両方について、追加の外部 Alertmanager を追加および設定することができます。
- ローカルの Alertmanager インスタンスを無効にすることができます。

1.3.18.4. Prometheus

- Prometheusでは、プラットフォーム監視とユーザー定義プロジェクトの両方に対してリモート書き込みストレージを有効にして構成できます。この機能を使用すると、取り込んだメトリックを長期ストレージに送信できます。
- Prometheus のメモリー使用率全体を減らすために、空の **pod** および **namespace** ラベルの両方を持つ以下の cAdvisor メトリクスは削除されました。
  - **container_fs_.***
  - **container_spec_.***
  - **container_blkio_device_usage_total**
  - **container_file_descriptors**
  - **container_sockets**
  - **container_threads_max**

    - **container_threads**
    - **container_start_time_seconds**
    - **container_last_seen**

- プラットフォームモニタリング用に永続ストレージが設定されていない場合は、アップグレード、およびクラスターの中断により、データが失われる可能性があります。プラットフォームモニタリング用に永続ストレージが設定されていないことをシステムが検出すると、警告メッセージが **Degraded** 状態に追加されました。
- **openshift.io/user-monitoring: "false"** ラベルを追加して、**openshift-user-workload-monitoring** プロジェクトから個々のユーザー定義プロジェクトを除外できます。
- **openshift-user-workload-monitoring** プロジェクトの **enforcedTargetLimit** パラメーターを設定し、収集されるターゲット数に全体の制限を設定できます。

1.3.18.5. Prometheus UI リンクの削除

サードパーティーの Prometheus UI へのリンクは、OpenShift Container Platform Web コンソールの **Observe → Metrics** ページから削除されます。Prometheus UI へのルートへは、**openshift-monitoring** プロジェクトの **Networking → Routes** ページに移動し、**Administrator** パースペクティブの Web コンソールで引き続きアクセスすることができます。

1.3.18.6. Grafana

デフォルトの Grafana ダッシュボードを実行すると、ユーザーのワークロードからリソースを取得できるため、Grafana ダッシュボードのデプロイメントを無効にできます。

1.3.19. メータリング

このリリースでは、OpenShift Container Platform Metering Operatorが削除されています。

1.3.20. スケーラビリティーおよびパフォーマンス

1.3.20.1. Special Resource Operator（テクノロジープレビュー）

Special Resource Operator（SRO）を使用して、既存のOpenShift Container Platformクラスターでのカーネルモジュールとドライバーのデプロイメントを管理できるようになりました。これは現在、テクノロジープレビュー機能です。

詳細は、About the Special Resource Operatorを参照してください。

1.3.20.2. Memory Manager機能（テクノロジープレビュー）

Memory Manager 機能は、以下の Topology Manager ポリシーのいずれかで設定されるノードで実行されているすべての Pod に対してデフォルトで有効化されるようになりました。

- **single-numa-node**
- **restricted**

詳細は、Topology Manager policiesを参照してください。

1.3.20.3. レイテンシーテストの追加ツール

OpenShift Container Platform 4.9 では、システムレイテンシーを測定するための 2 つのツールが追加されました。

- **hwladetect** が、ベアメタルハードウェアが達成できるベースラインを測定します。
- **cyclictest** は、**hwlatdetect** が検証をパスした後に繰り返しタイマーをスケジュールし、希望のトリガー時間と実際のトリガー時間の違いを測定します。

詳細は、Running the latency tests を参照してください。

1.3.20.4. クラスターの最大数

OpenShift Container Platform 4.9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。

重要

本リリースでは、OVN-Kubernetes テストに対してパフォーマンスの大規模なスケーリングテストは実行されません。

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

1.3.20.5. ゼロタッチプロビジョニング（テクノロジープレビュー）

OpenShift Container Platform 4.9 は、ゼロタッチプロビジョニング (ZTP) をサポートします。これにより、リモートサイトでのベアメタル機器の宣言的な設定で新しいエッジサイトをプロビジョニングすることができます。ZTP は、インフラストラクチャーのデプロイメントに GitOps デプロイメントセットを使用します。GitOps は、YAML ファイルや他の定義パターンなどの Git リポジトリーに保存される宣言型仕様を使用してこれらのタスクを実行します。これは、インフラストラクチャーをデプロイするためのフレームワークを提供します。宣言型の出力は、マルチサイトのデプロイメントに Open Cluster Manager (OCM) によって使用されます。詳細は、Provisioning edge sites at scale を参照してください。

1.3.21. Insights Operator

1.3.21.1. RHEL Simple Content Access 証明書のインポート（テクノロジープレビュー）

OpenShift Container Platform 4.9 では、Insights Operator は Red Hat OpenShift Cluster Manager から RHEL Simple Content Access(SCA)証明書をインポートすることができます。

詳細は、Importing RHEL Simple Content Access certificates with Insights Operatorを参照してください。

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

OpenShift Container Platform 4.9 では、Insights Operator は以下の追加情報を収集します。

- クラスターからのすべての **MachineConfig** リソース定義。
- クラスターにインストールされている **PodSecurityPolicies** の名前。
- インストールされている場合、**ClusterLogging** リソース定義。

- **SamplesImagestreamImportFailing** アラートが実行される場合、**ImageStream** の定義と、**openshift-cluster-samples-operator** namespace からのコンテナーログの最後の 100 行。

この追加情報により、Red Hat は Insights Advisor の改善された修復手順を提供できます。

1.3.22. 認証および認可

1.3.22.1. 手動モードの Cloud Credential Operator を使用した Microsoft Azure Stack Hub のサポート

今回のリリースにより、Microsoft Azure Stack Hub へのインストールは、Cloud Credential Operator(CCO)を手動モードに設定して実行できます。

詳細は、Using manual mode を参照してください。

1.3.23. OpenShift Container Platform での OpenShift サンドボックスコンテナーのサポート (テクノロジープレビュー)

OpenShift サンドボックスコンテナーの新機能、バグ修正、既知の問題、および非同期エラータ更新を確認するには、OpenShift sandboxed containers 1.1 release notes を参照してください。

1.4. 主な技術上の変更点

OpenShift Container Platform 4.9 では、以下に示す顕著な技術的な変更点が加えられています。

etcd データの自動デフラグ
OpenShift Container Platform 4.9 では、etcd データは etcd Operator によって自動的にデフラグされます。

Octavia OVN NodePort の変更
以前のバージョンでは、Red Hat OpenStack Platform(RHOSP)デプロイメントでは、NodePort の開始トラフィックは、ノードのサブネットの CIDR に制限されていました。Octavia Open Virtual Network(OVN)プロバイダーを使用して LoadBalancer サービスをサポートするために、マスターおよびワーカーノードへのNodePort トラフィックを許可するセキュリティーグループルールがオープン **(0.0.0.0/0)** に変更されました。

OpenStack Platform LoadBalancer 設定の変更
Red Hat OpenStack Platform(RHOSP)クラウドプロバイダー LoadBalancer 設定はデフォルトで **use-octavia=True** になりました。このルールの例外は Kuryr を使用するデプロイメントです。この場合、Kuryr は独自に LoadBalancer サービスを処理するため、**use-octavia** が **false** に設定されます。

Ingress コントローラーを **HAProxy 2.2.15** にアップグレード
OpenShift Container Platform Ingress コントローラーが HAProxy version 2.2.15 にアップグレードされます。

CoreDNS がバージョン **1.8.4** に更新される
OpenShift Container Platform 4.9 では、CoreDNS はバージョン 1.8.4 を使用します。これにはバグ修正が含まれます。

クラウドプロバイダーのクラウドコントローラーマネージャーの実装
クラウドプロバイダーのデプロイメントを管理する Kubernetes コントローラーマネージャーには、プロバイダーとしての Azure Stack Hub のサポートは含まれません。クラウドコントローラーマネージャーの使用は基礎となるクラウドプラットフォームと対話するための推奨される方法であるため、このサポートを追加する計画はありません。その結果、OpenShift Container Platform の Azure Stack Hub 実装はクラウドコントローラーマネージャーを使用します。

また、本リリースは、テクノロジープレビューとして Amazon Web Services(AWS)、Microsoft Azure、および Red Hat OpenStack Platform(RHOSP)のクラウドコントローラーマネージャーの使用をサポートしています。OpenShift Container Platform に追加される新しいクラウドプラットフォームサポートも、クラウドコントローラーマネージャーを使用します。

クラウドコントローラーマネージャーの詳細は、Kubernetes documentation on this component を参照してください。

クラウドコントローラーマネージャーおよびクラウドノードマネージャーのデプロイメントおよびライフサイクルを管理するために、本リリースで Cluster Cloud Controller Manager Operator が導入されました。

詳細は、**Red Hat Operators reference**のCluster Cloud Controller Manager Operator エントリーを参照してください。

カナリアロールアウト更新の実行
OpenShift Container Platform 4.9 では、カナリアロールアウト更新を実行する新規プロセスが導入されました。このプロセスの詳細な概要は、Performing a canary rollout update を参照してください。

大規模な **Operator** バンドルのサポート
Operator Lifecycle Manager(OLM)は、大規模なカスタムリソース定義(CRD)マニフェストなどの大量のメタデータを持つ Operator バンドルを圧縮し、etcd によって設定される 1 MB の制限未満に保つようになりました。

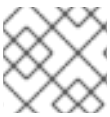
Operator Lifecycle Manager のリソース使用の削減
Operator Lifecycle Management(OLM)カタログ Pod はより効率的となり、少ない RAM を使用するようになりました。

"Extras" アドバイザリーからの **Operator** のデフォルト更新チャネル
RHBA-2021:3760 などの OpenShift Container Platform の "Extras" アドバイザリーに同梱される Operator は、Red Hat が提供するカタログに公開され、Operator Lifecyle Manager (OLM) で実行されます。OpenShift Container Platform 4.9 以降、これらの Operator はバージョン固有の **4.9** チャネルに加え、**stable** 更新チャネルに含まれるようになりました。

OpenShift Container Platform 4.9 および今後のリリースでは、**stable** はこれらの Operator のデフォルトチャネルになります。OLM でのこれらの Operator の更新チャネルの変更が、今後のクラスターのアップグレードで不要になるように、クラスター管理者は **stable** チャネルを使用する必要があります。

OLM ベースの Operator の詳細は、Red Hat-provided Operator catalogs および Understanding OperatorHub を参照してください。OLM での更新チャネルの詳細は、Upgrading installed Operators を参照してください。

Operator SDK v1.10.1
OpenShift Container Platform 4.9 は Operator SDK v1.10.1. をサポートします。この最新バージョンをインストールまたは更新するには、Installing the Operator SDK CLI を参照してください。



注記

Operator SDK v1.10.1 は Kubernetes 1.21 をサポートします。

以前にOperator SDK v1.8.0で作成または保守された Operator プロジェクトがある場合は、Upgrading projects for newer Operator SDK versionsを参照してプロジェクトをアップグレードし、Operator SDK v1.10.1との互換性が維持されていることを確認してください。

1.5. 非推奨および削除された機能

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

非推奨の機能は依然として OpenShift Container Platform に含まれており、引き続きサポートされますが、本製品の今後のリリースで削除されるため、新規デプロイメントでの使用は推奨されません。OpenShift Container Platform 4.9 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
- **TP**: テクノロジープレビュー
- **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 4.7	OCP 4.8	OCP 4.9
Package Manifest Format (Operator Framework)	DEP	REM	REM
Operator カタログの SQLite データベース形式	GA	GA	DEP
oc adm catalog build	DEP	REM	REM
oc adm catalog mirror の **--filter-by-os** フラグ	DEP	REM	REM
v1beta1 CRD	DEP	DEP	REM
Docker Registry v1 API	DEP	DEP	REM
メータリング Operator	DEP	DEP	REM
スケジューラーポリシー	DEP	DEP	DEP
Cluster Samples Operator の **ImageChangesInProgress** 状態	DEP	DEP	DEP
Cluster Samples Operator の **MigrationInProgress** 状態	DEP	DEP	DEP
OpenShift Container Platform リソースの **apiVersion** でグループなしで **v1** の使用	DEP	DEP	REM
RHCOS での **dhclient** の使用	DEP	DEP	REM

機能	OCP 4.7	OCP 4.8	OCP 4.9
クラスターローダー	GA	DEP	DEP
独自の RHEL 7 コンピュートマシンの持ち込み	DEP	DEP	DEP
ビルドの **BuildConfig** 仕様の **lastTriggeredImageID** フィールド	GA	DEP	REM
Jenkins Operator	TP	DEP	DEP
Prometheus に基づく HPA カスタムメトリクスアダプター	TP	REM	REM
vSphere 6.7 Update 2 以前および仮想ハードウェアバージョン 13	GA	GA	DEP
Red Hat Virtualization (RHV) の**instance_type_id**インストール設定パラメーター	DEP	DEP	DEP

1.5.1. 非推奨の機能

1.5.1.1. Operator カタログの SQLite データベース形式

カタログおよびインデックスイメージ用にOperator Lifecycle Manager（OLM）が使用するSQLiteデータベース形式は、関連する**opm** CLIコマンドを含めて非推奨になりました。クラスター管理者およびカタログメンテナーには、OpenShift Container Platform 4.9で導入された新しいファイルベースのカタログ形式に習熟し、カタログワークフローの移行を開始することをお勧めします。

注記

OpenShift Container Platform 4.6 以降のデフォルトの Red Hat が提供する Operator カタログ は、現時点では引き続き SQLite データベース形式で提供されています。

1.5.1.2. vSphere 6.7 Update 2 以前のクラスターインストールおよび仮想ハードウェアバージョン 13 が非推奨に

VMware vSphere バージョン 6.7 Update 2 以前および仮想ハードウェアバージョン 13 へのクラスターのインストールが非推奨になりました。これらのバージョンのサポートは、OpenShift Container Platform の今後のバージョンで終了します。

ハードウェアバージョン 15 が、OpenShift Container Platform の vSphere 仮想マシンのデフォルトになりました。ハードウェアバージョン 15 は、今後の OpenShift Container Platform バージョンでサポートされる唯一のバージョンになります。

1.5.1.3. Red Hat Virtualization (RHV) のinstance_type_idインストール設定パラメーター

instance_type_idインストール設定パラメータは非推奨になり、今後のリリースで削除される予定です。

1.5.2. 削除された機能

1.5.2.1. メータリング

このリリースでは、OpenShift Container Platform Metering Operator機能が削除されています。

1.5.2.2. ベータ版 API が Kubernetes 1.22 から削除

Kubernetes 1.22 では、以下の非推奨化された **v1beta1** API が削除されました。**v1** API バージョンを使用するようにマニフェストおよび API クライアントを移行します。削除された API の移行についての詳細は、Kubernetes documentation を参照してください。

表1.2 **v1beta1** API が Kubernetes 1.22 から削除

リソース	API	主な変更
APIService	**apiregistration.k8s.io/v1beta1**	不要
CertificateSigningRequest	**certificates.k8s.io/v1beta1**	必要
ClusterRole	**rbac.authorization.k8s.io/v1beta1**	不要
ClusterRoleBinding	**rbac.authorization.k8s.io/v1beta1**	不要
CSIDriver	**storage.k8s.io/v1beta1**	不要
CSINode	**storage.k8s.io/v1beta1**	不要
CustomResourceDefinition	**apiextensions.k8s.io/v1beta1**	必要
Ingress	**extensions/v1beta1**	必要
Ingress	**networking.k8s.io/v1beta1**	必要
IngressClass	**networking.k8s.io/v1beta1**	不要
Lease	**coordination.k8s.io/v1beta1**	不要
LocalSubjectAccessReview	**authorization.k8s.io/v1beta1**	必要
MutatingWebhookConfiguration	**admissionregistration.k8s.io/v1beta1**	必要
PriorityClass	**scheduling.k8s.io/v1beta1**	不要
ロール	**rbac.authorization.k8s.io/v1beta1**	不要
RoleBinding	**rbac.authorization.k8s.io/v1beta1**	不要

リソース	API	主な変更
SelfSubjectAccessReview	**authorization.k8s.io/v1beta1**	必要
StorageClass	**storage.k8s.io/v1beta1**	不要
SubjectAccessReview	**authorization.k8s.io/v1beta1**	必要
TokenReview	**authentication.k8s.io/v1beta1**	不要
ValidatingWebhookConfiguration	**admissionregistration.k8s.io/v1beta1**	必要
VolumeAttachment	**storage.k8s.io/v1beta1**	不要

1.5.2.3. Descheduler v1beta1 APIの削除

descheduler用の非推奨の**v1beta1** APIは、OpenShift Container Platform4.9で削除されました。descheduler **v1beta1** APIバージョンを使用するリソースを**v1**に移行します。

1.5.2.4. RHCOSでのdhclientの使用の削除

非推奨の**dhclient**バイナリはRHCOSから削除されました。OpenShift Container Platform 4.6以降、RHCOSは初回の起動時にネットワークを設定するために、**initramfs** で **NetworkManager**を使用するように切り替えました。その代わりに、**NetworkManager** の内部 DHCP クライアントをネットワーク設定に使用します。詳細は、BZ#1908462 を参照してください。

1.5.2.5. lastTriggeredImageID フィールド更新を停止して無視

現在のリリースでは、**buildConfig.spec.triggers[i].imageChage**が参照する**ImageStreamTag**が新しいイメージを指定している場合は、**buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID**フィールドの更新を停止しています。このリリースでは、**buildConfig.status.imageChangeTriggers[i].lastTriggeredImageID** フィールドが更新されました。

さらに、Build Image Change Trigger コントローラーは **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID** フィールドを無視します。

Build Image Change Triggerコントローラは、**buildConfig.status.imageChangeTriggers[i].lastTriggeredImageID**フィールドと、**buildConfig.spec.triggers[i].imageChange**で参照される**ImageStreamTag**で参照されるイメージIDとの比較に基づいて、ビルドを開始します。

したがって、**buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID** を検査するスクリプトとジョブを適切に更新します。(BUILD-190)

1.5.2.6. OpenShift Container Platform リソースの apiVersion でグループなしで v1 の使用

OpenShift Container Platform リソースの **apiVersion** のグループなしで **v1** を使用するサポートが削除されました。***.openshift.io** が含まれるすべてのリソースは API インデックス にある **apiVersion** 値と一致している必要があります。

1.6. バグ修正

APIサーバーと認証

- 以前は、暗号化状態が無期限に残る場合があり、一部のOperatorのパフォーマンスが低下した状態として報告されることがありました。古い暗号化状態が適切にクリアされ、不適切に報告されなくなりました。(BZ#1974520)

- 以前は、APIサーバークライアント証明書のCAは、クラスターの存続期間の早い段階でローテーションされていました。これにより、同じ名前の以前のCSRがまだ存在していたため、認証Operatorは証明書署名要求（CSR）を作成できませんでした。**TokenReview**リクエストを送信するときに、Kubernetes APIサーバーがOAuth APIサーバーに対して自身を認証できなかったため、認証が失敗していました。生成された名前は、認証OperatorがCSRを作成するときに使用されるようになったため、APIサーバークライアント証明書のCAを早期にローテーションしても、認証が失敗することはなくなりました。(BZ#1978193)

ベアメタルハードウェアのプロビジョニング

- 以前のバージョンでは、metal3 Pod は、initContainers の作成による Red Hat Enterprise Linux CoreOS (RHCOS)イメージをダウンロードできませんでした。この問題は、initContainers の作成の順序を変更し、**metal3-machine-os-downloader** initContainer の前に **metal-static-ip-set** initContainer が作成されることで修正されています。RHCOS イメージが期待どおりにダウンロードされるようになりました。(BZ#1973724)

- 以前のバージョンでは、**idrac-virtualmedia** を使用するように設定されたホストでベアメタルでインストーラーでプロビジョニングされるインストールを使用する場合は、そのホストの **bios_interface** はデフォルトで **idrac-wsman** に設定されていました。これにより、BIOS 設定が利用できなくなり、例外が発生します。この問題は、**idrac-virtualmedia** を使用する際にデフォルトの **bios_interface** に **idrac-redfish** を使用して修正されています。(BZ#1928816)

- 以前のバージョンでは、UEFI モードでは、RHCOS イメージのダウンロード後に **ironic-python-agent** が UEFI ブートローダーエントリーを作成していました。RHEL 8.4 に基づく RHCOS イメージを使用する場合、このエントリーを使用してイメージを起動できず、BIOS エラー画面が出力されることがありました。これは、固定のブートエントリーを使用する代わりに、イメージにある CSV ファイルに基づいてブートエントリーを設定する **ironic-python-agent** により修正されています。イメージはエラーなしで正常に起動します。(BZ#1966129)

- 以前のバージョンでは、**provisioningHostIP** が **install-config** に設定されていると、provisioning ネットワークが無効になっていても metal3 Pod に割り当てられました。これは修正されています。(BZ#1972753)

- 以前のバージョンでは、アシスト付きインストーラーでは、sushy リソースライブラリーの不一致があるため、Supermicro X11/X12 ベースのシステムをプロビジョニングできませんでした。不一致により、仮想メディアを**Inserted**属性と**WriteProtected**属性にアタッチできず、**VirtualMedia.InsertMedia**リクエスト本文で許可されないため、インストールの問題が発生しました。この問題は、sushyリソースライブラリを変更し、厳密に必要でない場合にこれらの任意の属性の送信を停止する条件を追加することで修正され、インストールをこの時点を超えて進めることができます。(BZ#1986238)

- 以前のバージョンでは、プロビジョニングされた状態の一部のエラータイプにより、ホストのプロビジョニングが解除されていました。これは、ベアメタルホストにプロビジョニングされるイメージが利用不可になった場合に、metal3 Pod の再起動後に発生しました。この場合、ホストはプロビジョニング解除状態になります。この問題は、プロビジョニングされた状態でのエラーのアクションを変更することで修正され、イメージが使用できなくなった場合にエラーが報告されますが、プロビジョニング解除は開始しません。(BZ#1972374)

ビルド

- OpenShift Container Platform 以降では、バグ BZ#1884270 の修正により、SCP 形式の URL を提供しようとして、SSH プロトコル URL が誤ってプルーニングされました。このエラーにより、**oc new-build** コマンドは自動ソースクローンシークレットを選択しませんでした。ビルドは、**build.openshift.io/sbuild.openshift.io/source-secret-match-uri-1ource-secret-match-uri-1**アノテーションを使用して、SSHキーを、関連するシークレットにマップすることができず、git クローンを実行できませんでした。今回の更新により、BZ#1884270 からの変更が元に戻され、ビルドがアノテーションを使用し、git クローンを実行できるようになりました。

- この更新の前は、クラスターイメージ構成のさまざまな許可されたブロックレジストリ構成オプションにより、Cluster Samples Operatorによるイメージストリームの作成がブロックされることがありました。この問題が発生すると、samples Operator 自体が **degraded** とマークされ、一般的な OpenShift Container Platform のインストールおよびアップグレードステータスに影響が出ます。
  Cluster Samples Operator は、さまざまな状況で **removed** としてブートストラップできます。今回のアップデートでは、イメージコントローラの設定パラメータにより、デフォルトのイメージレジストリまたは**samplesRegistry** 設定で指定されたイメージレジストリを使用してイメージストリームを作成できない場合が含まれています。Operator ステータスは、クラスターイメージ設定がサンプルイメージストリームの作成を阻止するタイミングも指定します。

クラウドコンピュート

- 以前は、新しいサーバーのrootボリュームが作成され、そのサーバーが正常に作成されなかった場合、ボリュームに関連付けられたサーバーの削除がなかったため、ボリュームの自動削除はトリガーされませんでした。状況によっては、これにより多くのボリュームが追加で作成され、ボリュームクォータに達した場合にエラーが発生しました。このリリースでは、サーバー作成の呼び出しが失敗すると、新しく作成されたrootボリュームが削除されます。
  (BZ#1943378)

- 以前は、**instanceType**のデフォルト値を使用すると、Machine APIはAWSで**m4.large**インスタンスを作成していました。これは、OpenShift Container Platformインストーラーによって作成されるマシンの**m5.large**インスタンスタイプとは異なります。このリリースでは、デフォルト値が指定されている場合、Machine APIはAWSで新しいマシンの**m5.large**インスタンスを作成します。(BZ#1953063)

- 以前のバージョンでは、コンピュートノードのマシンセット定義は、ポートがトランキングすべきかどうかを指定しませんでした。これは、ユーザーが同じマシンにトランクポートと非トランクポートを設定する必要がある技術で問題でした。今回のリリースにより、新しいフィールド **spec.Port.Trunk = bool** が追加されました。これにより、ユーザーはトランクとなるポートをより柔軟に判断できるようになりました。値が指定されていない場合、**spec.Port.Trunk** は **spec.Trunk** の値を継承します。また、作成されたトランクの名前は、使用するポートの名前と一致します。(BZ#1964540)

- 以前は、Machine API Operatorは、すでにアタッチされている場合でも、常に新しいターゲットをアタッチしていました。AWS APIを過度に呼び出すことで、多数のエラーが発生していました。このリリースでは、Operator は、アタッチメントプロセスを試行する前に、ロードバランサーのアタッチメントが必要かどうかを確認します。この変更により、APIリクエストが失敗する頻度が減少します。(BZ#1965080)

- 以前は、仮想マシンに自動ピン留めを使用すると、プロパティの名前は**disabled**、**existing**、または**adjust**されていました。このリリースでは、名前が各ポリシーをより適切に説明するようになり、**existing**はoVirtでブロックされているため削除されました。新しいプロパティ名は**none**と**resize_and_pin**で、oVirtユーザーインターフェイスと一致します。(BZ#1972747)

- 以前は、クラスターオートスケーラーが**csidrivers.storage.k8s.io** または **csistoragecapacities.storage.k8s.io**リソースにアクセスできなかったため、パーミッションエラーが発生していました。この修正により、クラスターオートスケーラーに割り当てられた

ロールが更新され、これらのリソースへのパーミッションが含まれるようになります。(BZ#1973567)

- 以前は、ノードが削除されたマシンを削除することが可能でした。これにより、マシンはいつまでも削除フェーズのままとなっていました。この修正により、この状態のマシンを適切に削除できます。(BZ#1977369)

- **boot-from-volume**イメージを使用する場合、マシンコントローラーが再起動されると、新規インスタンスを作成すると、ボリュームをリークします。これにより、以前に作成されたボリュームがクリーンアップされることはありませんでした。この修正により、以前に作成されたボリュームがプルーニングまたは再利用されることが保証されます。(BZ#1983612)

- 以前のリリースでは、Red Hat Virtualization(RHV)プロバイダーは、マシン用の **br-ex** という名前の NIC を無視していました。**OVNKubernetes** のネットワーク種別により **br-ex** 名で NIC が作成されるため、マシンが OVN-Kubernetes で IP アドレスを取得しなくなりました。今回の修正により、ネットワークが **OVNKubernetes** に設定された状態で、OpenShift Container Platform を RHV にインストールできるようになりました。(BZ#1984481)

- 以前は、プロキシとカスタムCA証明書を組み合わせてRed Hat OpenStack Platform（RHOSP）にデプロイすると、クラスターが完全に機能するようにはなりませんでした。この修正により、カスタムCA証明書で接続する際に、使用されるHTTPトランスポートにプロキシ設定が渡され、すべてのクラスターコンポーネントが想定どおりに機能します。(BZ#1986540)

クラスターバージョン Operator

- 以前は、Cluster Version Operator（CVO）は、プロキシ設定リソースの**noProxy**プロパティを尊重していませんでした。その結果、プロキシされていない接続のみが完了したときに、CVOは更新の推奨事項またはリリース署名へのアクセスを拒否されました。現在は、プロキシリソースが、直接のプロキシされていないアクセスを要求すると、CVOはアップストリームの更新サービスと署名ストアに直接到達します。(BZ#1978749)

- 以前は、Cluster Version Operator（CVO）は、Network Operatorで検証されたステータスプロパティからではなく、プロキシリソース仕様プロパティからプロキシ設定をロードしていました。その結果、誤って設定された値があると、CVOがアップストリームの更新サービスまたは署名ストアに到達できなくなっていました。現在、CVOは、検証済みのステータスプロパティからのみプロキシ設定をロードします。(BZ#1978774)

- 以前は、Cluster Version Operator（CVO）は、マニフェストの外部に追加されたボリュームマウントを削除しませんでした。その結果、ボリューム障害時にPodの作成が失敗する可能性があります。CVO は、マニフェストに表示されないすべてのボリュームマウントを削除するようになりました。(BZ#2004568)

コンソールストレージプラグイン

- 以前は、Cephストレージを操作するときに、コンソールストレージプラグインにnamespaceパラメーターの冗長な使用が不必要に含まれていました。このバグは、お客様に見える形での影響はありませんでしが、namespaceの冗長な使用を回避するために、プラグインが更新されました。(BZ#1982682)

イメージレジストリー

- レジストリがカスタム容認を使用する必要があるかどうかを確認するOperatorは、**spec.tolerations**ではなく**spec.nodeSelector**を確認していました。**spec.tolerations** のカスタム容認は、**spec.nodeSelector**が設定されている場合にのみ適用されます。この修正で

は、フィールド**spec.tolerations**を使用して、カスタム容認の存在を確認します。現在、**spec.tolerations**が設定されている場合、Operatorはカスタム容認を使用します。(BZ#1973318)

- **configs.imageregistry**の**spec.managementState**は**Removed**に設定（これにより、イメージプルーナーPodは**v1.21**以降の非推奨となったCronJobに関する警告を生成）されるため、**batch/v1**を使用する必要があります。この修正は、OpenShift Container Platform **oc**における**batch/v1**で**batch/v1beta1**を更新します。現在は、イメージプルーナーPodの非推奨のCronJobに関する警告が表示されなくなりました。(BZ#1976112)

Installer

- 以前は、Azureコントロールプレーンノードのネットワークインターフェイスで、インターフェイス名にハイフンがありませんでした。これは、他のプラットフォームと比較して一貫性がなく、問題を引き起こしていました。不足しているハイフンが追加されました。プラットフォームに関係なく、すべてのコントロールプレーンノードの名前は同じになりました。(BZ#1882490)

- oVirt の **install-config.yaml**ファイルの**autoPinningPolicy**および**hugepages**フィールドを設定できるようになりました。**autoPinningPolicy**フィールドでは、クラスターに対する Non-Uniform Memory Access（NUMA）ピニング設定およびCPUトポロジーの変更を自動的に設定できます。**hugepages** フィールドでは、ハイパーバイザーの Hugepages を設定できます。(BZ#1925203)

- 以前は、FIPSを有効にしてEd25519 SSHキータイプを使用した場合、インストールプログラムを使用できなくても、エラーは出力されませんでした。現在は、インストールプログラムはSSHキータイプを検証し、FIPSが有効なSSHキータイプがサポートされていない場合にエラーを出力します。FIPSが有効になっている場合は、RSAおよびECDSA SSHキータイプのみが許可されます。(BZ#1962414)

- 特定の条件では、Red Hat OpenStack Platform（RHOSP）ネットワークのトランクには、トランクがクラスターに属していることを示すタグが含まれていません。その結果、クラスターの削除によりトランクポートがなくなり、タイムアウトするまでループに陥りました。クラスターを削除すると、タグ付けされたポートが親となるトランクが削除されるようになりました。(BZ#1971518)

- 以前は、Red Hat OpenStack Platform（RHOSP）でクラスターをアンインストールするときに、インストーラーは非効率的なアルゴリズムを使用して、リソースを削除していました。非効率的なアルゴリズムにより、アンインストールプロセスに必要以上の時間がかかりました。インストーラーは、クラスターをより迅速にアンインストールする、より効率的なアルゴリズムで更新されます。(BZ#1974598)

- 以前は、**AWS_SHARED_CREDENTIALS_FILE**環境変数が空のファイルに設定されていた場合、インストーラーは認証情報の入力を求めてから、環境変数の値を無視し、場合によっては既存の認証情報を上書きして、**aws/credentials**ファイルを作成しました。この修正により、指定されたファイルに認証情報を保存するようにインストーラーが更新されます。指定されたファイルに無効な認証情報がある場合、インストーラーはファイルを上書きして情報が失われるリスクを冒す代わりに、エラーを生成します。(BZ#1974640)

- 以前は、別のクラスターとリソースを共有しているAzure上のクラスターをユーザーが削除すると、あいまいなエラーメッセージが表示され、削除が失敗した理由を理解するのが困難でした。この更新では、障害が発生する理由を説明するエラーメッセージが追加されます。(BZ#1976016)

- 以前は、タイプミスが原因で、Kuryrのデプロイメントは間違った要件に対してチェックされていました。つまり、Kuryrの最小要件を満たしていない場合でも、Kuryrを使用したインストールが、正常に実行される可能性がありました。この修正によりエラーが解消され、インストー

ラーが適切な要件を確認できるようになります。(BZ#1978213)

- この更新の前は、**keepalived**のIngressチェックにfallおよびraiseディレクティブが含まれていませんでした。つまり、1回のチェックに失敗すると、Ingress仮想IPフェイルオーバーが発生する可能性がありました。このバグ修正では、fallおよびraiseディレクティブを導入し、このようなフェイルオーバーを防ぎます。(BZ#1982766)

Kubernetes API サーバー

- 以前は、デプロイメントとイメージストリームが同時に作成されると、デプロイメントコントローラーが無限ループでレプリカセットを作成する原因となる競合状態が発生する可能性がありました。APIサーバーのイメージポリシープラグインの役割が軽減され、デプロイメントとイメージストリームを同時に作成しても、無限のレプリカセットが発生することはなくなりました。(BZ#1925180), (BZ#1976775)

- 以前は、同じパスに書き込んでいたインストーラーPodとcert-syncerコンテナーの間に競合がありました。これにより、一部の証明書を空のままにし、サーバーの実行が妨げられる可能性があります。Kubernetes APIサーバー証明書は、複数のプロセス間の競合を防ぐために、アトミックな方法で記述されるようになりました。(BZ#1971624)

ネットワーキング

- OVN-Kubernetes クラスターネットワークプロバイダーを使用する場合、論理フローキャッシュはメモリー制限なしで設定されていました。その結果、状況によっては、メモリの負荷が高くなると、ノードが使用できなくなる可能性がありました。この更新により、論理フローキャッシュはデフォルトで1GBのメモリ制限で設定されます。(BZ#1961757)

- OVN-Kubernetesクラスターネットワークプロバイダーを使用する場合、OpenShift Container Platform 4.5クラスターで作成され、その後アップグレードされたネットワークポリシーは、予期しないトラフィックを許可またはドロップする可能性があります。OpenShift Container Platformの後のバージョンでは、OVN-KubernetesはIPアドレスセットの管理に異なる規則を使用し、OpenShift Container Platform4.5で作成されたネットワークポリシーは、この規則を使用しませんでした。現在は、アップグレード中に、すべてのネットワークポリシーが新しい規則に移行されます。(BZ#1962387)

- OVN-Kubernetesクラスターネットワークプロバイダーの場合、**must-gather**を使用してOpen vSwitch（OVS）ログを取得すると、収集されたログデータには、**INFO**ログレベルがありませんでした。現在は、すべてのログレベルがOVSログデータに含まれます。(BZ#1970129)

- 以前は、パフォーマンステストにより、ラベル要件が原因で、サービスコントローラーメトリックスのカーディナリティが大幅に増加していることが明らかになりました。その結果、Open Virtual Network（OVN）Prometheus Podのメモリ使用量が増加しました。この更新により、ラベル要件が削除されました。サービスコントローラーのカーディナリティメトリックスとメモリ使用量が削減されました。(BZ#1974967)

- 以前は、**ovnkube-trace**は、インターフェイスの**link**インデックスを検出する必要があったため、送信元Podや宛先Podにiprouteをインストールする必要がありました。これにより、iproute がインストールされていない場合、Podで**ovnkube-trace**が失敗します。iprouteではなく、**/sys/class/net/<interface>/iflink**から**link**インデックスを取得できるようになりました。その結果、**ovnkube-trace**では、送信元Podおよび宛先Podにiprouteをインストールする必要がなくなりました。(BZ#1978137)

- 以前は、Cluster Network Operator（CNO）は、**network-check-source**サービスのサービスモニターをデプロイして、正しいアノテーションとロールベースのアクセス制御（RBAC）なしで、Prometheusによって検出されていました。その結果、サービスとそのメトリックスがPrometheusに入力されることはありませんでした。現在は、正しいアノテーションとRBAC

が、**network-check-source**サービスのnamespaceに追加されました。現在は、サービス**network-check-source**のメトリックスは、Prometheusによってスクレイプされます。(BZ#1986061)

- 以前のリリースでは、IPv6 DHCP を使用する場合、ノードインターフェースアドレスは **/128** 接頭辞でリースされる可能性がありました。その結果、OVN-Kubernetesは同じプレフィックスを使用してノードのネットワークを推測し、他のクラスターノードへのトラフィックを含む他のアドレストラフィックをゲートウェイ経由でルーティングします。今回の更新により、OVN-Kubernetesはノードのルーティングテーブルを検査し、ノードのインターフェースアドレスのより広いルーティングエントリをチェックし、そのプレフィックスを使用してノードのネットワークを推測します。その結果、他のクラスターノードへのトラフィックはゲートウェイ経由でルーティングされなくなりました。(BZ#1980135)

- 以前のバージョンでは、クラスターが OVN-Kubernetes Container Network Interface プロバイダーを使用する場合、IPv6 アドレスでの egress ルーターの追加の試行に失敗していました。この修正により、IPv6のサポートが出力ルーターCNIプラグインに追加され、出力ルーターの追加が成功します。(BZ#1989688)

ノード

- 以前は、コンテナでは、CRI-Oは**/proc/mounts**ファイルから**/etc/mtab**ファイルへのシンボリックリンクを作成しませんでした。その結果、ユーザーはコンテナの**/etc/mtab**ファイルにマウントされたデバイスのリストを表示できませんでした。CRI-Oはシンボリックリンクを追加するようになりました。その結果、ユーザーはコンテナにマウントされたデバイスを表示できます。(BZ#1868221)

- 以前は、Podが作成後にすぐに削除された場合、kubeletがPodを適切にクリーンアップしない可能性がありました。これにより、Podが終了状態でスタックし、アップグレードの可用性に影響を与える可能性がありました。この修正により、Podのライフサイクルロジックが改善され、この問題が回避されます。(BZ#1952224)

- 以前は、システムメモリの使用量が予約済みメモリの90%を超えたときに、**SystemMemoryExceedsReserved**アラートが発生していました。その結果、クラスターは必要以上のアラート数を発生させる可能性がありました。このアラームのしきい値は、予約済みメモリの95%で発生するように変更されました。(BZ#1980844)

- 以前は、CRI-Oのバグにより、CRI-Oの作成したプロセスの子PIDがリークされていました。その結果、負荷がかかっている場合、systemdはかなりの数のゾンビプロセスを作成する可能性があります。これにより、ノードでPIDが不足した場合に、ノード障害が発生する可能性があります。リークを阻止するため、CRI-Oが修正されました。その結果、これらのゾンビプロセスは作成されなくなりました。(BZ#2003197)

OpenShift CLI (oc)

- 以前は、レジストリのミラーリング中に**oc**コマンドラインツールがクラッシュし、**--max-components**引数を使用したときにスライスのインデックス操作がチェックされていないため、**slice bounds out of range**パニックランタイムエラーが発生していました。この修正により、コンポーネントチェックが範囲外のインデックス値を要求しないようにするチェックが追加され、**--max-components**引数を使用するときに**oc**ツールがパニックにならないようにしました。(BZ#1786835)

- 以前は、**oc describe quota**コマンドで、**ClusterResourceQuota**値の**Used**メモリに一貫性のない単位が表示されていました。これは予測不可能で読みにくいものでした。この修正により、**Used**メモリは常に**Hard**メモリと同じ単位を使用するようになり、**oc describe quota**コマンドで予測可能な値が表示されるようになりました。(BZ#1955292)

- 以前は、クライアントセットアップがないために、**oc logs**コマンドはパイプラインビルドでは機能しませんでした。クライアントのセットアップが**oc logs**コマンドで修正され、パイプラインビルドで機能するようになりました。(BZ#1973643)

Operator Lifecycle Manager (OLM)

- 以前は、インストールされたOperatorが、**olm.maxOpenShiftVersion**を現在のバージョン以下のマイナーなOpenShift Container Platformバージョンに設定した場合、Operator Lifecycle Manager（OLM）のアップグレード可能な条件メッセージが不明確でした。これにより、**olm.maxOpenShiftVersion**が現在のOpenShift Container Platformバージョンとは異なるバージョンに設定されている場合に、マイナーバージョンとメジャーバージョンのアップグレードのみがブロックされるように指定するように修正された誤ったエラーメッセージが発生しました。(BZ#1992677)

- 以前は、**opm**コマンドは、バンドルがインデックスに存在する場合、バンドルの非推奨に失敗していました。その結果、同じ呼び出しでの別の非推奨の一部として切り捨てられたバンドルは、存在しないと報告されました。この更新により、非推奨となる前にバンドルのチェックが追加され、存在しないバンドルと切り捨てられたバンドルが区別されます。その結果、同じアップグレードパスに沿った非推奨のバンドルが存在しないと報告されることはなくなりました。(BZ#1950534)

- Operator Lifecycle Manager（OLM）がクラスター内のカスタムリソース定義（CRD）オブジェクトを更新しようとすると、一時的なエラーが発生する可能性があります。これにより、OLMは、CRDを含むインストール計画に永続的に失敗しました。このバグ修正により、OLMが更新され、リソースが変更された競合エラーでCRDの更新が再試行されます。その結果、OLMは、このクラスの一時的なエラーに対し、以前よりも回復力があります。インストール計画は、OLMが再試行して解決できる競合エラーで永続的に失敗しなくなりました。(BZ#1923111)

- **opm index|registry add**コマンドは、インデックスからすでに切り捨てられているかどうかに関わらず、置き換えられるインデックスにおけるOperatorバンドルの有無を検証しようとしました。特定のパッケージでバンドルが非推奨になった後、コマンドは常に失敗していました。このバグ修正により、**opm** CLIが更新され、このエッジケースが処理され、切り捨てられたバンドルの存在が確認されなくなりました。その結果、特定のパッケージでバンドルが非推奨になった後、コマンドが失敗することはなくなりました。(BZ#1952101)

- Operator Lifecycle Manager（OLM）は、カタログソースリソースのラベルを使用して、優先度クラスをレジストリPodに展開できるようになりました。デフォルトのカタログソースは、クラスターによって管理されるnamespaceの重要なコンポーネントであり、優先度クラスを義務付けています。今回の機能拡張により、**openshift-marketplace**namespace のすべてのデフォルトカタログソースには、**system-cluster-critical**優先順位クラスが含まれるようになりました。(BZ#1954869)

- Marketplace Operatorは、リース所有者のIDを保持する設定マップにコントローラーのPodによって配置された所有者参照がある、Leader-for-lifeの実装を使用していました。これは、Podがスケジュールされていたノードが使用できなくなり、Podを終了できなかった場合に問題になります。これにより、設定マップでは、新しいリーダーを選出するためのガベージコレクションが適切に実行されなくなりました。新しいMarketplace Operatorバージョンがリーダー選出を獲得できなかったため、マイナーバージョンのクラスターアップグレードはブロックされました。ロックを解除してMarketplaceコンポーネントのアップグレードを完了するには、リーダー選出リースを保持している設定マップを手動でクリーンアップする必要がありました。このバグ修正は、Leader-for-leaseリーダー選出の実装の使用に切り替わります。その結果、リーダー選出がこのシナリオで立ち往生することはなくなりました。(BZ#1958888)

- 以前は、インストールプランに新しい**Failed**フェーズが導入されていました。インストール計画が作成されていたnamespaceの有効なOperatorグループ（OG）またはサービスアカウント（SA）リソースを検出できないと、インストール計画は失敗状態に移行していました。つま

り、インストール計画が最初に調整された際にこれらのリソースを検出できなかった場合は、永続的な障害と見なされました。これは、以下に示すインストール計画の以前の動作からのリグレッションでした。

- OGまたはSAリソースの検出に失敗すると、調整のためにインストール計画が再キューイングされます。
- インフォーマキューの再試行制限に達する前に必要なリソースを作成すると、バンドルのアンパック手順が失敗しない限り、インストール計画は**Installing**フェーズから**Complete**フェーズに移行します。

このリグレッションにより、一連のマニフェストを同時に適用して、インストール計画を作成するサブスクリプションを含むOperatorをインストールするインフラストラクチャを構築したユーザーに、必要なOGおよびSAリソースとともに未知の動作が導入されました。このような場合、OGとSAの調整に遅延が発生するたびに、インストール計画は永続的な障害の状態に移行します。

このバグ修正により、インストール計画を**Failed**フェーズに移行したロジックが削除されます。代わりに、調整エラーが発生した場合、インストール計画が再キューイングされるようになりました。その結果、OGが検出されない場合、次の条件が設定されます。

```
conditions:
 - lastTransitionTime: ""2021-06-23T18:16:00Z""
 lastUpdateTime: ""2021-06-23T18:16:16Z""
 message: attenuated service account query failed - no operator group found that
 is managing this namespace
 reason: InstallCheckFailed
 status: ""False""
 type: Installed
```

有効なOGが作成されると、次の条件が設定されます。

```
conditions:
 - lastTransitionTime: ""2021-06-23T18:33:37Z""
 lastUpdateTime: ""2021-06-23T18:33:37Z""
 status: ""True""
```

(BZ#1960455)

- カタログソースを更新する場合、**Get**呼び出しの直後に、カタログソースに関連するいくつかのリソースに対する**Delete**呼び出しが続きます。場合によっては、リソースがすでに削除されていても、引き続きキャッシュに存在していました。これにより **Get**呼び出しは成功しましたが、以下の**Delete**呼び出しは、リソースがクラスターに存在しなかったため、失敗しました。このバグ修正により、Operator Lifecycle Manager（OLM）が更新され、リソースが見つからない場合に**Delete**呼び出しによって返されるエラーが無視されるようになります。その結果、**Delete**呼び出しから"Resource Not Found"エラーが発生するキャッシュの問題が原因で、カタログソースを更新するときにOLMがエラーを報告しなくなりました。(BZ#1967621)

- 名前が63文字の制限を超えるクラスターサービスバージョン（CSV）は、無効な**ownerref**ラベルを引き起こします。以前は、Operator Lifecycle Manager（OLM）が**ownerref**参照を使用して、クラスターロールバインディングを含む所有リソースを取得すると、ラベルが無効であるため、リスターはnamespace内のすべてのクラスターロールバインディングを返しました。このバグ修正により、OLMが更新され、別の方法を使用してサーバーが無効な**ownerref**ラベルを代わりに拒否できるようになります。その結果、CSVの名前が無効な場合、OLMはクラスターロールバインディングを削除しなくなりました。(BZ#1970910)

- 以前は、Operator の依存関係は、インストール後に常に永続化されませんでした。依存関係を宣言するOperatorをインストールした後、同じnamespace内でのその後の更新とインストールは、以前にインストールされたOperatorの依存関係を尊重できない可能性があります。このバグ修正により、依存関係は、Operatorの宣言されたすべてのプロパティとともに、Operatorの**ClusterServiceVersion**（CSV）オブジェクトのアノテーションに保持されるようになりました。その結果、インストールされたOperatorの宣言された依存関係は、今後のインストールでも引き続き尊重されます。(BZ#1978310)

- 以前は、非推奨のバンドルでOperatorを削除すると、非推奨の履歴がガベージコレクションに含まれていませんでした。その結果、Operatorを再インストールした場合、バンドルバージョンは非推奨のテーブルを表示していました。今回の更新では、非推奨のバンドルのガベージコレクションを改善し、問題を修正しています。(BZ#1982781)

- 以前は、クラスターのz-streamバージョンがOperatorの互換性の計算に使用されていました。その結果、OpenShift Container Platformのマイクロリリースがブロックされました。この更新では、Operatorの互換性の比較でクラスターのz-streamバージョンを無視することにより、この問題を修正しています。(BZ#1993286)

OpenShift API サーバー

- 以前は、サービスの検出エンドポイントへの単一の失敗した要求により、Operatorは**Available=False**を報告する可能性がありました。耐障害性を高めるために、一連の改善が導入され、さまざまな一時的なエラーによる更新中に、一部のOperator が**Available=False** を報告しないようにしました。(BZ#1948089)

OpenShift Update Service

- 以前は、Webコンソールから更新サービスアプリケーションを作成すると、無効なホストエラーが発生していました。これは、デフォルトのOpenShift Update Service（OSUS）アプリケーション名が長すぎるために発生していました。デフォルト名が短く設定され、エラーは発生しなくなりました。(BZ#1939788)

Red Hat Enterprise Linux CoreOS (RHCOS)

- 以前は、systemd は**/etc/kubernetes**内の環境ファイルを読み取ることができませんでした。これは、SELinuxポリシーが原因で、その結果、kubeletが起動しませんでした。ポリシーが変更されました。kubeletが起動し、環境ファイルが読み込まれます。(BZ#1969998)

- ECKD DASDが接続されたs390xカーネル仮想マシン（KVM）では、DASDは通常のvirtioストレージデバイスのように見えますが、VTOCが削除されるとアクセスできなくなります。その結果、KVMにRed Hat Enterprise Linux CoreOS（RHCOS）をインストールする際は、DASDをvirtioブロックデバイスとして使用できませんでした。**coreos-installer** プログラムが更新され、インストール先がKVMに接続されたECKD DASDなどのvirtioストレージデバイスである場合に、VTOC形式のパーティションテーブルを使用してRed Hat Enterprise Linux CoreOS (RHCOS)をインストールするようになりました。(BZ#1960485)

- 以前は、**NetworkManager-wait-online-service**のタイムアウトが早すぎたため、**coreos-installer** プログラムの起動前に接続を確立できませんでした。その結果、ネットワークの起動に時間がかかりすぎると、**coreos-installer**プログラムはIgnition設定をフェッチできませんでした。今回の更新で、**NetworkManager-wait-online-service**タイムアウトがデフォルトのアップストリーム値まで増えました。その結果、**coreos-installer**プログラムがIgnition設定のフェッチに失敗することはなくなりました。(BZ#1967483)

Routing (ルーティング)

- 以前は、Cluster Network Operator（CNO）がプロキシ設定（特に **no_proxy** 設定）をサニタイズしようとすると、設定はドリフトされました。これにより、特定のIPv6 CIDRが**no_proxy**にはありませんでした。この修正により、すべてのシナリオでデュアルスタック

（IPV4およびIPV6）を更新するロジックが実装されます。(BZ#1981975)

- 以前は、**dns.config.openshift.io** Operatorの**.spec.privateZone**フィールドに誤って入力し、Ingress Operatorがプライベートホストゾーンを見つけることができないようにした場合、Ingress Operatorの機能が低下していました。ただし、**.spec.privateZone** フィールドを修正した後でも、Ingress Operator の機能は低下したままでした。Ingress Operatorはホストゾーンを検索し、**.apps**リソースレコードを追加しますが、Ingress Operatorはパフォーマンスが低下したステータスをリセットしません。この修正により、DNS設定オブジェクトが監視され、**spec.privateZone**フィールドに関する変更が監視されます。適切なロジックを適用し、Operator ステータスを適宜更新します。適切な**.spec.privateZone**フィールドが設定されると、Operatorのステータスはdegradedまたは**False**に戻ります。(BZ#1942657)

サンプル

- 以前は、接続タイムアウトがないため、遅延が長くなりました。これは、**managementState** が **Removed** に設定されているCluster Samples Operatorが、**registry.redhat.io**への接続をテストしたときに発生しました。接続タイムアウトを追加すると、遅延がなくなります。(BZ#1990140)

ストレージ

- 以前は、使用中のPVで**LocalVolumeSets**を削除できましたが、手動でクリーンアップする必要がありました。この修正により、リリースされたすべてのPVが自動的にクリーンアップされます。(BZ#1862429)

- 以前は、**oc get volumesnapshotcontent**コマンドは、ボリュームスナップショットのnamespaceを表示しませんでした。これは、ボリュームスナップショットが一意に識別されなかったことを意味します。このコマンドにより、ボリュームスナップショットのnamespaceが表示されます。(BZ#1965263)

- 以前のバージョンでは、Manila CSI Operator は自己署名証明書を使用する Red Hat OpenStack Platform (RHOSP)エンドポイントとの通信時にカスタムトランスポートを使用していました。このカスタムトランスポートはプロキシー環境変数を使用していなかったため、Manila CSI Operator は Manila の通信に失敗しました。この更新により、カスタムトランスポートがプロキシー環境変数を使用するようになります。その結果、Manila CSI Operator がプロキシーおよびカスタム CA 証明書とともに機能するようになりました。(BZ#1960152)

- 以前のバージョンでは、Cinder CSI ドライバー Operator は Red Hat OpenStack Platform (RHOSP) API に接続する設定済みのプロキシーを使用しないため、インストールが失敗する可能性がありました。今回の更新により、プロキシー環境変数がコンテナーに設定されるように、アノテーションが Cinder CSI Driver Operator デプロイメントに含まれるようになりました。その結果、インストールは失敗しなくなりました。(BZ#1985391)

- Local Storage Operator が新規に追加されたブロックデバイスを検査する頻度は、CPU 消費を減らすために 5 秒から 60 秒に変更されました。(BZ#1994035)

- 以前のバージョンでは、Manila CSI Operator との通信の失敗により、クラスターが低下しました。今回の更新により、Manila CSI Operator エンドポイントとの通信に失敗し、致命的ではないエラーが生じました。その結果、Manila CSI Operator は、クラスターを低下させる代わりに無効になります。(BZ#2001958)

- 以前のバージョンでは、Local Storage Operator は 10 秒の遅延で孤立した永続ボリューム(PV)を削除し、遅延は累積的でした。複数の永続ボリュームクレーム（PVC）が同時に削除されると、PVが削除されるまでに数分または数時間かかる場合があります。そのため、対応するローカルディスクは数時間の新しい PVC で利用できませんでした。今回の修正により、10 秒の遅延が削除されました。その結果、PV は検出され、対応するローカルディスクが新規 PVC について利用可能になります。(BZ#2007684)

Web コンソール（Administrator パースペクティブ）

- 以前は、**PF4**テーブルのすべての行が再レンダリングされていました。今回の更新では、**React.memo**のコンテンツがラップされたため、すべてのスクロールイベントでコンテンツが再レンダリングされることはありません。(BZ#1856355)

- 以前は、OpenShift Container Platform Webコンソールのクラスター使用率のチャートに、データの期間がわかりにくい方法で表示されていました。たとえば、6時間の期間オプションが選択されているが、データは最後の3時間のみ存在する場合、これらの3つのデータポイントはチャート全体を埋めるように引き伸ばされます。最初の3時間は表示されません。これにより、チャートが6時間の全期間を示していると想定される可能性があります。混乱を避けるために、チャートには情報が不足していることを示す空白が表示されるようになりました。この例では、チャートには6時間の期間全体が表示され、データは4時間目から始まっています。最初の3時間は空白です。(BZ#1904155)

- 以前は、**NetworkPolicy**は、Webコンソールで韓国語または中国語に翻訳されていませんでした。今回の更新で、韓国または中国語でWebコンソールを表示する際に、**NetworkPolicy** が正しく翻訳されるようになりました。(BZ#1965930)

- 以前は、**Console Overview** セクションの**Needs Attention**状態の問題により、Operatorはアップグレード中でなくても**upgrading**と表示されていました。この更新により、**Needs Attention**状態が修正され、Operatorの正しいステータスが表示されるようになります。(BZ#1967047)

- 以前は、失敗したCluster Service Version（CSV）のアラートに、失敗したCSVのトラブルシューティングに役立たない一般的な**status.message**が表示されていました。今回の更新により、コピーされたCSVには、トラブルシューティングに役立つメッセージと元のCSVへのリンクが表示されます。(BZ#1967658)

- 以前は、ユーザーはキーボードを使用して、マストヘッドのドロップダウンオプションを使用できませんでした。この更新により、ユーザーはキーボードを使用して、ドロップダウンオプションにアクセスできるようになりました。(BZ#1967979)

- 以前は、Operator所有のリソースをその所有者と一致させるために使用されるユーティリティ関数が、誤った一致を返していました。その結果、Operator所有のリソースページの**Managed by**リンクは、誤ったURLにリンクすることがありました。この修正により、所有するOperatorと正しく一致するように関数ロジックが更新されます。その結果、**Managed by**リンクが正しいURLにリンクされるようになりました。(BZ#1970011)

- 以前は、**OperatorHub**Webコンソールインターフェイスにより、ユーザーは無関係のインストールプランに誘導されていました。今回の更新では、**OperatorHub** は Operator **Subscription** のdetails タブにユーザーをリンクし、これにより、インストールの進捗状況が表示されるようになりました。(BZ#1970466)

- 以前は、**OAuth** の詳細ページの追加ドロップダウンリストのアイテムは、国際化されていませんでした。今回の更新で、これらのアイテムは国際化され、英語を母語としないユーザーのユーザーエクスペリエンスが改善されました。(BZ#1970604)

- 以前は、無効なローカリゼーションプロパティにより、一部のメッセージを国際化できませんでした。今回の更新で、無効なプロパティーが削除されました。その結果、これらのメッセージは国際化され、英語を母語としないユーザーのユーザーエクスペリエンスが改善されました。(BZ#1970980)

- この更新により、リストページのリソースリンクにマウスをかざした際に表示されていたツールチップが削除されます。これは、表示されていた情報によって、ユーザーエクスペリエンスが向上することがなかったためです。(BZ#1971532)

- 以前のバージョンでは、コンソール Pod は **preferredDuringSchedulingIgnoredDuringExecution** の非アフィニティールールでデプロイされていたため、両方のコンソール Pod が同じコントロールプレーンノードでスケジュールされることがありました。この修正により、ルールは **requiredDuringSchedulingIgnoredDuringExecution** に変更され、条件が一致した場合にPodが別々のノードでスケジュールされるようになりました。(BZ#1975379)

- 以前は、Operatorをアンインストールしても、有効なプラグインをすべて削除できませんでした。このリリースでは、Operatorをアンインストールすると、有効になっているすべてのプラグインが削除されるようになりました。(BZ#1975820)

- 以前は、フロントエンドのOperator Lifecycle Manager（OLM）記述子の処理では、最初のx記述子のみを使用して、オペランドの詳細ページにプロパティをレンダリングしていました。その結果、プロパティに複数のx記述子が定義されていて、リストの最初のx記述子が無効またはサポートされていない場合、期待どおりにレンダリングされませんでした。この修正により、記述子検証ロジックが更新され、サポートされていないx記述子よりもサポートされているx記述子が優先されます。そのため、記述子で装飾されたプロパティは、一覧にある最初の有効かつサポートされているx記述子を使用して、**Operand** の詳細ページでレンダリングされます。(BZ#1976072)

- 以前は、文字列データがエンコードされたシークレットに使用されていました。その結果、バイナリシークレットデータがWebコンソールによって適切にアップロードされませんでした。この更新では、シークレットがエンコードされ、APIで文字列データの代わりにデータが使用されます。その結果、バイナリシークレットが適切にアップロードされるようになりました。(BZ#1978724)

- 以前は、クラスターで実行されているプロセスが手動で終了された場合、ターミナルの **ps -aux** コマンドは、一部のプロセスがクリアされなかったことを示していました。これにより、迷子のプロセスが残り、クラスターが無効な状態のままとなりました。この修正により、すべてのプロセスがクラスター上で正しく終了し、ターミナルに記載されているアクティブなプロセスのリストに表示されないようになります。(BZ#1979571)

- 以前のバージョンでは、デフォルトのプルシークレットが新規プロジェクトに追加され、複数のレジストリーの認証情報がアップロードされると、最初の認証情報のみが **Project Details** ページに表示されていました。また、一覧が切り捨てられていることを示すものはありませんでした。その結果、ユーザーが **Default pull secret** からプロジェクトの詳細をクリックすると、最初の認証情報のみが一覧表示されました。今回の修正により、すべての認証情報が一覧表示されるようになり、現在のページに一覧表示されていない場合には、追加の認証情報が存在することをユーザーに通知します。(BZ#1980704)

- 以前のバージョンでは、ユーザーがデフォルトのブラウザー言語を簡体字中国語に変更すると、Web コンソールの **Overview** ページのクラスター使用率リソースメトリックスが、英語と簡体字中国語の組み合わせで表示されていました。今回の修正により、選択された言語のみで、クラスター使用率リソースを表示できるようになりました。(BZ#1982079)

- 以前のバージョンでは、言語が簡体字中国語に変更された場合に、クラスター使用率の使用統計が、左側のメニューにある **project**、**pod**、および**node**の翻訳と一致しませんでした。この修正により、簡体字中国語の翻訳が修正され、クラスター使用率のメトリックスが**top consumers**フィルターと一致するようになります。(BZ#1982090)

- 以前のバージョンでは、サービスアカウントからのデフォルトのプルシークレットではなく、エラーがユーザーに表示されていました。その結果、プロジェクトの詳細画面の情報が不完全になりました。ユーザーは、デフォルトのプルシークレットの一覧全体を表示するために、デフォルトの ServiceAccount に移動する必要がありました。この修正により、ユーザーはプロジェクトの詳細ページで、デフォルトのServiceAccountからプルシークレットのリスト全体を表示できるようになります。(BZ#1983091)

- 以前は、ターミナルタブを表示している際に、ノードまたはPodのWebページのサイズを変更すると、ブラウザに2つの垂直スクロールバーが表示されることがありました。コンソールが更新され、ウィンドウのサイズが変更されると、スクロールバーが1つだけ表示されるようになりました。(BZ#1983220)

- 以前は、シングルノード開発者プロファイルを使用してOpenShift Container Platform 4.8.2をインストールするときに、Webコンソールがデプロイされませんでした。インストール計画が作成されていたnamespaceに対して、有効なOperatorグループまたはサービスアカウントが検出されなかった場合、インストール計画は失敗状態になりました。これ以上の試みは行われませんでした。このリビジョンでは、失敗したインストールプランは、Operatorグループまたはサービスアカウントが検出されるまで、再度実行されるように設定されています。(BZ#1986129)

- 以前は、イベントダッシュボードで、**More** および **Show Less** が国際化されていなかったため、ユーザーエクスペリエンスは十分ではありませんでした。今回の更新で、テキストは国際化対応となりました。(BZ#1986754)

- 以前は、コンソールページでサービスの完全修飾ドメイン名（FQDN）を構築するロジックがありませんでした。その結果、サービスの詳細ページにFQDN情報が表示されませんでした。今回の更新で、FQDN を構成するロジックが追加され、サービスの FQDN 情報がページで利用できるようになります。(BZ#1996816)

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、タイプ **sink** の kamelets は、ソース kamelets とともにイベントソースのカタログに表示されていました。現在のリリースでは、イベントソースのカタログにはタイプ **source** kamelets のみが表示されます。(BZ#1971544)

- 以前のバージョンでは、ログファイルには改行なしで 1 行に情報が含まれていました。現在のリリースでは、ログファイルに予想される改行が含まれ、ログヘッダーの前後に改行が追加されています。(BZ#1985080)

1.7. テクノロジープレビューの機能

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

テクノロジープレビュー機能のサポート範囲

以下の表では、機能は以下のステータスでマークされています。

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

表1.3 テクノロジープレビュートラッカー

機能	OCP 4.7	OCP 4.8	OCP 4.9
Precision Time Protocol (PTP)	TP	TP	TP

機能	OCP 4.7	OCP 4.8	OCP 4.9
oc CLI プラグイン	TP	GA	GA
Descheduler	GA	GA	GA
メモリー使用率のための HPA	GA	GA	GA
サービスバインディング	TP	TP	TP
Cinder での raw ブロック	TP	GA	GA
CSI ボリュームスナップショット	GA	GA	GA
CSI ボリューム拡張	TP	TP	TP
vSphere Problem Detector Operator	GA	GA	GA
CSI Azure Disk Driver Operator	-	TP	TP
CSI Azure Stack Hub Driver Operator	-	-	GA
CSI GCP PD Driver Operator	TP	GA	GA
CSI OpenStack Cinder Driver Operator	GA	GA	GA
CSI AWS EBS ドライバー Operator	TP	TP	GA
CSI AWS EFS Driver Operator	-	-	TP
CSI の自動移行	-	TP	TP
CSI インラインの一時ボリューム	TP	TP	TP
CSI vSphere Driver Operator	-	TP	TP
Local Storage Operator を使用した自動デバイス検出およびプロビジョニング	TP	TP	TP
OpenShift Pipeline	TP	GA	GA
OpenShift GitOps	TP	GA	GA
OpenShift サンドボックスコンテナー	-	TP	TP
Vertical Pod Autoscaler	TP	GA	GA

機能	OCP 4.7	OCP 4.8	OCP 4.9
Cron ジョブ	TP	GA	GA
PodDisruptionBudget	TP	GA	GA
kvc を使用したノードへのカーネルモジュールの追加	TP	TP	TP
egress ルーター CNI プラグイン	TP	GA	GA
スケジューラーのプロファイル	TP	TP	GA
プリエンプションを実行しない優先順位クラス	TP	TP	TP
Kubernetes NMState Operator	TP	TP	TP
支援付きインストーラー	TP	TP	TP
AWS Security Token Service (STS)	TP	GA	GA
Kdump	TP	TP	TP
OpenShift Serverless	-	GA	GA
Serverless functions	-	TP	TP
Data Plane Development Kit (DPDK) サポート。	TP	TP	GA
Memory Manager機能	-	-	TP
CNI VRF プラグイン	TP	TP	GA
クラスタクラウドコントローラマネジャ Operator	-	-	GA
AWS 用クラウドコントローラーマネージャー	-	-	TP
Azure 用クラウドコントローラーマネージャー	-	-	TP
OpenStack 用クラウドコントローラーマネージャー	-	-	TP
ドライバツールキット	-	TP	TP
Special Resource Operator(SRO)	-	-	TP
Node Health Check Operator	-	-	TP

1.8. 既知の問題

- OpenShift Container Platform 4.1 では、匿名ユーザーは検出エンドポイントにアクセスできました。後のリリースでは、一部の検出エンドポイントは集約された API サーバーに転送されるため、このアクセスを無効にして、セキュリティーの脆弱性の可能性を減らすことができます。ただし、既存のユースケースに支障がで出ないように、認証されていないアクセスはアップグレードされたクラスターで保持されます。
  OpenShift Container Platform 4.1 から 4.8 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)

- クラスター管理者は、503、404、または両方のエラーページのカスタムHTTPエラーコード応答ページを指定できます。カスタムエラーコードの応答ページに適した形式を指定しない場合は、ルーター Pod が停止し、解決されません。ルーターは、カスタムのエラーコードページの更新を反映するようにリロードされません。回避策として、**oc rsh** コマンドを使用してルーター Pod にローカルでアクセスできます。次に、カスタム http エラーコードページを提供するすべてのルーター Pod で **reload-haproxy** を実行します。

  ```
  $ oc -n openshift-ingress rsh router-default-6647d984d8-q7b58
  sh-4.4$ bash -x /var/lib/haproxy/reload-haproxy
  ```

  または、ルートにアノテーションを付け、リロードを強制的に実行できます。(BZ#1990020), (BZ#2003961)

- Open Virtual Network (OVN) のバグにより、Octavia ロードバランサーで永続的な接続の問題が発生します。Octavia ロードバランサーが作成されると、OVN はそれらを一部の Neutron サブネットにプラグインしない可能性があります。これらのロードバランサーは、Neutron サブネットの一部では到達できなくなる可能性があります。この問題は、Kuryr の設定時に各 OpenShift namespace に作成される Neutron サブネットに影響を与えます。その結果、この問題が発生すると、OpenShift **Service** オブジェクトを実装するロードバランサーが問題の影響を受ける OpenShift namespace から到達できなくなります。このバグにより、Kuryr SDN を使用する OpenShift Container Platform 4.8 デプロイメントの使用は、OVN および OVN Octavia が設定された Red Hat OpenStack Platform (RHOSP) 16.1 では推奨されません。これは、RHOSP の今後のリリースで修正されます。(BZ#1937392)

- Kuryr を使用した Red Hat OpenStack Platform(RHOSP)へのインストールは、RHOSP API にアクセスするためにクラスター全体のプロキシーが必要な場合にクラスター全体のプロキシーで設定されている場合は機能しません。(BZ#1985486)

- 競合状態により、Red Hat OpenStack Platform(RHOSP)クラウドプロバイダーが適切に起動しないことがあります。そのため、LoadBalancer サービスは **EXTERNAL-IP** セットを取得できない場合があります。一時的な回避策として、BZ#2004542 で説明されている手順に従って kube-controller-manager Pod を再起動することができます。

- **ap-northeast-3** AWS リージョンは、サポートされる AWS リージョンである場合でも、OpenShift Container Platform のインストール時にインストールプログラムのオプションとしては提供されません。一時的な回避策として、インストールプロンプトで別の AWS リージョンを選択し、クラスターをインストールする前に、生成された **install-config.yaml** ファイルでリージョン情報を更新できます。(BZ#1996544)

- クラスターを **us-east-1** リージョンの AWS にインストールする場合、ローカルの AWS ゾーンは使用できません。一時的な回避策として、クラスターのインストール時に **install-config.yaml** ファイルにローカル以外のアベイラビリティーゾーンを指定する必要があります。(BZ#1997059)

- OpenShift Container Platformは、公的に信頼されている認証局（CA）によって署名された証明書で保護されている、ARMエンドポイントなどのパブリックエンドポイントを備えたAzure Stack Hubにのみインストールできます。内部 CA のサポートは、今後の OpenShift Container Platform の z-stream リリースに追加されます。(BZ#2012173)

- クラスター管理者は、503、404、または両方のエラーページのカスタムHTTPエラーコード応答ページを指定できます。ルーターは、カスタムのエラーコードページの更新を反映するようにリロードされません。回避策として、ルーターPodでrshを実行し、カスタムhttpエラーコードページを提供するすべてのルーターPodで**reload-haproxy**を実行します。

```
$ oc -n openshift-ingress rsh router-default-6647d984d8-q7b58
sh-4.4$ bash -x /var/lib/haproxy/reload-haproxy
```

または、ルートにアノテーションを付け、リロードを強制的に実行できます。(BZ#1990020)

- 本リリースには既知の問題が含まれています。OpenShift OAuth ルートのホスト名および証明書をカスタマイズする場合、Jenkins は OAuth サーバーエンドポイントを信頼しなくなりました。そのため、ユーザーは、アイデンティティーおよびアクセスを管理する OpenShift OAuth 統合に依存する場合に、Jenkins コンソールにログインできません。現時点では、回避策は利用できません。(BZ#1991448)

- 特定のカーディナリティの高い監視メトリックが誤って削除されたため、このリリースでは、**pod**、**qos**、および**System**のコンテナパフォーマンスの入力および出力メトリックは使用できません。
この問題に対する回避策はありません。実稼働環境のワークロードのこれらのメトリクスを追跡するには、初期 4.9 リリースにアップグレードしないでください。(BZ#2008120)

- Special Resource Operator (SRO)は、ソフトウェア定義ネットワークポリシーにより、Google Cloud Platform へのインストールに失敗する可能性があります。その結果、simple-kmod Pod は作成されません。これは、OpenShift Container Platform 4.9.4 リリースで修正されています。(BZ#1996916)

- OpenShift Container Platform 4.9 では、クラスターロールを持つユーザーは、デプロイメントまたはデプロイメント設定の編集権限がない場合、コンソールを使用してデプロイメントまたはデプロイメント設定をスケーリングできません。(BZ#1886888)

- OpenShift Container Platform 4.9 では、**Developer Console** に最小限のデータまたはデータがない場合、大半のモニタリングチャートまたはグラフ (CPU 消費、メモリー使用量、および帯域幅など) には -1 から 1 の範囲が表示されます。ただし、これらの値はいずれもゼロ未満となる可能性があるため、負の値は正しくありません。(BZ#1904106)

- **cgroups** の不一致により **ip vrf exec** コマンドは機能しません。そのため、このコマンドは OpenShift Pod 内では使用できません。VRF (Virtual Routing and Forwarding) を使用するには、アプリケーションを VRF に対応する 必要があり、VRF インターフェースに直接バインドする必要があります。(BZ#1995631)

- NonUniform Memory Access (NUMA)のバグにより、コンテナーに対して不必要な NUMA ピニングが発生する可能性があり、レイテンシーやパフォーマンスが低下する可能性があります。Topology Managerは、**single-numa-node**トポロジ管理ポリシーが満たすことができるリソースを使用して、コンテナーを複数のNUMAノードに固定できます。コンテナーは、Quality of Service (QoS) Podの下に固定されます。回避策として、コンテナーのメモリーリソース要求が **single-numa-node** ポリシーよりも大きな場合は、Guaranteed QoS Pod を起動しないでください。(BZ#1999603)

- 時折、削除用に選択される Pod が削除されることがありました。これは、クラスターがリソース不足になると発生します。リソースを回収するために、システムは削除用に 1 つ以上の Pod を選択します。リソースが少ないと処理が遅くなるため、削除操作が設定された削除の猶予期間を超えて失敗する可能性があります。これが実行される場合は、Pod を手動で削除します。その後、クラスターは解放されたリソースを回収します。(BZ#1997476)

- 断続的に、ポッドは**ContainerCreating**状態でハングし、Open vSwitch（OVS）ポートバインディングを待機している間にタイムアウトする可能性があります。報告されたイベントは、**failed to configure pod interface: timed out waiting for OVS port binding**です。この問題は、OVN-Kubernetes プラグイン用に多くの Pod が作成されると発生する可能性があります。(BZ#2005598)

- 出力ノードを再起動した後、**lr-policy-list**には、レコードの重複や内部IPアドレスの欠落などのエラーが含まれています。期待される結果は、**lr-policy-list**が出力ノードをリブートする前と同じレコードを持つことです。回避策として、**ovn-kubemaster** Podを再起動できます。(BZ#1995887)

- 分散ゲートウェイポートが含まれる論理ルーターで IP マルチキャストリレーが有効になっている場合は、分散ゲートウェイポート上でマルチキャストトラフィックが正しく転送されません。その結果、OVN-Kubernetes の IP マルチキャスト機能が壊れています。(BZ#2010374)

- Web コンソールの **Administrator** パースペクティブでは、ノードの一覧を表示することが可能なページは、ノードの一覧が利用可能になる前にレンダリングされます。これにより、ページが応答しなくなります。回避策はありませんが、この問題は今後のリリースで対処されます。(BZ#2013088)

- Operator Lifecycle Manager (OLM)は、タイムスタンプチェックと廃止された API 呼び出しの組み合わせを使用します。これは **skipRange** アップグレードでは機能せず、特定のサブスクリプションのアップグレードを実行する必要があるかどうかを判断します。**skipRange** アップグレードを使用する Operator の場合は、解決までに最大 15 分かかるアップグレードプロセスには遅延があり、さらに長くブロックされる可能性があります。
  回避策として、クラスター管理者は **openshift-operator-lifecycle-manager** namespace で **catalog-operator** Pod を削除できます。これにより、Pod が自動的に再作成され、**skipRange** アップグレードがトリガーされます。(BZ#2002276)

- 現在、FIPSモードを有効にしてGoogle Cloud PlatformでRed Hat Enterprise Linux（RHEL）8を起動すると、Red Hat Update Infrastructure（RHUI）からパッケージをインストールしようとすると、RHEL8はメタデータのダウンロードに失敗します。一時的な回避策として、RHUIリポジトリーを無効にして、Red Hat Subscription Management を使用してコンテンツを取得できます。(BZ#2001464), (BZ#1997516).

- OpenShift Container Platformのシングルノードのリブートに続いて、すべての Pod が再起動します。これにより、大きな負荷が発生し、通常の Pod 作成時間が長くなります。これは、Container Network Interface (CNI)が **pod add** イベントを素早く処理できないために発生します。**timed out waiting for OVS port binding** エラーメッセージが表示されます。OpenShift Container Platform の単一ノードインスタンスは最終的には想定よりも遅くなります。(BZ#1986216)

- MetalLB が OVN-Kubernetes Container Network Interface ネットワークプロバイダーを使用してレイヤー 2 モードで実行される場合、スピーカー Pod がARPまたはNDP要求に応答する単一ノードではなく、クラスター内のすべてのノードが要求に応答します。予期しない ARP 応答の数は、ARP スプーフィング攻撃のようになります。エクスペリエンスは設計とは異なりますが、ホストまたはサブネット上のソフトウェアが ARP をブロックするように構成されていない限り、トラフィックはサービスにルーティングされます。このバグは、今後の OpenShift Container Platform リリースで修正されます。(BZ#1987445)

- Tangディスク暗号化と静的IPアドレス構成がVMWare vSphereユーザープロビジョニングインフラストラクチャクラスターに適用されると、ノードは最初にプロビジョニングされた後、正しく起動できません。(BZ#1975701)

- オペレーターは、Operator Lifecycle Manager（OLM）をローカルソースから実行するために、関連するイメージをリストする必要があります。現在、**ClusterServiceVersion** (CSV) オブジェクトの**relatedImages**パラメーターが定義されていない場合、**opm render**は関連するイメージにデータを入力しません。これは、今後のリリースで修正される予定です。(BZ#2000379)

- 以前は、Open vSwitch（OVS）は各OpenShift Container Platformクラスターノードのコンテナーで実行され、ノードエクスポーターエージェントはノードからOVS CPUおよびメモリメトリックを収集していました。OVS は systemd ユニットとしてクラスターノードで実行され、メ

トリクスは収集されなくなりました。これは、今後のリリースで修正される予定です。OVSパケットメトリックは引き続き収集されます。(BZ#2002868)

- OpenShift Container Platform Webコンソールの**Storage → Overview**ページを表示または非表示にするために使用されるフラグが正しく設定されていません。その結果、OpenShift Cluster Storage を含むクラスターのデプロイ後に概要ページが表示されません。これは、今後のリリースで修正される予定です。(BZ#2013132)

- OpenShift Container Platform 4.6 以降では、プルのイメージ参照は、以下の Red Hat レジストリーを指定する必要があります。

  - **registry.redhat.io**
  - **registry.access.redhat.com**
  - **quay.io**

  それらのレジストリーが指定されていない場合、ビルド Pod はイメージをプルできません。

  回避策として、イメージのプル仕様で **registry.redhat.io/ubi8/ubi:latest** や **registry.access.redhat.com/rhel7.7:latest** などの完全修飾名を使用します。

  オプションで、イメージの短縮名を許可するレジストリーを追加 して、イメージレジストリー設定を更新できます。(BZ#2011293)

- OpenShift Container Platform 4.8 以前のデフォルトのロードバランシングアルゴリズムは**leastconn** でした。パススルーでないルートの場合、OpenShift Container Platform 4.8.0ではデフォルトが**random**に変更されました。**random**に切り替えると、長時間のウェブソケット接続を使用する必要がある環境では、メモリ消費量が大幅に増加するため、互換性がありません。この大幅なメモリ消費を軽減するために、OpenShift Container Platform 4.9 では、デフォルトのロードバランシングアルゴリズムが **leastconn** に戻されました。大幅なメモリ使用量を発生させないソリューションが開発されれば、OpenShift Container Platformの将来のリリースでデフォルトが**random**に変更される予定です。
  以下のコマンドを入力することで、デフォルトの設定を確認することができます。

  ```
  $ oc get deployment -n openshift-ingress router-default -o yaml | grep -A 2
  ROUTER_LOAD_BALANCE_ALGORITHM
        - name: ROUTER_LOAD_BALANCE_ALGORITHM
          value: leastconn
  ```

  randomのオプションはまだ利用可能です。しかし、このアルゴリズムの選択の恩恵を受けたいルートは、以下のコマンドを入力して、ルートごとにアノテーションでそのオプションを明示的に設定する必要があります。

  ```
  $ oc annotate -n <NAMESPACE> route/<ROUTE-NAME>
  "haproxy.router.openshift.io/balance=random"
  ```

  (BZ#2015829)

- ローカルレジストリーでホストされるイメージが指定されると、**oc adm release extract --tools** コマンドが失敗します。(BZ#1823143)

- OpenShift Container Platformのシングルノード構成では、リアルタイムカーネル (**kernel-rt**) を使用した場合、非リアルタイムカーネルを使用した場合に比べて Pod の作成に 2 倍以上の時間がかかります。**kernel-rt** を使用した場合、ノードの再起動後のリカバリータイムが影響を受けるため、Pod の作成に時間がかかり、サポートされる Pod の最大数に影響が出ます。

回避策として、**kernel-rt** を使用する場合は、**rcupdate.rcu_normal_after_boot=0** カーネル引数で起動することで、復旧時間を短縮できます。これには、リアルタイムカーネルバージョン **kernel-rt-4.18.0-305.16.1.rt7.88.el8_4** 以上が必要です。この既知の問題は、OpenShift Container Platform のバージョン 4.8.15 以上に該当します。(BZ#1975356)

- OpenShift Container Platformのシングルノードのリブートに続いて、すべての Pod が再起動します。これにより、大きな負荷が発生し、通常の Pod 作成時間が長くなります。これは、Container Network Interface (CNI)が **pod add** イベントを素早く処理できないために発生します。**timed out waiting for OVS port binding** エラーメッセージが表示されます。OpenShift Container Platform の単一ノードインスタンスは最終的は復帰しますが、想定よりも遅くなります。この既知の問題は、OpenShift Container Platform のバージョン 4.8.15 以上に該当します。(BZ#1986216)

- **bootkube** が **oc** を使用して、クラスターのブートストラッププロセスの最後の方に使用しようとする SNO クラスターのプロビジョニング中にエラーが発生します。kube API はシャットダウン要求を受け取り、これによりクラスターのブートストラッププロセスが失敗します。(BZ#2010665)

- 同じホストへの 4.8 デプロイメントに成功した後に OpenShift Container Platform バージョン 4.9 SNO クラスターをデプロイすると、ブートテーブルエントリーが変更されたために失敗します。(BZ#2011306)

- 受信トレイ iavf ドライバーが不安定であるという問題があります。これは、DPDK ベースのワークロードが OpenShift Container Platform バージョン 4.8.5 にデプロイされている場合に明らかです。この問題は、RHEL for Real Time 8 を実行しているホストに DPDK ワークロードがデプロイされている場合にも明らかです。この問題は、Intel XXV710 NIC がインストールされているホストで発生します。(BZ#2000180)

- クロックジャンプエラーは、PTP Operator によってデプロイされる **linuxptp** サブシステムで発生します。**clock jumped backward or running slower than expected!** というエラーメッセージが報告されます。OpenShift Container Platform バージョン 4.8 または 4.9 クラスターに Intel Columbiaville E810 NIC がインストールされているホストでエラーが発生します。このエラーは、**linuxptp** サブシステムのエラーではなく、Intel ice ドライバー関連のエラーである可能性が高いです。(BZ#2013478)

- DU ノードのゼロタッチプロビジョニング(ZTP)のインストール時に Operator のインストールが失敗する場合があります。**InstallPlan** API はエラーを報告します。報告されたエラーメッセージは **Bundle unpacking failed** です。理由： **DeadlineExceeded**.このエラーは、Operator インストールジョブが 600 秒を超えると発生します。
  回避策として、失敗した Operator に対して以下の **oc** コマンドを実行して、Operator のインストールを再試行します。

  1. カタログソースを削除します。

     ```
     $ oc -n openshift-marketplace delete catsrc <failed_operator_name>
     ```

  2. インストール計画を削除します。

     ```
     $ oc -n <failed_operator_namespace> delete ip <failed_operator_install_plan>
     ```

  3. サブスクリプションを削除し、Operator **CatalogSource** および **Subscription** リソースが、関連するカスタムリソースポリシーによって再作成されるのを待ちます。

     ```
     $ oc -n <failed_operator_namespace> delete sub <failed_operator_subscription>
     ```

想定される結果

Operator **InstallPlan** および **ClusterServiceVersion** リソースが作成され、Operator がインストールされている。

(BZ#2021456)

- SR-IOV Operator と Machine Config Operator(MCO)の間に競合状態が存在します。これは、DU ノードの ZTP インストールプロセス中に断続的に発生し、さまざまな形で現れます。競合状態により、以下のエラーが生じる可能性があります。
  - ZTP インストールプロセスが DU ノードのプロビジョニングを終了すると、パフォーマンスプロファイルの設定が適用されない場合があります。ZTP インストールプロセスで DU ノードのプロビジョニングが終了すると、パフォーマンスプロファイル設定はノードに適用されず、**MachineConfigPool** リソースは **Updating** 状態のままになります。
    回避策として、以下の手順を実施してください。
    1. 障害が発生した DU ノードの名前を取得します。

       ```
       $ oc get mcp
       ```

       出力例

       ```
       NAME              CONFIG                                   UPDATED   UPDATING   DEGRADED
       control-plane-1   rendered-control-plane-1-90fe2b00c718    False     True       False
       compute-1         rendered-compute-1-31197fc6da09          True      False      False
       ```

    2. 障害が発生したノードの遮断を解除し、**machine-config-daemon** がパフォーマンスプロファイルを適用するまで待機します。以下は例になります。

       ```
       $ oc adm uncordon compute-compute-1-31197fc6da09
       ```

       想定される結果

       machine-config-daemon は、パフォーマンスプロファイル設定をノードに適用します。
  - パフォーマンスプロファイル設定が、DU ノードの設定時に適用されないことがあります。回避策として、DU ノードにポリシーを適用するシーケンスを変更します。Machine Config Operator(MCO)および Performance Addon Operator(PAO)ポリシーを最初に適用してから、SR-IOV ポリシーを適用します。
  - DU ノードのポリシー設定時に、再起動に数十分かかる場合があります。このインスタンスの回避策は必要ありません。システムは最終的に回復します。
    (BZ#2021151)

1.9. エラータの非同期更新

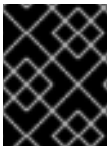
OpenShift Container Platform 4.9 のセキュリティー、バグ修正、拡張機能の更新は、Red Hat Network 経由で非同期エラータとして発表されます。OpenShift Container Platform 4.9 のすべてのエラータは Red Hat カスタマーポータルから入手できます。非同期エラータについては、OpenShift Container Platform ライフサイクルを参照してください。

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 4.9 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 4.9.z などのバージョン付けされた非同期リリースについてはサブセクションで説明します。さらに、エラータの本文がアドバイザリーで指定されたスペースに収まらないリリースについては、詳細についてその後のサブセクションで説明します。



重要

OpenShift Container Platform のいずれのリリースについても、クラスターの更新 に関する指示には必ず目を通してください。

1.9.1. RHSA-2021:3759 - OpenShift Container Platform 4.9.0 イメージのリリース、バグ修正およびセキュリティー更新アドバイザリー

発行日: 2021-10-18

セキュリティー更新を含む OpenShift Container Platform リリース 4.9.0 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHSA-2021:3759 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-2021:3758 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 4.9.0 コンテナーイメージの一覧

1.9.2. RHBA-2021:3935 - OpenShift Container Platform 4.9.4 バグ修正およびセキュリティー更新

発行日: 2021-10-26

OpenShift Container Platform リリース 4.9.4 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-2021:3935 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-2021:3934 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 4.9.4 コンテナーイメージの一覧

1.9.2.1. 機能拡張

SamplesImagestreamImportFailing アラート用に新しい条件付きギャザーが実装されました。これは、実行時に **openshift-cluster-samples-operator** namespace のログおよびイメージストリームを収集します。追加のデータの収集により、外部レジストリーからイメージストリームをプルする際の問題

に対する洞察が深くなります。(BZ#1966153)

1.9.2.2. バグ修正

- 以前のバージョンでは、ノードの一覧が利用可能になる前に、**Nodes** ページがレンダリングされていました。今回の更新により、ノードの一覧が利用可能になると、**Nodes** ページが正しくレンダリングされるようになりました。(BZ#2013088)

1.9.2.3. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster by using the CLI を参照してください。

1.9.3. RHBA-2021:4005 - OpenShift Container Platform 4.9.5 バグ修正の更新

発行日: 2021-11-01

OpenShift Container Platform リリース 4.9.5 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-2021:4005 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-2021:4004 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 4.9.5 コンテナーイメージの一覧

1.9.3.1. 既知の問題

- OpenShift Container Platform Webコンソールの **Storage → Overview** ページを表示または非表示にするために使用されるフラグが正しく設定されていません。その結果、**Overview** ページは、OpenShift Cluster Storage を含むクラスターのデプロイ後に非表示になりました。このバグの修正は、今後のリリースで予定されています。(BZ#2013132)

1.9.3.2. バグ修正

- ビルド設定の**lastTriggeredImageID**フィールドが非推奨なったため、イメージ変更トリガーコントローラーがビルドを開始する前に ID フィールドをチェックしなくなりました。その結果、クラスタがOpenShift Container Platform 4.7以前を実行しているときに、ビルド設定が作成され、イメージ変更のトリガー開始があった場合、継続してビルドのトリガーを試みていました。今回の更新により、これらの不要なビルド起動の試みは発生しなくなりました。(BZ#2006793)

1.9.3.3. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster by using the CLI を参照してください。

1.9.4. RHBA-2021:4119 - OpenShift Container Platform 4.9.6 バグ修正およびセキュリティー更新

発行日: 2021-11-10

セキュリティー更新を含む OpenShift Container Platform リリース 4.9.6 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHBA-2021:4119 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-2021:4118 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 4.9.6 コンテナーイメージの一覧

1.9.4.1. 既知の問題

- 現在のopt-in難読化は、現在**hostsubnets.network.openshift.io**がOVNクラスターにないため、OVNを使用するクラスターでは機能しません。(BZ#2014633)

1.9.4.2. バグ修正

- 以前のバージョンでは、**nmstate-handler** Pod のロック実装のバグにより、複数のノードによる制御が可能となっていました。今回の更新で、1 つのノードのみがロックを制御できるようにロックの実装が修正されました。(BZ#1954309)

- 以前のリリースでは、OpenStack フレーバーの検証では、誤った単位を使用する RAM 要件を満たさないフレーバーが許可されていました。今回の更新で、OpenStack によって返される値と最小 RAM を比較する際に正しいユニットが使用されるようになりました。(BZ#2009787)

- 以前のバージョンでは、OpenStack での OpenShift Container Platform デプロイメントは、コントロールプレーンノードに Ingress セキュリティーグループルールがないため、専用ワーカーがないコンパクトクラスターでは失敗していました。今回の更新により、コントロールプレーンがスケジュール可能な場合に Ingress セキュリティーグループが OpenStack に追加されました。(BZ#2016267)

- 以前は、全体的なメモリー消費量を削減するために一部の **cAdvisor** メトリクスが削除されましたが、コンソールの **Utilization** ダッシュボードには結果が表示されませんでした。今回の更新により、ダッシュボードが再び正しく表示されるようになりました。(BZ#2018455)

1.9.4.3. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster by using the CLI を参照してください。

1.9.5. RHBA-2021:4579 - OpenShift Container Platform 4.9.7 バグ修正の更新

発行日: 2021-11-15

OpenShift Container Platform リリース 4.9.7 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-2021:4579 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 4.9.7 コンテナーイメージの一覧

1.9.5.1. 特長

1.9.5.1.1. Kubernetes 1.22.2 からの更新

この更新には、Kubernetes 1.22.2 からの変更が含まれています。より詳しい情報は、1.22.2 のチェンジログをご覧ください。

1.9.5.2. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster within a minor version by using the CLI を参照してください。

1.9.6. RHBA-2021:4712 - OpenShift Container Platform 4.9.8 バグ修正の更新

発行日: 2021-11-22

OpenShift Container Platform リリース 4.9.8 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-2021:4712 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-2021:4711 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 4.9.8 コンテナーイメージの一覧

1.9.6.1. バグ修正

- 以前のバージョンでは、**SriovNetworkNodePolicy** カスタムリソース（CR）を追加または削除した場合、SriovNetworkNodeState CR のいずれかが **Succeeded** 以外の値を持つ **syncStatus** オブジェクトを持っていた場合、SR-IOV ネットワーク設定デーモン Pod は、ノードを遮断し、これを unschedulable とマークしていました。今回の更新でこの問題が修正されています。(**BZ#2002508**)

1.9.6.2. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster within a minor version by using the CLI を参照してください。

1.9.7. RHBA-2021:4834 - OpenShift Container Platform 4.9.9 バグ修正およびセキュリティー更新

発行日: 2021-11-29

セキュリティー更新を含む OpenShift Container Platform リリース 4.9.9 が利用可能になりました。この更新に含まれるバグ修正の一覧は、RHBA-2021:4834 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-2021:4833 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 4.9.9 コンテナーイメージの一覧

1.9.7.1. 特長

1.9.7.1.1. Kubernetes 1.22.3 からの更新

この更新には、Kubernetes 1.22.3 からの変更が含まれています。より詳しい情報は、1.22.3 のチェンジログをご覧ください。

1.9.7.2. バグ修正

- 以前のバージョンでは、Cluster Version Operator(CVO)は、マニフェストを上書きするかどうかを決定する際に **spec.overrides[].group** を無視していました。そのため、上書きされたエントリーは複数のリソースと一致し、管理者が意図したよりも多くのリソースを上書きする可能性があります。さらに、無効なグループを持つオーバーライドされたエントリーは一致とみなされ、**kubeadmin** ユーザーは、気付かないうちに無効なグループ値を使用していた可能性があります。今回の更新により、CVO では、設定されたオーバーライドを適用する際にグループの一致が必要になりました。その結果、CVO は単一のオーバーライドで、複数のマニフェストに一致させることはなくなりました。代わりに、CVO はマニフェストを正しいグループとのみ一致させます。以前に無効なグループを使用していた **Kubeadmin** ユーザーは、オーバーライドが引き続き一致するようにするために、正しいグループに対して更新される必要があります。(BZ#2022570)

1.9.7.3. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster within a minor version by using the CLI を参照してください。

1.9.8. RHBA-2021:4889 - OpenShift Container Platform 4.9.10 バグ修正の更新

発行日: 2021-12-06

OpenShift Container Platform リリース 4.9.10 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-2021:4889 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-2021:4888 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 4.9.10 コンテナーイメージの一覧

1.9.8.1. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster within a minor version by using the CLI を参照してください。

1.9.9. RHBA-2021:5003 - OpenShift Container Platform 4.9.11 バグ修正およびセキュリティー更新

発行日: 2021-12-13

OpenShift Container Platform リリース 4.9.11 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-2021:5003 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-2021:5002 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 4.9.11 コンテナーイメージの一覧

1.9.9.1. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster within a minor version by using the CLI を参照してください。

1.9.10. RHBA-2021:5214 - OpenShift Container Platform 4.9.12 バグ修正の更新

発行日: 2022-01-04

OpenShift Container Platform リリース 4.9.12 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-2021:5214 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-2021:5213 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 4.9.12 コンテナーイメージの一覧

1.9.10.1. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster within a minor version by using the CLI を参照してください。

1.9.11. RHBA-2022:0029 - OpenShift Container Platform 4.9.13 バグ修正の更新

発行日： 2022-01-10

OpenShift Container Platform リリース 4.9.13 が公開されました。この更新に含まれるバグ修正の一覧は、RHBA -2022:0029 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 4.9.13 コンテナーイメージの一覧

1.9.11.1. バグ修正

- 以前のバージョンでは、Windows ファイルパスではコロン文字を受け入れず、Windows マシンのミラーリングがブロックされていました。今回の更新により、コロンがダッシュに置き換えられ、Windows マシンのミラーリングが可能になりました。(BZ#1903545)
- 以前のバージョンでは、クラスターの カスタム API 名証明書 に属する証明書には、0644 のファイルパーミッションに一貫性がありませんでした 。今回の更新により、パーミッションが一貫して 0600 に設定されるようになりました。(BZ#1977730)

1.9.11.2. アップグレード

既存の OpenShift Container Platform 4.9 クラスターをこの最新リリースにアップグレードする手順については、Updating a cluster within a minor version by using the CLI を参照してください。