OpenShift Container Platform 4.18

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: 2025-12-12

OpenShift Container Platform 4.18 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

Legal Notice

Abstract

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

Table of Contents

第1章 OPENSHIFT CONTAINER PLATFORM 4.18 リリースノート

Red Hat OpenShift Container Platform は、開発者と IT 組織に対して、最小限の設定と管理により、新規および既存のアプリケーションの両方をセキュアでスケーラブルなリソースにデプロイするための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提供します。OpenShift Container Platform は、Java、JavaScript、Python、Ruby および PHP など、幅広いプログラミング言語およびフレームワークをサポートしています。

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

1.1. このリリースについて

OpenShift Container Platform (RHSA-2024:6122) が利用可能になりました。このリリースでは、CRI-O ランタイムで Kubernetes 1.31 を使用します。以下では、OpenShift Container Platform 4.18 に関連する新機能、変更点および既知の問題を説明します。

OpenShift Container Platform 4.18 クラスターは、https://console.redhat.com/openshift で入手できます。Red Hat Hybrid Cloud Console から、オンプレミス環境またはクラウド環境に OpenShift Container Platform クラスターをデプロイできます。

OpenShift Container Platform 4.18 は、Red Hat Enterprise Linux (RHEL) 8.8 および OpenShift Container Platform 4.18 のライフサイクル終了前にリリースされるそれ以降のバージョンの Red Hat Enterprise Linux (RHEL) 8 でサポートされます。OpenShift Container Platform 4.18 は、Red Hat Enterprise Linux CoreOS (RHCOS) 4.18 でもサポートされています。RHCOS で使用される RHEL バージョンを理解するには、RHEL Versions Utilized by Red Hat Enterprise Linux CoreOS (RHCOS) and OpenShift Container Platform (ナレッジベース記事) を参照してください。

コントロールプレーンには RHCOS マシンを使用する必要があり、コンピュートマシンに RHCOS または RHEL のいずれかを使用できます。RHEL マシンは OpenShift Container Platform 4.16 では非推奨となり、今後のリリースでは削除される予定です。

OpenShift Container Platform 4.14 以降、偶数リリースの Extended Update Support (EUS) フェーズでは、**x86_64**、64 ビット ARM (**aarch64**)、IBM Power® (**ppc64le**)、IBM Z® (**s390x**) アーキテクチャーを含むすべてのサポート対象アーキテクチャーで、利用可能なライフサイクルの合計が 24 カ月に延長されます。これに加えて、Red Hat は、**Additional EUS Term 2** と呼ばれる 12 カ月間の追加の EUS アドオンも提供しており、これにより利用可能なライフサイクルが 24 カ月から 36 カ月に延長されます。Additional EUS Term 2 は、OpenShift Container Platform のすべてのアーキテクチャーバリアントで利用できます。すべてのバージョンのサポートの詳細は、Red Hat OpenShift Container Platform のライフサイクルポリシー を参照してください。

OpenShift Container Platform 4.14 リリース以降、Red Hat では 3 つの新しいライフサイクル分類 (Platform Aligned、Platform Agnostic、Rolling Stream) を導入し、同梱されるクラスター Operator の管理を簡素化しています。これらのライフサイクル分類により、クラスター管理者にはさらなる簡素化と透明性が提供され、各 Operator のライフサイクルポリシーを理解し、予測可能なサポート範囲でクラスターのメンテナンスおよびアップグレード計画を形成できるようになります。詳細は、OpenShift Operator のライフサイクル を参照してください。

OpenShift Container Platform は FIPS 用に設計されています。FIPS モードでブートされた Red Hat Enterprise Linux (RHEL) または Red Hat Enterprise Linux CoreOS (RHCOS) を実行する場合、OpenShift Container Platform コアコンポーネントは、**x86_64**、**ppc64le**、および **s390x** アーキテクチャーのみで、FIPS 140-2/140-3 検証のために NIST に提出された RHEL 暗号化ライブラリーを使用します。

NIST の検証プログラムの詳細は、Cryptographic Module Validation Program を参照してください。検証用に提出された RHEL 暗号化ライブラリーの個別バージョンの最新の NIST ステータスについては、Compliance Activities and Government Standards を参照してください。

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

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

1.3. 新機能および機能拡張

このリリースにより、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. 認証および認可

1.3.1.1. OIDC にバインドされたサービスアカウントの署名者キーのローテーション

このリリースでは、Cloud Credential Operator (CCO) ユーティリティー (**ccoctl**) を使用して、以下のクラウドプロバイダーにインストールされているクラスターの OpenID Connect (OIDC) のバインドされたサービスアカウント署名者キーをローテーションできます。

- Security Token Service (STS) を使用する Amazon Web Services (AWS)
- GCP Workload Identity を使用する Google Cloud
- Workload ID を使用する Microsoft Azure

1.3.2. バックアップおよび復元

1.3.2.1. クラスターを最大 90 日間ハイバネート状態にする

このリリースにより、OpenShift Container Platform クラスターを最大 90 日間ハイバネート状態にし、クラスターが正常に回復することを期待できるようになりました。このリリースより前は、最大 30 日間ハイバネートすることしかできませんでした。

詳細は、OpenShift Container Platform クラスターのハイバーネート を参照してください。

1.3.2.2. etcd のバックアップと復元に関するドキュメントの強化

etcd 障害復旧ドキュメントが更新され、簡素化されました。通常の障害復旧の場合も、以前のバックアップを使用したクラスターの完全復元の場合も、より迅速にクラスターを復旧できるようになりました。

復元手順の多くのステップを完了できる 2 つのスクリプト (**quorum-restore.sh** と **cluster-restore.sh**) が導入されました。

さらに、正常なノードが少なくとも 1 つ存在する場合にクラスターをより迅速に復元するための手順が追加されました。残存ノードのいずれかが特定の基準を満たしている場合は、それを使用して復元を実行できます。

詳細は、障害復旧について を参照してください。

1.3.3. エッジコンピューティング

1.3.3.1. クラスターのインストール後 1 年間以内のシングルノード OpenShift クラスターのシャットダウンと再起動

このリリースでは、クラスターをインストールしてから最大 1 年間は、シングルノード OpenShift クラスターをシャットダウンして再起動できます。クラスターのシャットダウン中に証明書の有効期限が切れた場合は、クラスターの再起動時に証明書署名要求 (CSR) を承認する必要があります。

この更新前は、シングルノード OpenShift クラスターをシャットダウンして再起動できるのは、クラスターのインストール後 120 日間でした。

重要

シャットダウンする前に、シングルノード OpenShift クラスターからすべてのワークロード Pod を退避させてください。

詳細は、クラスターのグレースフルシャットダウン を参照してください。

1.3.4. 拡張機能 (OLM v1)

1.3.4.1. Operator Lifecycle Manager (OLM) v1 (一般提供)

Operator Lifecycle Manager (OLM) は、最初のリリースから OpenShift Container Platform 4 に含まれており、Operator として実行されるソリューションや高度なワークロードの実質的なエコシステムの実現と発展に貢献してきました。

OpenShift Container Platform 4.18 では、OpenShift Container Platform での Operator 管理方法を改善するために設計された次世代 Operator Lifecycle Manager である **OLM v1** が一般提供 (GA) 機能として導入されました。

OpenShift Container Platform 4.18 で OLM v1 の一般提供が開始されたことに伴い、OpenShift Container Platform 4 のリリース以降に含まれる既存の OLM バージョンは **OLM (Classic)** と呼ばれるようになりました。

これまではテクノロジープレビュー機能としてのみ利用可能でしたが、OLM v1 の更新されたフレームワークでは、Operator 管理の簡素化、セキュリティーの強化、信頼性の向上により、OLM (Classic) の一部であった多くの概念が進化しています。

重要

- OpenShift Container Platform 4.18 以降では、OLM (Classic) とともに OLM v1 がデフォルトで有効になっています。OLM v1 は、OpenShift Container Platform のインストール前に管理者がオプションで無効にできる クラスター機能 です。
- OLM (Classic) は、OpenShift Container Platform 4 のライフサイクル全体で引き続きフルサポートが提供されます。

API の単純化

OLM v1 では、新しいユーザーフレンドリーな API である **ClusterExtension** オブジェクト を使用することで、Operator 管理が単純化されています。Operator をクラスターの不可欠な拡張機能として

管理することにより、OLM v1 はカスタムリソース定義 (CRD) の特別なライフサイクル要件に対応します。この設計は Kubernetes の原則とより密接に連携し、カスタムコントローラーと CRD で構成される Operator をクラスター全体のシングルトンとして扱います。

OpenShift Container Platform では、OpenShift Container Platform 4.18 の OLM v1 においてデフォルトで有効になっているデフォルトの Red Hat Operator カタログ を通じて、最新の Operator パッケージ、パッチ、および更新に引き続きアクセスできます。OLM v1 では、クラスターに **ClusterExtension** API オブジェクトを作成して適用することで、Operator パッケージをインストールできます。**ClusterExtension** オブジェクトを操作することで、Operator パッケージのライフサイクルを管理し、そのステータスを迅速に把握し、問題のトラブルシューティングを行えます。

合理化された宣言的ワークフロー

単純化された API を活用することで、目的の Operator の状態を宣言的に定義して、Git や Zero Touch Provisioning などのツールとの統合時に OLM v1 がそれらの状態を自動的に維持するようにできます。これにより、人的エラーが最小限に抑えられ、より幅広いユースケースに対応できます。

継続的な調整とオプションのロールバックによる中断のない運用

OLM v1 は、継続的な調整を通じて信頼性を高めます。OLM v1 は、1 回の試行に頼るのではなく、問題が解決するまで自動的に再試行して Operator のインストールと更新の失敗をプロアクティブに解決します。これにより、**InstallPlan** API オブジェクトの削除など、これまで必要だった手動のステップが不要になり、コンテナーイメージの欠落やカタログの問題など、クラスター外の問題の解決が大幅に単純化されます。

さらに、OLM v1 ではオプションのロールバックが提供されており、潜在的なリスクを慎重に評価した後、特定の条件下で Operator バージョンの更新を元に戻すことが可能です。

デプロイメント更新の詳細な制御

詳細な更新制御により、特定の Operator バージョンを選択したり、許容されるバージョン範囲を定義したりできます。たとえば、ステージ環境で Operator のバージョン **1.2.3** をテストして承認した場合、最新バージョンが実稼働環境で同様に動作することを期待する代わりに、バージョンを固定できます。希望するバージョンとして **1.2.3** を指定すると、それが安全で予測可能な更新を行うためにデプロイされる正確なバージョンになります。

また、自動 z-stream 更新では、手動による介入のない自動セキュリティー修正を適用することで、シームレスでセキュアなエクスペリエンスが提供され、運用の中断が最小限に抑えられます。

ユーザー提供のサービスアカウントによるセキュリティー強化

OLM v1 はセキュリティーを優先しており、権限要件を最小限に抑え、アクセスをより強力に制御します。Operator ライフサイクル運用のためのユーザー提供 **ServiceAccount** オブジェクト を使用することで、OLM v1 アクセスは必要な権限のみに制限され、コントロールプレーンの攻撃対象領域が大幅に削減され、全体的なセキュリティーが向上します。このように、OLM v1 は、侵害の影響を最小限に抑えるために最小権限モデルを採用しています。

注記

OLM v1 のドキュメントとして、拡張機能 という独立したガイドがあります。以前は、OLM v1 ドキュメントは、OLM (Classic) 機能セットに関するドキュメントである Operator ガイドのサブセクションとして構成されていました。

更新後のガイドの場所と名前は、より焦点を絞ったドキュメントエクスペリエンスを反映しており、OLM v1 と OLM (Classic) を区別することを目的としています。

1.3.4.2. OLM v1 でサポートされる拡張機能

現在、Operator Lifecycle Manager (OLM) v1 は、次のすべての条件を満たすクラスター拡張機能のインストールをサポートしています。

- 拡張機能では、OLM (Classic) で導入された **registry+v1** バンドル形式を使用する必要があります。
- 拡張機能は、**AllNamespaces** インストールモードによるインストールをサポートする必要があります。
- 拡張機能は Webhook を使用してはなりません。
- 拡張機能は、次に示すいずれかのファイルベースのカタログプロパティーを使用して依存関係を宣言してはなりません。
  - **olm.gvk.required**
  - **olm.package.required**
  - **olm.constraint**

OLM v1 は、インストールする拡張機能がこれらの制約を満たしているかどうかを確認します。インストールする拡張機能がこれらの制約を満たしていない場合、クラスター拡張機能の条件にエラーメッセージが出力されます。

1.3.4.3. OLM v1 での非接続環境のサポート

特にミッションクリティカルな実稼働ワークロードのために、インターネット非接続環境でクラスターを実行することで高いセキュリティーを優先するクラスター管理者をサポートするために、OLM v1 は OpenShift Container Platform 4.18 以降で非接続環境をサポートします。

OpenShift CLI の oc-mirror プラグイン (**oc**) を使用して、クラスターに必要なイメージを完全または部分的な非接続環境のミラーレジストリーにミラーリングした後、oc-mirror プラグイン v1 または v2 のいずれかによって生成されたリソースセットを利用することで、OLM v1 はこれらの環境で適切に機能できます。

詳細は、OLM v1 での非接続環境のサポート を参照してください。

1.3.4.4. OLM v1 のカタログ選択の改善

このリリースでは、クラスター拡張機能のインストール時または更新時に、次のアクションを実行してカタログコンテンツの選択を制御できます。

- カタログを選択するためのラベルを指定します
- match 式を使用してカタログ全体をフィルタリングします
- カタログの優先順位を設定します

詳細は、カタログコンテンツの解決 を参照してください。

1.3.4.5. プロキシー環境と信頼済み CA 証明書の基本的なサポート

このリリースでは、Operator Controller と catalogd がプロキシー環境で実行できるようになり、信頼済み CA 証明書の基本的なサポートが含まれるようになりました。

1.3.4.6. OpenShift Container Platform バージョンとの互換性

クラスター管理者は、OpenShift Container Platform クラスターを次のマイナーバージョンに更新する前に、インストールされているすべての Operator がクラスターの次のマイナーバージョン (4.y+1) と互換性のあるバンドルバージョンに更新されていることを確認する必要があります。

OpenShift Container Platform 4.18 以降、OLM v1 は Operator のクラスターサービスバージョン (CSV) で **olm.maxOpenShiftVersion** アノテーションをサポートします。これは、OLM (Classic) の動作と同じように、インストールされた Operator を互換性のあるバージョンに更新する前に管理者がクラスターを更新することを防ぎます。

詳細は、OpenShift Container Platform バージョンとの互換性 を参照してください。

1.3.4.7. 拡張機能リソースへのユーザーアクセス

クラスター拡張機能がインストールされ、Operator Lifecycle Manager (OLM) v1 によって管理されるようになると、多くの場合、拡張機能はクラスター上で新しい API リソースを公開する **CustomResourceDefinition** オブジェクト (CRD) を提供できるようになります。通常、クラスター管理者はデフォルトでこれらのリソースへの完全な管理アクセス権を持ちますが、クラスター管理者以外のユーザー、つまり **通常のユーザー** は十分な権限を持たない可能性があります。

OLM v1 では、インストールされた拡張機能が提供する API を通常のユーザーが操作できるように、ロールベースのアクセス制御 (RBAC) を自動的に設定または管理することはありません。クラスター管理者は、このようなユーザー向けにカスタムリソース (CR) を作成、表示、または編集するために必要な RBAC ポリシーを定義する必要があります。

詳細は、拡張機能リソースへのユーザーアクセス を参照してください。

1.3.4.8. OLM v1 の sigstore 署名を使用したコンテナーイメージのランタイム検証 (テクノロジープレビュー)

OpenShift Container Platform 4.18 以降では、コンテナーイメージの sigstore 署名のランタイム検証を処理するための OLM v1 サポートがテクノロジープレビュー (TP) 機能として利用可能になっています。

1.3.4.9. OLM v1 の既知の問題

Operator Lifecycle Manager (OLM) v1 は、OLM (Classic) で導入された **OperatorConditions** API をサポートしていません。

拡張機能が **OperatorConditions** API のみに依存して更新を管理している場合、拡張機能が正しくインストールされない可能性があります。この API に依存する拡張機能のほとんどは起動時に失敗しますが、一部は調整中に失敗する可能性があります。

回避策として、拡張機能を特定のバージョンに固定できます。拡張機能を更新する場合は、拡張機能のドキュメントを参照して、いつ拡張機能を新しいバージョンに固定すれば安全か確認してください。

1.3.4.10. SiteConfig v1 が非推奨に

SiteConfig v1 は、OpenShift Container Platform 4.18 以降で非推奨になります。**ClusterInstance** カスタムリソースを使用する SiteConfig Operator を通じて、同等の改良された機能が利用できるようになりました。詳細は、Red Hat ナレッジベースの Procedure to transition from SiteConfig CRs to the ClusterInstance API を参照してください。

SiteConfig Operator の詳細は、SiteConfig を参照してください。

1.3.5. Hosted Control Plane

Hosted Control Plane のリリースは OpenShift Container Platform と同期しないため、独立したリリースノートがあります。詳細は、Hosted Control Plane リリースノート を参照してください。

1.3.6. IBM Power

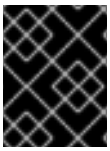
OpenShift Container Platform 4.18 の IBM Power® リリースでは、OpenShift Container Platform コンポーネントに改良点と新機能が追加されました。

このリリースにより、IBM Power で次の機能がサポートされます。

- PowerVS Installer Provisioned Infrastructure デプロイメントへの 4 つの新しいデータセンターの追加
- OpenShift CLI (**oc**) を使用したオンプレミスクラスターへのコンピュートノードの追加

1.3.7. IBM Z と IBM LinuxONE

このリリースにより、IBM Z® および IBM® LinuxONE は OpenShift Container Platform 4.18 と互換性を持つようになりました。z/VM、LPAR、または Red Hat Enterprise Linux (RHEL) カーネルベースの仮想マシン (KVM) を使用して、インストールを実行できます。インストール手順については、インストール方法 を参照してください。



重要

コンピュートノードは、Red Hat Enterprise Linux CoreOS (RHCOS) を実行する必要があります。

1.3.7.1. IBM Z および IBM LinuxONE の主な機能拡張

OpenShift Container Platform 4.18 の IBM Z® および IBM® LinuxONE リリースでは、OpenShift Container Platform のコンポーネントと概念に、改良点と新機能が追加されました。

このリリースにより、IBM Z® および IBM® LinuxONE 上で次の機能がサポートされます。

- OpenShift CLI (**oc**) を使用したオンプレミスクラスターへのコンピュートノードの追加

1.3.8. IBM Power、IBM Z、IBM LinuxONE サポートマトリクス

OpenShift Container Platform 4.14 以降、Extended Update Support (EUS) は IBM Power® および IBM Z® プラットフォームに拡張されています。詳細は、OpenShift EUS の概要 を参照してください。

表1.1 OpenShift Container Platform の機能

機能	IBM Power®	IBM Z® および IBM® LinuxONE
OpenShift CLI (**oc**) を使用したオンプレミスクラスターへのコンピュートノードの追加	サポート対象	サポート対象
代替の認証プロバイダー	サポート対象	サポート対象
Agent-based Installer	サポート対象	サポート対象

機能	IBM Power®	IBM Z® および IBM® LinuxONE
Assisted Installer	サポート対象	サポート対象
ローカルストレージ Operator を使用した自動デバイス検出	サポート対象外	サポート対象
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	サポート対象外	サポート対象外
IBM Cloud® 向けクラウドコントローラーマネージャー	サポート対象	サポート対象外
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	サポート対象外	サポート対象外
CPU マネージャー	サポート対象	サポート対象
Cron ジョブ	サポート対象	サポート対象
Descheduler	サポート対象	サポート対象
Egress IP	サポート対象	サポート対象
etcd に保存されるデータの暗号化	サポート対象	サポート対象
FIPS 暗号	サポート対象	サポート対象
Helm	サポート対象	サポート対象
水平 Pod 自動スケーリング	サポート対象	サポート対象
Hosted Control Plane	サポート対象	サポート対象
IBM Secure Execution	サポート対象外	サポート対象
IBM Power® Virtual Server の installer-provisioned infrastructure の有効化	サポート対象	サポート対象外
シングルノードへのインストール	サポート対象	サポート対象
IPv6	サポート対象	サポート対象
ユーザー定義プロジェクトのモニタリング	サポート対象	サポート対象
マルチアーキテクチャーコンピュートノード	サポート対象	サポート対象
マルチアーキテクチャーコントロールプレーン	サポート対象	サポート対象

機能	IBM Power®	IBM Z® および IBM® LinuxONE
マルチパス化	サポート対象	サポート対象
Network-Bound Disk Encryption - 外部 Tang サーバー	サポート対象	サポート対象
不揮発性メモリーエクスプレスドライブ (NVMe)	サポート対象	サポート対象外
Power10 用の nx-gzip (ハードウェアアクセラレーション)	サポート対象	サポート対象外
oc-mirror プラグイン	サポート対象	サポート対象
OpenShift CLI (**oc**) プラグイン	サポート対象	サポート対象
Operator API	サポート対象	サポート対象
OpenShift Virtualization	サポート対象外	サポート対象
IPsec 暗号化を含む OVN-Kubernetes	サポート対象	サポート対象
PodDisruptionBudget	サポート対象	サポート対象
Precision Time Protocol (PTP) ハードウェア	サポート対象外	サポート対象外
Red Hat OpenShift Local	サポート対象外	サポート対象外
スケジューラーのプロファイル	サポート対象	サポート対象
セキュアブート	サポート対象外	サポート対象
SCTP (Stream Control Transmission Protocol)	サポート対象	サポート対象
複数ネットワークインターフェイスのサポート	サポート対象	サポート対象
IBM Power® 上のさまざまな SMT レベルをサポートする **openshift-install** ユーティリティー (ハードウェアアクセラレーション)	サポート対象	サポート対象
3 ノードクラスターのサポート	サポート対象	サポート対象
Topology Manager	サポート対象	サポート対象外
SCSI ディスク上の z/VM Emulated FBA デバイス	サポート対象外	サポート対象
4k FCP ブロックデバイス	サポート対象	サポート対象

表1.2 永続ストレージのオプション

機能	IBM Power®	IBM Z® および IBM® LinuxONE
iSCSI を使用した永続ストレージ	サポート対象 [1]	サポート対象 [1], [2]
ローカルボリュームを使用した永続ストレージ (LSO)	サポート対象 [1]	サポート対象 [1], [2]
hostPath を使用した永続ストレージ	サポート対象 [1]	サポート対象 [1], [2]
ファイバーチャネルを使用した永続ストレージ	サポート対象 [1]	サポート対象 [1], [2]
Raw Block を使用した永続ストレージ	サポート対象 [1]	サポート対象 [1], [2]
EDEV/FBA を使用する永続ストレージ	サポート対象 [1]	サポート対象 [1], [2]

1. 永続共有ストレージは、Red Hat OpenShift Data Foundation またはその他のサポートされているストレージプロトコルを使用してプロビジョニングする必要があります。

2. 永続的な非共有ストレージは、iSCSI、FC などのローカルストレージを使用するか、DASD、FCP、または EDEV/FBA での LSO を使用してプロビジョニングする必要があります。

表1.3 演算子

機能	IBM Power®	IBM Z® および IBM® LinuxONE
cert-manager Operator for Red Hat OpenShift	サポート対象	サポート対象
Cluster Logging Operator	サポート対象	サポート対象
Cluster Resource Override Operator	サポート対象	サポート対象
Compliance Operator	サポート対象	サポート対象
Cost Management Metrics Operator	サポート対象	サポート対象
File Integrity Operator	サポート対象	サポート対象
HyperShift Operator	サポート対象	サポート対象
IBM Power® Virtual Server Block CSI Driver Operator	サポート対象	サポート対象外
Ingress Node Firewall Operator	サポート対象	サポート対象
Local Storage Operator	サポート対象	サポート対象

機能	IBM Power®	IBM Z® および IBM® LinuxONE
MetalLB Operator	サポート対象	サポート対象
Network Observability Operator	サポート対象	サポート対象
NFD Operator	サポート対象	サポート対象
NMState Operator	サポート対象	サポート対象
OpenShift Elasticsearch Operator	サポート対象	サポート対象
Vertical Pod Autoscaler Operator	サポート対象	サポート対象

表1.4 Multus CNI プラグイン

機能	IBM Power®	IBM Z® および IBM® LinuxONE
ブリッジ	サポート対象	サポート対象
host-device	サポート対象	サポート対象
IPAM	サポート対象	サポート対象
IPVLAN	サポート対象	サポート対象

表1.5 CSI ボリューム

機能	IBM Power®	IBM Z® および IBM® LinuxONE
クローン	サポート対象	サポート対象
拡張	サポート対象	サポート対象
スナップショット	サポート対象	サポート対象

1.3.9. Insights Operator

1.3.9.1. Insights Runtime Extractor (テクノロジープレビュー)

このリリースでは、ワークロードデータを収集する **Insights Runtime Extractor**機能が Insights Operator に導入されました。これにより、Red Hat がお客様のコンテナーのワークロードをより的確

に把握できるようになります。テクノロジープレビューとして提供される Insights Runtime Extractor 機能は、ランタイムワークロードデータを収集し、Red Hat に送信します。Red Hat は、OpenShift Container Platform コンテナーの使用方法を推進および最適化するお客様の投資判断に役立つ分析情報を入手するために、収集したランタイムワークロードデータを使用します。詳細は、フィーチャーゲートを使用した機能の有効化 を参照してください。

1.3.9.2. Rapid Recommendations

このリリースでは、Insights Operator が収集するデータを決定するルールをリモートで設定するための Rapid Recommendations メカニズムが強化されました。

Rapid Recommendations 機能はバージョンに依存せず、既存の条件付きデータ収集メカニズムに基づいてビルドされます。

Insights Operator は、**console.redhat.com** で実行されているセキュアなリモートエンドポイントサービスに接続し、Red Hat がフィルタリングおよび収集するコンテナーログメッセージを決定するルールが含まれる定義を取得します。

条件付きデータ収集の定義は、**pod.yml** 設定ファイルの **conditionalGathererEndpoint** 属性を通じて設定されます。

```
conditionalGathererEndpoint: https://console.redhat.com/api/gathering/v2/%s/gathering_rules
```

注記

以前のイテレーションでは、Insights Operator が収集するデータを決定するルールはハードコードされており、対応する OpenShift Container Platform バージョンに関連付けられていました。

事前設定済みのエンドポイント URL に、OpenShift Container Platform のターゲットバージョンを定義するためのプレースホルダー (**%s**) が追加されました。

1.3.9.3. 収集されるデータの増加と推奨事項の追加

Insights Operator は、以下の状況を検出するために、さらに多くのデータを収集するようになりました。このデータを他のアプリケーションで使用して、OpenShift Container Platform のデプロイメントをプロアクティブに管理するための修復推奨事項を生成できます。

- **nmstate.io/v1** API グループからリソースを収集します。
- **clusterrole.rbac.authorization.k8s.io/v1** インスタンスからデータを収集します。

1.3.10. インストールおよび更新

1.3.10.1. Cluster API Provider IBM Cloud の新バージョン

インストールプログラムでは、Transit Gateway の修正が含まれる新しいバージョンの Cluster API Provider IBM Cloud プロバイダーが使用されるようになりました。IBM Cloud の Transit Gateway のコストを考慮して、OpenShift Container Platform クラスターの作成時に OpenShift Container Platform を使用して Transit Gateway を作成できるようになりました。詳細は、(OCPBUGS-37588) および (OCPBUGS-41938) を参照してください。

1.3.10.2. 仮想ネットワークの暗号化を使用した Microsoft Azure へのクラスターのインストール

このリリースにより、暗号化された仮想ネットワークを使用して Azure にクラスターをインストールできるようになりました。**premiumIO** パラメーターが **true** に設定され、NVMe ストレージをサポートしていない Azure 仮想マシンを使用する必要があります。詳細は、Microsoft のドキュメント Creating a virtual network with encryption および Requirements and Limitations を参照してください。

1.3.10.3. クラスターのインストール中に ovn-kubernetes join サブネットを設定する

このリリースにより、クラスターのインストール時に **ovn-kubernetes** によって内部で使用される IPv4 join サブネットを設定できるようになりました。**install-config.yaml** ファイルで **internalJoinSubnet** パラメーターを設定し、クラスターを既存の Virtual Private Cloud (VPC) にデプロイできます。

詳細は、ネットワーク設定パラメーター を参照してください。

1.3.10.4. oc adm upgrade recommend コマンドの導入 (テクノロジープレビュー)

クラスターの更新時に、**oc adm upgrade** コマンドは次の利用可能なバージョンのリストを返します。4.18 **oc** クライアントバイナリーを使用している限り、更新を開始する前に、**oc adm upgrade recommend** コマンドを使用して提案を絞り込み、新しいターゲットリリースを推奨することができます。この機能は、更新サービスに接続されている OpenShift Container Platform バージョン 4.16 以降のクラスターで利用できます。

詳細は、CLI を使用したクラスター更新 を参照してください。

機能	4.16	4.17	4.18
oc adm upgrade status	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
oc adm upgrade recommend	利用不可	利用不可	テクノロジープレビュー

1.3.10.5. Amazon Web Services (AWS) 上の Nutanix Cloud Clusters (NC2) と Microsoft Azure 上の NC2 のサポート。

このリリースでは、AWS の Nutanix Cloud クラスター (NC2)、Azure の NC2 に OpenShift Container Platform をインストールできます。

詳細は、インフラストラクチャーの要件 を参照してください。

1.3.10.6. C4 および C4A マシンシリーズを使用した Google Cloud へのクラスターのインストール

このリリースでは、コンピュートまたはコントロールプレーンマシン用の C4 および C4A マシンシリーズを使用して、Google Cloud にクラスターをデプロイできます。これらのマシンでサポートされるディスクタイプは **hyperdisk-balanced** です。Hyperdisk ストレージを必要とするインスタンスタイプを使用する場合は、クラスター内のすべてのノードが Hyperdisk ストレージをサポートする必要があり、Hyperdisk ストレージを使用するようにデフォルトのストレージクラスを変更する必要があります。

マシンタイプの設定に関する詳細は、GCP のインストール設定パラメーター、C4 machine series (Compute Engine ドキュメント)、および C4A machine series (Compute Engine ドキュメント) を参照してください。

1.3.10.7. Google Cloud にクラスターをインストールするときに、独自のプライベートホストゾーンを提供する

このリリースでは、Google Cloud 上のクラスターを共有 VPC にインストールするときに、独自のプライベートホストゾーンを提供できます。その場合、Bring Your Own (BYO) ゾーンの要件として、そのゾーンは **<cluster_name>.<base_domain>.** などの DNS 名を使用し、ゾーンをクラスターの VPC ネットワークにバインドする必要があります。

詳細は、GCP 上のクラスターを共有 VPC にインストールするための前提条件 および Deployment Manager テンプレートを使用して GCP の共有 VPC にクラスターをインストールするための前提条件を参照してください。

1.3.10.8. 事前にロードされた RHCOS イメージオブジェクトを使用して Nutanix にクラスターをインストールする

このリリースでは、プライベートクラウドまたはパブリッククラウドから名前付きの事前ロードされた RHCOS イメージオブジェクトを使用して、Nutanix にクラスターをインストールできます。OpenShift Container Platform クラスターごとに RHCOS イメージオブジェクトを作成してアップロードする代わりに、**install-config.yaml** ファイルで **preloadedOSImageName** パラメーターを使用できます。

詳細は、追加の Nutanix 設定パラメーター を参照してください。

1.3.10.9. RHOSP 上のシングルスタック IPv6 クラスター

RHOSP にシングルスタック IPv6 クラスターをデプロイできるようになりました。

OpenShift Container Platform クラスターをデプロイする前に、RHOSP を設定する必要があります。詳細は、シングルスタック IPv6 ネットワークを使用したクラスターの設定 を参照してください。

1.3.10.10. 複数のサブネットを持つ Nutanix にクラスターをインストールする

このリリースでは、OpenShift Container Platform クラスターをデプロイする Prism Element に対して、複数のサブネットを持つ Nutanix クラスターをインストールできます。

詳細は、障害ドメインの設定 および 追加の Nutanix 設定パラメーター を参照してください。

既存の Nutanix クラスターの場合、コンピュート または コントロールプレーン のマシンセットを使用して複数のサブネットを追加できます。

1.3.10.11. 複数のネットワークインターフェイスコントローラーを備えた VMware vSphere へのクラスターのインストール (テクノロジープレビュー)

このリリースでは、ノードに複数のネットワークインターフェイスコントローラー (NIC) を備えた VMware vSphere クラスターをインストールできます。

詳細は、複数の NIC の設定 を参照してください。

既存の vSphere クラスターの場合、コンピュートマシンセット を使用して複数のサブネットを追加できます。

1.3.10.12. Agent-based Installer を使用して 4 ノードおよび 5 ノードのコントロールプレーンを設定する

このリリースでは、Agent-based Installer を使用していれば、4 ノードまたは 5 ノードのコントロールプレーンをインストールできるようにクラスターを設定できるようになりました。この機能は、**install-config.yaml** ファイルで **controlPlane.replicas** パラメーターを **4** または **5** に設定することで有効になります。

詳細は、Agent-based Installer の オプションの設定パラメーター を参照してください。

1.3.10.13. Agent-based Installer で最小限の ISO イメージをサポート

このリリースでは、Agent-based Installer は、すべてのサポート対象プラットフォームで最小限の ISO イメージの作成をサポートします。以前は、最小限の ISO イメージは **external** プラットフォームでのみサポートされていました。

この機能は、**agent-config.yaml** ファイルの **minimalISO** パラメーターを使用して有効にできます。

詳細は、Agent-based Installer の オプションの設定パラメーター を参照してください。

1.3.10.14. Agent-based Installer の Internet Small Computer System Interface (iSCSI) ブートサポート

このリリースでは、Agent-based Installer は、iSCSI ターゲットから OpenShift Container Platform クラスターを起動するために使用できるアセットの作成をサポートします。

詳細は、iSCSI ブート用のインストールアセットの準備 を参照してください。

1.3.11. Machine Config Operator

1.3.11.1. GA にプロモートされた AWS クラスターのブートイメージの更新

ブートイメージの更新が、Amazon Web Services (AWS) クラスターで GA にプロモートされました。詳細は、ブートイメージの更新 を参照してください。

1.3.11.2. マシン設定ノード情報の拡張 (テクノロジープレビュー)

マシン設定ノードのカスタムリソースは、ノードへのマシン設定の更新の進行状況を監視するために使用できます。このカスタムリソースに、更新に関する詳細情報が表示されるようになりました。**oc get machineconfignodes** コマンドの出力で、以下の状態やその他の状態が報告されるようになりました。これらのステータスを使用して更新を追跡したり、更新中にエラーが発生した場合にノードのトラブルシューティングを行ったりできます。

- 各ノードがスケジューリング対象から除外された、または復帰したかどうか
- 各ノードがドレインされたどうか
- 各ノードが再起動したどうか
- ノードで CRI-O がリロードされたかどうか
- ノードのオペレーティングシステムとノードファイルが更新されたかどうか

1.3.11.3. クラスター上のレイヤー化の変更 (テクノロジープレビュー)

クラスター上のレイヤー化機能にいくつかの重要な変更があります。

- **MachineConfig** オブジェクトを使用して、クラスター上のカスタムレイヤードイメージに拡張機能をインストールできるようになりました。
- **MachineOSConfig** オブジェクト内の Containerfile を更新すると、ビルドの実行がトリガーされるようになりました。
- **MachineOSConfig** オブジェクトからラベルを削除することで、クラスター上のカスタムレイヤーイメージをベースイメージに戻せるようになりました。
- Machine Config Operator の **must-gather** に、**MachineOSConfig** および **MachineOSBuild** オブジェクトのデータが含まれるようになりました。

クラスター上のレイヤー化の詳細は、クラスター上のレイヤー化を使用してカスタムレイヤーイメージを適用する を参照してください。

1.3.12. マシン管理

1.3.12.1. Microsoft Azure の Cluster API を使用したマシン管理 (テクノロジープレビュー)

このリリースにより、Microsoft Azure クラスターのテクノロジープレビューとして、OpenShift Container Platform に統合されたアップストリーム Cluster API を使用してマシンを管理する機能が導入されました。この機能は、Machine API を使用してマシンを管理するための追加または代替の機能になります。詳細は、Cluster API について を参照してください。

1.3.13. 管理コンソール

1.3.13.1. クラスター監視を有効にするチェックボックスがデフォルトでオンに設定

この更新により、OpenShift Lightspeed Operator のインストール時に、クラスター監視を有効にするためのチェックボックスがデフォルトでオンに設定されるようになりました。(OCPBUGS-42381)

1.3.14. モニタリング

このリリースのクラスター内モニタリングスタックには、以下の新機能および修正された機能が含まれます。

1.3.14.1. モニタリングスタックコンポーネントおよび依存関係の更新

このリリースには、クラスター内モニタリングスタックのコンポーネントと依存関係に関する、以下のバージョン更新が含まれています。

- Metrics Server が 0.7.2 へ
- Prometheus 2.55.1 への更新
- Prometheus Operator 0.78.1 への更新
- Thanos 0.36.1 への更新

1.3.14.2. ユーザーワークロードモニタリング Prometheus のスクレイピングと評価の間隔を追加

この更新により、ユーザーのワークロードを監視するために、Prometheus の連続スクレイピングの間隔とルール評価の間隔を設定できるようになりました。

1.3.14.3. モニタリング config map のモニタリング設定の早期検証を追加

この更新では、**cluster-monitoring-config** および **user-workload-monitoring-config** config map のモニタリング設定の変更に対する早期検証が導入され、フィードバックループが短縮され、ユーザーエクスペリエンスが向上します。

1.3.14.4. Alertmanager コンテナーにプロキシー環境変数を追加

この更新により、Alertmanager はプロキシー環境変数を使用するようになります。したがって、クラスター全体の HTTP プロキシーを設定した場合は、アラートレシーバーまたは Alertmanager のグローバル設定レベルで **proxy_from_environment** パラメーターを **true** に設定することで、プロキシーを有効にできます。

1.3.14.5. プロジェクト間のユーザーワークロードアラートと記録ルールを追加

この更新により、複数のプロジェクトに対して同時にクエリーを実行するユーザーワークロードアラートおよび記録ルールを作成できるようになります。

1.3.14.6. クラスターメトリクスと RHOSO メトリクスの相関関係

Red Hat OpenStack Services on OpenShift (RHOSO) で実行されるクラスターの可観測性メトリクスを相関させることができるようになりました。両方の環境からメトリクスを収集することで、インフラストラクチャーレイヤーとアプリケーションレイヤー全体の問題を監視およびトラブルシューティングできます。

詳細は、RHOSO で実行されるクラスターのモニタリング を参照してください。

1.3.15. Network Observability Operator

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

1.3.16. ネットワーク

1.3.16.1. ARM アーキテクチャーで実行されるクラスターへの SR-IOV ネットワーク Operator のデプロイ

SR-IOV Network Operator を ARM アーキテクチャーで実行されるクラスターにデプロイできるようになりました。(OCPBUGS-56496)

1.3.16.2. GNSS をソースとするグランドマスタークロックのホールドオーバー

このリリースでは、ソースとして Global Navigation Satellite System (GNSS) を使用して、グランドマスター (T-GM) クロックのホールドオーバー動作を設定できます。ホールドオーバーにより、GNSS ソースが利用できない場合でも T-GM クロックは同期パフォーマンスを維持できます。この期間中、T-GM クロックは内部オシレーターとホールドオーバーパラメーターに依存してタイミングの中断を削減します。

PTPConfig カスタムリソース (CR) で次のホールドオーバーパラメーターを設定することにより、ホールドオーバー動作を定義できます。

- **MaxInSpecOffset**
- **LocalHoldoverTimeout**
- **LocalMaxHoldoverOffSet**

詳細は、GNSS をソースとするグランドマスタークロックのホールドオーバー を参照してください。

1.3.16.3. IPVLAN および Bond CNI のマルチネットワークポリシー設定をサポート

このリリースでは、次のネットワークタイプに対してマルチネットワークポリシーを設定できます。

- IPVLAN (IP 仮想ローカルエリアネットワーク)
- SR-IOV 上のボンディング Container Network Interface (CNI)

詳細は、マルチネットワークポリシーの設定 を参照してください。

1.3.16.4. ホワイトリストおよびブラックリストアノテーションの用語を更新

ip_whitelist アノテーションおよび **ip_blacklist** アノテーションの用語が、それぞれ **ip_allowlist** および **ip_denylist** に更新されました。現在、OpenShift Container Platform は、 **ip_whitelist** および **ip_blacklist** アノテーションを引き続きサポートしています。ただし、これらのアノテーションは今後のリリースで削除される予定です。

1.3.16.5. CLI を使用して OVS サンプリングで OVN-Kubernetes ネットワークトラフィックを確認する

OVN-Kubernetes ネットワークトラフィックは、CLI を介した次のネットワーク API の OVS サンプリングで表示できます。

- **NetworkPolicy**
- **AdminNetworkPolicy**
- **BaselineNetworkPolicy**
- **UserDefinedNetwork** 分離
- **EgressFirewall**
- マルチキャスト ACL。

CLI を使用して OVS サンプリングで OVN-Kubernetes ネットワークトラフィックを確認することは、パケットのトレースに役立つことを目的としています。これは、Network Observability Operator のインストール時にも使用できます。

詳細は、CLI を使用して OVS サンプリングで OVN-Kubernetes ネットワークトラフィックを確認する を参照してください。

1.3.16.6. ユーザー定義のネットワークセグメンテーション (一般提供)

OpenShift Container Platform 4.18 では、ユーザー定義のネットワークセグメンテーションが一般利用可能になりました。ユーザー定義ネットワーク (UDN) では、管理者が、namespace がスコープ指定された UserDefinedNetwork とクラスターがスコープ指定された ClusterUserDefinedNetwork カスタムリソースを使用してカスタムネットワークトポロジーを定義できるようにすることで、ネットワークセグメンテーション機能を強化しました。

管理者は、UDN を使用して、強化された分離機能、ワークロードの IP アドレス管理機能、および高度なネットワーク機能を備えた、カスタマイズしたネットワークトポロジーを作成できます。レイヤー 2 とレイヤー 3 の両方のトポロジータイプをサポートするユーザー定義のネットワークセグメンテーションにより、幅広いネットワークアーキテクチャーとトポロジーが可能になり、ネットワークの柔軟性、セキュリティー、パフォーマンスが向上します。サポートされている機能の詳細は、UDN サポートマトリックス を参照してください。

UDN のユースケースとしては、仮想マシン (仮想マシン) に静的 IP アドレスの有効期間を割り当てる場合や、レイヤー 2 のプライマリー Pod ネットワークを提供してユーザーがノード間で仮想マシンをライブマイグレーションできるようにする場合などがあります。これらの機能はすべて OpenShift Virtualization に完全に装備されています。ユーザーは UDN を使用して、より強力なネイティブマルチテナント環境を作成し、デフォルトでオープンになっているオーバーレイ Kubernetes ネットワークを保護できます。詳細は、ユーザー定義ネットワークについて を参照してください。

1.3.16.7. Dynamic Configuration Manager は、デフォルトで有効になっています (テクノロジープレビュー)

Ingress Controller の Dynamic Configuration Manager を使用すると、メモリーフットプリントを削減できます。Dynamic Configuration Manager は、動的 API 経由でエンドポイントの変更を伝播します。このプロセスにより、基礎となるルーターはリロードなしで変更 (スケールアップおよびスケールダウン) に適応できます。

Dynamic Configuration Manager を使用するには、次のコマンドを実行して **TechPreviewNoUpgrade** 機能セットを有効にします。

```
$ oc patch featuregates cluster -p '{"spec": {"featureSet": "TechPreviewNoUpgrade"}}' --type=merge
```

1.3.16.8. ネットワークフローマトリックスの追加環境

このリリースにより、以下の環境で OpenShift Container Platform サービスへの Ingress フローのネットワーク情報を表示できるようになりました。

- ベアメタル上の OpenShift Container Platform
- ベアメタル上のシングルノード OpenShift
- Amazon Web Services (AWS) 上の OpenShift Container Platform
- AWS 上のシングルノード OpenShift

詳細は、OpenShift Container Platform ネットワークフローマトリックス を参照してください。

1.3.16.9. Border Gateway Protocol の MetalLB 更新

このリリースでは、MetalLB に Border Gateway Protocol (BGP) ピアカスタムリソース用の新しいフィールドが含まれています。**dynamicASN** フィールドを使用して、BGP セッションのリモートエンドに使用する自律システム番号 (ASN) を検出できます。これは、**spec.peerASN** フィールドに ASN を明示的に設定する代わりに使用できます。

1.3.16.10. SR-IOV 用の RDMA サブシステムの設定

このリリースでは、Single Root I/O Virtualization (SR-IOV) で Remote Direct Memory Access (RDMA) Container Network Interface (CNI) を設定して、コンテナー間の高パフォーマンスで低遅延の通信を実現できます。RDMA と SR-IOV を組み合わせると、Data Plane Development Kit (DPDK) アプリケーション内で使用するために Mellanox Ethernet デバイスのハードウェアカウンターを公開するメカニズムが提供されます。

1.3.16.11. Mellanox カードのセキュアブート対応環境で SR-IOV Network Operator の設定をサポート

このリリースでは、システムでセキュアブートが有効になっている場合に、Single Root I/O Virtualization (SR-IOV) Network Operator を設定できます。SR-IOV Operator は、最初に Mellanox デバイスのファームウェアを手動で設定した後に設定されます。セキュアブートを有効にすると、システムの回復力が強化され、コンピューターの全体的なセキュリティーに対する重要な防御層が提供されます。

詳細は、セキュアブートが有効な場合における Mellanox カードでの SR-IOV Network Operator の設定を参照してください。

1.3.16.12. Ingress コントローラーでの事前作成済み RHOSP Floating IP アドレスのサポート

このリリースでは、RHOSP で実行されているクラスターの Ingress コントローラーで、事前に作成された Floating IP アドレスを指定できるようになりました。

詳細は、Ingress Controller で Floating IP アドレスを指定する を参照してください。

1.3.16.13. SR-IOV Network Operator サポートの拡張

SR-IOV Network Operator は、Intel NetSec アクセラレーターカードと Marvell Octeon 10 DPU をサポートするようになりました。(OCPBUGS-43451)

1.3.16.14. Linux ブリッジインターフェイスを OVS のデフォルトポート接続として使用する

OVN-Kubernetes プラグインは、Open vSwitch (OVS) のデフォルトポート接続として Linux ブリッジインターフェイスを使用できるようになりました。これは、SmartNIC などのネットワークインターフェイスコントローラーが、基盤となるネットワークとホストをブリッジできるようになったことを意味します。(OCPBUGS-39226)

1.3.16.15. 問題のネットワーク重複メトリクスを公開する Cluster Network Operator

制限付きライブマイグレーションメソッドを開始し、ネットワークの重複に関する問題が存在する場合、Cluster Network Operator (CNO) は、その問題のネットワーク重複メトリクスを公開できるようになりました。これは、**openshift_network_operator_live_migration_blocked** メトリクスに新しい **NetworkOverlap** ラベルが含まれるようになったために可能になりました。(OCPBUGS-39096)

1.3.16.16. ネットワークアタッチメントが動的な再設定をサポート

以前は、**NetworkAttachmentDefinition** CR はイミュータブルでした。このリリースでは、既存の **NetworkAttachmentDefinition** CR を編集できます。編集がサポートされていることにより、ネットワークインターフェイスの MTU の調整など、基盤となるネットワークインフラストラクチャーの変更に簡単に対応できます。

同じネットワーク **name** と **type: ovn-k8s-cni-overlay** を参照する各 **NetworkAttachmentDefinition**

CR の設定が同期されていることを確認する必要があります。これらの値が同期している場合にのみ、ネットワークアタッチメントの更新は成功します。設定が同期されていない場合、OpenShift Container Platform がどの **NetworkAttachmentDefinition** CR を設定に使用するかが確定されないため、動作は未定義になります。

ネットワークの変更を Pod で有効にするには、ネットワークアタッチメント定義を使用するワークロードを再起動する必要があります。

1.3.17. Nodes

1.3.17.1. crun がデフォルトのコンテナーランタイムに

crun は、OpenShift Container Platform で作成された新しいコンテナーのデフォルトのコンテナーランタイムになりました。runC ランタイムは引き続きサポートされており、必要に応じてデフォルトのランタイムを runC に変更できます。crun の詳細は、コンテナーエンジンとコンテナーランタイムについて を参照してください。デフォルトを runC に変更する方法については、CRI-O パラメーターを編集するための ContainerRuntimeConfig CR の作成 を参照してください。

OpenShift Container Platform 4.17.z から OpenShift Container Platform 4.18 に更新しても、コンテナーのランタイムは変更されません。

1.3.17.2. sigstore のサポート (テクノロジープレビュー)

sigstore プロジェクトはテクノロジープレビューとして提供されており、これを OpenShift Container Platform でサプライチェーンのセキュリティー向上のために使用できます。クラスター全体のレベル、または特定の namespace に対して署名ポリシーを作成できます。詳細は、sigstore を使用したセキュアな署名管理 を参照してください。

1.3.17.3. ノード追加プロセスの拡張

OpenShift Container Platform 4.17 で導入された オンプレミスクラスターにワーカーノードを追加する プロセスが拡張されました。このリリースでは、ISO イメージファイルの代わりに Preboot Execution Environment (PXE) アセットを生成できるようになりました。また、ノード作成プロセスが失敗したかどうかにかかわらず、レポートが生成されるように設定することもできます。

1.3.17.4. Node Tuning Operator がカーネル引数を適切に選択

Node Tuning Operator が、Intel および AMD CPU のカーネル引数と管理オプションを適切に選択できるようになりました。(OCPBUGS-43664)

1.3.17.5. デフォルトのコンテナーランタイムが適切に設定されない場合がある

クラスター Node Tuning Operator によって設定されるデフォルトのコンテナーランタイムは、必ずクラスターから継承され、Operator によりハードコードされることはありません。このリリースから、デフォルト値は **crun** になります。(OCPBUGS-45450)

1.3.18. OpenShift CLI (oc)

1.3.18.1. oc-mirror プラグイン v2 (一般提供)

oc-mirror プラグイン v2 が一般公開されました。これを使用するには、oc-mirror コマンドを実行するときに **--v2** フラグを追加します。**--v2** フラグが設定されていない場合に実行される以前のバージョン (oc-mirror プラグイン v1) は非推奨になりました。継続的なサポートと改善のために、oc-mirror プラグ

イン v2 に移行することが推奨されます。

詳細は、oc-mirror プラグイン v2 を使用した非接続インストールのイメージのミラーリング を参照してください。

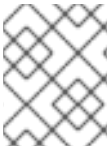
oc-mirror プラグイン v2 は、Helm チャートのミラーリングをサポートするようになりました。また、oc-mirror プラグイン v2 は、**HTTP/S** プロキシーが有効になっている環境でも使用できるようになりました。これにより、エンタープライズセットアップとの幅広い互換性が確保されます。

oc-mirror プラグイン v2 では、Operator カタログの v1 後方互換フィルタリングが導入され、フィルタリングされたカタログが生成されます。この機能により、クラスター管理者は、元のカタログの完全なリストではなく、ミラーリングされた Operator のみを表示できます。

1.3.19. Operator ライフサイクル

1.3.19.1. Operator Lifecycle Manager の既存バージョンの呼称を OLM (Classic) に変更

OpenShift Container Platform 4.18 以降で Operator Lifecycle Manager (OLM) v1 が一般提供 (GA) 機能としてリリースされるため、OpenShift Container Platform 4 以降に含まれている OLM の既存バージョンは **OLM (Classic)** と呼ばれるようになりました。



注記

OLM (Classic) は引き続きデフォルトで有効になっており、OpenShift Container Platform 4 のライフサイクル全体を通して完全にサポートされます。

OLM v1 の GA リリースの詳細は、拡張機能 (OLM v1) リリースノートセクションを参照してください。OLM v1 に重点を置いた完全なドキュメントについては、拡張機能 ガイドを参照してください。

OLM (Classic) に重点を置いた完全なドキュメントについては、引き続き Operator ガイドを参照してください。

1.3.20. Oracle(R) Cloud Infrastructure (OCI)

1.3.20.1. Oracle (R) Cloud Infrastructure (OCI) でのベアメタルサポート

Oracle® Cloud Infrastructure (OCI) 上の OpenShift Container Platform クラスターのインストールが、ベアメタルマシンでサポートされるようになりました。Assisted Installer または Agent-based Installer を使用して、OCI にベアメタルクラスターをインストールできます。OCI にベアメタルクラスターをインストールするには、次のいずれかのインストールオプションを選択します。

- Assisted Installer を使用して Oracle Cloud Infrastructure (OCI) にクラスターをインストールする
- Agent-based Installer を使用して Oracle Cloud Infrastructure (OCI) にクラスターをインストールする

1.3.21. インストール後の設定

1.3.21.1. Amazon Web Services で x86 コントロールプレーンを arm64 アーキテクチャーに移行する

このリリースでは、Amazon Web Services (AWS) 上のクラスター内のコントロールプレーンを **x86** から **arm64** アーキテクチャーに移行できます。詳細は、Amazon Web Services で x86 コントロールプレーンを arm64 アーキテクチャーに移行する を参照してください。

1.3.21.2. イメージストリームのインポートモードの動作設定 (テクノロジープレビュー)

この機能では、**image.config.openshift.io/cluster** リソースに新しいフィールド **imageStreamImportMode** が導入されます。**imageStreamImportMode** フィールドは、イメージストリームのインポートモードの動作を制御します。**imageStreamImportMode** フィールドを、次のいずれかの値に設定できます。

- **レガシー**
- **PreserveOriginal**

詳細は、イメージコントローラーの設定パラメーター を参照してください。

imageStreamImportMode 機能を有効にするには、**FeatureGate** カスタムリソース (CR) で **TechPreviewNoUpgrade** 機能セットを有効にする必要があります。詳細は、フィーチャーゲートについて を参照してください。

1.3.22. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.22.1. RHCOS が RHEL 9.4 を使用

RHCOS は、OpenShift Container Platform 4.18 で Red Hat Enterprise Linux (RHEL) 9.4 パッケージを使用します。これらのパッケージにより、OpenShift Container Platform インスタンスが最新の修正、機能、機能拡張、ハードウェアサポート、およびドライバーの更新を確実に受け取ることができます。

1.3.23. レジストリー

1.3.23.1. 読み取り専用レジストリーの強化

以前のバージョンの OpenShift Container Platform では、読み取り専用としてマウントされたストレージは、ストレージエラーに関する特定のメトリクスや情報を返しませんでした。これにより、ストレージバックエンドが読み取り専用であった場合に、レジストリーがサイレントな失敗となる可能性がありました。このリリースでは、バックエンドが読み取り専用に設定されている場合にストレージ情報を返すために、次のアラートが追加されました。

アラート名	メッセージ
ImageRegistryStorageReadOnly	イメージレジストリーストレージは読み取り専用で、イメージはストレージにコミットされません。
ImageRegistryStorageFull	イメージレジストリーストレージディスクが満杯になり、イメージはストレージにコミットされません。

1.3.24. スケーラビリティーおよびパフォーマンス

1.3.24.1. cluster-compare プラグインを使用したクラスター検証

cluster-compare プラグインは、クラスター設定とターゲット設定を比較する OpenShift CLI (**oc**) プラグインです。このプラグインは、設定可能な検証ルールとテンプレートを使用して、設定の差異を報告する一方で、想定内の差異は除外します。

たとえばプラグインは、オプションのコンポーネントやハードウェア固有のフィールドなど、想定内の違いを無視する一方で、フィールドの値の不一致、リソースの欠落、バージョンの不一致など、想定外の違いを強調できます。このように比較することで、ターゲット設定でクラスターコンプライアンスを簡単に評価できます。

cluster-compare プラグインは、開発、実稼働、およびサポートのシナリオで使用できます。

cluster-compare プラグインの詳細は、cluster-compare プラグインの概要 を参照してください。

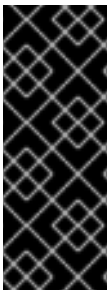
1.3.24.2. Node Tuning Operator: チューニング更新の延期

このリリースでは、Node Tuning Operator にチューニング更新の延期に対するサポートが導入されました。管理者はこの機能を使用して、メンテナンス期間中に更新を適用するようにスケジュールできます。

詳細は、チューニング変更適用の延期 を参照してください。

1.3.24.3. NUMA Resources Operator でデフォルトの SELinux ポリシーを使用

このリリースでは、NUMA Resources Operator は、ターゲットノードへの Operator コンポーネントのインストールを有効にするカスタム SELinux ポリシーを作成しなくなりました。代わりに、Operator は組み込みのコンテナー SELinux ポリシーを使用します。この変更により、以前はインストール中にカスタム SELinux ポリシーを適用する際に必要であった追加のノードの再起動が不要になります。



重要

既存の NUMA 対応スケジューラー設定を持つクラスターでは、OpenShift Container Platform 4.18 にアップグレードすると、設定済みの各ノードで追加の再起動が必要になる可能性があります。このシナリオでアップグレードを管理して中断を制限する方法の詳細は、Red Hat ナレッジベースの記事 Managing an upgrade to OpenShift Container Platform 4.18 or later for a cluster with an existing NUMA-aware scheduler configuration を参照してください。

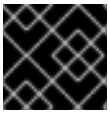
1.3.24.4. Node Tuning Operator プラットフォーム検出

このリリースでは、パフォーマンスプロファイルを適用すると、Node Tuning Operator がプラットフォームを検出し、それに応じてカーネル引数やその他のプラットフォーム固有のオプションを設定します。このリリースでは、次のプラットフォームを検出するためのサポートが追加されました。

- AMD64
- AArch64
- Intel 64

1.3.24.5. AMD EPYC Zen 4 CPU を搭載したワーカーノードのサポート

このリリースでは、**PerformanceProfile** カスタムリソース (CR) を使用して、AMD EPYC Zen 4 CPU (Genoa および Bergamo など) を搭載したマシンでワーカーノードを設定できます。これらの CPU は、単一の NUMA ドメイン (NPS=1) で設定されている場合に完全にサポートされます。



重要

Pod ごとの電源管理機能は、AMD EPYC Zen 4 CPU では機能しません。

1.3.25. ストレージ

1.3.25.1. LVMCluster カスタムリソースの作成後のオーバープロビジョニング比率の更新

以前は、**LVMCluster** カスタムリソース (CR) の **thinPoolConfig.overprovisionRatio** フィールドは、**LVMCluster** CR の作成中にのみ設定できました。このリリースにより、**LVMCluster** CR の作成後にも **thinPoolConfig.overprovisionRatio** フィールドを更新できるようになりました。

1.3.25.2. シンプールのメタデータサイズ設定のサポート

この機能により、**LVMCluster** カスタムリソース (CR) に次の新しいオプションフィールドが提供されます。

- **thinPoolConfig.metadataSizeCalculationPolicy**: 基になるボリュームグループのメタデータサイズを計算するポリシーを指定します。このフィールドは、**Static** または **Host** のいずれかに設定できます。デフォルトでは、このフィールドは **Host** に設定されています。
- **thinPoolConfig.metadataSize**: シンプールのメタデータサイズを指定します。**MetadataSizeCalculationPolicy** フィールドが **Static** に設定されている場合にのみ、このフィールドを設定できます。

詳細は、LVMCluster カスタムリソースについて を参照してください。

1.3.25.3. CIFS/SMB CSI Driver Operator を使用する永続ストレージの一般提供開始

OpenShift Container Platform は、Common Internet File System (CIFS) ダイアレクト/Server Message Block (SMB) プロトコル用の Container Storage Interface (CSI) ドライバーを使用して永続ボリューム (PV) をプロビジョニングできます。このドライバーを管理する CIFS/SMB CSI Driver Operator は、OpenShift Container Platform 4.16 でテクノロジープレビューステータスで導入されました。OpenShift Container Platform 4.18 では、一般提供が開始されました。

詳細は、CIFS/SMB CSI Driver Operator を参照してください。

1.3.25.4. Secret Store CSI Driver Operator の一般提供開始

Secrets Store Container Storage Interface (CSI) Driver Operator である **secrets-store.csi.k8s.io** を使用すると、OpenShift Container Platform がエンタープライズグレードの外部シークレットストアに保存されている複数のシークレット、キー、証明書をインラインの一時ボリュームとして Pod にマウントできます。Secrets Store CSI Driver Operator は、gRPC を使用してプロバイダーと通信し、指定された外部シークレットストアからマウントコンテンツを取得します。ボリュームがアタッチされると、その中のデータがコンテナーのファイルシステムにマウントされます。Secrets Store CSI Driver Operator は、OpenShift Container Platform 4.14 でテクノロジープレビュー機能として利用可能でした。OpenShift Container Platform 4.18 では、この機能の一般提供が開始されました。

Secrets Store CSI Driver の詳細は、Secrets Store CSI Driver Operator を参照してください。

Secrets Store CSI Driver Operator を使用して外部シークレットストアから CSI ボリュームにシークレットをマウントする方法については、外部シークレットストアを使用した機密データの Pod への提供 を参照してください。

1.3.25.5. 永続ボリュームの最終フェーズ遷移時間パラメーターの一般提供開始

OpenShift Container Platform 4.16 では、永続ボリューム (PV) が別のフェーズ (**pv.Status.Phase**) に移行するたびに更新されるタイムスタンプを持つ新しいパラメーター **LastPhaseTransitionTime** が導入されました。OpenShift Container Platform 4.18 では、この機能の一般提供が開始されました。

永続ボリュームの最終フェーズ遷移時間パラメーターの使用に関する詳細は、最終フェーズ遷移時間 を参照してください。

1.3.25.6. vSphere CSI の複数の vCenter に対するサポートの一般提供開始

OpenShift Container Platform 4.17 では、テクノロジープレビュー機能として、複数の vSphere クラスター (vCenter) をまたいで OpenShift Container Platform をデプロイする機能が導入されました。OpenShift Container Platform 4.18 では、複数の vCenter に対するサポートが一般提供されるようになりました。

詳細は、vSphere CSI の複数の vCenter サポート および vSphere のインストール設定パラメーター を参照してください。

1.3.25.7. 永続ボリュームの回収ポリシーを常に適用 (テクニカルプレビュー)

OpenShift Container Platform 4.18 より前は、永続ボリューム (PV) 回収ポリシーが常に適用されるとは限りませんでした。

バインドされた PV と永続ボリューム要求 (PVC) のペアの場合、PV 削除回収ポリシーが適用されるかどうは PV-PVC の削除順序によって決まります。PV を削除する前に PVC が削除された場合、PV は回収ポリシーを適用していました。しかし、PVC を削除する前に PV が削除された場合、回収ポリシーは適用されませんでした。この動作では、外部インフラストラクチャー内の関連付けられたストレージ資産は削除されませんでした。

OpenShift Container Platform 4.18 では、PV 回収ポリシーが常に一貫して適用されます。この機能はテクニカルプレビューです。

詳細は、永続ボリュームの回収ポリシー を参照してください。

1.3.25.8. LSO の LV または LVS を簡単に削除できる機能の改良と一般提供

OpenShift Container Platform 4.18 では、Local Storage Operator (LSO) のローカルボリューム (LV) とローカルボリュームセット (LVS) を削除する機能が向上し、アーティファクトが自動的に削除され、必要とする手順数が削減されます。

詳細は、ローカルボリュームまたはローカルボリュームセットの削除 を参照してください。

1.3.25.9. CSI ボリュームグループスナップショット (テクノロジープレビュー)

OpenShift Container Platform 4.18 では、テクノロジープレビュー機能として Container Storage Interface (CSI) ボリュームグループスナップショットが導入されています。この機能は CSI ドライバーによってサポートされている必要があります。CSI ボリュームグループスナップショットは、ラベルセレクターを使用して、スナップショット用に複数の永続ボリューム要求 (PVC) をグループ化します。ボリュームグループスナップショットは、同じ時点で取得された複数のボリュームからのコピーを表します。これは、複数のボリュームが含まれるアプリケーションに役立ちます。

OpenShift Data Foundation は、ボリュームグループのスナップショットをサポートしています。

CSI ボリュームグループスナップショットの詳細は、CSI ボリュームグループスナップショット を参照してください。

1.3.25.10. GCP PD CSI ドライバーにおけるベアメタル用 C3 インスタンスタイプのサポートと、N4 マシンシリーズの一般提供開始

Google Cloud Platform Persistent Disk (GCP PD) Container Storage Interface (CSI) ドライバーは、ベアメタルおよび N4 マシンシリーズの C3 インスタンスタイプをサポートしています。C3 インスタンスタイプと N4 マシンシリーズは、ハイパーディスクバランスディスクをサポートします。

さらに、大規模ストレージ向けにハイパーディスクストレージプールがサポートされています。ハイパーディスクストレージプールは、購入した容量、スループット、および IOPS のコレクションであり、必要に応じてアプリケーションにプロビジョニングできます。

OpenShift Container Platform 4.18 では、この機能の一般提供が開始されました。

詳細は、ベアメタルおよび N4 マシンシリーズの C3 インスタンスタイプ を参照してください。

1.3.25.11. OpenStack Manila 拡張永続ボリュームの一般提供開始

OpenShift Container Platform 4.18 では、OpenStack Manila は Container Storage Interface (CSI) 永続ボリューム (PV) の拡張をサポートしています。この機能は一般提供されています。

詳細は、永続ボリュームの拡張 および OpenShift Container Platform がサポートする CSI ドライバー を参照してください。

1.3.25.12. ワークロードアイデンティティーをサポートする GCP Filestore の一般提供開始

OpenShift Container Platform 4.18 では、Google Compute Platform (GCP) Filestore Container Storage Interface (CSI) ストレージが Workload Identity をサポートしています。これにより、ユーザーはサービスアカウントキーの代わりにフェデレーションアイデンティティーを使用して Google Cloud リソースにアクセスできます。OpenShift Container Platform 4.18 では、この機能の一般提供が開始されました。

詳細は、Google Compute Platform Filestore CSI Driver Operator を参照してください。

1.3.26. Web コンソール

1.3.26.1. 管理者パースペクティブ

このリリースでは、Web コンソールの **Administrator** パースペクティブに次の更新が導入されています。

- **Overview** ページの **Getting started resources** カードを非表示にして、ダッシュボードを最大限に活用できる新しい設定。
- CronJob の **List** と **Details** ページに **Start Job** オプションが追加されました。これにより、**oc** CLI を使用せずに、Web コンソールで個々の CronJob を手動で直接開始できるようになりました。
- マストヘッドの **Import YAML** ボタンが **Quick Create** ボタンになりました。このボタンは、YAML、Git からのインポート、またはコンテナーイメージの使用によってワークロードを迅速にデプロイするために使用できます。
- チャットボットのサンプルを使用して、独自の生成 AI チャットボットを構築できます。生成 AI チャットボットのサンプルは Helm を使用してデプロイされ、完全な CI/CD パイプラインが含まれています。このサンプルは、CPU のないクラスターでも実行できます。

- OpenShift Lightspeed を使用して YAML をコンソールにインポートできます。

1.3.26.1.1. コンテンツセキュリティーポリシー (CSP)

このリリースでは、コンソールのコンテンツセキュリティーポリシー (CSP) がレポート専用モードでデプロイされます。CSP 違反はブラウザーのコンソールに記録されますが、関連する CSP ディレクティブは適用されません。動的プラグインの作成者は、独自のポリシーを追加できます。

さらに、セキュリティーポリシーに違反するプラグインを報告することもできます。管理者は、これらのポリシーに違反するプラグインを無効にできます。CSP 違反はブラウザーのコンソールに記録されますが、関連する CSP ディレクティブは適用されません。この機能は **feature-gate** の背後にあるため、手動で有効にする必要があります。

詳細は、コンテンツセキュリティーポリシー (CSP) および Web コンソールを使用した機能セットの有効化 を参照してください。

1.3.26.2. Developer パースペクティブ

このリリースでは、Web コンソールの **開発者** パースペクティブに次の更新が導入されています。

- OpenShift Container Platform ツールキット、Quarkus ツールと JBoss EAP、および Visual Studio Code と IntelliJ 用の Language Server Protocol Plugin が追加されました。
- 以前は、Monaco エディターでライトモードからダークモードに切り替えても、コンソールはダークモードのままでした。この更新により、Monaco コードエディターは選択したテーマに一致するようになります。

1.4. 主な技術上の変更点

1.4.1. SR-IOV Network Operator のアンインストールの変更

OpenShift Container Platform 4.18 以降、SR-IOV Network Operator を正常にアンインストールするには、**sriovoperatorconfigs** カスタムリソースとカスタムリソース定義も削除する必要があります。

詳細は、SR-IOV Network Operator のアンインストール を参照してください。

1.4.2. iSCSI イニシエーター名とサービスの変更

以前は、**/etc/iscsi/initiatorname.iscsi** ファイルは RHCOS イメージにデフォルトで存在していました。このリリースでは、**initiatorname.iscsi** ファイルはデフォルトで存在しなくなりました。代わりに、**iscsi.service** および後続の **iscsi-init.service** サービスが開始するときに実行時に作成されます。このサービスはデフォルトでは有効になっていないため、サービスを開始する前に **initiatorname.iscsi** ファイルの内容を読み取る必要がある CSI ドライバーに影響する可能性があります。

1.4.3. Operator SDK 1.38.0

OpenShift Container Platform 4.18 は Operator SDK 1.38.0 をサポートします。この最新バージョンのインストール、または最新バージョンへの更新は、Operator SDK CLI のインストール を参照してください。

Operator SDK 1.38.0 は Kubernetes 1.30 をサポートし、Kubebuilder v4 を使用します。

メトリクスエンドポイントは、削除された **kube-rbac-proxy** の代わりに、ネイティブの Kubebuilder メトリクス設定 を使用して保護されるようになりました。

以下のサポートも Operator SDK から削除されました。

- ハイブリッド Helm ベースの Operator プロジェクト用のスキャフォールディングツール
- Java ベースの Operator プロジェクト用のスキャフォールディングツール

Operator SDK 1.36.1 で以前に作成または保守された Operator プロジェクトがある場合は、Operator SDK 1.38.0 との互換性を維持するためにプロジェクトを更新します。

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

1.4.4. kube-apiserver のループバック証明書の有効期間が 3 年に延長される

以前は、Kubernetes API Server の自己署名ループバック証明書が 1 年で期限切れになりました。このリリースにより、証明書の有効期限が 3 年に延長されました。

1.4.5. VMware vSphere 7 および VMware Cloud Foundation 4 の一般サポートの終了

Broadcom は、VMware vSphere 7 および VMware Cloud Foundation (VCF) 4 の一般サポートを終了しました。既存の OpenShift Container Platform クラスターがこれらのいずれかのプラットフォームで実行されている場合は、VMware インフラストラクチャーをサポート対象バージョンに移行またはアップグレードすることを計画する必要があります。OpenShift Container Platform は、vSphere 8 Update 1 以降、または VCF 5 以降へのインストールをサポートしています。

1.5. 非推奨および削除された機能

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

非推奨の機能は依然として OpenShift Container Platform に含まれており、引き続きサポートされますが、この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 4.18 内で非推奨化および削除された主な機能の最新のリストは、以下の表を参照してください。非推奨となり、削除された機能の詳細は、表の後に記載されています。

次の表では、機能は次のステータスでマークされています。

- **利用不可**
- **テクノロジープレビュー**
- **一般提供**
- **非推奨**
- **削除済み**

1.5.1. ベアメタルモニタリングの非推奨機能と削除された機能

表1.6 Bare Metal Event Relay Operator トラッカー

機能	4.16	4.17	4.18
Bare Metal Event Relay Operator	非推奨	削除済み	削除済み

1.5.2. イメージに関する非推奨機能および削除された機能

表1.7 イメージに関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
Cluster Samples Operator	非推奨	非推奨	非推奨

1.5.3. インストールに関する非推奨機能および削除された機能

表1.8 インストールに関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
oc adm release extract の **--cloud** パラメーター	非推奨	非推奨	非推奨
cluster.local ドメインの CoreDNS ワイルドカードクエリー	非推奨	非推奨	非推奨
RHOSP の **compute.platform.openstack.rootVolume.type**	非推奨	非推奨	非推奨
RHOSP の **controlPlane.platform.openstack.rootVolume.type**	非推奨	非推奨	非推奨
installer-provisioned infrastructure クラスターにおける **install-config.yaml** ファイル内の **ingressVIP** および **apiVIP** 設定	非推奨	非推奨	非推奨
パッケージベースの RHEL コンピュートマシン	非推奨	非推奨	非推奨
Amazon Web Services (AWS) の **platform.aws.preserveBootstrapIgnition** パラメーター	非推奨	非推奨	非推奨
AWS Outposts 内のコンピュートノードを使用して AWS にクラスターをインストール	非推奨	非推奨	非推奨

1.5.4. マシン管理の非推奨機能と削除された機能

表1.9 マシン管理の非推奨トラッカーと削除されたトラッカー

機能	4.16	4.17	4.18
Alibaba Cloud の Machine API でのマシン管理	削除	削除済み	削除済み
Alibaba Cloud のクラウドコントローラーマネージャー	削除	削除済み	削除済み

1.5.5. 非推奨および削除された機能の監視

表1.10 モニタリングの非推奨トラッカーと削除されたトラッカー

機能	4.16	4.17	4.18
Alertmanager v1 API	非推奨	削除済み	削除

1.5.6. ネットワークの非推奨機能と削除された機能

表1.11 ネットワーキングに関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
OpenShift SDN ネットワークプラグイン	非推奨	削除	削除
iptables	非推奨	非推奨	非推奨

1.5.7. ノードに関する非推奨機能と削除された機能

表1.12 ノードに関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
ImageContentSourcePolicy (ICSP) オブジェクト	非推奨	非推奨	非推奨
Kubernetes トポロジーラベル **failure-domain.beta.kubernetes.io/zone**	非推奨	非推奨	非推奨
Kubernetes トポロジーラベル **failure-domain.beta.kubernetes.io/region**	非推奨	非推奨	非推奨
cgroup v1	非推奨	非推奨	非推奨

1.5.8. OpenShift CLI (oc) に関する非推奨機能と削除された機能

表1.13 OpenShift CLI (oc) に関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
oc-mirror plugin v1	一般提供	一般提供	非推奨

1.5.9. Operator のライフサイクルと開発に関する非推奨機能と削除された機能

表1.14 Operator のライフサイクルと開発に関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
Operator SDK	非推奨	非推奨	非推奨
Ansible ベースの Operator プロジェクト用のスキャフォールディングツール	非推奨	非推奨	非推奨
Helm ベースの Operator プロジェクト用のスキャフォールディングツール	非推奨	非推奨	非推奨
Go ベースの Operator プロジェクト用のスキャフォールディングツール	非推奨	非推奨	非推奨
ハイブリッド Helm ベースの Operator プロジェクト用のスキャフォールディングツール	非推奨	非推奨	削除
Java ベースの Operator プロジェクト用のスキャフォールディングツール	非推奨	非推奨	削除
Operator カタログの SQLite データベース形式	非推奨	非推奨	非推奨

1.5.10. ストレージに関する非推奨機能と削除された機能

表1.15 ストレージに関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
FlexVolume を使用した永続ストレージ	非推奨	非推奨	非推奨
Shared Resources CSI Driver Operator	テクニカルプレビュー	非推奨	削除
AliCloud Disk CSI Driver Operator	一般提供	削除	削除

1.5.11. Web コンソールに関する非推奨機能と削除された機能

表1.16 Web コンソールに関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
Patternfly 4	非推奨	非推奨	非推奨
React Router 5	非推奨	非推奨	非推奨

1.5.12. ワークロードの非推奨機能と削除された機能

表1.17 ワークロードに関する非推奨および削除されたトラッカー

機能	4.16	4.17	4.18
DeploymentConfig オブジェクト	非推奨	非推奨	非推奨

1.5.13. 非推奨の機能

1.5.13.1. Kubernetes API の非推奨化

OpenShift Container Platform 4.17 では、削除された Kubernetes API **admissionregistration.k8s.io/v1beta1** が誤って再導入されました。この API は非推奨であり、今後の OpenShift Container Platform リリースで削除される予定です。この API を使用している箇所がある場合は、すべて **admissionregistration.k8s.io/v1** に移行してください。

削除予定の Kubernetes API がクラスターにあるかどうかを確認する方法は、Kubernetes API の非推奨化と削除 を参照してください。

1.5.14. 削除された機能

1.5.14.1. Shared Resource CSI Driver を削除

Shared Resource CSI Driver 機能は、OpenShift Container Platform 4.17 で非推奨となり、OpenShift Container Platform 4.18 からは削除されました。この機能は現在、Builds for Red Hat OpenShift 1.1 で一般提供されています。この機能を使用するには、Builds for Red Hat OpenShift 1.1 以降を使用している必要があります。

1.5.14.2. selected bundles 機能を oc-mirror v2 で削除

selected bundles 機能は、oc-mirror v2 の一般提供リリースから削除されました。この変更により、間違った Operator バンドルバージョンを指定するとクラスター内の Operator が壊れる可能性があるという問題が防止されます。(OCPBUGS-49419)

1.5.15. 今後の非推奨に関する通知

1.5.15.1. 今後の Kubernetes API の削除

OpenShift Container Platform の次のマイナーリリースでは、Kubernetes 1.32 を使用する予定です。Kubernetes 1.32 では、非推奨の API が削除されました。

削除予定の Kubernetes API リストについては、アップストリームの Kubernetes ドキュメントで Deprecated API Migration Guide を参照してください。

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

1.6. バグ修正

1.6.1. API サーバーと認証

- 以前は、API 検証によって、認可済みクライアントが kube-apiserver などの静的 Pod オペランドの現行リビジョンを減らすことや、オペランドが 2 つのノードで同時進行することを防ぐことはできませんでした。このリリースでは、どちらかを実行しようとするリクエストは拒否されるようになりました。(OCPBUGS-48502)

- 以前は、スペースが含まれるコールバックパスを使用して oath アイデンティティープロバイダー (IDP) を設定すると、oauth-server がクラッシュしていました。このリリースで、この問題は解決されています。(OCPBUGS-44099)

1.6.2. ベアメタルハードウェアのプロビジョニング

- 以前は、Bare Metal Operator (BMO) が、Intelligent Platform Management Interface (IPMI) ベースでサポートされていないものを含む、すべての Bare Metal Host (BMH) に対して **HostFirmwareComponents** カスタムリソースを作成していました。このリリースでは、**HostFirmwareComponents** カスタムリソースは、それをサポートする BMH に対してのみ作成されます。(OCPBUGS-49699)

- 以前は、プロビジョニングネットワークが無効になっているが、**bootstrapProvisioningIP** フィールドが設定されている bare-metal 設定では、bare-metal プロビジョニングコンポーネントが起動に失敗する可能性がありました。このような障害は、コンテナーイメージのプルプロセス中にプロビジョニングプロセスがブートストラップ仮想マシン上の外部ネットワークインターフェイスを再設定するときに発生します。このリリースでは依存関係が追加され、他のプロセスとの競合を防ぐためにネットワークがアイドル状態のときにのみインターフェイスの再設定が実行されるようになりました。その結果、**bootstrapProvisioningIP** フィールドが設定され、プロビジョニングネットワークが無効になっている場合でも、bare-metal プロビジョニングコンポーネントが確実に起動するようになりました。(OCPBUGS-36869)

- 以前は、ブロックデバイスのシリアル番号に特殊文字または無効な文字が存在する場合、Ironic 検査は失敗していました。これは、**lsblk** コマンドが文字をエスケープできなかったために発生しました。このリリースでは、コマンドが文字をエスケープするようになったため、この問題は発生しなくなりました。(OCPBUGS-36492)

- 以前は、metal3 Pod の起動中にプロビジョニングインターフェイス上の予期しない IP アドレスのチェックがトリガーされていました。この問題は、別のノード上に存在する Pod の以前のバージョンから DHCP によって提供された IP アドレスが存在するために発生していました。このリリースでは、Pod の起動チェックでプロビジョニングネットワークサブネットの外部に存在する IP アドレスのみが検索されるようになったため、ノードが別のノードに移動した場合でも、metal3 Pod がすぐに起動するようになりました。(OCPBUGS-38507)

- 以前は、プラットフォームタイプが **baremetal** の installer-provisioned infrastructure クラスターでのみ、クラスター全体の **Provisioning** リソースを編集してプロビジョニングネットワークを有効にできました。ベアメタル、シングルノード OpenShift、および user-provisioned infrastructure クラスター上でこのリソースを編集すると、検証エラーが発生しました。このリリースでは、過剰検証チェックが削除され、プラットフォームタイプ **none** のベアメタルクラ

スターでプロビジョニングネットワークを有効化できるようになりました。ユーザーは、installer-provisioned infrastructure クラスターと同様に、この操作のすべてのネットワーク要件が満たされていることを確認する責任があります。(OCPBUGS-43371)

1.6.3. クラウドコンピュート

- 以前は、可用性セット障害ドメイン数は **2** にハードコードされていました。通常、障害ドメイン数は **2** 以上であるため、この値は Microsoft Azure のほとんどのリージョンで機能しますが、**centraluseuap** および **eastusstg** リージョンでは機能しませんでした。このリリースでは、リージョン内の可用性セット障害ドメイン数が動的に設定されます。(OCPBUGS-48659)

- 以前は、Google Cloud からゾーン API エラーメッセージが更新されて粒度が増したため、マシンコントローラーがマシンを、無効なマシン設定のエラーとして認識するのではなく、一時的なクラウドエラーと認識してマシンを誤って有効としてマークしていました。これにより、無効なマシンが **failed** 状態に遷移できませんでした。この更新により、マシンコントローラーは新しいエラーメッセージを正しく処理し、無効なゾーンまたはプロジェクト ID を持つマシンが適切に failed 状態に遷移するようになりました。(OCPBUGS-47790)

- 以前は、証明書署名要求 (CSR) 承認者は、過負荷状態にあるかどうか、および証明書の承認を停止する必要があるかどうかの計算に、他のシステムからの証明書も含めていました。CSR を使用する他のサブシステムがある大規模なクラスターでは、CSR 承認者は関連しない未承認の CSR を合計に含め、それ以上の承認が妨げられていました。このリリースでは、CSR 承認者は、**signerName** プロパティーをフィルターとして使用して、承認できる CSR のみを含めるようになりました。その結果、CSR 承認者は、関連する **signerName** 値に対して未承認の CSR が多数ある場合にのみ、新規承認を妨げます。(OCPBUGS-46425)

- 以前は、一部のクラスターオートスケーラーメトリクスが初期化されず、使用できませんでした。このリリースにより、これらのメトリクスが初期化され、利用可能になりました。(OCPBUGS-46416)

- 以前は、一時的な切断のためにインフォーマー監視ストリームがイベントを見逃した場合、特にインフォーマーが一時的な切断中に EndpointSlice オブジェクトが削除されたことを認識すると、ネットワークに再接続された後にインフォーマーは特別なシグナルタイプを返すことがありました。返されたシグナルタイプは、イベントの状態が停止し、オブジェクトが削除されたことを示していました。返されたシグナルタイプは不正確で、OpenShift Container Platform ユーザーが混乱する原因となった可能性があります。このリリースでは、Cloud Controller Manager (CCM) が予期しないシグナルタイプを処理するため、OpenShift Container Platform ユーザーが返されたタイプから混乱を招く情報を受け取ることはありません。(OCPBUGS-45972)

- 以前は、末尾にピリオド (.) が含まれるカスタムドメイン名を使用するように AWS DHCP オプションセットが設定されていた場合、OpenShift Container Platform のインストールは失敗していました。このリリースでは、EC2 インスタンスのホスト名を抽出して Kubelet ノード名に変換するロジックが末尾のピリオドを削除するように更新されたため、結果として取得する Kubernetes オブジェクト名が有効になります。DHCP オプションセットの末尾のピリオドがインストールの失敗を引き起こすことがなくなりました。(OCPBUGS-45889)

- 以前は、**MachineSet** オブジェクトの **publicIp** パラメーターが明示的に **false** に設定されていると、既存のサブネット上の特定の環境で AWS クラスターのインストールが失敗していました。このリリースでは、インストールプログラムが特定の環境で AWS クラスターのマシンをプロビジョニングするときに、**publicIp** に設定された設定値によって問題が発生しなくなりました。(OCPBUGS-45130)

- 以前は、プラットフォームタイプが **baremetal** のクラスター (installer-provisioned infrastructure インストールプログラムによって作成されたクラスターなど) でのみ、クラスター全体の **Provisioning** リソースを編集してプロビジョニングネットワークを有効にできまし

た。ベアメタルのシングルノード OpenShift および user-provisioned infrastructure クラスターでは、このリソースを編集すると、検証エラーが発生します。過剰な検証が削除され、プラットフォームタイプが **none** のベアメタルクラスターでプロビジョニングネットワークを有効にできるようになりました。ユーザーは、installer-provisioned infrastructure と同様に、この操作のすべてのネットワーク要件が満たされていることを確認する責任があります。(OCPBUGS-43371)

- 以前は、インストールプログラムは、VMware vSphere コントロールプレーンマシンセットのカスタムリソース (CR) の **spec.template.spec.providerSpec.value** セクションの **network.devices**、**template**、および **workspace** フィールドに値を入力していました。これらのフィールドは vSphere 障害ドメインで設定する必要があり、インストールプログラムでこれらのフィールドを設定すると、意図しない動作が発生していました。これらのフィールドを更新してもコントロールプレーンマシンの更新はトリガーされず、コントロールプレーンマシンセットが削除されるとこれらのフィールドはクリアされていました。このリリースにより、インストールプログラムが更新され、障害ドメイン設定に含まれる値が入力されなくなりました。これらの値が障害ドメイン設定で定義されていない場合 (たとえば、以前のバージョンから OpenShift Container Platform 4.18 に更新されたクラスターの場合)、インストールプログラムによって定義された値が使用されます。(OCPBUGS-42660)

- 以前は、クラスターオートスケーラーは、削除中に **PreferNoSchedule** taint のあるノードを残すことがありました。このリリースでは、一括削除の上限が無効になっているため、この taint を持つノードは削除後に残らなくなります。(OCPBUGS-42132)

- 以前は、IBM Cloud クラスターのインストールで使用される Cloud Controller Manager (CCM) の liveness probe はループバックを使用できなかったため、プローブが再起動を繰り返していました。このリリースでは、プローブはループバックを使用できるようになり、この問題は発生しなくなりました。(OCPBUGS-41936)

- 以前は、証明書署名要求 (CSR) の承認メカニズムは、CSR のノード名と内部 DNS エントリーが大文字と小文字の不一致により失敗していました。このリリースでは、CSR の承認メカニズムが更新され、大文字と小文字を区別するチェックがスキップされるようになりました。これにより、ノード名と内部 DNS エントリーが一致する CSR が、大文字と小文字の不一致によりチェックに失敗することがなくなりました。(OCPBUGS-36871)

- 以前は、クラウドノードマネージャーには、実行中のノードのみを更新する必要がある場合に、任意のノードオブジェクトを更新する権限がありました。このリリースでは、あるノードのノードマネージャーが別のノードのノードオブジェクトを更新することを防止するための制限が設けられました。(OCPBUGS-22190)

1.6.4. Cloud Credential Operator

- 以前は、**aws-sdk-go-v2** ソフトウェア開発キット (SDK) が、Amazon Web Services (AWS) Security Token Service (STS) クラスターで **AssumeRoleWithWebIdentity** API 操作の認証に失敗していました。このリリースにより、**pod-identity-webhook** にデフォルトのリージョンが含まれるようになったため、この問題が発生しなくなりました。(OCPBUGS-45937)

- 以前は、クラスター内のシークレットは 1 回の呼び出しで取得していました。シークレットの数が多いと、API がタイムアウトする原因になります。このリリースでは、Cloud Credential Operator は 100 個に限定されたシークレットをバッチで取得します。この変更により、クラスター内に大量のシークレットがある場合のタイムアウトが防止されます。(OCPBUGS-39531)

1.6.5. Cluster Resource Override Admission Operator

- 以前は、**ClusterResourceOverride** カスタムリソース (CR) で **forceSelinuxRelabel** フィールドを指定し、その後変更した場合、その変更は、SELinux 再ラベル付け回避策機能を適用する

ために使用される **clusterresourceoverride-configuration** config map に反映されませんでした。この更新により、Cluster Resource Override Operator は、**forceSelinuxRelabel** 機能への変更を追跡して、config map オブジェクトを調整できるようになりました。その結果、**ClusterResourceOverride** CR フィールドを変更すると、config map オブジェクトが正しく更新されるようになりました。(OCPBUGS-48692)

1.6.6. Cluster Version Operator

- 以前は、カスタムセキュリティーコンテキスト制約 (SCC) により、Cluster Version Operator によって生成されたすべての Pod がクラスターバージョンのアップグレードを受け取れなくなっていました。このリリースにより、OpenShift Container Platform が各 Pod にデフォルトの SCC を設定するようになったため、作成されたカスタム SCC は Pod に影響を与えません。(OCPBUGS-46410)

- 以前は、Cluster Version Operator (CVO) が、**ClusterVersion Failing** 状態メッセージに伝播される内部エラーをフィルタリングしていませんでした。その結果、更新に悪影響を与えないエラーが **ClusterVersion Failing** 状態メッセージに表示されていました。このリリースでは、**ClusterVersion Failing** 状態メッセージに伝播されるエラーがフィルタリングされます。(OCPBUGS-15200)

1.6.7. 開発者コンソール

- 以前は、**PipelineRun** がリゾルバーを使用している場合、その **PipelineRun** を再実行するとエラーが発生しました。この修正により、ユーザーはリゾルバーを使用していても **PipelineRun** を再実行できるようになります。(OCPBUGS-45228)

- 以前は、**Form view** でデプロイメント設定を編集すると、**ImagePullSecrets** 値が重複していました。この更新により、フォームを編集しても重複したエントリーは追加されなくなります。(OCPBUGS-45227)

- 以前は、**OperatorHub** または別のカタログで検索すると、キーを押すたびに遅延が発生していました。この更新により、カタログ検索バーの入力がデバウンスされるようになりました。(OCPBUGS-43799)

- 以前は、**Administrator** パースペクティブの **Getting started resources** セクションを閉じるオプションはありませんでした。この変更により、ユーザーは **Getting started resources** セクションを閉じることができます。(OCPBUGS-38860)

- 以前は、cronjob が作成されると、その後の Pod 作成が早すぎるために、cronjob から新しい Pod を取得するコンポーネントが失敗していました。この更新では、cronjob の Pod 取得を開始する前に 3 秒の遅延が追加されました。(OCPBUGS-37584)

- 以前は、新規ユーザーの作成時に作成されたリソースは、そのユーザーが削除されても自動的に削除されませんでした。これにより、クラスター上に設定マップ、ロール、ロールバインディングなどが乱雑に存在していました。この更新では **ownerRefs** がリソースに追加されたため、ユーザーが削除されるとそれらもクリアされ、クラスター上でユーザーが乱雑に存在することはなくなりました。(OCPBUGS-37560)

- 以前は、サーバーレスインポートストラテジーを使用して Git リポジトリーをインポートすると、**func.yaml** からの環境変数がフォームに自動的にロードされませんでした。この更新により、環境変数がインポート時にロードされるようになりました。(OCPBUGS-34764)

- 以前は、devfile インポートストラテジーが選択された場合に、パイプラインビルドストラテジーを使用してリポジトリーをインポートするオプションが誤って表示されていましたが、これは実際には不可能でした。この更新では、devfile インポートストラテジーが選択された場合

はパイプラインストラテジーが削除されるようになりました。(OCPBUGS-32526)

- 以前は、カスタムテンプレートを使用する場合、秘密鍵などの複数行のパラメーターを入力できませんでした。このリリースでは、単一行モードと複数行モードを切り替えることができるため、テンプレートフィールドに複数行を入力できます。(OCPBUGS-23080)

1.6.8. Image Registry

- 以前は、OpenShift Container Platform の内部レジストリーがサポートしていなかったため、**ap-southeast-5** リージョンまたはその他のリージョンの AWS にクラスターをインストールできませんでした。このリリースでは、次のリージョンを含むように内部レジストリーが更新されたため、この問題は発生しなくなりました。
  - **ap-southeast-5**
  - **ap-southeast-7**
  - **ca-west-1**
  - **il-central-1**
  - **mx-central-1**
    (OCPBUGS-49693)

- 以前は、Microsoft Azure で Image Registry Operator が **networkAccess: Internal** で設定されていた場合、Operator 設定で **managementState** を **Removed** に正常に設定できませんでした。これは、Operator がストレージコンテナーの削除を試行した際の認可エラーが原因で発生していました。この更新により、Image Registry Operator はストレージアカウントの削除を続行するようになりました。これにより、ストレージコンテナーが自動的に削除され、正常に **Removed** 状態に遷移します。(OCPBUGS-42732)

- 以前は、クラスターのリソースグループ以外のリソースグループに配置された Microsoft Azure ストレージアカウントを使用するようにイメージレジストリーを設定すると、検証エラーにより Image Registry Operator のパフォーマンスが低下していました。この更新により、Image Registry Operator が変更され、他の認証要件を検証しない、ストレージアカウントキーのみ使用する認証が可能になります。(OCPBUGS-42514)

- 以前は、OpenShift インストーラーによるインストールではクラスター API を使用していました。クラスター API によって作成された仮想ネットワークでは、異なるタグテンプレートが使用されます。その結果、Image Registry Operator の **config.yaml** ファイルで **.spec.storage.azure.networkAccess.type: Internal** を設定すると、Image Registry Operator は仮想ネットワークを検出できなくなっていました。この更新により、Image Registry Operator は新旧のタグテンプレート両方を検索するようになり、問題が解決されました。(OCPBUGS-42196)

- 以前は、S3 互換のストレージプロバイダーから失敗したアップロードを消去しようとすると、イメージレジストリーでパニックが発生することがありました。これは、イメージレジストリーの s3 ドライバーが空のディレクトリーパスを誤って処理したために発生していました。この更新により、イメージレジストリーは空のディレクトリーパスを適切に処理し、パニックが修正されました。(OCPBUGS-39108)

1.6.9. インストーラー

- 以前は、Nutanix に Dynamic Host Configuration Protocol (DHCP) ネットワークを備えたクラスターをインストールすると、失敗していました。このリリースでは、この問題は解決されました。(OCPBUGS-38118)

- 以前は、インストールプログラムによってサポートされていないセキュリティーグループがロードバランサーに追加されていたため、Commercial Cloud Services (C2S) リージョンまたは Secret Commercial Cloud Services (SC2S) リージョンに AWS クラスターをインストールすると失敗していました。このリリースでは、インストールプログラムは、C2S リージョンまたは SC2S リージョンのいずれかでインストールする必要があるクラスターのロードバランサーに、サポート対象外のセキュリティーグループを追加しなくなりました。(OCPBUGS-33311)

- 以前は、インスタンスで IP 転送が設定されていてはならない Google Cloud クラスターをインストールすると、インストールが失敗しました。このリリースでは、すべての Google Cloud マシンで IP 転送が無効になり、問題は解決されました。(OCPBUGS-49842)

- 以前は、エッジゾーンで独自の仮想プライベートクラウド (BYO VPC) を使用するために、既存サブネットの AWS にクラスターをインストールする場合、インストールプログラムはサブネットエッジリソースに **kubernetes.io/cluster/<InfraID>:shared** のタグを付けませんでした。このリリースでは、**install-config.yaml** ファイルで使用されるすべてのサブネットに必要なタグが含まれています。(OCPBUGS-49792)

- 以前は、Amazon Web Services (AWS) で作成されたクラスターは、EIP アドレス **ec2:ReleaseAddress** を解放する権限がない場合、クラスターのプロビジョニング解除に失敗する可能性がありました。この問題は、管理されていない VPC や独自の (BYO) VPC、BYO Public IPv4 Pool アドレスなど、既存の仮想プライベートクラウド (VPC) において最小限の権限でクラスターが作成された場合に発生しました。このリリースでは、**ec2:ReleaseAddress** 権限が、インストール中に生成されたアイデンティティーおよびアクセス管理 (IAM) ポリシーにエクスポートされます。(OCPBUGS-49735)

- 以前は、Nutanix にクラスターをインストールすると、イメージを Prism Central にアップロードしているときにインストールプログラムがタイムアウトで失敗する可能性がありました。これは、Prism API が Red Hat Enterprise Linux CoreOS (RHCOS) イメージをロードしようとしたときに、一部の低速 Prism Central 環境で発生しました。Prism API 呼び出しのタイムアウト値は 5 分でした。このリリースでは、Prism API 呼び出しのタイムアウト値は **install-config.yaml** ファイル内の設定可能なパラメーター **platform.nutanix.prismAPICallTimeout** となり、デフォルトのタイムアウト値は 10 分です。(OCPBUGS-49148)

- 以前は、一時的な API サーバーの切断により **oc adm node-image monitor** コマンドが失敗し、エラーまたは End of File メッセージが表示されていました。このリリースでは、インストールプログラムは API サーバーの一時的な切断を無視し、モニターコマンドは API サーバーへの再接続を試みます。(OCPBUGS-48714)

- 以前は、Google Cloud でバックエンドサービスリソースを削除すると、削除対象の一部のリソースが見つかりませんでした。たとえば、関連付けられている転送ルール、ヘルスチェック、ファイアウォールルールが削除されませんでした。このリリースでは、インストールプログラムはまず名前でバックエンドサービスを検索し、次に転送ルール、ヘルスチェック、ファイアウォールルールを検索してから、その結果がバックエンドサービスと一致するか判断します。リソースを関連付けるアルゴリズムが逆転し、適切なリソースが削除されます。バックエンドサービスのリソースはリークせず、問題が解決されました。プライベートクラスターを削除しても、Ingress Operator によって作成された転送ルール、バックエンドサービス、ヘルスチェック、ファイアウォールルールは削除されません。(OCPBUGS-48611)

- 以前は、OpenShift Container Platform は PCI-DSS/BAFIN 規制に準拠していませんでした。このリリースでは、Microsoft Azure のテナント間でのオブジェクトレプリケーションは利用できません。そのため、不正なデータアクセスの可能性が低減され、データガバナンスポリシーへの厳格な遵守が確保されます。(OCPBUGS-48118)

- 以前は、OpenShift Container Platform を Amazon Web Services (AWS) にインストールし、インスタンスタイプなしでエッジマシンプールを指定すると、エッジノードが失敗することがありました。このリリースでは、インスタンスタイプなしでエッジマシンプールを指定する場合は、**ec2:DescribeInstanceTypeOfferings** 権限を使用する必要があります。権限は、使用される AWS Local Zones または Wavelength Zones の場所に基づき、利用可能な正しいインスタンスタイプを導出します。(OCPBUGS-47502)

- 以前は、API サーバーが一時的に切断されると、**oc adm node-image monitor** コマンドによりファイル終了 (EOF) エラーが報告されていました。このリリースでは、API サーバーが一時的に切断されても、モニターコマンドが失敗しなくなりました。(OCPBUGS-46391)

- 以前は、共有 Virtual Private Cloud (VPC) の作成時に **install-config.yaml** ファイルで **HostedZoneRole** 権限を指定する場合、**sts:AssumeRole** 権限も指定する必要がありました。そうしない場合はエラーが発生しました。このリリースでは、**HostedZoneRole** 権限を指定すると、インストールプログラムは **sts:AssumeRole** 権限が存在するかどうかを検証します。(OCPBUGS-46046)

- 以前は、インストール中に **publicIpv4Pool** 設定パラメーターが使用されても、**ec2:AllocateAddress** 権限と **ec2:AssociateAddress** 権限は検証されませんでした。その結果、インストール中に権限エラーが発生する可能性がありました。このリリースでは、クラスターのインストール前に必要な権限が検証され、問題は解決されました。(OCPBUGS-45711)

- 以前は、非接続環境でのインストールの場合、**imageContentSources** パラメーターがソースの複数のミラーに対して設定されていれば、ミラー設定の順序によっては、エージェント ISO イメージを作成するコマンドが失敗する可能性がありました。このリリースにより、エージェント ISO の作成時に複数のミラーが正しく処理されるようになり、問題は解決されました。(OCPBUGS-45630)

- 以前は、installer-provisioned infrastructure の Cluster API を使用してクラスターをインストールするときに、ユーザーは **machineNetwork** パラメーターを指定していました。このリリースでは、インストールプログラムはランダム **machineNetwork** パラメーターを使用します。(OCPBUGS-45485)

- 以前は、Amazon Web Services (AWS) へのインストール中に **hostedZone** ID を検索する際に、インストールプログラムが間違ったロードバランサーを使用し、エラーが発生していました。このリリースでは、正しいロードバランサーが使用され、問題は解決されました。(OCPBUGS-45301)

- 以前は、IBM Power Virtual Server のエンドポイントオーバーライドに条件は付けられていませんでした。その結果、エンドポイントオーバーライドが誤って作成され、仮想プライベート環境 (VPE) で障害が発生しました。このリリースでは、非接続環境でのエンドポイントオーバーライドに対してのみ条件付きになります。(OCPBUGS-44922)

- 以前は、共有仮想プライベートクラウド (VPC) のインストール中に、インストールプログラムは、クラスターのプライベート DNS ゾーンではなく、インストールプログラムによって作成されたプライベート DNS ゾーンにレコードを追加していました。その結果、インストールは失敗しました。このリリースでは、インストールプログラムは既存のプライベート DNS ゾーンを検索し、見つかった場合はそのゾーンを **install-config.yaml** ファイルが提供するネットワークとペアリングすることで、問題が解決されました。(OCPBUGS-44641)

- 以前は、**oc adm drain --delete-local-data** コマンドは 4.18 **oc** CLI ツールではサポートされていませんでした。このリリースでは、コマンドが **oc adm drain --delete-emptydir-data** に更新されました。(OCPBUGS-44318)

- 以前は、米国東部 (**wdc04**)、米国南部 (**dal13**)、シドニー (**syd05**)、およびトロント (**tor01**) リージョンは、IBM Power Virtual Server でサポートされていませんでした。このリリースで

は、**PowerEdgeRouter** (PER) 機能が含まれるこれらのリージョンが IBM Power Virtual Server でサポートされるようになりました。(OCPBUGS-44312)

- 以前は、Google Cloud のインストール中に、インストールプログラムがサブネットなどの大量の返されたデータを含むフィルターを作成すると、一定期間内にリソースをフィルターできる最大回数のクォータを超えていました。このリリースでは、関連するすべてのフィルタリングがクライアントに移動されるため、フィルターのクォータが超過せず、問題が解決されました。(OCPBUGS-44193)

- 以前は、Amazon Web Services (AWS) をインストールする際に、**propogateTags** を true に設定した場合にのみ、インストールプログラムにより **install-config.yaml** ファイル内のすべてのタグが検証されていました。このリリースでは、インストールプログラムは **install-config.yaml** ファイル内のすべてのタグを検証します。(OCPBUGS-44171)

- 以前は、**RendezvousIP** 値がコンピュートノード設定の **next-hop-address** フィールド内の部分文字列と一致すると、検証エラーが報告されていました。**RendezvousIP** 値は、コントロールプレーンホストアドレスのみと一致する必要があります。このリリースでは、**RendezvousIP** 値の部分文字列比較がコントロールプレーンホストアドレスに対してのみ使用されるため、エラーは発生しなくなりました。(OCPBUGS-44167)

- 以前は、IBM Power Virtual Server でクラスターを削除すると、Transit Gateway 接続がクリーンアップされていました。このリリースでは、**tgName** パラメーターが設定されている場合、クラスターを削除しても Red Hat OpenStack Platform (RHOSP) は Transit Gateway 接続をクリーンアップしません。(OCPBUGS-44162)

- 以前は、IBM プラットフォームにクラスターをインストールし、既存の VPC をクラスターに追加する場合、Cluster API Provider IBM Cloud はポート 443、5000、および 6443 を VPC のセキュリティーグループに追加しませんでした。そのため、VPC をクラスターに追加できませんでした。このリリースでは、Cluster API Provider IBM Cloud が VPC のセキュリティーグループにポートを追加し、VPC がクラスターに追加されるように修正されました。(OCPBUGS-44068)

- 以前は、Cluster API Provider IBM Cloud モジュールは非常に冗長でした。このリリースでは、モジュールの詳細度が削減され、それが **.openshift_install.log** ファイルの出力に反映されています。(OCPBUGS-44022)

- 以前は、IBM Power Virtual Server ゾーンにクラスターをデプロイすると、ロードバランサーの作成に時間がかかりました。その結果、クラスターは失敗しました。このリリースでは、Cluster API Provider IBM Cloud は、すべてのロードバランサーの準備が整うまで待機する必要がなくなり、問題が解決されました。(OCPBUGS-43923)

- 以前は、Agent-based Installer の場合、すべてのホスト検証ステータスログは、最初に登録されたホストの名前を参照していました。そのため、ホスト検証に失敗すると、問題のあるホストを特定できませんでした。このリリースでは、各ログメッセージで正しいホストが識別され、ホスト検証ログに対応するホストが正しく記録されるようになり、問題は解決されました。(OCPBUGS-43768)

- 以前は、Agent-based Installer の実行中に **oc adm node-image create** コマンドを使用してイメージを生成し、そのステップが失敗すると、付随するエラーメッセージにコンテナーログが表示されませんでした。**oc adm node-image create** コマンドは、コンテナーを使用してイメージを生成します。イメージ生成ステップが失敗すると、基本エラーメッセージには、イメージ生成が失敗する原因となった根本的な問題は表示されません。このリリースでは、トラブルシューティングを支援するために、**oc adm node-image create** コマンドでコンテナーログが表示されるようになり、根本的な問題が表示されるようになりました。(OCPBUGS-43757)

- 以前は、Agent-based Installer は **install-config.yaml** 設定ファイル内の **cloud_controller_manager** パラメーターを解析できませんでした。その結果、Assisted Service API は空の文字列を受け取ったために失敗し、Oracle® Cloud Infrastructure (OCI) でのクラスターのインストールが失敗しました。このリリースでは、解析ロジックが更新され、Agent-based Installer が **cloud_controller_manager** パラメーターを正しく解釈し、Assisted Service API が正しい文字列値を受け取るようになりました。その結果、Agent-based Installer は OCI 上にクラスターをインストールできるようになりました。(OCPBUGS-43674)

- 以前は、Azure SDK for Go の更新により **SendCertificateChain** オプションが削除され、証明書の送信動作が変更されました。その結果、完全な証明書チェーンが送信されませんでした。このリリースでは、完全な証明書チェーンを送信するオプションが利用可能になり、問題は解決されました。(OCPBUGS-43567)

- 以前は、Cluster API 実装を使用して Google Cloud にクラスターをインストールすると、インストールプログラムはファイアウォールルールの作成時に内部ロードバランサーと外部ロードバランサーを区別しませんでした。その結果、内部ロードバランサーのファイアウォールルールはすべての IP アドレスソース、つまり **0.0.0.0/0** に対して開かれていました。このリリースでは、Cluster API Provider GCP が更新され、内部ロードバランサーの使用時にファイアウォールルールがマシン CIDR に制限されるようになりました。内部ロードバランサーのファイアウォールルールはマシンネットワーク、つまりクラスター内のノードに正しく制限され、問題は解決されました。(OCPBUGS-43520)

- 以前は、IBM Power Virtual Server にクラスターをインストールするときに、必要なセキュリティーグループルールが作成されませんでした。このリリースでは、インストールに欠落しているセキュリティーグループルールが特定および作成され、問題は解決されました。(OCPBUGS-43518)

- 以前は、Red Hat OpenStack Platform (RHOSP) で以前に作成されたインスタンスを使用して、**oc adm node-image** コマンドでコンピュートノードを追加しようとすると、操作が失敗していました。このリリースでは、ユーザー管理のネットワーク設定を正しく設定することで問題が解決されました。(OCPBUGS-43513)

- 以前は、Google Cloud 上のクラスターを破棄するときに、転送ルールによってインストールプログラムが誤ってブロックされていました。その結果、破棄プロセスは完了できませんでした。このリリースでは、インストールプログラムが状態を正しく設定し、破棄されたすべてのリソースを削除済みとしてマークすることで、この問題が解決されました。(OCPBUGS-42789)

- 以前は、同じソースに対して複数のミラーがある非接続環境で Agent-based Installer のインストールを設定すると、インストールが失敗する可能性がありました。これは、ミラーの 1 つがチェックされなかったために発生しました。このリリースでは、同じソースに対して複数のミラーが定義されている場合にすべてのミラーを使用することで、問題が解決されました。(OCPBUGS-42705)

- 以前は、Agent-based Installer の **install-config.yaml** ファイル内の **AdditionalTrustBundlePolicy** パラメーターを変更できませんでした。パラメーターは常に **ProxyOnly** に設定されていました。このリリースでは、**AdditionalTrustBundlePolicy** を **Always** などの他の値に設定できます。デフォルトでは、パラメーターは **ProxyOnly** に設定されています。(OCPBUGS-42670)

- 以前は、クラスターをインストールし、**oc adm node-image** コマンドを使用してコンピュートノードを追加しようとすると、日付、時刻、またはその両方が不正確であったために失敗していました。このリリースでは、ターゲットクラスターの **MachineConfig** chrony リソース内の同じ Network Time Protocol (NTP) 設定をノードの一時的なライブ環境に適用することで、問題が解決されました。(OCPBUGS-42544)

- 以前は、インストール中に **oc adm node-image create** コマンドによって生成されたアーティファクトの名前のファイル名に **<arch>** が含まれていませんでした。その結果、ファイル名が生成された他の ISO と一致しませんでした。このリリースでは、**oc adm node-image create** コマンドで生成されるアーチファクトの名前がパッチで修正され、参照されるアーキテクチャーがファイル名の一部として含まれるようになりました。これにより、問題は解決されました。(OCPBUGS-42528)

- 以前は、Agent-based Installer は **assisted-service** オブジェクトをデバッグログモードに設定していました。意図せずに、ポート **6060** を使用する **assisted-service** オブジェクト内の **pprof** モジュールがオンになってしまいました。その結果、ポートの競合が発生し、Cloud Credential Operator (CCO) が実行されませんでした。VMware vSphere Cloud Controller Manager (CCM) から要求されたときに、vSphere シークレットが生成されず、RHOSP CCM はノードの初期化に失敗し、クラスターのインストールがブロックされました。このリリースでは、Agent-based Installer によって呼び出されたときに、**assisted-service** オブジェクト内の **pprof** モジュールは実行されません。その結果、CCO は正しく実行され、Agent-based Installer を使用する vSphere 上のクラスターインストールが成功します。(OCPBUGS-42525)

- 以前は、コンピュートノードがクラスターに参加しようとすると、プロセスが完了する前にランデブーノードが再起動していました。コンピュートノードはランデブーノードと期待どおりに通信できないため、インストールは成功しませんでした。このリリースでは、ランデブーノードが早期に再起動する原因となっていた競合状態を修正するパッチが適用され、問題は解決されました。(OCPBUGS-41811)

- 以前は、Assisted Installer を使用する場合、Red Hat Hybrid Cloud Console で **s390x** CPU アーキテクチャーのマルチアーキテクチャーイメージを選択すると、インストールが失敗することがありました。インストールプログラムは、MCO 再起動のスキップに **s390x** CPU アーキテクチャーとの互換性がないため、新しいクラスターが作成されなかったというエラーを報告しました。このリリースにより、この問題は解決されました。(OCPBUGS-41716)

- 以前は、コーディングの問題により、コンパクトクラスターのプロビジョニング中に RHOSP user-provisioned infrastructure インストール上の Ansible スクリプトが失敗していました。これは、3 ノードクラスターで IPv6 が有効になっている場合に発生しました。このリリースでは問題が解決され、コンパクトな 3 ノードクラスターをプロビジョニングできるようになりました。(OCPBUGS-41538)

- 以前は、コーディングの問題により、コンパクトクラスターのプロビジョニング中に RHOSP ユーザーがプロビジョニングしたインストールインフラストラクチャー上の Ansible スクリプトが失敗していました。これは、3 ノードクラスターで IPv6 が有効になっている場合に発生しました。このリリースでは問題が解決され、ユーザーがプロビジョニングしたインストールインフラストラクチャー用にコンパクトな 3 ノードクラスターを RHOSP 上にプロビジョニングできるようになりました。(OCPBUGS-39402)

- 以前は、Ansible Playbook の順序が変更され、**metadata.json** ファイルの作成前に実行されていたため、古いバージョンの Ansible で問題が発生していました。このリリースの Playbook は、古いバージョンの Ansible に対応するためにファイルの欠落に対してより寛容になり、問題は解決されました。(OCPBUGS-39285)

- 以前は、クラスターをインストールすると、日付、時刻、またはその両方が不正確であったためにコンピュートノードの使用に問題が発生していました。このリリースでは、ライブ ISO 時刻同期にパッチが適用されます。このパッチは、ユーザーが **agent-config.yaml** ファイルで提供する追加の Network Time Protocol (NTP) サーバーのリストを使用して **/etc/chrony.conf** ファイルを設定するため、コンピュートノードを使用してもクラスターのインストール問題が発生しなくなります。(OCPBUGS-39231)

- Previously, when installing a cluster on bare metal using installer-provisioned infrastructure, the installation could time out if the network to the bootstrap virtual machine is slow.この更新によ

り、タイムアウト期間が延長され、より広範なネットワークパフォーマンスの状況をカバーできるようになりました。(OCPBUGS-39081)

- 以前は、プロキシーを使用する制限付き環境内のクラスターに対して **oc adm node-image create** コマンドを実行すると、クラスター全体のプロキシー設定が無視されることが原因でコマンドが失敗していました。このリリースでは、コマンドが正常に実行されるように、コマンド実行時に (利用可能な場合) クラスタープロキシーリソース設定が含まれるようになり、問題が解決されました。(OCPBUGS-38990)

- 以前は、Google Cloud 上のクラスターを、Bring Your Own (BYO) のホステッドゾーンを持つ共有 Virtual Private Cloud (VPC) にインストールすると、プライベートマネージドゾーンの作成エラーが原因でインストールが失敗する可能性がありました。このリリースでは、修正により、既存のプライベートマネージドゾーンがある場合、インストールプログラムが新規ゾーンの作成をスキップするようになり、問題が解決されました。(OCPBUGS-38966)

- 以前は、テンプレートをダウンロードできないため、非接続環境で OpenShift Container Platform 4.16 を実行するために VMware vSphere 上でインストーラーによってプロビジョニングされたインストールが失敗していました。このリリースでは、テンプレートが正しくダウンロードされ、問題は解決されました。(OCPBUGS-38918)

- Previously, during installation the **oc adm node-image create** command used the **kube-system/cluster-config-v1** resource to determine the platform type.このリリースでは、インストールプログラムは、プラットフォームタイプに関するより正確な情報を提供するインフラストラクチャーリソースを使用します。(OCPBUGS-38802)

- 以前は、まれに発生する VMware vSphere Cluster API マシンの状況により、vCenter セッション管理が予期せずタイムアウトすることがありました。このリリースでは、Cluster API Provider vSphere の現行バージョン以降で Keep Alive サポートが無効になり、問題は解決されました。(OCPBUGS-38657)

- 以前は、フォルダーが未定義で、データセンターがデータセンターフォルダーに配置されていた場合、vCenter Server のルートを起点とする間違ったフォルダー構造が作成されていました。Govmomi **DatacenterFolders.VmFolder** を使用すると、間違ったパスが使用されていました。このリリースでは、フォルダー構造がデータセンターのインベントリーパスを使用し、それを仮想マシン (VM) およびクラスター ID 値と結合するようになり、問題が解決されました。(OCPBUGS-38599)

- 以前は、Google Cloud のインストールプログラムは、アドレスをフィルタリングして内部アドレスのみを検索して削除していました。Cluster API Provider Google Cloud Platform (GCP) でプロビジョニングされたリソースの追加には、アドレスリソースへの変更が含まれていました。このリリースでは、Cluster API Provider GCP によって外部アドレスが作成され、これらをクラスターのクリーンアップ操作に含める必要があります。(OCPBUGS-38571)

- 以前は、**install-config.yaml** ファイルでサポートされていないアーキテクチャーを指定すると、**connection refused** メッセージが表示されてインストールプログラムが失敗していました。この更新により、インストールプログラムは指定されたクラスターアーキテクチャーが OpenShift Container Platform と互換性があることを正しく検証し、インストールが正常に実行されるようになりました。(OCPBUGS-38479)

- 以前は、Agent-based Installer を使用してクラスターをインストールすると、**assisted-installer-controller** は、ランデブーホストで **assisted-service** が使用不可かどうかにより、タイムアウトになるか、インストールプロセスを終了していました。この状況により、CSR 承認チェック中にクラスターのインストールが失敗しました。このリリースでは、**assisted-installer-controller** が更新され、**assisted-service** が使用不可の場合でもコントローラーがタイムアウトしたり終了したりしないようになりました。現在は、CSR 承認チェックは期待どおりに動作します。(OCPBUGS-38466)

- 以前は、Nutanix に Dynamic Host Configuration Protocol (DHCP) ネットワークを備えたクラスターをインストールすると、失敗していました。このリリースでは、この問題は解決されました。(OCPBUGS-388118)

- 以前は、VMware vSphere vCenter クラスターに標準ポートグループが定義されていない ESXi ホストが含まれている場合に、インストールプログラムがそのホストを選択して OVA をインポートしようとすると、インポートが失敗し、**Invalid Configuration for device 0** エラーが報告されていました。このリリースでは問題が解決され、インストールプログラムは ESXi ホストの標準ポートグループが定義されているかどうかを確認し、定義されていない場合は、定義済み標準ポートグループを持つ ESXi ホストが見つかるまで続行するか、見つからない場合はエラーメッセージを報告します。(OCPBUGS-37945)

- 以前は、SCOS での EFI セキュアブートの失敗により、FCOS が SCOS に切り替わると仮想マシン (VM) の起動に失敗しました。このリリースでは、`coreos.ovf ` 設定ファイルでセキュアブートが有効になっている場合にのみセキュアブートが無効になり、問題が解決されました。(OCPBUGS-37736)

- 以前は、VMware vSphere 上のインストールプログラムで非推奨フィールドとサポート対象フィールドが使用されると、検証エラーメッセージが報告されていました。このリリースでは、VMware vSphere のインストールプログラムでは非推奨フィールドとサポート対象フィールドの使用は推奨されないことを示す警告メッセージが追加されました。(OCPBUGS-37628)

- 以前は、Microsoft Azure 上の既存の Azure Virtual Network (VNet) を使用して 2 番目のクラスターをインストールしようとすると、インストールは失敗していました。API サーバーロードバランサーのフロントエンド IP アドレスが指定されていない場合、Cluster API はアドレスを **10.0.0.100** に固定します。この IP アドレスは最初のクラスターによってすでに使用されていたため、2 番目のロードバランサーのインストールに失敗しました。このリリースでは、動的 IP アドレスはデフォルトの IP アドレスが使用可能かどうかを確認します。使用できない場合は、動的 IP によって次の使用可能アドレスが選択され、別のロードバランサー IP を使用して 2 番目のクラスターを正常にインストールできます。(OCPBUGS-37442)

- 以前は、インストールプログラムは、テンプレートフィールドが定義されているかどうかにかかわらず、VMware vSphere に OVA をダウンロードしようとしていました。この更新により、この問題は解決されました。インストールプログラムは、テンプレートフィールドが定義されているかどうかを確認します。テンプレートフィールドが定義されていない場合は、OVA がダウンロードされます。テンプレートフィールドが定義されている場合、OVA はダウンロードされません。(OCPBUGS-36494)

- 以前は、IBM Cloud にクラスターをインストールする場合、インストールプログラムは、サブネットの詳細を名前で検索するときに限りサブネットの最初のグループ (つまり 50) をチェックしていました。このリリースでは、すべてのサブネットを検索するためのページネーションサポートが提供されます。(OCPBUGS-36236)

- 以前は、必要な **compute.firewalls.create** 権限なしで Cluster API Provider Google Cloud Platform (GCP) を共有 Virtual Private Cloud (VPC) にインストールすると、ファイアウォールルールが作成されないためにインストールが失敗しました。このリリースでは、インストール中にファイアウォールを作成するルールをスキップするように修正され、問題が解決されました。(OCPBUGS-35262)

- 以前は、Agent-based Installer の場合、すべてのホストのインターフェイスセクションに **networkConfig** セクションのエントリーと一致するエントリーがない場合、nmstate で定義されたネットワークレイアウトによって設定エラーが発生する可能性がありました。ただし、**networkConfig** セクションのエントリーで物理インターフェイス名を使用する場合は、interfaces セクションのエントリーは必要ありません。

この修正により、**networkConfig** セクションのエントリーに物理インターフェイス名があり

この修正により、**networkConfig** セクションのエントリーに物理インターフェイス名があり、インターフェイステーブルに対応するエントリーがない場合でも、設定でエラーが発生しなくなります。(OCPBUGS-34849)

- 以前は、コンテナーツールモジュールは RHEL ノードでデフォルトで有効になっていました。このリリースでは、競合するリポジトリー間で正しいパッケージをインストールするために、container-tools モジュールが無効になっています。(OCPBUGS-34844)

1.6.10. Insights Operator

- 以前は、IBM Z ハードウェア上で実行されている Red Hat OpenShift Container Platform クラスターでエンタイトルビルドの実行中に、リポジトリーが有効になっていませんでした。この問題は解決されています。IBM Z ハードウェア上で実行されている Red Hat OpenShift Container Platform クラスターで、エンタイトルビルドに実行中にリポジトリーを有効にできるようになりました。(OCPBUGS-32233)

1.6.11. Machine Config Operator

- 以前は、Machine Config Operator (MCO) と出荷された Red Hat Enterprise Linux (RHEL) CoreOS テンプレートが原因で、Red Hat OpenStack Platform (RHOSP) でのノードのスケーリングが失敗していました。この問題は、**systemd** の問題と、古い OpenShift Container Platform バージョンのレガシーブートイメージの存在が原因で発生しました。このリリースでは、パッチによって **systemd** の問題が修正され、レガシーのブートイメージが削除されるため、ノードのスケーリングが期待どおりに継続されます。(OCPBUGS-42324)

- 以前は、クラスター上のレイヤー化を有効にし、マシン設定でカーネル引数を設定しようとすると、マシン設定プール (MCP) とノードがデグレード状態になっていました。これは設定の不一致が原因で発生しました。このリリースでは、引数が設定され、クラスター内のノードに適用されていることを確認するために、OCL が有効になっているクラスターのカーネル引数がチェックされます。この更新により、マシン設定とノード設定の間で以前に発生した不一致が防止されます。(OCPBUGS-34647)

1.6.12. 管理コンソール

- 以前は、Lightspeed モーダルダイアログの "Don't show again" リンクをクリックしても、他のいずれかの **User Preference** タブが表示されている場合、汎用の **User Preference** タブに正しく移動しませんでした。この更新後は、"Don't show again" リンクをクリックすると、汎用の **User Preference** タブに正しく移動します。(OCPBUGS-48106)

- 以前は、OperatorHub モーダルのプライマリーアクションボタンに複数の外部リンクアイコンが表示されることがありました。この更新により、外部リンクアイコンが 1 つだけ表示されます。(OCPBUGS-47742)

- 以前は、クラスター認証設定で認可タイプが **None** に設定されている場合、Web コンソールは無効になっていました。この更新により、認可タイプが **None** に設定されていても、Web コンソールが無効にならなくなりました。(OCPBUGS-46068)

- 以前は、1 つ以上の **spec.config.storage.file** にオプションのデータが含まれていない場合、**MachineConfig Details** タブにエラーが表示されていました。この更新により、エラーは発生しなくなり、**Details** タブが期待どおりにレンダリングされるようになります。(OCPBUGS-44049)

- 以前は、**CSV details** ページに関連するオペランドをリストするために使用されるリソースリストページ拡張機能に、追加の名前プロパティーが渡されていました。その結果、オペランドリストはクラスターサービスバージョン (CSV) 名でフィルター処理され、頻繁に空のリストが

返されました。この更新により、オペランドが期待どおりにリストされるようになりました。(OCPBUGS-42796)

- 以前は、クラスター上に 1 つ以上の ConfigMap ConsoleYAMLSamples が存在する状態で新しい ConfigMap を作成する際に、**Sample** タブは表示されませんでした。この更新後、**Sample** タブには 1 つ以上の ConfigMap ConsoleYAMLSamples が表示されます。(OCPBUGS-41492)

- 以前は、3 つ以上のリソースが選択されている場合、**Events** ページのリソースタイプフィルターでリソース数が誤って報告されていました。この更新により、フィルターは常に正しいリソース数を報告するようになります。(OCPBUGS-38701)

- 以前は、Firefox のダークモードでページを表示すると、**Cluster Settings** ページの更新グラフのバージョン番号テキストが、暗い背景の上に黒いテキストとして表示されていました。この更新により、テキストが白いテキストとして表示されるようになりました。(OCPBUGS-37988)

- 以前は、空の状態の **Alerting** ページにリソース情報は表示されませんでした。この更新により、**Alerting** ページでリソース情報が利用できるようになります。(OCPBUGS-36921)

- 以前は、Operator Lifecycle Manager (OLM) CSV アノテーションに予期しない JSON が含まれていました。これは正常に解析されましたが、結果の値を使用しようとするとランタイムエラーが発生しました。この更新により、OLM アノテーションからの JSON 値は使用前に検証され、エラーがログに記録され、予期しない JSON がアノテーションで受信されてもコンソールが失敗しなくなります。(OCPBUGS-35744)

- 以前は、OpenShift Container Platform Web コンソールの **Overview** ページに、サイレント化されたアラートが表示されていました。これは、アラートに外部ラベルが含まれていなかったために発生しました。このリリースでは、サイレント化されたアラートには外部ラベルが含まれるため、フィルタリングされ、非表示になります。(OCPBUGS-31367)

1.6.13. モニタリング

- 以前は、**emailConfigs** オブジェクトの SMTP **smarthost** または **from** フィールドが **AlertmanagerConfig** カスタムリソース (CR) のグローバルレベルまたは受信者レベルで指定されていない場合、これらのフィールドは必須であるため Alertmanager がクラッシュしていました。このリリースでは、これらのフィールドが指定されていない場合、Prometheus Operator は調整に失敗します。したがって、Prometheus Operator は無効な設定を Alertmanager にプッシュしなくなり、クラッシュを防止できます。(OCPBUGS-48050)

- 以前は、Cluster Monitoring Operator (CMO) は、**cluster-monitoring-config** および **user-workload-monitoring-config** config map 内の設定で、不明なフィールド (サポートされなくなったフィールドなど) または重複したフィールドを無効としてマークしませんでした。このリリースでは、このようなエラーを識別するのに役立つ、より厳格な検証が追加されました。(OCPBUGS-42671)

- 以前は、ユーザーが **POST** リクエストを使用して、ユーザーワークロードモニタリング Thanos API エンドポイントを照会できませんでした。この更新により、クラスター管理者は、新しい **pod-metrics-reader** クラスターロールをロールバインディングまたはクラスターロールバインディングにバインドして、ユーザーまたはサービスアカウントの **POST** クエリーを許可できるようになります。(OCPBUGS-41158)

- 以前は、コアプラットフォームモニタリング、ユーザーワークロードモニタリング、またはその両方の無効な config map 設定により、Cluster Monitoring Operator (CMO) が **InvalidConfiguration** エラーを報告していました。このリリースでは、ユーザーワークロードモニタリング設定のみが無効な場合、CMO は **UserWorkloadInvalidConfiguration** を報告し、問題の場所を明確にします。(OCPBUGS-33863)

- 以前は、**telemeter-client containers** は複数のクラスターで **TelemeterClientFailures Warnings** メッセージを表示していました。このリリースでは、アラートがトリガーされる原因を説明するための **TelemeterClientFailures** アラートの runbook が追加され、アラートで解決ステップが提供されます。(OCPBUGS-33285)

- 以前は、無効な子ルートを持つ **AlertmanagerConfig** オブジェクトによって無効な Alertmanager 設定が生成され、Alertmanager の中断を引き起こしていました。このリリースでは、Prometheus Operator はこのような **AlertmanagerConfig** オブジェクトを拒否し、ユーザーはログで無効な子ルートに関する警告を受け取ります。(OCPBUGS-30122)

- 以前は、**ServiceMonitor** 設定で未設定の環境変数が使用されている場合、ユーザー定義プロジェクトの Prometheus の **config-reloader** が失敗し、Prometheus Pod が失敗していました。このリリースでは、未設定の環境変数が検出されてもリローダーが失敗しなくなりました。代わりに、未設定の環境変数はそのまま残され、設定済みの環境変数は通常どおり展開されます。抑制されているかどうかにかかわらず、すべての拡張エラーは **reloader_config_environment_variable_expansion_errors** 変数を通じて追跡できます。(OCPBUGS-23252)

1.6.14. ネットワーク

- 以前は、Open vSwitch 接続インターフェイスで IPSec を使用するときに Encapsulated Security Payload (ESP) オフロードハードウェアを有効にすると、クラスターの接続が切断されました。この問題を解決するために、OpenShift Container Platform では、Open vSwitch 接続インターフェイス上の ESP オフロードハードウェアがデフォルトで無効になりました。これにより問題が解決されました。(OCPBUGS-42987)

- 以前は、デフォルトの **sriovOperatorConfig** カスタムリソース (CR) を削除すると、最初に **ValidatingWebhookConfiguration** が削除されないため、デフォルトの **sriovOperatorConfig** CR を再作成できませんでした。このリリースでは、**sriovOperatorConfig** CR を削除すると、Single Root I/O Virtualization (SR-IOV) Network Operator が検証 Webhook を削除するため、新しい **sriovOperatorConfig** CR を作成できます。(OCPBUGS-41897)

- 以前は、カスタムリソース (CR) にカスタムアノテーションを設定すると、SR-IOV Operator によって **SriovNetwork** CR 内のすべてのデフォルトアノテーションがオーバーライドされていました。このリリースでは、CR でカスタムアノテーションを定義しても、SR-IOV Operator によってデフォルトのアノテーションがオーバーライドされません。(OCPBUGS-41352)

- 以前は、**active-backup** モードで設定されたボンディングでは、基礎となるリンクが IPsec Encapsulating Security Payload (ESP) オフロードをサポートしていなくても、ESP オフロードがアクティブになっていました。これにより、IPsec アソシエーションが失敗しました。このリリースでは、IPsec アソシエーションが通過できるように、ボンディングの ESP オフロードが無効になっています。(OCPBUGS-39438)

- 以前は、Machine Config Operator (MCO) の vSphere **resolve-prepender** スクリプトが、OpenShift Container Platform 4 で使用されていた古いブートイメージバージョンと互換性のない **systemd** ディレクティブを使用していました。このリリースでは、手動による介入か、この修正を含むリリースへのアップグレードによって、新しいブートイメージバージョン 4.18 4.13 以降を使用してノードをスケーリングできるようになりました。(OCPBUGS-38012)

- 以前は、**CanaryRepetitiveFailures** 条件の移行時間の問題により、Ingress Controller のステータスが **Degraded=False** と誤表示されていました。このリリースでは、**CanaryRepetitiveFailures** 条件が存在する間 (適切な表示期間) は、Ingress Controller のステータスが **Degraded=True** として正しくマークされるようになりました。(OCPBUGS-37491)

- 以前は、Egress IPv6 が割り当てられているノードで Pod が実行されている場合、その Pod はデュアルスタッククラスター内の Kubernetes サービスと通信できませんでした。その結果、egressIP が適用されない IP ファミリーのトラフィックがドロップされました。このリリースでは、Egress IP が適用された IP ファミリーの Source Network Address Translation (SNAT) のみが削除され、トラフィックがドロップされるリスクがなくなります。(OCPBUGS-37193)

- 以前は、Single-Root I/O Virtualization (SR-IOV) Operator は、Operator のシャットダウン操作中に取得したリースを期限切れにしませんでした。新規インスタンスはリースの有効期限が切れなければ動作可能にならないため、これは Operator の新規インスタンスに影響を与えました。このリリースでは、Operator シャットダウンロジックが更新され、Operator がシャットダウンするときに Operator のリースが期限切れになるようになりました。(OCPBUGS-23795)

- 以前は、**IngressWithoutClassName** アラートを持つ Ingress リソースの場合、Ingress コントローラーはリソース削除時にアラートを削除しませんでした。アラートは、引き続き OpenShift Container Platform Web コンソールに表示されました。このリリースでは、Ingress コントローラーは Ingress リソースを削除する前に **openshift_ingress_to_route_controller_ingress_without_class_name** メトリクスを **0** にリセットするため、アラートが削除され、Web コンソールに表示されなくなります。(OCPBUGS-13181)

- 以前は、**clusterNetwork** または **serviceNetwork** IP アドレスプールのいずれかがデフォルトの **transit_switch_subnet 100.88.0.0/16** IP アドレスと重複し、**transit_switch_subnet** のカスタム値が有効にならない場合、ライブマイグレーション操作後に **ovnkube-node** Pod がクラッシュしていました。このリリースでは、**transit_switch_subnet** のカスタム値を **ovnkube node** Pod に渡すことができるため、この問題は発生しなくなりました。(OCPBUGS-43740)

- 以前は、**appProtocol** 値の **h2c** を **kubernetes.io/h2c** に標準化する OVN-Kubernetes の変更は、OpenShift ルーターによって認識されませんでした。その結果、サービスで **appProtocol: kubernetes.io/h2c** を指定しても、OpenShift ルーターはクリアテキスト HTTP/2 を使用してサービスエンドポイントに接続しませんでした。このリリースでは、OpenShift ルーターが変更され、**appProtocol: h2c** を処理するのと同じ方法で **appProtocol: kubernetes.io/h2c** を処理するようになり、問題が解決されました。(OCPBUGS-42972)

- 以前は、IBM Power Virtual Server、Alibaba Cloud、および Red Hat OpenStack Platform (RHOSP) では、**LoadBalancer** パラメーターを **External** から **Internal** に変更した後にユーザーをガイドする手順がありませんでした。これにより、Ingress コントローラーは永続的に **Progressing** の状態になりました。このリリースでは、**The IngressController scope was changed from Internal to External** のメッセージの後に **To effectuate this change, you must delete the service** のメッセージが表示され、**Progressing** 状態が永続化される問題が解決されました。(OCPBUGS-39151)

- 以前は、Ingress からルートへの変換に失敗してエラーが発生した場合、イベントはログに記録されませんでした。この更新により、このエラーがイベントログに表示されるようになりました。(OCPBUGS-29354)

- 以前は、cgroup v1 を使用するノード上の **ovnkube-node** Pod は、kubelet cgroup パスを見つけられないため失敗していました。このリリースでは、ノードが cgroup v1 を使用している場合でも **ovnkube-node** Pod が失敗しなくなりました。ただし、OVN-Kubernetes ネットワークプラグインは、**UDNKubeletProbesNotSupported** イベント通知を出力します。各ノードに対して cgroup v2 を有効にすると、OVN-Kubernetes はイベント通知を出力しなくなります。(OCPBUGS-50513)

- 以前は、Layer 2 トポロジーを使用する kubevirt 仮想マシンのライブマイグレーションを完了すると、古いノードは引き続き IPv4 Egress トラフィックを仮想マシンに送信していました。

このリリースでは、OVN-Kubernetes プラグインはライブマイグレーションプロセス中に kubevirt 仮想マシンのゲートウェイ MAC アドレスを更新するため、この問題は発生しなくなりました。(OCPBUGS-49857)

- 以前は、DNS ベースの Egress ファイアウォールは、大文字の DNS 名が含まれるファイアウォールルールの作成を誤って妨げていました。このリリースでは、Egress ファイアウォールの修正により、大文字の DNS 名が含まれるファイアウォールルールの作成が妨げられなくなりました。(OCPBUGS-49589)

- 以前は、Cluster Network Operator (CNO) を使用して既存の **localnet** ネットワークを持つクラスターをアップグレードしようとすると、**ovnkube-control-plane** Pod の実行が失敗していました。これは、**ovnkube-cluster-manager** コンテナーが、サブネットが定義されていない OVN-Kubernetes **localnet** トポロジーネットワークを処理できなかったために発生していました。このリリースでは、修正により、**ovnkube-cluster-manager** コンテナーが、サブネットが定義されていない OVN-Kubernetes **localnet** トポロジーネットワークを処理できるようになりました。(OCPBUGS-44195)

- 以前は、クラウドネイティブネットワーク (CNF) ワーカーが Red Hat OpenStack Platform (RHOSP) 上のコンフィグドライブを使用してデプロイされた場合、SR-IOV Network Operator がメタデータを取得できませんでした。イミュータブルなシステムでは、ブート操作後にコンフィグドライブがアンマウントされることが多いため、この Operator は必要に応じて設定ドライブを動的にマウントするようになりました。Operator はメタデータを取得し、コンフィグドライブをアンマウントできるようになりました。つまり、コンフィグドライブを手動でマウントまたはアンマウントする必要がなくなります。(OCPBUGS-41829)

- 以前は、別のロードバランサーを使用するためにクラスターを切り替えると、Ingress Operator は **IngressController** カスタムリソース (CR) ステータスの **classicLoadBalancer** および **networkLoadBalancer** パラメーターから値を削除しませんでした。この状況により、CR のステータスで **classicLoadBalancer** および **networkLoadBalancer** パラメーターからの誤った情報が報告されました。このリリースでは、別のロードバランサーを使用するためにクラスターを切り替えると、これらのパラメーターから Ingress Operator が値を削除し、CR はより正確で混乱の少ないメッセージステータスを報告します。(OCPBUGS-38217)

- 以前は、重複したフィーチャーゲートである **ExternalRouteCertificate** が **FeatureGate** CR に追加されていました。このリリースでは、OpenShift Container Platform クラスターがこのフィーチャーゲートを使用しないため、**ExternalRouteCertificate** は削除されました。(OCPBUGS-36479)

- 以前は、ユーザーがルート作成後にルートの **.spec.tls.externalCertificate** フィールドを編集するには、**routes/custom-host** サブリソースに対する **create** 権限と **update** 権限の両方が必要でした。このリリースでは、この権限要件が修正され、ルートの **.spec.tls.externalCertificate** フィールドを編集するためにユーザーに必要な権限が **create** のみになりました。**update** 権限はオプションの権限としてマークされるようになりました。(OCPBUGS-34373)

1.6.15. ノード

- 以前は、コンテナーネットワークメトリクスを収集して報告する **cadvisor** コードに、不正確な結果を引き起こすバグが含まれていました。このリリースでは、コンテナーネットワークメトリクスが正しく報告されるようになりました。(OCPBUGS-38515)

1.6.16. Node Tuning Operator (NTO)

- 以前は、256 個を超える CPU を搭載したマシンでは、割り込み処理およびネットワーク処理の CPU アフィニティーの CPU マスクが正しく計算されませんでした。この問題により、CPU の適切な分離が妨げられ、内部ノードの設定中に **systemd** ユニット障害が発生しました。この修

正により、CPU アフィニティーが正確に計算されるようになり、256 個を超える CPU を搭載したマシンで CPU を正しく分離できるようになります。(OCPBUGS-36431)

- 以前は、**PerformanceProfile** リソースの **spec.cpu** 配下の **cpuset** フィールドに無効な値を入力すると、Webhook 検証がクラッシュしていました。このリリースでは、**PerformanceProfile** 検証 Webhook のエラー処理が改善され、これらのフィールドの無効な値が情報エラーとして返されるようになりました。(OCPBUGS-45616)

- 以前は、パフォーマンスプロファイル内の CPU セットに対して無効な文字列を入力すると、クラスターが壊れる可能性がありました。このリリースでは、修正により、入力できる文字列が有効なものだけになり、クラスターが破損するリスクが排除されました。(OCPBUGS-47678)

- 以前は、**PerformanceProfiles** を使用して Node Tuning Operator (NTO) を設定すると、 **ocp-tuned-one-shot systemd** サービスが作成され、これが kubelet の前に実行され、その実行をブロックしていました。**systemd** サービスは、NTO イメージを使用する Podman を呼び出しました。NTO イメージが存在しない場合、Podman がイメージを取得しようとしました。このリリースでは、**/etc/mco/proxy.env** で定義されたクラスター全体のプロキシー環境変数のサポートが追加されました。このサポートにより、Podman は、クラスター外接続に **http(s)** プロキシーを使用する必要がある環境で NTO イメージをプルできるようになります。(OCPBUGS-39005)

1.6.17. 可観測性

- 以前は、アラートグラフの完全なクラスタークエリーに namespace が渡されることで、テナンシー API パスが使用されていました。API にはデータの取得権限がなかったため、アラートグラフにデータが表示されませんでした。このリリースにより、アラートグラフの完全なクラスタークエリーに namespace が渡されなくなりました。この API にはデータを取得するための適切な権限があるため、非テナンシー API パスが使用されるようになりました。アラートグラフでデータは利用できません。(OCPBUGS-46371)

- 以前は、境界は棒グラフの最初のバーに基づいていました。バーのサイズが最初のバーよりも大きい場合、そのバーは棒グラフの境界を超えて拡張されます。このリリースにより、棒グラフの境界は最大のバーに基づいているため、棒グラフの境界の外側にバーが伸びることがなくなりました。(OCPBUGS-46059)

- 以前は、Red Hat Advanced Cluster Management (RHACM) Alerting UI リファクタリングの更新により、**Observe → Metrics** メニューで **isEmpty** チェックがありませんでした。チェックが欠落していたために、**Show all Series** および **Hide all Series** 状態の動作が反転していました。このリリースでは、**isEmpty** チェックが再度追加されたため、シリーズが非表示のときに **Show all Series** が表示されるようになり、シリーズが表示されているときに **Hide all Series** が表示されるようになりました。(OCPBUGS-46047)

- 以前は、**Observe → Alerting → Silences**タブで、**DateTime** コンポーネントによってイベントの順序とその値が変更されていました。この問題が原因で、**Developer** または **Administrator** のどちらのパースペクティブでも、サイレントアラートの **until** パラメーターを編集できませんでした。このリリースにより、**DateTime** コンポーネントが修正され、サイレントアラートの **until** パラメーターを編集できるようになりました。(OCPBUGS-46021)

- 以前は、カスタムエディターで **Developer** パースペクティブを使用する場合、**n** キーをクリックすると **Namespace** メニューが予期せず開きました。この問題は、キーボードショートカットがカスタムエディターを考慮しないために発生しました。このリリースでは、**Namespace** メニューはカスタムエディターを考慮し、**n** キーを押しても開きません。(OCPBUGS-38775)

- 以前は、**Observe → Alerting → Silences**タブの **creator** フィールドが自動入力されず、必須として指定されていませんでした。この問題は、OpenShift Container Platform 4.15 以降で API

がフィールドを空にすると発生しました。この更新により、フィールドが必須としてマークされ、正しい検証のために現行ユーザーが入力されるようになりました。(OCPBUGS-35048)

1.6.18. oc-mirror

- 以前は、**oc-mirror --v2 delete --generate** コマンドを使用すると、**working-dir/cluster-resources** ディレクトリーの内容がクリアされていました。この修正により、削除機能が使用されたときに **working-dir/cluster-resources** ディレクトリーはクリーンアップされなくなります。(OCPBUGS-48430)

- 以前は、リリースイメージは **SHA-1** キーを使用して署名されていました。RHEL 9 FIPS STIG 準拠のマシンでは、弱いキーに対するセキュリティー制限のため、古い **SHA-1** キーを使用したリリース署名の検証が失敗しました。このリリースでは、リリースイメージは新しい **SHA-256** 信頼済みキーを使用して署名されるため、リリース署名が失敗しなくなりました。(OCPBUGS-48314)

- 以前は、**--force-cache-delete** フラグを使用してリモートレジストリーからイメージを削除すると、削除プロセスが期待どおりに機能しませんでした。この更新により問題は解決され、フラグを使用するとイメージが適切に削除されるようになりました。(OCPBUGS-47690)

- 以前は、部分的に切り離されたミラーリングワークフロー (ミラー間) をミラーリングに使用すると、oc-mirror プラグイン v2 はグラフイメージを削除できませんでした。この更新により、使用されているミラーリングワークフローに関係なく、グラフイメージを削除できるようになりました。(OCPBUGS-46145)

- 以前は、複数の OpenShift Container Platform リリースコンポーネントで同じイメージが使用されている場合、oc-mirror プラグイン v2 はイメージの削除を複数回試行し、最初の試行の後は失敗していました。この問題は、oc-mirror プラグイン v2 が **--generate** 削除フェーズ中に一意のイメージのリストを生成するようにしたことで解決されました。(OCPBUGS-45299)

- 以前は、ディスク上の **oci** カタログは oc-mirror プラグイン v2 で正しくミラーリングされませんでした。この更新により、**oci** カタログが正常にミラーリングされるようになりました。(OCPBUGS-44225)

- 以前は、**oc-mirror** コマンドを再実行すると、**oci** カタログの再構築が失敗し、エラーが生成されていました。このリリースでは、**oc-mirror** コマンドを再実行すると、ワークスペースファイルが削除されるため、カタログが失敗する問題が発生しなくなります。(OCPBUGS-45171)

- 以前は、最初の試行で **oc adm node-image create** コマンドを実行すると、**image can't be pulled** のエラーメッセージが生成されることがありました。このリリースでは、再試行メカニズムにより、リリースペイロードからイメージをプルする際の一時的な障害に対処します。(OCPBUGS-44388)

- 以前は、**clusterresource** オブジェクトで作成された署名付き **ConfigMap YAML** ファイルおよび **JSON** ファイルに重複したエントリーが表示される場合があり、クラスターへの適用時に問題が発生していました。この更新により、生成されたファイルに重複が含まれなくなります。(OCPBUGS-42428)

- 以前は、oc-mirror プラグイン v2 のリリース署名 **ConfigMap** が、**cluster-resources** フォルダーではなく、アーカイブされた TAR ファイルに誤って保存されていました。これにより、**mirror2disk** が失敗しました。このリリースでは、oc-mirror プラグイン v1 と互換性のある JSON 形式または YAML 形式の oc-mirror プラグイン v2 のリリース署名 **ConfigMap** が、**cluster-resources** フォルダーに保存されるようになりました。(OCPBUGS-38343) および (OCPBUGS-38233)

- 以前は、無効なログレベルフラグを使用すると、oc-mirror プラグイン v2 がパニックを起こしていました。この更新により、oc-mirror プラグイン v2 が無効なログレベルを適切に処理できるようになります。さらに、ユーザーの利便性を考慮して、**loglevel** フラグの名前が Podman などのツールに合わせて **log-level** に変更されました。(OCPBUGS-37740)

1.6.19. OpenShift CLI (oc)

- 以前は、**oc adm node-image create --pxe generated** コマンドでは、Preboot Execution Environment (PXE) アーティファクトのみが作成されませんでした。代わりに、**node-joiner** Pod からの他のアーティファクトとともに PXE アーティファクトが作成され、それらすべてが間違ったサブディレクトリーに保存されていました。さらに、PXE アーティファクトに、**node** ではなく **agent** という接頭辞が誤って付けられていました。このリリースにより、生成された PXE アーティファクトは正しいディレクトリーに保存され、正しい接頭辞が付けられます。(OCPBUGS-46449)

- 以前は、リクエストに一致するアドミッション Webhook があると、**deploymentconfig/scale** サブリソースへのリクエストが失敗しました。このリリースでは、問題は解決され、**deploymentconfig/scale** サブリソースへのリクエストは成功します。(OCPBUGS-41136)

1.6.20. Operator Lifecycle Manager (OLM)

- 以前は、Operator Lifecycle Manager (OLM) Classic で同じ namespace を同時に調整すると、サブスクリプションで **ConstraintsNotSatisfiable** エラーが発生しました。今回の更新で問題が解決されました。(OCPBUGS-48660)

- 以前は、カタログソーススナップショットが多すぎると、パフォーマンスに重大なリグレッションが発生していました。この更新でこの問題が修正されています。(OCPBUGS-48644)

- 以前は、kubelet が **TerminationByKubelet** メッセージでカタログレジストリー Pod を終了すると、catalog Operator によってレジストリー Pod が再作成されませんでした。この更新でこの問題が修正されています。(OCPBUGS-46474)

- 以前は、TLS 検証エラーが原因で OLM (Classic) は Operator クラスターサービスバージョン (CSV) のアップグレードに失敗しました。この更新でこの問題が修正されています。(OCPBUGS-43581)

- 以前は、Operator グループのサービスアカウントトークンは、Operator Lifecycle Manager (OLM) Classic で自動的に生成されませんでした。この更新でこの問題が修正されています。(OCPBUGS-42360)

- 以前は、Operator Lifecycle Manager (OLM) v1 がカスタムリソース定義 (CRD) のアップグレードを検証した場合、変更されたデフォルト値を検出したときのメッセージ出力は、人間が判読できる言語ではなくバイトでレンダリングされていました。この更新により、関連メッセージが更新され、人間が判読できる値が表示されるようになりました。(OCPBUGS-41726)

- 以前は、Catalog Operator で接続エラーが発生してもステータス更新機能はエラーを返しませんでした。その結果、IP アドレスが **nil** ステータスを返すために Operator がクラッシュする可能性がありました。この更新により問題が解決され、エラーメッセージが返され、Operator がクラッシュしなくなりました。(OCPBUGS-37637)

- 以前は、カタログソースレジストリー Pod はクラスターノードの障害から回復しませんでした。この更新でこの問題が修正されています。(OCPBUGS-36661)

- 以前は、カスタムリソース (CR) を多数持つ Operator が API サーバーのタイムアウトを超えていました。その結果、Operator のインストールプランが保留状態のままになっていました。こ

の更新では、クラスターにデプロイされた CR のリストのページビューを追加することで、問題が修正されます。(OCPBUGS-35358)

1.6.21. Performance Addon Operator

- 以前は、論理プロセッサーのコア ID 番号 (ソケットあたりのコア) が異なり、同じノードプールに存在するコンピュートノードのパフォーマンスプロファイルを、Performance Profile Creator (PPC) が構築できませんでした。たとえば、論理プロセッサー **2** と **18** を持つ 2 つのコンピュートノードがあり、一方のノードがそれらをコア ID **2** としてグループ化し、もう一方のノードがそれらをコア ID **9** としてグループ化している状況で、PPC が失敗しました。
このリリースにより、論理プロセッサーのコア ID 番号がそれぞれ異なるコンピュートノードを持つクラスターのパフォーマンスプロファイルを、PPC が作成できるようになりました。そのため、PPC がパフォーマンスプロファイルの作成に失敗しなくなりました。PPC は、生成されたパフォーマンスプロファイルを注意して使用する必要があることを示す警告メッセージを出力するようになりました。コア ID 番号が異なると、システムの最適化や分離されたタスク管理に影響が生じる可能性があるためです。(OCPBUGS-45903)

- 以前は、パフォーマンスプロファイルで **0,1,2,...,512** などの分離された CPU の長い文字列を指定すると、**tuned**、Machine Config Operator、および **rpm-ostree** コンポーネントが期待どおりに文字列を処理できませんでした。その結果、パフォーマンスプロファイルの適用後に、あるはずのカーネル引数が欠落していました。システムは失敗し、エラーは報告されませんでした。このリリースにより、パフォーマンスプロファイル内の分離された CPU の文字列が、**0-512** などの連続した範囲に変換されます。その結果、ほとんどのシナリオでカーネル引数が期待どおりに適用されます。(OCPBUGS-45472)

注記

パフォーマンスプロファイル内の分離された CPU の入力の組み合わせによっては、**1,3,5,...,511** のような奇数の長いリストなど、引き続き問題が発生する可能性があります。

1.6.22. Red Hat Enterprise Linux CoreOS (RHCOS)

- 以前は、暗号化されたローカルディスクを開こうとすると、**kdump** initramfs が応答しなくなりました。これは、**kdump** の送信先がローカルディスクにアクセスする必要がないリモートマシンの場合でも発生しました。このリリースでは、この問題が修正され、**kdump** initramfs が暗号化されたローカルディスクを正常に開くようになりました。(OCPBUGS-43040)

- 以前は、**fips=0** で FIPS モードを明示的に無効にすると、FIPS モードが要求されたと想定した一部の systemd サービスが実行され、結果的に失敗していました。この問題により、RHCOS の起動に失敗しました。このリリースでは、**fips=1** を指定して FIPS モードを有効にしている場合にのみ、関連する systemd サービスが実行されるようになりました。その結果、**fips=0** が指定されている場合、RHCOS は FIPS モードを有効にせずに正しく起動するようになりました。(OCPBUGS-39536)

1.6.23. スケーラビリティーおよびパフォーマンス

- 以前は、NUMA Resources Operator を設定して、**nodeGroup** を複数の **MachineConfigPool** にマッピングできました。この実装は、**nodeGroup** と **MachineConfigPool** 間の 1 対 1 のマッピングを前提とした Operator の意図した設計に反しています。このリリースでは、**nodeGroup** が複数の **MachineConfigPool** にマッピングされている場合、Operator は設定を受け入れますが、Operator の状態は **Degraded** に遷移します。以前の動作を維持するに

は、NUMA Resources Operator に **config.node.openshift-kni.io/multiple-pools-per-tree: enabled** アノテーションを適用できます。ただし、**nodeGroup** を複数の **MachineConfigPool** に割り当てる機能は、今後のリリースでは削除される予定です。(OCPBUGS-42523)

1.6.24. ストレージ

- 以前は、アップストリームパッチを含めない場合、Portworx プラグインの Container Storage Interface (CSI) の移行が失敗していました。このリリースでは、Portworx プラグインの CSI 変換によって、シークレット名と namespace が Kubernetes バージョン 1.31 にコピーされるようになったため、アップストリームパッチは不要になりました。(OCPBUGS-49437)

- 以前は、VSphere Problem Detector Operator は、VMware vSphere クラスターの **clustercsidrivers.managementState** パラメーターの **Managed** から **Removed** への変更を反映するのに最大 24 時間待機していました。このリリースでは、VSphere Problem Detector Operator がこの状態の変更を約 1 時間で反映するようになりました。(OCPBUGS-39358)

- 以前は、Azure File Driver は既存のストレージアカウントを再利用しようとしていました。このリリースでは、Azure File Driver は動的プロビジョニング中にストレージアカウントを作成します。つまり、新しく作成された永続ボリューム (PV) を使用する更新されたクラスターも新しいストレージアカウントを使用します。以前にプロビジョニングされた PV は、クラスターの更新前に使用されたのと同じストレージアカウントを引き続き使用します。(OCPBUGS-38922)

- 以前は、**INI** が成功したときに、設定ローダーによって YAML **unmarshall** エラーがログに記録されていました。このリリースでは、**INI** が成功したときに、**unmarshall** エラーがログに記録されなくなりました。(OCPBUGS-38368)

- 以前は、Storage Operator はクラスター内に存在するコントロールプレーンノードの数を誤ってカウントしていました。この数は、Operator がコントローラーのレプリカの数を決定するために必要です。このリリースでは、Storage Operator がコントロールプレーンノードの数を正しくカウントするようになり、レプリカコントローラーの数がより正確になりました。(OCPBUGS-36233)

- 以前は、設定の問題により、**manila-csi-driver** およびノード registrar Pod のヘルスチェックが欠落していました。このリリースでは、両方のリソースにヘルスチェックが追加されました。(OCPBUGS-29240)

1.7. テクノロジープレビュー機能のステータス

現在、こ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

次の表では、機能は次のステータスでマークされています。

- **利用不可**
- **テクノロジープレビュー**
- **一般提供**
- **非推奨**
- **削除**

1.7.1. 認証と認可のテクノロジープレビュー機能

表1.18 認証と認可のテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
Pod セキュリティーアドミッションの制限付き適用	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

1.7.2. エッジコンピューティングのテクノロジープレビュー機能

表1.19 エッジコンピューティングのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
GitOps ZTP の高速プロビジョニング	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
TPM と PCR の保護によるディスク暗号化の有効化	利用不可	テクノロジープレビュー	テクノロジープレビュー

1.7.3. インストールのテクノロジープレビュー機能

表1.20 インストールのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
kvc を使用したノードへのカーネルモジュールの追加	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
SR-IOV デバイスの NIC パーティショニングの有効化	テクノロジープレビュー	一般提供	一般提供
Google Cloud のユーザー定義ラベルとタグ	テクノロジープレビュー	一般提供	一般提供
Assisted Installer を使用して Alibaba Cloud にクラスターをインストールする	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
RHEL の BuildConfigs で共有資格をマウントする	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

機能	4.16	4.17	4.18
OpenShift Container Platform on Oracle® Cloud Infrastructure (OCI)	一般提供	一般提供	一般提供
選択可能なクラスターインベントリー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Cluster API 実装を使用して Google Cloud にクラスターをインストールする	テクノロジープレビュー	一般提供	一般提供
Oracle Compute Cloud@Customer (C3) 上の OpenShift Container Platform	利用不可	利用不可	一般提供
Oracle Private Cloud Appliance (PCA) 上の OpenShift Container Platform	利用不可	利用不可	一般提供
複数のネットワークインターフェイスコントローラーを備えた VMware vSphere にクラスターをインストールする	利用不可	利用不可	テクノロジープレビュー

1.7.4. Machine Config Operator のテクノロジープレビュー機能

表1.21 Machine Config Operator のテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
MCO の状態レポート機能の改善 (**oc get machineconfignode**)	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
クラスター上の RHCOS イメージのレイヤー化	テクノロジープレビュー	テクノロジープレビュー	一般提供
node disruption policy	テクノロジープレビュー	一般提供	一般提供
GCP クラスターのブートイメージの更新	テクノロジープレビュー	一般提供	一般提供
AWS クラスターのブートイメージの更新	テクノロジープレビュー	テクノロジープレビュー	一般提供

機能	4.16	4.17	4.18
ピン留めされたイメージセット	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

1.7.5. マシン管理テクノロジープレビュー機能

表1.22 マシン管理のテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
Amazon Web Services の Cluster API を使用したマシン管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Google Cloud の Cluster API を使用したマシン管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
IBM Power® Virtual Server の Cluster API を使用したマシンの管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Microsoft Azure の Cluster API を使用してマシンを管理する	利用不可	利用不可	テクノロジープレビュー
RHOSP の Cluster API を使用したマシンの管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
VMware vSphere の Cluster API を使用したマシンの管理	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
IBM Power® Virtual Server のクラウドコントローラーマネージャー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
コントロールプレーンマシンセットの vSphere 障害ドメインの定義	一般提供	一般提供	一般提供
Alibaba Cloud のクラウドコントローラーマネージャー	削除	削除	削除
コンピュートマシンセットを使用して既存の VMware vSphere クラスターに複数のサブネットを追加する	利用不可	利用不可	テクノロジープレビュー

1.7.6. モニタリングのテクノロジープレビュー機能

表1.23 モニタリングのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
メトリクス収集プロファイル	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

1.7.7. Web コンソールのテクノロジープレビュー機能

表1.24 Web コンソールのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
OpenShift Container Platform Web コンソール内の Red Hat OpenShift Lightspeed	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

1.7.8. マルチアーキテクチャーのテクノロジープレビュー機能

表1.25 マルチアーキテクチャーのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
arm64 アーキテクチャーでの **kdump**	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
s390x アーキテクチャーでの **kdump**	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
ppc64le アーキテクチャーでの **kdump**	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Multiarch Tuning Operator	一般提供	一般提供	一般提供
イメージストリームのインポートモードの動作を設定するためのサポート	利用不可	利用不可	テクノロジープレビュー

1.7.9. ネットワークのテクノロジープレビュー機能

表1.26 ネットワークのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
eBPF マネージャー Operator	該当なし	テクノロジープレビュー	テクノロジープレビュー
特定の IP アドレスプールを使用した、ノードのサブセットから MetalLB サービスの L2 モードを使用したアドバタイズ	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
インターフェイス固有の安全な sysctls リストの更新	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Egress サービスのカスタムリソース	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
BGPPeer カスタムリソースの VRF 仕様	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
NodeNetworkConfigurationPolicy カスタムリソースの VRF 仕様	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
SR-IOV VF のホストネットワーク設定	テクノロジープレビュー	一般提供	一般提供
MetalLB と FRR-K8 のインテグレーション	テクノロジープレビュー	一般提供	一般提供
PTP グランドマスタークロックの自動うるう秒処理	利用不可	一般提供	一般提供
PTP イベント REST API v2	利用不可	一般提供	一般提供
NMState を使用するために OVN-Kubernetes で必要なカスタマイズされた **br-ex** ブリッジ	一般提供	一般提供	一般提供
OpenShift SDN から OVN-Kubernetes へのライブマイグレーション	利用不可	一般提供	利用不可
ユーザー定義のネットワークセグメンテーション	利用不可	テクノロジープレビュー	一般提供

機能	4.16	4.17	4.18
Dynamic Configuration Manager	利用不可	利用不可	テクノロジープレビュー
Intel C741 Emmitsburg Chipset の SR-IOV Network Operator サポート	利用不可	利用不可	テクノロジープレビュー
ARM アーキテクチャーでの SR-IOV Network Operator のサポート	利用不可	利用不可	一般提供

1.7.10. ノードテクノロジープレビュー機能

表1.27 ノードのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
MaxUnavailableStatefulSet featureset	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
sigstore サポート	利用不可	テクノロジープレビュー	テクノロジープレビュー

1.7.11. OpenShift CLI (oc) のテクノロジープレビュー機能

表1.28 OpenShift CLI (oc) のテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
oc-mirror プラグイン v2	テクノロジープレビュー	テクノロジープレビュー	一般提供
oc-mirror プラグイン v2 エンクレーブのサポート	テクノロジープレビュー	テクノロジープレビュー	一般提供
oc-mirror プラグイン v2 削除機能	テクノロジープレビュー	テクノロジープレビュー	一般提供

1.7.12. 拡張機能のテクノロジープレビュー機能

表1.29 拡張機能のテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
Operator Lifecycle Manager (OLM) v1	テクノロジープレビュー	テクノロジープレビュー	一般提供
sigstore 署名を使用したコンテナーイメージの OLM v1 ランタイム検証	利用不可	利用不可	テクノロジープレビュー

1.7.13. Operator のライフサイクルと開発テクノロジープレビュー機能

表1.30 Operator のライフサイクルおよび開発のテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
Operator Lifecycle Manager (OLM) v1	テクノロジープレビュー	テクノロジープレビュー	一般提供
ハイブリッド Helm ベースの Operator プロジェクト用のスキャフォールディングツール	非推奨	非推奨	削除
Java ベースの Operator プロジェクト用のスキャフォールディングツール	非推奨	非推奨	削除

1.7.14. Red Hat OpenStack Platform (RHOSP) テクノロジープレビュー機能

表1.31 RHOSP テクノロジープレビュートラッカー

機能	4.16	4.17	4.18
Cluster CAPI Operator への RHOSP の統合	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
ローカルディスク上の **rootVolumes** と **etcd** を備えたコントロールプレーン	テクノロジープレビュー	一般提供	一般提供

1.7.15. スケーラビリティとパフォーマンステクノロジープレビュー機能

表1.32 スケーラビリティとパフォーマンスのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18

機能	4.16	4.17	4.18
factory-precaching-cli ツール	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
ハイパースレッディング対応の CPU マネージャーポリシー	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
マウント namespace のカプセル化	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Node Observability Operator	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
etcd データベースサイズの増加	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
RHACM **PolicyGenerator** リソースを使用して GitOps ZTP クラスターポリシーを管理する	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

1.7.16. ストレージのテクノロジープレビュー機能

表1.33 ストレージのテクノロジープレビュートラッカー

機能	4.16	4.17	4.18
AWS EFS ストレージ CSI 使用状況メトリクス	利用不可	一般提供	一般提供
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	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー
Azure File CSI スナップショットのサポート	利用不可	テクノロジープレビュー	テクノロジープレビュー
Read Write Once Pod アクセスモード	一般提供	一般提供	一般提供
OpenShift ビルドの共有リソース CSI Driver	テクノロジープレビュー	テクノロジープレビュー	テクノロジープレビュー

機能	4.16	4.17	4.18
Secrets Store CSI Driver Operator	テクノロジープレビュー	テクノロジープレビュー	一般提供
CIFS/SMB CSI Driver Operator	テクノロジープレビュー	テクノロジープレビュー	一般提供
VMware vSphere 複数 vCenter のサポート	利用不可	テクノロジープレビュー	一般提供
vSphere でのストレージの無効化/有効化	利用不可	テクノロジープレビュー	テクノロジープレビュー
RWX/RWO SELinux マウント	利用不可	開発者プレビュー	開発者プレビュー
データストア間での CNS ボリュームの移行	利用不可	開発者プレビュー	開発者プレビュー
CSI ボリュームグループスナップショット	利用不可	利用不可	テクノロジープレビュー
GCP PD による C3/N4 インスタンスタイプとハイパーディスクバランスディスクのサポート	利用不可	利用不可	一般提供
GCP Filestore による Workload Identity のサポート	利用不可	一般提供	一般提供
OpenStack Manila による CSI サイズ変更のサポート	利用不可	利用不可	一般提供

1.8. 既知の問題

- 以前は、Google Cloud サービスアカウントのポリシーを設定しようとすると、API によって **400: Bad Request** 検証エラーが報告されていました。サービスアカウントを作成すると、アカウントがアクティブになるまでに最大 60 秒かかることがあり、これにより検証エラーが発生します。このエラーが発生した場合は、少なくとも 60 秒間続く真の指数バックオフを持つサービスアカウントを作成してください。(OCPBUGS-48187)

- 最小限の権限を使用し、**install-config.yaml** ファイルで `controlPlane.platform.gcp.serviceAccount` を指定せずに、Google Cloud の共有仮想プライベートネットワーク (VPC) にクラスターをインストールすると、インストールが成功する場合があります。Kubernetes (K8s) のファイアウォールルールが共有 VPC に作成されますが、ホストプロジェクトに権限がないため、クラスターを破棄しても K8s のこれらのファイアウォールルールは削除されません。(OCPBUGS-38689)

- oc-mirror プラグイン v2 は現在、ミラーリングエラーが発生した場合でも、"success" を意味す

る終了ステータス **0** を返します。そのため、自動化されたワークフローでは終了ステータスに依存できません。この問題が解決されるまで、**oc-mirror** によって生成された **mirroring_errors_XXX_XXX.txt** ファイルでエラーを手動で確認してください。(OCPBUGS-49880)

- Red Hat Enterprise Linux CoreOS (RHCOS) イメージに含まれる DNF パッケージマネージャーは、実行時に使用できません。これは DNF が、Red Hat サブスクリプションに登録されたクラスター内の有資格ノードにアクセスするために追加のパッケージに依存しているためです。回避策として、代わりに **rpm-ostree** コマンドを使用します。(OCPBUGS-35247)

- OpenShift Container Platform バージョン 4.18 には、インストール中に Nutanix クラスターの障害ドメインに複数のサブネットを設定できないという既知の問題があります。この問題に対する回避策はありません。(OCPBUGS-49885)

- コントロールプレーンマシンセットを使用して既存の Nutanix クラスターに複数のサブネットを設定する場合、次の既知の問題が存在します。

  - **subnets** スタンザ内の既存のサブネットの上にサブネットを追加すると、コントロールプレーンノードが **Deleting** 状態のままになります。回避策として、**subnets** スタンザ内の既存のサブネット配下にのみサブネットを追加します。

  - サブネットを追加した後、更新されたコントロールプレーンマシンが Nutanix コンソールに表示されても、OpenShift Container Platform クラスターにアクセスできないことがあります。この問題に対する回避策はありません。

  これらの問題は、サブネットが障害ドメインまたはプロバイダー仕様で指定されているかどうかに関係なく、サブネットを設定するためにコントロールプレーンマシンセットを使用するクラスターで発生します。(OCPBUGS-50904)

- **cgroupv1** Linux コントロールグループ (cgroup) を使用する RHEL 8 ワーカーノードには既知の問題があります。影響を受けるノードに表示されるエラーメッセージの例として、**UDN are not supported on the node ip-10-0-51-120.us-east-2.compute.internal as it uses cgroup v1** があります。回避策として、ユーザーはワーカーノードを **cgroupv1** から **cgroupv2** に移行する必要があります。(OCPBUGS-49933)

- 現在の PTP グランドマスタークロック (T-GM) 実装には、バックアップ NMEA センテンスジェネレーターなしで GNSS から供給される単一の National Marine Electronics Association (NMEA) センテンスジェネレーターがあります。NMEA センテンスが e810 NIC に到達する前に失われた場合、T-GM はネットワーク同期チェーン内のデバイスを同期できず、PTP Operator はエラーを報告します。修正案は、NMEA 文字列が失われたときに **FREERUN** イベントを報告することです。この制限が解決されるまで、T-GM は PTP クロックの holdover 状態をサポートしません。(OCPBUGS-19838)

- Google Cloud Platform (GCP) 上で実行されているクラスターのレイヤー 2 ネットワークトポロジーには既知の問題があります。現時点では、**UserDefinedNetwork** (UDN) リソースによって作成されたレイヤー 2 ネットワークで使用されている Egress IP アドレスは、間違った送信元 IP アドレスを使用しています。その結果、GCP のレイヤー 2 で UDN はサポートされません。現在、この問題の修正方法はありません。(OCPBUGS-48301)

- ユーザー定義ネットワーク (UDN) には、OVN-Kubernetes が管理していない 1000 以上のルーティングテーブル ID を削除するという既知の問題があります。その結果、OVN-Kubernetes の外部で作成された Virtual Routing and Forwarding (VRF) インスタンスはすべて削除されます。この問題は、テーブル ID が 1000 以上のユーザー定義 VRF を作成したユーザーに影響します。これらは OpenShift Container Platform 用に予約されているため、回避策としてユーザーは VRF を 1000 未満のテーブル ID に変更する必要があります。(OCPBUGS-50855)

- OpenShift Container Platform 4.18 の一部としてインストールした OpenShift CLI (**oc**) を使用して OpenShift Container Platform 4.17 サーバーにログインしようとすると、ターミナルに次の警告メッセージが表示されます。

```
Warning: unknown field "metadata"
You don't have any projects. You can try to create a new project, by running

    oc new-project <projectname>
```

この警告メッセージは既知の問題ですが、OpenShift Container Platform の機能上の問題を示すものではありません。警告メッセージを無視しても問題はなく、OpenShift Container Platform も引き続き意図したとおり使用できます。(OCPBUGS-44833)

- OpenShift Container Platform 4.18 には、**ovnkube-node** デーモンセットが削除されるとクラスターのマスカレードサブネットが **169.254.169.0/29** に設定されるという既知の問題があります。マスカレードサブネットが **169.254.169.0/29** に設定されている場合、**UserDefinedNetwork** カスタムリソース (CR) を作成できません。

注記

  - Day 2 で **network.operator** CR を変更することでマスカレードサブネットが設定された場合、**169.254.169.0/29** には戻されません。
  - クラスターが OpenShift Container Platform 4.16 からアップグレードされている場合、下位互換性のためにマスカレードサブネットは **169.254.169.0/29** のままになります。ユーザー定義ネットワーク機能を使用するには、マスカレードサブネットを、より多くの IP を持つサブネット (**169.254.0.0/17** など) に変更する必要があります。

この既知の問題は、次のいずれかのアクションを実行した後に発生します。

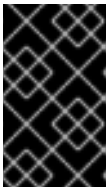
アクション	結果
ovnkube-node DaemonSet オブジェクトを再起動した	マスカレードサブネットが、**UserDefinedNetwork** CR をサポートしない **169.254.169.0/29** に設定されます。
ovnkube-node DaemonSet オブジェクトを削除した	マスカレードサブネットが、**UserDefinedNetwork** CR をサポートしない **169.254.169.0/29** に設定されます。さらに、**ovnkube-node** Pod がクラッシュし、**CrashLoopBackOff** 状態のままになります。

一時的な回避策として、次のコマンドを実行して **UserDefinedNetwork** CR を削除し、すべての **ovnkube-node** Pod を再起動できます。

```
$ oc delete pod -l app=ovnkube-node -n openshift-ovn-kubernetes
```

ovnkube-node Pod が自動的に再起動し、クラスターが再び安定します。次にマスカレードサブネットを、IPv4 の場合は **169.254.0.0/17** などのように、より大きな IP アドレスに設定でき

ます。その結果、**NetworkAttachmentDefinition** または **UserDefinedNetwork** CR を作成できます。



重要

ovnkube-node Pod を削除するときに、**ovnkube-node DaemonSet** オブジェクトを削除しないでください。そうすることで、マスカレードサブネットが **169.254.169.0/29** に設定されます。

詳細は、Day 2 オペレーションとして OVN-Kubernetes マスカレードサブネットを設定する を参照してください。

(OCPBUGS-49662)

- クラスターにノードを追加または削除すると、ノードのステータスをめぐる所有権の競合が発生する可能性があります。これにより、新しいノードが表示されるまでに長時間かかる可能性があります。回避策として、**openshift-kube-apiserver-operator** namespace で **kube-apiserver-operator** Pod を再起動して、プロセスを迅速化することができます。(OCPBUGS-50587)

- RHOSP 上で実行されるデュアルスタックネットワーククラスターの場合、Floating IP (FIP) にアタッチされた仮想 IP (VIP) がマスターノード間で移動するときに、新しいマスターが別のコンピュートノードにあると、仮想 IP と FIP 間の関連付けが機能しなくなる可能性があります。この問題は、OVN が共有 Neutron ポート上の IPv4 アドレスと IPv6 アドレスの両方が同じノードに属していると想定するために発生します。(OCPBUGS-50599)

- ブート操作中に追加の Extensible Firmware Interface (EFI) エントリーを自動的に作成するシステムでは、PCR 1 および PCR 7 保護によるディスク暗号化が失敗します。この追加のエントリーによって EFI 変数が変更されるため、PCR 1 によるサーバー構成証明が阻止されます。(**OCPBUGS-54593**)

- OpenShift Container Platform クラスターでクラウドネイティブネットワーク関数 (CNF) のレイテンシーテストを実行すると、テストのレイテンシーしきい値 (たとえば、**cyclictest** テストの場合は 20 マイクロ秒) を超える結果が返されることがあります。その結果、テストは失敗します。(OCPBUGS-42328)

- グランドマスタークロック (T-GM) が **Locked** 状態に遷移するタイミングが早すぎる場合に発生する既知の問題があります。これは、Digital Phase-Locked Loop (DPLL) が **Locked-HO-Acquired** 状態への移行を完了する前、Global Navigation Satellite Systems (GNSS) のタイムソースが復元された後に発生します。(OCPBUGS-49826)

- Kubernetes の問題により、CPU マネージャーは、ノードに許可された最後の Pod から利用可能な CPU リソースのプールに CPU リソースを戻すことができません。これらのリソースは、後続の Pod がノードに許可された場合は、割り当てることができます。ただし、この Pod が最後の Pod になり、CPU マネージャーはこの Pod のリソースを使用可能なプールに戻すことができなくなります。
  この問題は、CPU マネージャーが利用可能なプールに CPU を解放することに依存する CPU 負荷分散機能に影響します。その結果、保証されていない Pod は、少ない CPU 数で実行される可能性があります。回避策として、影響を受けるノード上で **best-effort** の Quality of Service (QOS) を持つ Pod をスケジュールします。この Pod は最後に許可された Pod となり、これによりリソースが使用可能なプールに正しく解放されます。(OCPBUGS-46428)

- Pod が、DHCP アドレス割り当てに他の CNI プラグインと組み合わせて CNI プラグインを使用すると、Pod のネットワークインターフェイスが予期せず削除される可能性があります。その結果、Pod の DHCP リースの有効期限が切れると、新しいリースの再作成時に DHCP プロキ

シーがループに入り、ノードが応答しなくなります。現在、回避策はありません。(OCPBUGS-45272)

- PXE ブートを使用してオンプレミスクラスターにワーカーノードを追加すると、ホストがディスクから適切に再起動できず、インストールが完了しないことがあります。回避策として、障害が発生したホストをディスクから手動で再起動する必要があります。(OCPBUGS-45116)

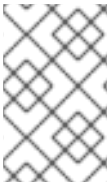
- GCP PD CSI ドライバーは、RWX モードのハイパーディスクバランスボリュームをサポートしていません。GCP PD CSI ドライバーを使用して RWX モードでハイパーディスクバランスボリュームをプロビジョニングしようとすると、エラーが発生し、目的のアクセスモードでボリュームがマウントされません。(OCPBUGS-44769)

- 現在、c3-standard-2、c3-standard-4、n4-standard-2、n4-standard-4 ノードが含まれる GCP PD クラスターは、アタッチ可能なディスクの最大数 (16 であるはず) を誤って超過する可能性があります。この問題により、ボリュームを Pod に正常に作成またはアタッチできない可能性があります。(OCPBUGS-39258)

1.9. 非同期エラータの更新

OpenShift Container Platform 4.18 のセキュリティー、バグ修正、機能拡張の更新は、Red Hat Network を通じて非同期エラータとしてリリースされます。すべての OpenShift Container Platform 4.18 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、エラータ通知を有効にできます。エラータ通知を有効にすると、登録されたシステムに関連するエラータが新たに発表されるたびに、メールで通知が送信されます。



注記

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

このセクションは、これからも継続して更新され、OpenShift Container Platform 4.18 の今後の非同期エラータリリースの機能拡張とバグ修正に関する情報を追加していきます。OpenShift Container Platform 4.18.z 形式などのバージョン管理された非同期リリースは、サブセクションで詳しく説明します。さらに、エラータの本文がアドバイザリーで指定されたスペースに収まらないリリースの詳細は、その後のサブセクションで説明します。

重要

クラスターの更新 の手順は、OpenShift Container Platform のすべてのリリースで必ず確認してください。

1.9.1. RHBA-2025:19865 - OpenShift Container Platform 4.18.28 のバグ修正とセキュリティー更新

発行日: 2025 年 11 月 12 日

OpenShift Container Platform リリース 4.18.28 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:19865 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:19863 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.28 --pullspecs
```

1.9.1.1. 機能拡張

- この更新により、**remoteWrite[].oauth2.proxyFromEnvironment** 設定を使用して、4.18.z でクラスター全体のプロキシーを設定できるようになりました。この改善により、以前は 4.19 以降のビルドでのみ利用可能だった機能がバックポートされ、より柔軟で一貫性のあるプロキシー設定が可能になります。(OCPBUGS-63410)

1.9.1.2. バグ修正

- この更新前は、ユーザー管理のロードバランサーが使用されている場合でも、API および Ingress 仮想 IP (VIP) アドレスが自動的に割り当てられていました。このリリースでは、API および Ingress VIP が自動的に割り当てられなくなりました。これらの値が **install-config.yaml** 設定ファイルで明に指定されていない場合、インストールはエラーで失敗し、値を指定するように求められます。(OCPBUGS-53235)

- この更新前は、リクエストの監査ログエントリーを生成する際に、Webhook の障害によって **kube-apiserver** のクラッシュが発生する可能性がありました。その結果、API サーバーの中断が発生する可能性がありました。このリリースでは、監査システムが更新され、**kube-apiserver** がクラッシュしなくなり、API の中断が解決されました。(OCPBUGS-61773)

- この更新前は、ベースボード管理コントローラー (BMC) が空の ETag を送信するため、一部のハードウェアモデルでの Redfish トランザクションが失敗していました。その結果、ユーザーは **HostFirmwareSettings** カスタムリソース (CR) を使用できませんでした。このリリースでは、空の ETag を持つ Redfish トランザクションの問題が解決され、警告なしで正しい ETag インスタンスが返されるようになりました。**その結果、Redfish トランザクションは失敗しなくなり、ユーザーは HostFirmwareSettings CR を使用できるようになりました。(OCPBUGS-62647)**

- **この更新前は、ホステされたクラスターの namespace 内の driver-config ConfigMap に対する一貫性のない更新により、driver-config ConfigMap のコンテンツがフラップし、一貫性のないストレージクラスが適用され、ユーザーエクスペリエンスに影響を及ぼしていました。このリリースでは、driver-config ConfigMap の安定性が復元され、ホストされたクラスターの namespace におけるストレージクラスのフラッピングが防止されます。(OCPBUGS-62808)**

- **この更新前は、コントローラーは Amazon Web Services (AWS) へのセッションを設定するときにランダムな名前でファイルを作成および削除していたため、コントローラーはセッションをキャッシュするために継続的にメモリーを割り当てていました。このリリースでは、コントローラーはランダムなファイル名ではなく同じファイル名を使用するようになり、カーネルはセッションごとに新しいファイル名を要求する代わりに dentry を再利用できるようになりました。その結果、過剰なメモリー割り当ての問題が解消されました。(OCPBUGS-63138)**

- この更新前は、gRPC 接続ログが非常に詳細なログレベルに設定されていました。これにより、過剰な数のメッセージが生成され、ログがオーバーフローしていました。このリリースでは、gRPC 接続ログのログレベルが V(4) に切り替えられました。その結果、該当するメッセージの詳細度が低くなったため、ログがオーバーフローしなくなりました。(OCPBUGS-63324)

- この更新前は、ユーザーが Node Tuning Operator (NTO) が所有する ocp-tuned-one-shot.service systemd ユニットを実行すると、kubelet の依存関係エラーが発生する場合がありました。そのため、kubelet が起動しませんでした。このリリースでは、`ocp-tuned-one-shot.service` ユニットを実行しても、依存関係エラーは発生しません。そのため、ユニットを実行すると kubelet が起動します。(OCPBUGS-63450)

- この更新前は、フェイルオーバー中に、システムの重複アドレス検出 (DAD) により、Egress IPv6 アドレスが両方のノードに一時的に存在する場合に、アドレスが誤って無効にされ、接続が切断されることがありました。このリリースでは、Egress IPv6 はフェイルオーバー中に DAD チェックをスキップするように設定されます。これにより、Egress IP アドレスが別のノードに正常に移動した後も Egress IPv6 トラフィックが中断されなくなり、ネットワークの安定性が向上します。(OCPBUGS-63459)

- この更新前は、Azure マシンプロバイダーが、コンピュートマシンセットの dataDisks 設定を Azure Stack Hub の仮想マシン作成 API リクエストに渡していませんでした。その結果、指定したデータディスクのない新しいマシンが作成されていました。これは、仮想マシンの作成プロセス中に、設定がサイレントに無視されていたためです。このリリースでは、Azure Stack Hub の仮想マシン作成が更新され、dataDisks 設定が含まれるようになりました。Azure Stack Hub ではこのオプションがネイティブにサポートされていないため、追加の更新により、deletionPolicy: Delete パラメーターの動作がコントローラーに手動で実装されました。そのため、Azure Stack Hub 仮想マシンにデータディスクが正しくプロビジョニングされます。Delete ポリシーも機能的にサポートされています。これにより、マシンが削除されたときに、ディスクも適切に削除されます。(OCPBUGS-63669)

1.9.1.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.2. RHSA-2025:19047 - OpenShift Container Platform 4.18.27 のバグ修正とセキュリティー更新

発行日: 2025 年 10 月 29 日

OpenShift Container Platform リリース 4.18.27 が公開されました。この更新に含まれるバグ修正のリストは、RHSA-2025:19047 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:19045 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.27 --pullspecs
```

1.9.2.1. バグ修正

- この更新前は、OVN-Kubernetes コントローラーが Kubernetes API サーバーからの更新を処理しておらず、各ノードでオープン仮想ネットワーク (OVN) データベースを設定していない場合、このデータベースを使用する OVN コントローラーは、OVN-Kubernetes コントローラーが設定を完了する前にデータベースに接続する可能性がありました。その結果、OVN コントローラーは古い OVN データベースと同期し、関連付けられた IP が別のノードに移動した可能性があるにもかかわらず、Egress IP をサポートするように設定された送信元ネットワークアドレス変換 (SNAT) を使用して、IP の Gratuitous Address Resolution Protocol (GARP) に進みました。このリリースでは、OVN-Kubernetes コントローラーが更新を処理していない場合、これらの GARP はブロックされます。(OCPBUGS-62671)

- この更新前は、4.19.9 および 4.18.23 の Cluster Version Operator (CVO) で、メトリクス要求でベアラートークンの認証が必要になっていました。その結果、メトリクススクレーパーがクライアント認証を提供しなかったため、Hosted Control Plane クラスターは壊れてしまいました。このリリースでは、CVO はメトリクス要求に対してクライアント認証を必要としません。そのため、CVO メトリクススクレイピングへのアクセスが Hosted Control Plane クラスター上で回復されます。(OCPBUGS-62869)

- この更新前は、リンクされた URL は開発者パースペクティブにありましたが、リンクをクリックしてもパースペクティブが切り替わりませんでした。その結果、空白のページが表示されました。このリリースでは、リンクをクリックするとパースペクティブが変更され、ページが正しく表示されます。(OCPBUGS-63041)

- この更新前は、ロールベースのアクセス制御 (RBAC) パーミッションが不十分であるため、プロジェクトのないユーザーは、Roles リストの一部しか見られませんでした。このリリースにより、アクセスロジックが修正されました。その結果、これらのユーザーは Roles ページを開けなくなり、機密データが安全に保たれます。(OCPBUGS-63247)

- この更新前は、4.18.21 から 4.19.6 への更新中に、1 つ以上のマシンセットの capacity.cluster-autoscaler.kubernetes.io/labels アノテーションに複数のラベルがあるために Machine Config Operator (MCO) が失敗していました。このリリースでは、MCO は capacity.cluster-autoscaler.kubernetes.io/labels アノテーションで複数のラベルを受け入れるようになりました。その結果、4.19.6 への更新中に MCO が失敗しなくなりました。(OCPBUGS-63346)

1.9.2.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.3. RHSA-2025:17657 - OpenShift Container Platform 4.18.26 のバグ修正とセキュリティー更新

発行日: 2025 年 10 月 15 日

OpenShift Container Platform リリース 4.18.26 が公開されました。この更新に含まれるバグ修正のリストは、RHSA-2025:17657 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:17655 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.26 --pullspecs
```

1.9.3.1. バグ修正

- この更新前は、キューが大きい場合は各マシンが順番に調整されていたため、多数のノードのスケーリングに時間がかかりました。このリリースでは、最大 10 台のマシンが同時に調整されるため、スケールイベントの速度が向上しました。(OCPBUGS-59387)

- この更新前は、OVN-Kubernetes Localnet ネットワーク上のセカンダリーインターフェイスを持つ Pod は、Localnet IP アドレスがホストネットワークと同じサブネット内にある場合にのみ、同じノード上の他の Pod と通信できました。このリリースでは、Localnet IP アド

レスを任意のサブネットから取得できるようになりました。その場合、外部ルーターが Localnet サブネットをホストネットワークに接続します。(OCPBUGS-61455)

- この更新前は、DNS Egress Firewall ルールの Address_Set 内の古い IP アドレスが削除されず、メモリーリークが発生していました。このリリースでは、IP アドレスは TTL の有効期限が切れてから 5 秒後に Address_Set から削除され、メモリーの増加を防ぎます。(OCPBUGS-61748)

- この更新前は、競合状態によりイグニッションサーバーの MIRRORED_RELEASE_IMAGE 環境変数が変動し、Pod の不要な再起動が発生する可能性がありました。このリリースでは、MIRRORED_RELEASE_IMAGE 値の一貫性が保たれ、Ignition サーバーのデプロイメントが安定しました。(OCPBUGS-61904)

- この更新前は、OpenShift Container Platform バージョン 4.12 より前に作成されたコントロールプレーンノードには、node-role.kubernetes.io/control-plane ラベルが含まれていませんでした。このリリースでは、Machine Config Operator (MCO) は、コントロールプレーンノードに対して uncordon を実行するたびにラベルを追加します。(OCPBUGS-62321)

- この更新前は、/auth/error ページにアクセスすると不適切なエラーが表示されることがありました。このリリースでは、ページに適切なエラーメッセージが表示されるようになりました。(OCPBUGS-62326)

- この更新前は、oc-mirror を使用するときに --v1 または --v2 フラグを省略すると、動作に一貫性がなくなる可能性がありました。このリリースでは、--v1 または --v2 の指定が必須になりました。(OCPBUGS-62432)

- この更新前は、PVC の作成直後に PVC のサイズを変更すると、PV が一時的に見つからないために失敗する可能性がありました。このリリースでは、PVC の作成後すぐにエラーが発生することなくサイズを変更できるようになりました。(OCPBUGS-62467)

- この更新前は、Machine Config Operator (MCO) は必要な証明書を /etc/docker/certs.d ディレクトリーで検索しなかったため、Operator Controller と catalogd が失敗していました。このリリースでは、MCO はこのディレクトリー内の証明書にアクセスできるようになり、Operator Controller と catalogd が正常に起動するようになりました。(OCPBUGS-54175)

- この更新前は、Machine Config Operator (MCO) がノードに対して drain を実行している間に外部アクターがそのノードに対して uncordon を実行できたため、MCO とスケジュー

ラーが Pod のスケジューリングと削除で競合する可能性がありました。このリリースでは、MCO は外部における uncordon の実行を検出し、競合することなく drain プロセスを続行します。(OCPBUGS-62637)

- この更新前は、バグレポートごとに oc-mirror バージョンを提供する必要があり、問題解決が遅れる可能性がありました。このリリースでは、oc-mirror v2 は標準出力とログの両方にバージョンを出力するため、トラブルシューティングの時間が短縮されます。(OCPBUGS-62696)

1.9.3.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.4. RHBA-2025:16732 - OpenShift Container Platform 4.18.25 のバグ修正更新

発行日: 2025 年 10 月 1 日

OpenShift Container Platform リリース 4.18.25 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:16732 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:16729 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.25 --pullspecs
```

1.9.4.1. 機能拡張

- この更新により、OpenShift Container Platform 4.18.25 が Kubernetes 1.31.12 にアップグレードされ、セキュアで安定した最新のプラットフォームが確保されます。この機能拡張により、最新のアップストリームの変更と修正が組み込まれることで、安定性が向上し、セキュリティーが強化され、パフォーマンスが向上します。(OCPBUGS-60511)

この更新により、OpenShift Container Platform クラスター全体の virt-launcher Pod からコマンドラインログを収集することが可能になります。JSON でエンコードされたログが、パス namespaces/<namespace_name>/pods/<pod_name>/virt-launcher.json に保存されます。これにより、仮想マシンのトラブルシューティングとデバッグが容易になります。(OCPBUGS-61656)

1.9.4.2. バグ修正

- この更新前は、シングルノードの OpenShift デプロイメントを使用する場合、agent-based-installer が etcd ディレクトリー /var/lib/etcd/member の権限を、0700 ではなく 0755 に設定していました。これはマルチノードデプロイメントでは正しく設定されます。このリリースでは、シングルノードの OpenShift デプロイメントでも、etcd ディレクトリー /var/lib/etcd/member の権限が 0700 に設定されます。(OCPBUGS-61529)

- この更新前は、リモートエンドポイントがデータを受信していない場合も、PrometheusRemoteWriteBehind アラートが発生していました。このリリースでは、リモートエンドポイントがまだデータを受信していない場合は、PrometheusRemoteWriteBehind アラートが発動しなくなりました。(OCPBUGS-61706)

- この更新前は、ベアメタルデプロイメントにおいて、NetworkManager-wait-online の依存関係が原因で、OpenShift Container Platform デプロイメントで NMState サービスに障害が発生していました。その結果、ネットワークの誤った設定によるデプロイメントの失敗がエンドユーザーに発生していました。このリリースでは、NMState サービスの依存関係の問題が解決され、br-ex 設定に NetworkManager-wait-online が不要になりました。(OCPBUGS-61840)

1.9.4.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.5. RHBA-2025:15714 - OpenShift Container Platform 4.18.24 のバグ修正更新

発行日: 2025 年 9 月 17 日

OpenShift Container Platform リリース 4.18.24 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:15714 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:15712 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.24 --pullspecs
```

1.9.5.1. 機能拡張

- この更新により、OpenShift Container Platform プラットフォームの cluster-etcd-operator がプロアクティブになり、etcdDatabaseQuotaLowSpace アラートが変更されました。etcd クォータの使用量が 95% に近づくにつれて、情報提供、警告、重大など、さまざまなレベルのアラートがトリガーされます。この機能拡張により、API サーバーが影響を受ける前にクラスター管理者が潜在的な問題に対処する時間を確保できるため、より安定した管理しやすい環境が実現します。(OCPBUGS-61235)

- Red Hat Enterprise Linux CoreOS (RHCOS) イメージのレイヤー化で使用される MachineOSConfig オブジェクトの名前は、カスタムレイヤーイメージがデプロイされるマシン設定プールと同じである必要があります。以前は、任意の名前を使用できました。この変更は、各マシン設定プールで多数の MachineOSConfig オブジェクトが使用されるのを防ぐために行われました。詳細は、OpenShift のイメージモード を参照してください。

- この更新により、プライマリーノードがオンラインのときに、システムがライブ API 接続を多数の Kubernetes API サーバーにバランスよく分散できるようになります。これにより、いずれか 1 つのプライマリーノードの CPU 使用率が 100% に達することが防止され、プライマリーノードの再起動時またはクォーラムの確立時のシステムパフォーマンスと安定性が向上します。この変更により、ライブ API 接続が均等に分散され、プライマリーノードまたは Kubernetes API サーバーの停止中に 1 台の Kubernetes API サーバーによりほとんどの接続を処理するのを防ぐことで、システムの最適なパフォーマンスと安定性が維持されます。(OCPBUGS-61039)

1.9.5.2. 既知の問題

- OpenShift Container Platform 4.18.22 では、コンテナーランタイムバージョン 1.23 で権限が拒否されるため、Berkley Packet Filter (BPF) プログラムの作成が失敗していました。その結果、グラフィックスプロセッシングユニット (GPU) スタックのデプロイが失敗していました。この障害を修正するために、GPU ワーカーノードの /var/usrlocal/nvidia/toolkit/.config/nvidia-container-runtime/config.toml ファイルに no-cgroups = true 変数が追加されました。その結果、GPU スタックが OpenShift Container Platform 4.18.22 に正常にデプロイされるようになりました。(OCPBUGS-60663)

1.9.5.3. バグ修正

- この更新前は、LDAP 統合時にユーザーごとに多数の config map が作成されていたため、過剰なヘルスチェックアラートが生成されていました。その結果、ユーザーインターフェイスが過剰なアラートで乱雑な状態になっていました。このリリースでは、ユーザーの config map による過剰なヘルスチェックアラートが取り除かれます。その結果、コンソールのアラートが減り、使いやすさが向上しました。(OCPBUGS-50983)

- この更新前は、Microsoft Azure Stack Hub のクラウド設定パスが正しくなかったため、Container Storage Interface (CSI) ドライバーが誤った環境設定を使用していました。その結果、CSI ドライバーの Pod が不健全な状態になっていました。このリリースでは、Azure Stack Hub 上の CSI Operator の誤った環境設定が修正され、CSI ドライバーがクラウド設定を正しく読み取るようになりました。(OCPBUGS-55053)

- この更新前は、imagecontentsourcepolicy ポリシー内に複数のミラーがあると、イメージ検索中に Hosted Control Plane のペイロードエラーが発生しました。その結果、Hosted Control Plane のペイロードが複数のミラーを処理できず、クラスターの作成に失敗していました。このリリースでは、Hosted Control Plane のペイロードが複数のミラーをサポートするようになり、作成エラーが発生しなくなりました。(OCPBUGS-57142)

- この更新前は、configure-ovs.sh ファイルの競合状態が原因で、mode=active-backup および fail_over_mac=follow 変数を使用したボンディングネットワーク設定が失敗していました。この状態により、インターフェイスが予期しない状態に変化していました。その結果、ボンディングされたネットワークのフラッピングが発生し、高可用性に影響を及ぼしていました。このリリースでは、configure-ovs.sh ファイルを処理する競合状態が改善され、fail_over_mac=follow 変数を使用したボンディングネットワーク設定が機能するようになり、フラッピングが発生しなくなりました。(OCPBUGS-57357)

- この更新前は、Alertmanager 設定内の誤った URL によって、OpenShift Container Platform 4.16 クラスター上の user-workload Pod にログが作成されていました。その結果、設定内の無効な Slack URL が原因で、ユーザーワークロードの監視が失敗していました。このリリースでは、Alertmanager 設定で無効な URL が許可されます。その結果、Alertmanager 設定エラーが解決され、OpenShift Container Platform 4.19 より前のクラスターで監視の安定性が向上しました。(OCPBUGS-58194)

- この更新前は、シングルノードの OpenShift Container Platform 4.18 のデプロイ時に、プライマリーインターフェイスに IP アドレスが複数あると、API サーバーが誤った etcd IP アドレスに接続していました。この動作により、デプロイ時に API サーバー Pod が失敗し、クラスターの初期化の問題が発生していました。このリリースでは、プライマリーインターフェイスに複数の IP アドレスを持つデプロイメントが修正されました。その結果、API サーバーが証

明書内の正しい IP アドレスを使用して etcd に接続するようになり、シングルノードのデプロイ時に障害が発生しなくなりました。(OCPBUGS-59992)

- この更新前は、Hosted Control Plane の新しいネットワークデータタイプの難読化が不十分だったため、ユーザーデータが公開されていました。その結果、機密情報は保護されませんでした。このリリースでは、新しいネットワークデータタイプの難読化が実装されています。その結果、Hosted Control Plane のネットワークデータの難読化により、データのプライバシーが向上しています。(OCPBUGS-60301)

- この更新前は、ホステッドクラスターが、Domain Name System (DNS) 名の競合により、複数のストレージエリアネットワーク (SAN) エントリーを持つ証明書を拒否していました。その結果、ユーザーが証明書を使用してホステッドクラスターをデプロイした後に無効な設定エラーが発生していました。このリリースでは、クラスターが複数の SAN エントリーを持つ証明書を受け入れるようになりました。その結果、デプロイ時のエラーが発生しなくなりました。(OCPBUGS-60485)

- この更新前は、OpenShift Container Platform 4.18.6 から OpenShift Container Platform 4.18.22 へのアップグレード中に、Cluster Network Operator (CNO) が DaemonSet API オブジェクトおよび openshift-multus namespace で release.openshift.io/version アノテーションを設定していませんでした。その結果、アノテーションがないためにアップグレードが失敗していました。このリリースでは、CNO がアップグレード中に DaemonSet オブジェクトとデプロイメントのアノテーションを設定します。その結果、クラスターのアップグレードが完了するようになり、openshift-multus namespace にアノテーションがないことが原因で停止しなくなりました。(OCPBUGS-60795)

- この更新前は、クラスターの自動スケーリング中にマシンの削除処理が不適切だったため、最後のノードに ToBeDeletedByClusterAutoscaler taint が残っていました。その結果、クラスターのスケーリング中にリソースの割り当てが影響を受けていました。このリリースでは、マシンセットをスケールダウンした後の ToBeDeletedByClusterAutoscaler taint の削除が実装されています。その結果、マシンセットをスケールダウンした後、最後のノードに不要な taint が残りません。(OCPBUGS-60908)

- この更新前は、OpenShift Container Platform のイメージレジストリーを無効にすると、古いプルシークレットにファイナライザーが残り続け、シークレットを削除できませんでした。その結果、ユーザーはイメージレジストリーを無効にした後、Dockercfg シークレットを削除できませんでした。このリリースでは、レジストリーが削除された後、古いプルシークレットによって namespace の削除がブロックされなくなりました。その結果、レジストリーが無効な場合にプルシークレットファイナライザーによって namespace の削除がブロックされなくなりました。(OCPBUGS-61002)

- この更新前は、検証コードで、シングルノードインストールをサポートするプラット

フォームのリストから IBM Cloud が除外されていました。その結果、検証エラーのため、ユーザーは IBM Cloud にシングルノード設定をインストールできませんでした。このリリースでは、シングルノードインストールに対する IBM Cloud のサポートが有効になっています。その結果、ユーザーは IBM Cloud でシングルノードインストールを完了できるようになりました。(OCPBUGS-61178)

1.9.5.4. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.6. RHSA-2025:14820 - OpenShift Container Platform 4.18.23 のバグ修正とセキュリティー更新

発行日: 2025 年 9 月 3 日

OpenShift Container Platform リリース 4.18.23 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:14820 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:14816 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.23 --pullspecs
```

1.9.6.1. 機能拡張

- この更新前は、--dry-run=server オプションを指定して istag リソースを削除すると、サーバーからイメージが誤って実際に削除されていました。この予期しない削除は、dry-run オプションが oc delete istag コマンドに誤って実装されていたために発生していました。このリリースでは、dry-run オプションが 'oc delete istag' コマンドに関連付けられました。その結果、イメージオブジェクトの誤削除が防止され、--dry-run=server オプションを使用する場合でも istag オブジェクトはそのまま残ります。(OCPBUGS-58461)

- この更新前は、cluster-policy-controller コンテナーはすべてのネットワークに対して 10357 ポートを公開していました (バインドアドレスが 0.0.0.0 に設定されていました)。KCM Pod マニフェストで hostNetwork が true に設定されていたため、ポートはノードのホスト

ネットワーク外に公開されていました。このポートはコンテナーのプローブ専用として使用されます。この機能拡張により、バインドアドレスは localhost のみをリッスンするように更新されました。その結果、ポートがノードネットワークの外部に公開されなくなり、ノードのセキュリティーが向上しました。(OCPBUGS-60131)

1.9.6.2. バグ修正

- この更新前は、oc adm inspect --all-namespaces コマンド構築のバグにより、must-gather はリース、csistoragecapacities、および assisted-installer namespace に関する情報を正しく収集していませんでした。このリリースにより、この問題は修正され、must-gather は情報を正しく収集するようになりました。(OCPBUGS-46437)

- この更新前は、OpenShift Container Platform のノードと Pod の間で、大きなパケットを含む特定のトラフィックパターンが実行されると、OpenShift Container Platform ホストが Internet Control Message Protocol (ICMP) の needs frag を別の OpenShift Container Platform ホストに送信するという状況が発生していました。この状況により、クラスター内で実現可能な最大転送単位 (MTU) が低下していました。そのため、ip route show cache コマンドを実行すると、物理リンクよりも低い MTU を持つキャッシュルートが表示されていました。ホストは大きなパケットを含む Pod 間トラフィックを送信しないため、パケットがドロップされ、OpenShift Container Platform コンポーネントのパフォーマンスが低下していました。このリリースでは、NF Tables のルールにより、OpenShift Container Platform のノードがこれらのトラフィックパターンに反応して自身の MTU を引き下げることが防止されます。(OCPBUGS-58288)

- この更新前は、Cluster Operator のアップグレードに時間がかかる場合、Cluster Version Operator はアップグレードが進行中かすでにスタックしているかを判別できないため、何も報告しませんでした。このリリースでは、Cluster Version Operator によって報告される Cluster Version のステータスの失敗条件に、新たに unknown ステータスが追加されました。これにより、クラスター管理者にクラスターの確認を促し、Cluster Operator のアップグレードがブロックされたまま待ち続ける事態を回避できるようになりました。(OCPBUGS-58450)

- この更新前は、一貫性のない状態更新による断続的な Egress IP 処理により、ユーザートラフィックでパケットドロップが発生していました。このリリースでは、Egress IP 処理の一貫性が向上しました。(OCPBUGS-59371)

- この更新前は、SELinux 関連のコマンドを実行する前に SELinux ステータスチェックは実行されませんでした。その結果、ターゲットの RHEL マシンで SELinux が有効になっていない場合、関連するステップが失敗しました。このリリースでは、ステップが正常に実行されたことを確認するために、SELinux ステータスチェックが追加されました。(OCPBUGS-59844)

- この更新前は、ダウンロード用のノードセレクターとコンソール Pod の不一致により、コントロールプレーンノードのダウンロードが一貫性なくスケジュールされていました。その結果、ダウンロードがランダムなノードでスケジュールされたため、潜在的なリソースの競合やパフォーマンスの低下を引き起こしていました。このリリースでは、ダウンロードされたワークロードがコントロールプレーンノードで一貫してスケジュールされるようになり、リソースの割り当てが改善されます。(OCPBUGS-59897)

- この更新前は、削除ワークフローで workflow mode: diskToMirror / delete が誤表示され、ユーザーが正しいワークフローモードについて混乱する原因となっていました。このリリースでは、削除操作中は workflow mode: delete が表示されます。(OCPBUGS-59966)

- この更新前は、netavark パッケージに 4.18 RHEL8 リポジトリーが含まれていなかったため、インストールされませんでした。このリリースでは、netavark パッケージが container-tools モジュールから正常にインストールされます。(OCPBUGS-59973)

- この更新前は、cloud-event-proxy コンテナーまたは Pod をリブートしてもイベントデータがまだ利用できない期間がありました。そのため、getCurrenState 関数は誤って clockclass を 0 として返していました。このリリースでは、getCurrentState 関数は不正な clockclass を返さなくなり、代わりに HTTP 400 Bad Request または 404 Not Found Error を返します。(OCPBUGS-59984)

- この更新前は、coredns テンプレートへの変更が含まれる OCP 更新によって、静的 Pod の再起動とノードのリブートが実行されていました。この問題は、ベースオペレーティングシステムイメージ更新のイメージプルの前に発生しました。その結果、ネットワークエラーと停止が原因となり、オペレーティングシステム (OS) 更新マネージャーである rpm-ostree がイメージのプルに失敗するという競合が発生しました。このリリースでは、coredns Pod の再起動による競合状態を回避するために、Machine Config Operator (MCO) OS 更新操作の再試行が追加されました。(OCPBUGS-60034)

- この更新前は、Vertical Pod Autoscaler (VPA) に複数のレコメンダーを使用すると、デフォルトの VPA レコメンダーが、デフォルト以外のレコメンダーに関連付けられた VPA オブジェクトに属する VPACheckpoint オブジェクトを誤ってガーベッジコレクションしていました。このリリースでは、デフォルトのレコメンダーは、他のレコメンダーが所有するチェックポイントをガベージコレクションしません。(OCPBUGS-60235)

- この更新前は、Events ページに、エラーメッセージではなく {error} が誤表示されていました。このリリースでは、エラーメッセージが表示されます。(OCPBUGS-60278)

-

この更新前は、プライマリーネットワークスタックとして IPv6 を使用するデュアルスタッククラスターでは、ベアメタル Installer-Provisioned Infrastructure (IP) が仮想メディア ISO イメージの IPv4 URL を誤って提供していました。そのため、IPv6 ネットワーク専用に設定されたベースボード管理コントローラー (BMC) は IPv4 アドレスに到達できず、インストールに失敗しました。このリリースでは、BMC が IPv6 アドレスを使用している場合は必ず IPv6 URL が提供されるようにインストーラーロジックが更新され、インストールプロセスが正常に完了するようになりました。(OCPBUGS-60592)

1.9.6.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.7. RHSA-2025:13325 - OpenShift Container Platform 4.18.22 のバグ修正とセキュリティー更新

発行日: 2025 年 8 月 13 日

OpenShift Container Platform リリース 4.18.22 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:13325 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:13326 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.22 --pullspecs
```

1.9.7.1. 機能拡張

- API サーバーの Readiness プローブ (/readyz エンドポイント) は、etcd チェックを除外するように変更されました。この変更により、etcd が一時的に利用できなくなった場合にクライアント接続が閉じられることが防止されます。その結果、クライアント接続がタイムアウトする前に etcd が再び準備完了となり、短時間 etcd が使用不可になってもクライアント接続が維持されます。この永続性により、一時的な API サーバーの停止が最小限に抑えられます。(OCPBUGS-49749)

1.9.7.2. 既知の問題

- 次の状況では、古い送信元ネットワークアドレス変換 (SNAT) またはルーティングポリシーが発生する可能性があります。

  - OVN-Kubernetes イメージの更新中に 4.17 から 4.18 にアップグレードしている。

  - アップグレード中、ovnkube-node Pod が実行されていないときに Egress IP によって選択された別のシステム上の Pod が削除された。

  (OCPBUGS-59531)

1.9.7.3. バグ修正

- この更新前は、サポート対象外のリージョン mx-central-1 内のクラスターを破棄すると、デストロイヤーはパーティションを見つけられず、正常に終了しませんでした。その結果、エラーが継続的に報告され、mx-central-1 リージョンの OpenShift Container Platform クラスターを破棄できませんでした。このリリースでは、デストロイヤーはサポート対象外のリージョン mx-central-1 のエラーを報告しないため、クラスターを正常に破棄できます。(OCPBUGS-56177)

- この更新前は、仕様とステータスの更新リストの組み合わせによって不要なファームウェアアップグレードがトリガーされ、システムのダウンタイムが発生していました。このリリースでは、ファームウェアアップグレードの最適化により、不要なファームウェアアップグレードがスキップされます。(OCPBUGS-56766)

- この更新前は、使用状況の追跡に間違った API エンドポイントを使用していたため、console-telemetry プラグインは Forbidden エラーを受け取っていました。その結果、Forbidden console-telemetry-plugin 使用状況追跡エラーが発生しました。このリリースでは、console-telemetry プラグインは使用状況データを /metrics/usage ではなく /api/metrics/usage に送信します。その結果、console-telemetry プラグインは Forbidden エラーを受信せず、正確に使用状況を追跡できます。(OCPBUGS-58364)

- この更新前は、Amazon Web Services (AWS) 認証情報が見つからず、サーベイがすべての AWS リージョンをリスト表示しようとしたため、ユーザーが install-config YAML ファイルを作成できず、インストールプログラムが失敗していました。このリリースでは、AWS 認証情報が設定されていない場合でもインストールプログラムが失敗しなくなり、ユーザーは survey で認証情報を入力できるようになりました。(OCPBUGS-59155)

- この更新前は、ホステッドクラスターが http://user:pass@host などのプロキシー URL で設定されている場合、認証ヘッダーが Konnectivity プロキシーによってユーザープロキシーに転送されず、認証が失敗していました。このリリースでは、プロキシー URL でユーザーとパスワードが指定されると、適切な認証ヘッダーが送信されます。(OCPBUGS-59503)

- この更新前は、oc-mirror は、エイリアスが設定されたサブチャートを使用した Helm チャートイメージを検出しませんでした。その結果、ミラーリング後に Helm チャートイメージが失われました。このリリースにより、oc-mirror は、エイリアスが設定されたサブチャートを使用した Helm チャートイメージを検出し、ミラーリングできるようになりました。(OCPBUGS-59798)

- この更新前は、container-tools モジュールから netavark をダウンロードできませんでした。このリリースでは、container-tools モジュールが netvark に対して有効になっています。その結果、netavark をモジュールからダウンロードできるようになりました。(OCPBUGS-59843)

- この更新前は、長さがゼロの TAR ファイルをクローンすると、アーカイブファイルが空であるため、oc-mirror が無期限に実行されていました。その結果、0 バイトの TAR ファイルをミラーリングしても、進捗が見られませんでした。このリリースでは、0 バイトの TAR ファイルが検出され、エラーとして報告されるようになり、oc-mirror がハングすることがなくなりました。(OCPBUGS-59864)

- この更新前は、ゾーンごとにコンピュートノードが 1 つだけ含まれるマルチゾーンクラスターで、連続してリブートするノードに Monitoring Operator の Prometheus Pod がスケジュールされ、両方のリブートがサービスに戻るまでに 15 分超かかった場合、Monitoring Operator のパフォーマンスが低下する可能性がありました。このリリースでは、一般的なクラスタートポロジーで Monitoring Operator のパフォーマンスが低下しないように、タイムアウトが 20 分に延長されました。Prometheus Pod を備えた 2 つのノードが連続してリブートし、リブートに 20 分超かかるクラスターでは、2 番目のノードと Prometheus Pod が通常の状態に戻るまで、パフォーマンスの低下が報告される可能性があります。(OCPBUGS-59962)

1.9.7.4. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.8. RHSA-2025:11677 - OpenShift Container Platform 4.18.21 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 30 日

OpenShift Container Platform リリース 4.18.21 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:11677 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:11678 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.21 --pullspecs
```

1.9.8.1. バグ修正

- この更新前は、Observe > Metrics > query > QueryKebab > Export as csv のドロップダウン項目で、未定義のタイトル要素が処理されませんでした。その結果、OpenShift Lister バージョン 4.16、4.17、および 4.18 の Metrics タブで、特定のクエリーの CSV ファイルをエクスポートすることができませんでした。このリリースでは、どのクエリーのメトリクスをダウンロードする際にも、ドロップダウンメニュー項目のオブジェクトプロパティーが正しく処理されるようになりました。その結果、すべてのクエリーの CSV エクスポートが Metrics ページで機能するようになりました。(OCPBUGS-54314)

- この更新前は、古いバージョンの Microsoft Azure API が原因で、サーバーの作成元のサブスクリプションとは異なるサブスクリプションに Capacity Reservation グループが存在する場合、そのグループを MachineSet に指定できませんでした。このリリースでは、最新バージョンの Azure API が使用されるため、サーバーの作成ポイントとは異なるサブスクリプションに Capacity Reservation グループがある場合でも、そのグループを MachineSet に指定できます。(OCPBUGS-56167)

- この更新前は、oc-mirror v2 が、--authfile パラメーターによって指定されるカスタム認証情報をグラフイメージの作成に使用していませんでした。その結果、認証の失敗によりグラフイメージの作成が妨げられていました。このリリースでは、--authfile パラメーターはミラーリングとグラフイメージ作成の両方にカスタム認証情報を正しく使用します。その結果、グラフイメージの作成時に認可エラーが発生しなくなりました。(OCPBUGS-57068)

- この更新前は、オンプレミスの installer-provisioned infrastructure (IPI) デプロイメントで Cilium Container Network Interface (CNI) を使用した場合、トラフィックをロードバランサーにリダイレクトするファイアウォールルールが適用されませんでした。このリリースでは、Cilium CNI および OVNKubernetes でルールが機能します。(OCPBUGS-57782)

- この更新前は、ビルドコントローラーが、イメージのプル専用のものではなく、汎用のものとしてリンクされたシークレットを検索していました。このリリースでは、デフォルトのイメージプルシークレットを検索するときに、ビルドはサービスアカウントにリンクされている ImagePullSecrets を使用します。(OCPBUGS-57949)

- この更新前は、oc-mirror v2 がコンテナーレジストリーに大量のリクエストを送信していました。その結果、コンテナーレジストリーが一部のリクエストを拒否し、too many requests エラーメッセージが表示されていました。このリリースでは、maxParallelLayerDownloads フラグと maxParallelImageDownloads フラグのデフォルト値が引き下げられ、再試行回数が引き上げられました。また、exp バックオフを有効にするために、再試行遅延が 0 に設定されました。その結果、コンテナーレジストリーに送信されるリクエストが少なくなり、リクエストの拒否も少なくなります。(OCPBUGS-58280)

- この更新以前は、OpenShift Container Platform 4.15 のリグレッションにより、console.tab/horizontalNav` パラメーターの 'href' 値でスラッシュが機能していませんでした。このリリースでは、console.tab/horizontalNav パラメーターの `href 値のスラッシュが期待どおりに機能します。(OCPBUGS-58457)

- この更新前は、有効なミラー tar ファイルなしで oc-mirror v2 のディスクからミラーへのミラーリングワークフローを実行したときに、問題を正しく示すエラーメッセージが返されませんでした。このリリースでは、oc-mirror v2 ワークフローは no tar archives matching "mirror_[0-9]{6}\.tar" found in "<directory>" というエラーメッセージを返します。(OCPBUGS-59235)

- この更新前は、マシンセットがスケールダウンされ、最小サイズに達すると、クラスターオートスケーラーによって、最後に残ったノードにスケジュールを拒否する taint が残され、ノードの使用が妨げられることがありました。この問題は、クラスターオートスケーラーのカウントエラーが原因で発生していました。このリリースでは、カウントエラーが修正され、マシンセットがスケールダウンされて最小サイズに達したときに、クラスターオートスケーラーが期待どおりに動作するようになりました。(OCPBUGS-59260)

- この更新前は、バンドルのアンパックジョブが、そのジョブを作成したカタログ Operator からコントロールプレーンの許容値を継承していませんでした。そのため、バンドルのアンパックジョブはワーカーノードでのみ実行されていました。taint によりワーカーノードが利用できない場合、管理者はクラスター上で Operator をインストールまたはアップグレードできませんでした。このリリースでは、バンドルのアンパックジョブにコントロールプレーンの toleration が適用されるようになりました。その結果、ジョブがコントロールプレーンの一部であるプライマリーノードで実行されるようになりました。(OCPBUGS-59421)

1.9.8.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.9. RHSA-2025:10767 - OpenShift Container Platform 4.18.20 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 17 日

OpenShift Container Platform リリース 4.18.20 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:10767 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:10768 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.20 --pullspecs
```

1.9.9.1. 新機能および機能拡張

1.9.9.1.1. クラスター上のレイヤー化の変更点が一般提供になる

クラスター上のレイヤー化機能にいくつかの重要な変更があります。

- API バージョンは、machineconfiguration.openshift.io/v1 になりました。新しいバージョンには次の変更が含まれています。
  - baseImagePullSecret パラメーターはオプションになりました。指定しない場合は、デフォルトの global-pull-secret-copy が使用されます。
  - buildInputs パラメーターは不要になりました。以前 buildInputs パラメーターの下にあったすべてのパラメーターが 1 レベル昇格されます。
  -

containerfileArch パラメーターは、複数のアーキテクチャーをサポートするようになりました。以前は、noarch のみがサポートされていました。

- 必要な imageBuilderType は Job になりました。以前は、必要なビルダーは PodImageBuilder でした。
- renderedImagePushspec パラメーターは renderedImagePushSpec になりました。
- buildOutputs および currentImagePullSecret パラメーターは不要になりました。

- MachineOSConfig オブジェクトにアノテーションを適用することで、カスタムのレイヤー化イメージを手動で再ビルドできます。
- 関連する MachineOSBuild オブジェクトを削除することで、カスタムのクラスター上のレイヤー化イメージを自動的に削除できるようになりました。
- クラスター上のレイヤー化が非接続環境でサポートされるようになりました。

詳細は、クラスター上のレイヤー化を使用してカスタムレイヤーイメージを適用する を参照してください。

1.9.9.2. バグ修正

- この更新前は、コンソールバックエンドの一部のエンドポイントが、API サーバーへの TokenReview リクエストによって制限されていました。場合によっては、API サーバーがこのリクエストにスロットリングを適用するため、UI の読み込み時間が長くなることがありました。このリリースでは、1 つを除くすべてのエンドポイントから TokenReview による制限が削除され、パフォーマンスが向上しました。(OCPBUGS-58317)
- この更新前は、`oc adm node-image create` コマンドが失敗したときに、有用なエラーメッセージが生成されませんでした。このリリースでは、oc adm node-image create コマンドが失敗した場合にエラーメッセージが生成されます。(OCPBUGS-58233)

- この更新前は、HAProxy 設定がヘルスチェックに /version エンドポイントを使用していたため、信頼性の低いヘルスチェックが生成されていました。このリリースでは、より正確なヘルスチェックを実現するために、IBM Cloud で /livez?exclude=etcd&exclude=log を使用するように liveness プローブがカスタマイズされています。この変更により、Hosted Control Plane での不適切なプローブ設定による障害を回避しながら、その他のプラットフォームで /version を維持できます。(OCPBUGS-58126)

- この更新前は、Machine Config Operator (MCO) が、現在のブートイメージがマーケットプレイスからのものであることを確認せずにブートイメージを更新していました。その結果、MCO はマーケットプレイスのブートイメージを標準の OpenShift Container Platform インストーラーイメージでオーバーライドしていました。このリリースでは、MCO はブートイメージを更新する前に、OpenShift Container Platform のすべての標準インストーラー Amazon Machine Images (AMI) を含む、Amazon Web Services (AWS) のルックアップテーブルを参照します。Google Cloud では、MCO はブートイメージを更新する前に URL ヘッダーをチェックします。その結果、MCO はマーケットプレイスのブートイメージを持つマシンセットを更新しなくなりました。(OCPBUGS-58044)

- の更新前は、oc-mirror プラグイン内の検証の問題により、コマンドが file://. 参照を拒否していました。コンテンツパスに file://. を使用すると、content filepath is tainted というエラーメッセージが生成されていました。このリリースでは、oc-mirror が . ディレクトリー参照を適切に検証します。(OCPBUGS-57970)

- この更新前は、oc-mirror v2 プラグインが操作中に正しくフィルタリングされたカタログを使用していませんでした。その結果、指定されていない Operator が設定に含まれており、エアギャップ環境であっても、ディスクからミラーへのミラーリングワークフロー中に、プラグインがカタログレジストリーへの接続を試みていました。このリリースでは、正しくフィルタリングされたカタログが使用されます。(OCPBUGS-57964)

- この更新前は、同じ useModal フックインスタンスを使用するモーダルが互いに上書きされていました。その結果、OpenShift Container Platform Lightspeed ユーザーインターフェイスが非表示になっていました。このリリースでは、モーダルに一意の ID が与えられます。その結果、モーダルの競合が解決され、Lightspeed、Troubleshooting Panel、および Networking ページのユーザーインターフェイスを同時に表示できるようになりました。(OCPBUGS-57931)

- この更新前は、リコンサイルの呼び出しごとにイメージが無視され再作成されていたため、新しいキャッシュが作成され、キャッシュされたイメージが使用できませんでした。その結果、Hosted Control Plane のメモリー使用量が急速に増加し、パフォーマンスの問題が発生していました。このリリースでは、リコンサイルの呼び出しごとにレジストリープロバイダーとリリースプロバイダーを再作成するのではなく、グローバルのレジストリープロバイダーを作成して使用することで、Hosted Control Plane 内のイメージが効率的にキャッシュされま

す。その結果、Hosted Control Plane でのメモリー使用量が最適化されます。(OCPBUGS-57818)

- この更新前は、olm.maxOpenShiftVersion が 4.19 に設定された Operator をインストールするために OLMv1 が使用されていました。浮動小数点形式の olm.maxOpenShiftVersion` 値に関する OLM v1 の解析ロジックの問題により、システムは OpenShift Container Platform 4.20 へのアップグレードを防止できませんでした。このリリースでは、olm.maxOpenShiftVersion の解析ロジックが修正されました。この修正により、olm.maxOpenShiftVersion:4.19 を含む Operator がインストールされている場合に OpenShift Container Platform 4.20 へのアップグレードが防止されます。(OCPBUGS-57767)

- この更新前は、catalog-operator が 5 分間隔でカタログのスナップショットをキャプチャーしていました。多数の namespace とサブスクリプションを使用している場合、4.15、4.16 で利用可能なカタログソースが大規模化したため、スナップショットが失敗していました。しかし、その失敗が複数のカタログソースに連鎖し、CPU 負荷の急上昇を引き起こしていました。この負荷の増加により、Operator のアップグレードとインストールを実行できませんでした。このリリースでは、キャッシュの有効期間が 30 分になりました。これにより、試行を解決するのに十分な時間が確保され、カタログソース Pod に過度の負荷がかからなくなりました。(OCPBUGS-57427)

- この更新前は、エンドポイントのない既存のサービスが、ある namespace 内の共通ユーザーデータネットワーク (CUDN) リソースを削除すると、ovnkube-node Pod の再起動が失敗していました。このリリースでは、エンドポイントのない既存のサービスを対象 namespace 内に持つ CUDN リソースを削除しても、ovnkube-node Pod が正常に再起動します。(OCPBUGS-57318)

- この更新前は、Create PodDisruptionBudget ページにタイプミスがありました。このリリースでは、タイプミスが修正されました。(OCPBUGS-57213)

- この更新前は、同じ作業ディレクトリーで oc-mirror プラグイン v2 を再実行すると、以前の実行で作成された既存の tar アーカイブファイルが削除されませんでした。その結果、古いアーカイブと新しいアーカイブが混在することになり、ターゲットレジストリーにプッシュするときにミラーリングが失敗する可能性がありました。このリリースでは、oc-mirror プラグイン v2 は各実行の開始時に古い tar アーカイブファイルを自動的に削除します。そのため、作業ディレクトリーには現在の実行で作成されたアーカイブのみが格納されます。(OCPBUGS-57197)

- この更新前は、oc-mirror v2 が、 mirror または delete という単語を含む有効な ImageSetConfiguration パラメーター値を拒否していました。このリリースでは、oc-mirror

v2 は ImageSetConfiguration パラメーター内の delete および mirror という単語を正しく検証し、無効な設定のみを拒否するようになりました。(OCPBUGS-57124)

- この更新前は、kubelet 上の cadvisor エンドポイントが無効なメトリクス値を報告していました。これにより、カウンターデータとさまざまなデバイスのデータが 1 つのメトリクスにまとめられていました。このリリースでは、cadvisor エンドポイントは有効なメトリクスを報告します。(OCPBUGS-57070)

- この更新前は、権限不足のため、keepalived ヘルスチェックスクリプトの 1 つが失敗していました。この失敗により、共有 Ingress サービスが使用されている場合に Ingress 仮想 IP が間違った場所に配置されることがありました。このリリースでは、必要な権限がコンテナーに再度追加されました。そのため、ヘルスチェックが正常に機能します。(OCPBUGS-56624)

- この更新前は、kube-rbac-proxy-crio Pod の hostPath ボリュームが、読み取り/書き込みアクセスで設定されていました。これは Kubernetes セキュリティーのベストプラクティスに違反するものでした。結果として、読み取り/書き込みの hostPath マウントにより、システムファイルの不正な変更が発生していました。このリリースでは、セキュリティーを向上させるために、`kube-rbac-proxy-crio` pod の hostPath マウントが読み取り専用になりました。(OCPBUGS-55246)

- この更新前は、バージョン 4.15.0 から 4.15.26 の Agent-based Installer を使用してインストールされたクラスターの場合、ユーザーが明示的に指定していなくても、CoreOS から組み込まれたルート証明書が user-ca-bundle に追加されていました。以前のリリースでは、oc adm node-image create コマンドを使用してこれらのクラスターの 1 つにノードを追加すると、クラスターの user-ca-bundle から取得された additionalTrustBundle 値が大きすぎて処理できず、ノードの追加が失敗していました。このリリースでは、additionalTrustBundle 値の生成時に組み込み証明書が除外されます。そのため、明示的にユーザーが設定した証明書のみが追加され、ノードを正常に追加できます。(OCPBUGS-54744)

- この更新前は、nodePort 設定の IP アドレス形式が無効であったため、HostedCluster コマンドがネットワークポリシーの作成に失敗していました。その結果、IP アドレスの特定が不正確になり、ホステッドクラスターの作成が失敗していました。このリリースでは、virt ランチャーのネットワークポリシーのリコンシリエーションに、IP アドレスタイプの特定に関するログメッセージが追加されました。この追加のログメッセージにより、kubevirt ホステッドクラスターにおける不正確な IP アドレス特定の問題が解決されます。その結果、HostedCluster コマンドによってネットワークポリシーとホステッドクラスターが正常に作成されます。(OCPBUGS-46629)

- この更新前は、動的 IPv6 設定の Kubernetes 仮想マシンが、プライマリーユーザー定義ネットワーク (UDN) レイヤー 2 を使用していたため、デフォルトの IPv6 ゲートウェイがマルチパスになっていました。その結果、複数のデフォルトの IPv6 ゲートウェイが原因で、ユー

ザートラフィックがノード間で誤って流れてしまいました。このリリースでは、新しい Open Virtual Network (OVN) トランジットルーターポロジーを使用しているため、デフォルトの IPv6 ゲートウェイが動的仮想マシン設定に適したものになっています。その結果、デフォルトの IPv6 ゲートウェイが正しいノードを指すようになりました。これにより、ノード間のトラフィックが削減され、ノードのメンテナンス中のネットワーク安定性が向上します。(OCPBUGS-46401)

1.9.9.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.10. RHSA-2025:9725 - OpenShift Container Platform 4.18.19 のバグ修正とセキュリティー更新

発行日: 2025 年 7 月 2 日

OpenShift Container Platform リリース 4.18.19 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:9725 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:9726 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.19 --pullspecs
```

1.9.10.1. バグ修正

- 以前は、ユーザーインターフェイスと API の不一致により、vSphere 接続の設定を含むリソースが壊れていました。このリリースでは、更新された API 定義がユーザーインターフェイスで使用されるため、リソースが壊れることはありません。(OCPBUGS-57580)

- 以前は、oc adm node-image create コマンドで、アーティファクトをディスクに保存するときに、ターゲットアセットフォルダーの既存の権限が誤って変更されていました。このリリースでは、バグ修正により、コマンドのコピー操作で保存先フォルダーの権限が維持されるようになりました。(OCPBUGS-57507)

- 以前は、openshift-monitoring/cluster-monitoring-config または openshift-user-workload-monitoring/user-workload-monitoring-config パラメーターで Alertmanager apiVersion v1 を使用すると、OpenShift Container Platform 4.19 が InvalidConfigXXX エラーで早い段階で失敗していました。この問題は、OpenShift Container Platform 4.19 が、Alertmanager apiVersion v1 をサポートしていない Prometheus v3 を使用しているために発生しました。このリリースでは、config map で apiVersion v1 が検出された場合、OpenShift Container Platform 4.19 にアップグレードした後に InvalidConfigXXX エラーが発生しないように、Cluster Monitoring Operator (CMO) が値を upgradable=false に設定します。その結果、OpenShift Container Platform 4.19 に移行する前に、OpenShift Container Platform 4.18.x を経由してクラスターをアップグレードすることになります。(OCPBUGS-56251)

1.9.10.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.11. RHSA-2025:9269 - OpenShift Container Platform 4.18.18 のバグ修正とセキュリティー更新

発行日: 2025 年 6 月 25 日

OpenShift Container Platform リリース 4.18.18 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:9269 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:9270 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.18 --pullspecs
```

1.9.11.1. バグ修正

- 以前は、画面サイズが縮小されると Started 列が非表示になり、並べ替え機能がないため VirtualizedTable コンポーネントが壊れていました。その結果、この壊れたテーブルコンポーネントにより、ユーザーが pipelinerun リストページを一貫して表示できませんでした。このリリースでは、画面サイズが縮小された場合に、不足していたデフォルトの列の並べ替え機能

を VirtualizedTable コンポーネントが処理するようになりました。その結果、画面サイズに関係なく、pipelinerun リストページを一貫して表示できるようになります。(OCPBUGS-57353)

- 以前は、Operator Lifecycle Management (OLM) の OperatorGroup の ClusterRole パラメーターでセレクターの順序を変更すると、不要な etcd 書き込みと認証キャッシュの無効化によってパフォーマンスが低下していました。このリリースでは、OLM の更新により、ClusterRole パラメーターでセレクターの順序を変更したときに、不要な etcd 書き込みと認証キャッシュの無効化が防止されます。(OCPBUGS-57314)

- 以前は、install-config.yaml ファイルにフィールドが不足していたため、Agent-based Installer がカスタムの additionalTrustBundlePolicy パラメーターを無視していました。その結果、オーバーライドが無視され、クラスターのインストールが指定した設定に準拠しないことがありました。このリリースでは、assisted-service の install-config.yaml ファイルに additionalTrustBundlePolicy 設定のオーバーライドが適切に適用されるようになりました。その結果、additionalTrustBundlePolicy パラメーターを正しく設定でき、その他のインストール設定のオーバーライドも正しく適用されるようになりました。(OCPBUGS-57306)

- 以前は、インプレース更新を使用するホステッドクラスターを更新しようとすると、プロキシー変数が考慮されず、更新が失敗していました。このリリースでは、インプレースアップグレードを実行する Pod がクラスタープロキシー設定を考慮します。その結果、インプレース更新を使用するホステッドクラスターでも更新が機能するようになりました。(OCPBUGS-57273)

- 以前は、Amazon Web Services (AWS) 上の既存の Virtual Private Cloud (VPC) にインストールする場合、コントロールプレーンノードのマシンセットカスタムリソースとそれに対応する AWS EC2 インスタンス間の AWS アベイラビリティーゾーンのサブネット情報に不一致が発生する可能性がありました。その結果、コントロールプレーンノードが 3 つのアベイラビリティーゾーンに分散されている状況でノードが 1 つ再作成されると、この不一致が原因で、同じアベイラビリティーゾーン内に 2 つのノードが配置され、コントロールプレーンのバランスが崩れる可能性がありました。このリリースでは、マシンセットのカスタムリソースと EC2 インスタンスのサブネットアベイラビリティーゾーン (AZ) 情報が一致するようになり、問題が解決されました。(OCPBUGS-57220)

- 以前は、カーネルからの stat 呼び出しが停止した場合 (たとえば、ネットワークファイルシステム (NFS) で実行されたディスク上の stat 呼び出しの場合など)、kubelet がメトリクスの報告を停止していました。このリリースでは、ディスクが停止している場合でも kubelet はメトリクスを報告します。(OCPBUGS-57219)

- 以前は、/metrics エンドポイントが、内部 Prometheus スクレイプリクエストの Authorization ヘッダーからベアラートークンを正しく解析していませんでした。その結果、TokenReview が失敗し、すべてのスクレイプリクエストが 401 レスポンスを返していま

した。このリリースでは、メトリクスエンドポイントのハンドラーが更新され、TokenReview の Authorization ヘッダー内のベアラートークンを正しく解析できるようになりました。この更新により、OpenShift Container Platform Web コンソールの TargetDown アラートが解決されました。(OCPBUGS-57181)

- 以前は、install-config.yaml 設定ファイルの machineNetwork パラメーターに独自 (BYO) のサブネットの CIDR を複数定義すると、ブートストラップステージでインストールが失敗していました。この状況は、コントロールプレーンノードがマシン設定サーバー (MCS) にアクセスできず、必要なセットアップ設定を取得できないために発生していました。根本的な原因は、AWS のセキュリティグループのルールが過度に厳格で、MCS へのアクセスを、指定された最初のマシンネットワーク CIDR のみに制限していたことでした。このリリースでは、AWS のセキュリティーグループが修正され、install-config.yaml の machineNetwork パラメーターに複数の CIDR が指定されている場合でもインストールが成功するようになりました。(OCPBUGS-57139)

- 以前は、管理クラスター内の IDMS または ICSP で registry.redhat.io または registry.redhat.io/redhat を参照するソースが定義されており、ミラーレジストリーに必要な OLM カタログイメージが含まれていない場合、不正なイメージプルが原因で HostedCluster オブジェクトのプロビジョニングが停止していました。その結果、HostedCluster オブジェクトがデプロイされず、ミラーリングされたレジストリーからの重要なカタログイメージのプルがブロックされていました。このリリースでは、認可エラーが原因で必要なイメージをプルできない場合、プロビジョニングが明示的に失敗し、ブロックされます。さらに、レジストリーのオーバーライドのロジックが改善され、OLM CatalogSource イメージの解決時に registry.redhat.io などのレジストリーのルートでのマッチングが可能になりました。また、レジストリーのオーバーライドによって正常なイメージが得られなかった場合に、元のイメージ参照を使用するためのフォールバックメカニズムも導入されています。そのため、ミラーレジストリーに必要な OLM カタログイメージが不足している場合でも、システムが必要に応じて元のソースからプルするために正しくフォールバックするため、HostedCluster オブジェクトがデプロイされます。(OCPBUGS-56955)

- 以前は、Kubernetes API Server の自己署名ループバック証明書が 1 年で期限切れになりました。このリリースにより、証明書の有効期限が 3 年に延長されました。(OCPBUGS-56835)

- 以前は、Machine Config Operator (MCO) が、クラスターに追加されたすべての新しいノードに Upgradeable=False 条件を誤って設定していました。この条件には、理由として PoolUpdating が指定されていました。このリリースでは、MCO がクラスターに追加されるすべての新しいノードに Upgradeable=True 条件を正しく設定するようになったため、問題が発生しなくなりました。(OCPBUGS-56517)

- 以前は、管理クラスターの IDMS または ICSP リソースが、ユーザーがイメージ置き換え用のミラーまたはソースとしてルートレジストリー名のみを指定する可能性があることを考慮せずに処理されていました。その結果、ルートレジストリー名のみを使用する IDMS または

ICSP エントリーが期待どおりに動作しませんでした。このリリースでは、ミラーの置き換えロジックが、ルートレジストリー名のみが指定されているケースを正しく処理するようになりました。その結果、問題が発生しなくなり、ルートレジストリーミラーの置き換えがサポートされるようになりました。(OCPBUGS-56166)

- 以前は、イメージのクリーンアップの際、イメージの削除中にエラーが発生した場合、oc-mirror プラグイン v2 は削除プロセスを停止していました。このリリースにより、oc-mirror プラグイン v2 は、エラーが発生した場合でも、残りのイメージの削除を試行し続けます。プロセスが完了すると、失敗した削除のリストが表示されます。(OCPBUGS-56125)

1.9.11.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.12. RHSA-2025:8560 - OpenShift Container Platform 4.18.17 のバグ修正とセキュリティー更新

発行日: 2025 年 6 月 10 日

OpenShift Container Platform リリース 4.18.17 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:8560 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:8561 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.17 --pullspecs
```

1.9.12.1. バグ修正

- 以前は、OpenShift Container Platform 4.11 上のシングルノード OpenShift デプロイメントは、Red Hat OpenStack Platform (RHOSP) プロバイダー上では機能しませんでした。このプラットフォームにインストールすることはサポートされていなかったためです。このリリースでは、シングルノード OpenShift デプロイメントで RHOSP へのインストールがサポートされるようになり、インストールの柔軟性が向上しました。(OCPBUGS-56864)

- 以前は、disk2mirror プロセスがキャッシュレジストリーの作成中にログを表示しなかったため、不完全なプロセスを引き起こしていました。このリリースでは、展開されたミラーアーカイブを追加する前に、作業ディレクトリーとキャッシュディレクトリーが検証されます。この更新により、disk2miror プロセス中の可視性が向上し、不完全なプロセスに関するユーザーの不安が軽減されます。(OCPBUGS-56659)

1.9.12.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.13. RHSA-2025:8284 - OpenShift Container Platform 4.18.16 バグ修正の更新

発行日: 2025 年 6 月 3 日

OpenShift Container Platform リリース 4.18.16 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:8284 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:8285 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.16 --pullspecs
```

1.9.13.1. バグ修正

- 以前は、非ゾーン Azure リージョンで、動的に計算される障害ドメイン数の更新のバグにより、スケーリングが失敗していました。この問題により、OpenShift Container Platform バージョン 4.15.48 以降にアップグレードしても、既存のマシンセットをスケーリングできませんでした。このリリースでは、障害ドメインの動的な計算を修正し、非ゾーンリージョンでのスケーリングの失敗を防ぐ更新が実装されています。この修正により、OpenShift Container Platform バージョン 4.15.48 以降にアップグレードした後、マシンセットのスケーリングがスムーズに実行されるようになりました。(OCPBUGS-56654)

- 以前は、公開鍵基盤 (PKI) の調整ステータスに関係なく、API サーバーのサブジェクト別

名 (SAN) 検証が実行されていました。その結果、無効な SAN が原因で Hosted Control Plane クラスターとの接続に潜在的な問題が生じていました。このリリースでは、修正により、PKI の調整が無効な場合に OpenShift Container Platform API サーバー SAN の検証が実行されなくされました。特に PKI の調整が管理対象外の場合は、不要な検証が排除されたことで Hosted Control Plane のパフォーマンスが向上します。(OCPBUGS-56627)

- 以前は、Bare Metal Operator (BMO) のバグにより、Baseboard Management Controller (BMC) の URL に Redfish のシステム ID がなかったため、JSON 解析エラーが発生していました。この問題により、URL にシステム ID がない場合にユーザーにエラーが表示されることがありました。このリリースでは、BMO が Redfish のシステム ID のない URL をシステム ID のないアドレスとして処理するようになりました。この修正により、BMC URL に Redfish システム ID がない場合のソフトウェア処理が改善されます。(OCPBUGS-56431)

- 以前は、Ironic Python Agent (IPA) のデプロイ時に、RAM ディスクログに NetworkManager ログが含まれていませんでした。そのため、効果的なデバッグが妨げられ、ネットワークの問題の解決に影響が出ていました。このリリースでは、NetworkManager ログが IPA のデバッグ用に RAM ディスクログに含まれるようになりました。その結果、IPA ログが強化され、デバッグ改善に役立つ包括的な NetworkManager データが提供されるようになりました。(OCPBUGS-56097)

- 以前は、Helm はタグとダイジェストを使用した Docker イメージのミラーリングをサポートしていませんでした。その結果、Helm リポジトリーのミラーリングが失敗し、イメージの重複とデプロイメントの不整合が発生していました。このリリースでは、Helm リポジトリーをミラーリングする際の Docker 参照の問題が修正によって解決され、タグとダイジェストが許容されるようになり、イメージミラーリングの成功率が向上しました。(OCPBUGS-56043)

- 以前は、Red Hat Enterprise Linux CoreOS (RHCOS) に使用されるバケット名が間違っていたために問題が発生していました。RHCOS イメージのインポートが失敗するため、ユーザーは OpenShift Container Platform クラスターを作成できませんでした。この問題は、PowerVS installer-provisioned infrastructure Cluster CAPI Operator の Madrid ゾーンでのクラスター作成を、正しいバケット名を使用して修正することで解決されました。このリリースでは、ユーザーはインストールプログラムを使用して、Madrid ゾーンに OpenShift Container Platform クラスターを作成できます。(OCPBUGS-53142)

- 以前は、ジョブ作成時に所有者参照が欠落していたために、MachineOSConfig (MOSC) から MachineOSBuild (MOSB) への接続で断続的なリソースリークが発生していました。その結果、リソース枯渇の可能性が発生し、Pod の更新に影響していました。このリリースでは、MOSC の削除時に MOSB リソースが一貫して削除されるように、ジョブ作成時に所有者参照が追加されます。これにより、リソースリークが防止されます。(OCPBUGS-52189)

1.9.13.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.14. RHBA-2025:8104 - OpenShift Container Platform 4.18.15 バグ修正の更新

発行日: 2025 年 5 月 27 日

OpenShift Container Platform リリース 4.18.15 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:8104 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:8106 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.15 --pullspecs
```

1.9.14.1. バグ修正

- 以前は、Web コンソールのバージョン 4.16 で、60 日間の更新制限に関するメッセージが誤って表示されていました。この古いメッセージは、OpenShift Container Platform 4.16 以降のバージョンのユーザーに誤解を与えるものでした。このリリースでは、Web コンソールから 60 日間の更新に関する警告が削除されました。これにより、正確で最新のユーザーエクスペリエンスが提供されるようになりました。(OCPBUGS-56255)

- 以前は、MachineConfigs シークレット内の機密情報と認証情報が監査ログに追加され、機密データが公開されていました。このリリースでは、更新により監査ログ内の MachineConfig シークレットが無視されるようになりました。その結果、ログから機密データが削除され、データセキュリティーが向上しました。(OCPBUGS-56030)

- 以前は、トークンのローテーションメカニズムによって、イメージ認証用の有効なトークンがない期間が誤って作成され、イメージレジストリーで一時的な認証エラーが発生していました。このエラーにより、Pod のスケジュールとビルドプロセスが影響を受けていました。このリリースでは、更新により OpenShift Container Platform のトークン更新メカニズムが強化され、無効なトークンが防止されるようになりました。この改善により、認証の失敗が減り、

イメージレジストリーと関連プロセスがよりスムーズに動作するようになりました。(OCPBUGS-54304)

- 以前は、VMware vSphere クラスターでの Open Virtual Appliance (OVA) のインポート中にホストがシャットダウンすると、障害が発生していました。更新により、インポートプロセス中に vSphere ESXi ホストが電源オフ状態やメンテナンスモードにならなくなりました。このリリースでは、更新により、中断することなく OVA を正常にインポートできるようになりました。(OCPBUGS-50690)

1.9.14.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.15. RHSA-2025:7863 - OpenShift Container Platform 4.18.14 のバグ修正更新とセキュリティー更新

発行日: 2025 年 5 月 20 日

OpenShift Container Platform リリース 4.18.14 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:7863 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:7865 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.14 --pullspecs
```

1.9.15.1. バグ修正

- 以前は、オブジェクト上の OLMManagedLabelKey ラベルを省略すると、クラスター操作が失敗していました。このリリースでは、更新により Pod の安定性が向上し、Operator Lifecycle Manager が適切に動作するようになりました。(OCPBUGS-56098)

以前は、無効な .tar 展開形式が原因で、ramdisk ログでファイルが不適切に分離され、ファイルの区切り文字がランダムに表示されていました。このリリースでは、.tar のエントリーを個別に処理するように ramdisk ログファイルが更新されました。この修正により、ログの読みやすさが向上し、解釈が容易になりました。(OCPBUGS-55938)

- 以前は、外部バイナリー内のプロキシー変数の形式が正しくなかったために、ビルドが失敗していました。このリリースでは、更新によりビルド Pod からプロキシー環境変数が削除され、ビルドの失敗が防止されるようになりました。(OCPBUGS-55699)

- 以前は、Ingress からルートへの変換に失敗してエラーが発生した場合、イベントがログに記録されませんでした。この更新により、このエラーがイベントログに表示されるようになりました。(OCPBUGS-55338)

- 以前は、afterburn パッケージが不足していたために gcp-hostname.service が失敗していました。その結果、scale-up ジョブが失敗して、エンドユーザーのデプロイメントに影響が出ていました。このリリースでは、afterburn パッケージが RHEL の scale-up ジョブにインストールされるようになりました。この修正により、scale-up アクションが正常に実行されるようになり、gcp-hostname サービスの障害が解決されました。(OCPBUGS-55158)

- 以前は、br-ex インターフェイスブリッジに接続された OVN-Kubernetes Localnet ネットワーク内のセカンダリーインターフェイスを持つ Pod は、同じノード上の他の Pod からはアクセスできませんでしたが、通信にはデフォルトのネットワークを使用していました。異なるノード上の Pod 間の通信には影響はありませんでした。このリリースでは、Localnet Pod と同じノードで実行されているデフォルトのネットワーク Pod 間の通信が可能になりますが、Localnet ネットワークで使用される IP アドレスは、ホストネットワークと同じサブネット内にある必要があります。(OCPBUGS-55016)

- 以前は、Zscaler プラットフォームがすべてのデータ転送をスキャンしていたため、イメージプルのタイムアウトが発生していました。その結果、イメージプルがタイムアウトしていました。このリリースでは、イメージプルのタイムアウトが 30 秒に延長され、更新が成功するようになりました。(OCPBUGS-54663)

- 以前は、Amazon Web Services (AWS) タグ名に空白を追加できましたが、インストールプログラムでは空白を含むタグ名がサポートされていませんでした。このような場合、インストールプログラムは ERROR failed to fetch Metadata というメッセージを返していました。このリリースでは、AWS タグの正規表現により、空白を含むタグ名が検証されるようになりました。インストールプログラムはこのようなタグを許可するようになり、空白によるエラーを返さなくなりました。(OCPBUGS-53221)

-

以前は、Open Virtual Network (OVN)-Kubernetes による不適切なリモートポートバインディングが原因で、クラスターノードの通信が何度も失われていました。これにより、ノード間の Pod 通信に影響が発生していました。このリリースでは、リモートポートバインディング機能が更新され、OVN によって直接処理されるようになりました。その結果、クラスターノード通信の信頼性が向上しました。(OCPBUGS-51144)

1.9.15.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.16. RHSA-2025:4712 - OpenShift Container Platform 4.18.13 のバグ修正更新とセキュリティー更新

発行日: 2025 年 5 月 14 日

OpenShift Container Platform リリース 4.18.13 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:4712 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:4714 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.13 --pullspecs
```

1.9.16.1. 既知の問題

- 他の Container Network Interface (CNI) プラグインと一緒に、DHCP アドレスの割り当てに CNI プラグインを Pod で使用すると、Pod のネットワークインターフェイスが予期せず削除される可能性があります。そのため、Pod の DHCP リースの有効期限が切れると、新しいリースの再作成時に DHCP プロキシーがループに入り、ノードが応答しなくなります。現在、既知の回避策はありません。(OCPBUGS-55354)

1.9.16.2. バグ修正

-

以前は、Progressing 条件でソートされていないイメージストリーム名によって、不要な更新が発生していました。これにより、ユーザーによって更新が過剰に行われ、パフォーマンスが低下する可能性がありました。このリリースでは、失敗したイメージのインポートが activeImageStreams 関数内でソートされるようになりました。この変更により、Cluster Samples Operator の効率が向上し、不要な更新が削減され、全体的なパフォーマンスが向上しました。(OCPBUGS-55783)

- 以前は、Progressing 条件のステータスが実際には変更されていない場合でも、Operator が条件の lastTransitionTime 値を更新していました。これにより、インストールエラーが発生することがあり、エンドユーザーが安定性の問題を感じることがありました。このリリースでは、ステータスが変更されない限り、Operator が lastTransitionTime 値を更新できなくなりました。これにより、Operator の安定性が向上し、インストーラーエラーが最小限に抑えられ、よりスムーズなユーザーエクスペリエンスが確保されます。(OCPBUGS-55782)

- 以前は、Cluster Samples Operator によってクラスター内のすべてのクラスター Operator が監視されていました。そのため、Cluster Samples Operator の同期ループが不必要に実行されていました。この動作は全体的なパフォーマンスに悪影響を及ぼしていました。このリリースでは、Cluster Samples Operator は特定のクラスター Operator のみを監視するようになりました。(OCPBUGS-55781)

- 以前は、非接続環境でノードを追加する場合、oc adm node-image コマンドでプライベートレジストリーイメージにアクセスできませんでした。その結果、イメージのプルに関する問題が発生し、ノードを追加できませんでした。このエラーは、mirror.openshift.com からダウンロードしたインストールプログラムバイナリーを使用してクラスターを最初にインストールした場合にのみ発生します。この問題はこのリリースで解決されています。(OCPBUGS-55449)

- 以前は、イメージ参照ダイジェストの計算に問題があり、SchemavVersion 1 イメージに基づくコンテナーの作成に失敗していました。これにより、新しいデプロイメントの作成が妨げられていました。このリリースでは、イメージダイジェストの計算が修正され、新しい Operator をインストールできるようになりました。(OCPBUGS-55435)

- 以前は、ノードが準備完了になる前にエビクトされた Microsoft Azure Spot 仮想マシン (VM) が、provisioned 状態のままになることがありました。このリリースでは、Azure Spot 仮想マシンが削除エビクションポリシーを使用するようになりました。これにより、プリエンプションが実行された場合に仮想マシンが failed 状態に正しく移行するようになりました。(OCPBUGS-55373)

- 以前は、自動化されたワークフローでミラーリングエラーが発生した場合でも、成功を示す終了ステータス 0 が oc-mirror プラグインによって返されていました。その結果、お客様は自動化されたワークフローの終了ステータスを信用できませんでした。このリリースでは、エ

ラーが発生した場合に、失敗を示す終了ステータス null が oc mirror プラグインによって返されるようになりました。(OCPBUGS-54626)

- 以前は、内部イメージレジストリー用に生成されたイメージプルシークレットが、埋め込まれた認証情報の有効期限が切れるまで再生成されませんでした。その結果、イメージプルシークレットが無効になる期間が短期間発生していました。このリリースでは、埋め込まれた認証情報の有効期限が切れる前に、イメージプルシークレットが更新されます。(OCPBUGS-54304)

- 以前は、OpenShift Container Platform 4.18 の Machine Config Operator (MCO) に、パッケージベースの Red Hat Enterprise Linux (RHEL) サポートが 4.19 で削除されたことが反映されていませんでした。このリリースでは、この Operator により、パッケージベースの RHEL ノードが存在するクラスター上の OpenShift Container Platform 4.19 への更新がブロックされるため、互換性が確保されます。(OCPBUGS-53427)

1.9.16.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.17. RHSA-2025:4427 - OpenShift Container Platform 4.18.12 のバグ修正更新とセキュリティー更新

発行日: 2025 年 5 月 8 日

OpenShift Container Platform リリース 4.18.12 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:4427 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:4429 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.12 --pullspecs
```

1.9.17.1. バグ修正

- 以前は、コードを処理するホスト名の競合状態が原因で、ブートホスト名とマシンホスト名の間に不整合が発生していました。このリリースでは、競合状態が解決され、オペレーティングシステムのインストール中に Ignition 設定ファイル内のホスト名の一貫性が確保されます。(OCPBUGS-55364)

- 以前は、特定のリージョンで Amazon Machine Image (AMI) ID が欠落していたため、インストールプログラムのバージョンでブートイメージの更新が失敗し、リージョン固有のユーザーの問題が発生していました。このリリースでは、リージョン AMI が見つからない場合、リージョンはデフォルトで us-east-1 AMI に設定され、インストールプログラムにはすべてのリージョンで信頼性の高いデフォルトの AMI が含まれます。(OCPBUGS-55290)

- 以前は、インストールされた Operator のリストを表示し、現在選択されているプロジェクトが Operator のデフォルトの namespace と一致し、コピーされたクラスターサービスバージョン (CSV) が Operator Lifecycle Manager (OLM) で無効になっている場合、リストに Operator が 2 回表示されました。このリリースでは、Operator は 1 回表示されます。(OCPBUGS-55195)

- 以前は、namedCertificates サーバー設定内の特定の IP アドレスが内部 API URL と競合していました。この状況により、証明書のサブジェクト代替名 (SAN) が一致しないため、HostedCluster カスタムリソース設定の問題が発生していました。このリリースでは、Kasm Workspaces エージェント (KAS) サーバー証明書内の競合する SAN が解決され、適切な設定が確保され、サービス機能が向上します。(OCPBUGS-54946)

- 以前は、socks5-proxy、konnectivity-proxy、http-proxy、client-token-minter などのプロキシーコンテナーに対するメモリー要求が不十分なために、頻繁にパフォーマンスの問題が発生していました。このリリースでは、これらのコンテナーに対するメモリー要求が 30 メガバイトに増加し、プロキシーコンテナーにさらに多くのメモリーを提供することで、パフォーマンスの安定性が向上します。(OCPBUGS-54737)

1.9.17.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.18. RHSA-2025:4211 - OpenShift Container Platform 4.18.11 のバグ修正更新とセキュリティー更新

発行日: 2025 年 5 月 1 日

OpenShift Container Platform リリース 4.18.11 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:4211 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:4213 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.11 --pullspecs
```

1.9.18.1. バグ修正

- 以前は、サービスを削除することで API サービスの関連付けが不適切に処理され、API サービスが利用できなくなっていました。ClusterResourceOverride リソースが削除されると、admission.autoscaling.openshift.io/v1 API サービスにアクセスできなくなり、Operator のインストールに影響が出ました。このリリースでは、ClusterResourceOverride リソースを削除すると、関連付けられている API サービスが削除され、Operator はインストールを正常に行うためにサーバー API のリストを取得できます。(OCPBUGS-55242)

- 以前は、OpenShift Container Platform バージョン 4.16 から 4.17 への Cluster Resource Override Operator (CROO) のアップグレード中に古いシークレットが削除されなかったため、OpenShift Container Platform のアップグレード後に CROO が失敗していました。このリリースでは、OpenShift Container Platform 4.17 のアップグレード中に Pod の作成と namespace の削除が正常に完了し、CROO エラーが解決されます。(OCPBUGS-55240)

- 以前は、catalogd 認証局 (CA) が見つからないため、Operator Lifecycle Manager (OLM) v1 のインストールが失敗していました。このリリースでは、更新された Operator Controller は新しいディレクトリーを CA 証明書に使用します。この変更により、システムの安定性が向上し、クラスター拡張機能が正しくインストールされ、ユーザーエクスペリエンスが向上します。(OCPBUGS-55172)

- 以前は、ロードバランサーのプライベート IP アドレスの不一致により、Azure IP の可用性を取得できず、OpenShift 4.17 デプロイメントでプライベート IP アドレスの競合が発生していました。この問題は、コントロールプレーンサブネット内の IP アドレスの可用性を確認することで解決されました。この修正により、OpenShift 4.17 デプロイメントの Azure IP アドレスの可用性に関するエラーが解決され、プライベート IP アドレスがサブネット範囲内で検証されるようになりました。(OCPBUGS-54947)

- 以前の 4.18 4.16 では、インターフェイス設定の問題により、OpenShift SDN から OVNKubernetes に移行するユーザーの再起動後に移行障害が発生していました。この失敗は、NMState が管理する br-ex 内の wait-for-primary-ip サービスの前にアクティブであった mtu-migration サービスが原因で発生しました。このリリースでは、移行の成功と、最初の再起動後に発生する mtu-migration サービスの障害回避を確実にするために、これらのサービスの順序が逆になっています。(OCPBUGS-54817)

- 以前は、monitoring.coreos.com API と monitoring.rhobs API の Cluster Network Operator (CNO) のクラスターロール権限が不足していたため、権限不足により監視の問題が発生していました。このリリースでは、CNO が servicemonitors および prometheusrules オブジェクトを管理するための権限があります。CNO は、monitoring.coreos.com API グループの servicemonitor および prometheusrules オブジェクトにパッチを適用し、監視の問題を修正します。(OCPBUGS-54698)

1.9.18.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.19. RHSA-2025:4019 - OpenShift Container Platform 4.18.10 のバグ修正更新とセキュリティー更新

発行日: 2025 年 4 月 22 日

OpenShift Container Platform リリース 4.18.10 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:4019 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:4021 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.10 --pullspecs
```

1.9.19.1. 機能拡張

-

OpenShift Container Platform 4.18 以降では、インストールプロセスのブートストラップフェーズで、metal3 httpd サーバーとノードのベースボード管理コントローラー (BMC) 間の Transport Layer Security (TLS) が、デフォルトで有効になります。TLS が有効な場合、httpd サーバーはポート 6180 ではなくポート 6183 上にあります。TLS 設定を無効にするには、ディスク上に作成されるプロビジョニングカスタムリソース (CR) ファイルに 'disableVirtualMediaTLS: true' を追加します。(OCPBUGS-39404)

1.9.19.2. バグ修正

- 以前は、Prometheus リモート書き込みプロキシー設定が Prometheus ユーザーワークロードカスタムリソース (CR) に正しく適用されていませんでした。そのため、クラスター内で通信とデータ収集の問題が発生していました。このリリースでは、ユーザーワークロードの Prometheus を含むユーザーワークロードモニタリング (UWM) の Prometheus 設定が、クラスタープロキシーリソースからプロキシー設定を正しく継承します。(OCPBUGS-38655)

- 以前は、アクティブ環境で Red Hat Enterprise Linux CoreOS (RHCOS) を実行すると、実行されていた rpm-ostree-fix-shadow-mode.service systemd サービスが原因でそのサービスが失敗していました。このリリースでは、インストールされた環境から RHCOS が実行されていない場合、rpm-ostree-fix-shadow-mode.service systemd サービスはアクティブになりません。(OCPBUGS-41625)

- 以前は、SimpleSelect.tsx ファイル内の誤ったコンポーネントのインポートにより、react-dom.production.min.js ファイル内に未定義の関数 r が発生していました。このコンポーネントにより、Dashboards および Metrics ページでドロップダウンリストに関連するエラーメッセージが表示されていました。このリリースでは、影響を受けるページのドロップダウンリストが正しく機能し、エラーメッセージが表示されなくなりました。(OCPBUGS-42845)

- 以前は、イメージプルシークレットコントローラーのシークレットトークンのローテーションロジックに関するエラーにより、認証用の一時的なトークンが無効になっていました。その結果、イメージのプルプロセスが中断されていました。このリリースでは、イメージプルシークレットコントローラーの更新により、トークンのローテーション中にトークンが無効になる期間が排除されます。その結果、イメージのプルプロセスがスムーズかつ継続的に実行されます。(OCPBUGS-54304)

- 以前は、kube-apiserver 設定で shutdown-watch-termination-grace-period 設定が省略されていたため、Hosted Control Plane によって管理されるクラスターでエラーが発生していました。このエラーにより、Hosted Control Plane によって管理されるクラスター内のアプリケーションが、不安定な形でシャットダウンされていました。このリリースでは、更新により、Hosted Control Plane によって管理されるクラスター内のアプリケーションのシャットダウンプロセスが改善され、kube-apiserver 設定に猶予期間が設けられます。シャットダウン中、アプリケーションの安定性が向上し、潜在的なエラーが減少します。(OCPBUGS-53404)

- 以前は、github.com/sherine-k/catalog-filter 要素のバージョンの問題により、要素が停止し、ミラーリングプロセスが不安定になっていました。このリリースでは、go.mod ファイル内の github.com/sherine-k/catalog-filter 要素が更新されました。そのため、問題が解決し、安定した信頼性の高いミラーリングプロセスが実現します。(OCPBUGS-54727)

- 以前は、scrapeCache 設定でイテレーションカウンターの増分が省略されていたため、後続のスクレイプのシリーズカウントが間違っていました。その結果、監視が中断され、Prometheus のスクレイププロセス中にデータが失われる可能性がありました。このリリースでは、Prometheus がエラーを解析しながらデータのスクレイピングと処理を継続するように更新されたため、監視が中断なく実行されます。(OCPBUGS-54940)

1.9.19.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.20. RHSA-2025:3775 - OpenShift Container Platform 4.18.9 のバグ修正更新とセキュリティー更新

発行日: 2025 年 4 月 15 日

OpenShift Container Platform リリース 4.18.9 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:3775 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:3777 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.9 --pullspecs
```

1.9.20.1. バグ修正

- 以前は、VMware vSphere のトポロジー関連機能用の manifest-topology.yaml ファイルが追加されていませんでした。このリリースでは、トポロジー関連機能用の manifest-topology.yaml ファイルが追加され、テストされています。その結果、トポロジー機能を使用

する際のパフォーマンスが向上し、エンドユーザーエクスペリエンスが強化されました。(OCPBUGS-54701)

- 以前は、EgressIP の論理ルーターポリシーでユーザー定義ネットワーク (UDN) が正しく処理されなかったため、OVN-Kubernetes コンテナーが起動に失敗していました。AWS で断続的にデプロイメントの失敗が発生し、長時間のダウンタイムとサービスの中断が発生していました。このリリースでは、UDN が設定された状態で OVN-Kubernetes コンテナーが正常に起動します。(OCPBUGS-54671)

- 以前は、アイデンティティープロバイダー (IdP) のリコンサイラーがお客様のプロキシーの追加トラストバンドルを考慮していませんでした。そのため、TLS 証明書の検証が失敗し、ホステッドクラスターで IdP 統合が失敗していました。その結果、エンドユーザーに対するサービスが中断されていました。このリリースでは、TLS 証明書の検証問題が解決され、追加のトラストバンドルを指定するプロキシー設定を使用してホステッドクラスターで IdP が正しく機能するようになりました。その結果、シームレスな IdP 統合によってエンドユーザーエクスペリエンスが向上します。(OCPBUGS-54627)

- 以前は、コントロールプレーンのコントローラーが、必要な機能セットに対して正しい Cluster Version Operator (CVO) マニフェストを選択していませんでした。このリリースでは、コントロールプレーンのコントローラーが正しい CVO マニフェストを選択し、そのマニフェストがホステッドクラスターにデプロイされます。(OCPBUGS-54625)

- 以前は、Ignition トークンの有効期限のタイムスタンプアノテーションがリセットされたときに、発生しないはずの問題が発生していました。これにより、古いトークンが蓄積され、クラスター内でリソースの管理が不十分になったり、セキュリティー上の脆弱性が生じたりしていました。このリリースでは、Hosted Control Plane Operator が期限切れの Ignition トークンを効果的にクリーンアップします。これにより、効率的なリソース管理が実現し、システムのセキュリティーが強化されるため、エンドユーザーエクスペリエンスが向上します。(OCPBUGS-54624)

- 以前は、コード内の HostedControlPlane および HostedCluster 仕様で IBM Cloud の最小サービス数が十分に適用されなかったためにバグが発生していました。この問題により、データの損失やユーザーが入力したデータの誤った処理が発生し、結果的に予期しないアプリケーションの動作が発生することがありました。このリリースでは、ユーザーインターフェイスに不正確なデータが表示される問題が修正されました。そのため、より信頼性が高く正確な情報がエンドユーザーに提供されます。(OCPBUGS-54609)

- 以前は、Hypershift Operator の Secret Janitor のスコープ設定が不適切だったため、不適切なシークレットのクリーンアップが発生していました。その結果、Hypershift Operator の 2 つのインスタンスでアノテーションスコープを使用している間、トークンシークレットが時間の経過とともに蓄積され、シークレット管理プロセスが中断されていました。このリリース

では、修正により、Hypershift Operator によって管理される Red Hat OpenShift Kubernetes Service (ROKS) クラスターで、シークレットのクリーンアップが期待どおりに継続されるようになりました。大量のトークンシークレットが排除され、適切なシークレット管理が維持されます。(OCPBUGS-54498)

- 以前は、etcd URL の不適切な処理によりバグが発生し、Kyverno サービスにアクセスできなくなっていました。その結果、kyverno 検証中に DNS エラーが発生し、Hosted Control Plane を備えた OpenShift Container Platform クラスターのユーザーが、追加のテストグループを作成できませんでした。このリリースでは、kyverno 検証中に DNS エラーが発生しなくなり、ユーザーが追加のテストグループを作成できるようになりました。(OCPBUGS-54411)

- 以前は、Microsoft Azure ディスク Container Storage Interface (CSI) ドライバーノードを作成した後、権限が不十分なために、disk.csi.azure.com/agent-not-ready=value:NoExecute taint が永続化していました。このリリースでは、修正により、Azure ディスク CSI ドライバーノードの not-ready taint の削除が無効になり、スケジューラーが volume-attach-limit 値に準拠するようになりました。(OCPBUGS-54383)

- 以前は、container_logreader_t という SELinux ドメインを使用してホスト上の /var/log ディレクトリーにあるコンテナーログを表示していたコンテナーが、/var/log/containers サブディレクトリーにあるログにアクセスできませんでした。これはシンボリックリンクの欠如により発生していました。このリリースでは、コンテナーが /var/log/containers サブディレクトリー内のログにアクセスできるように、シンボリックリンクが作成されます。(OCPBUGS-54342)

- 以前は、内部イメージレジストリー用に生成されたイメージプルシークレットが、埋め込まれた認証情報の有効期限が切れるまで再生成されませんでした。その結果、イメージプルシークレットが一時的に無効になっていました。このリリースでは、埋め込まれた認証情報の有効期限が切れる前に、イメージプルシークレットが更新されます。(OCPBUGS-54304)

- 以前は、マシンセット内のマシンの障害により、クラスターオートスケーラーがスケーリングを停止していました。この状況は、クラスターオートスケーラーがさまざまな非実行フェーズでマシンをカウントする方法が不正確だったために発生していました。このリリースでは、不正確さが修正され、クラスターオートスケーラーが正確なカウントを取得できるようになりました。(OCPBUGS-53241)

- 以前は、Global Navigation Satellite System (GNSS) のホールドオーバー中に Digital Phase-Locked Loop (DPLL) がロックされる前に、Telecom Grandmaster (T-GM) のステータスが誤って S2 と通知されていました。これにより、同期が不正確になっていました。このリリースでは、DPLL の状態決定ロジックが変更され、2 つの位相オフセットが両方とも有効になり、DPLL が "Locked Holdover Acquired" 状態になった後にのみ、T-GM のステータスが

S2 に遷移するようになりました。これにより、GNSS ソースの起動時に、T-GM のステータスが DPLL の状態を正確に反映するようになりました。(OCPBUGS-52956)

- 以前は、Egress IP アドレスを使用する資格がないユーザー定義ネットワーク (UDN) Pod は、外部に送信されるパケットの送信元 IP アドレスとして、ノード IP アドレスではなく独自の UDN Pod IP アドレスを使用する必要がありました。このリリースでは、UDN Pod ネットワークが正しくアドバタイズされるようになりました。(OCPBUGS-50965)

- 以前は、クラスター認証局 (CA) バンドルがカスタム CA バンドルで更新されると、変更が insights-runtime-extractor コンテナーに反映されるまでに遅延が発生していました。この問題は、CA バンドルが更新された後に Insights Operator がデータを収集した場合に発生していました。このリリースでは、修正により遅延が解消され、この問題は発生しなくなりました。(OCPBUGS-48790)

- 以前は、OpenShift Container Platform 4.17 で、コントロールプレーンサブネットの Classless Inter-Domain Routing (CIDR) 範囲内のロードバランサー IP アドレスがコードによって検証されなかったため、バグが発生していました。その結果、IP アドレスが有効範囲外となり、インストール中に 400 エラーが発生していました。このリリースでは、修正により、プライベート IP アドレスの競合による 400 エラーが発生しなくなりました。その結果、Azure 上のプライベート OpenShift Container Platform クラスターのデプロイメントが確実に成功するようになりました。(OCPBUGS-43724)

1.9.20.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.21. RHSA-2025:3577 - OpenShift Container Platform 4.18.8 のバグ修正更新とセキュリティー更新

発行日: 2025 年 4 月 10 日

OpenShift Container Platform リリース 4.18.8 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:3577 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:3579 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.8 --pullspecs
```

1.9.21.1. 既知の問題

- IPsec は Red Hat Enterprise Linux (RHEL) コンピュートノードではサポートされていません。これは、各コンピュートノードに存在するホストと ovn-ipsec コンテナー間の libreswan 非互換性の問題が原因です。(OCPBUGS-52949).

1.9.21.2. バグ修正

- 以前は、Microsoft Azure 上で実行されている仮想マシン (VM) に割り当てられているネットワークインターフェイスコントローラー (NIC) が ProvisioningFailed 状態であるために、NIC で障害が発生することがありました。このリリースでは、Machine API コントローラーが NIC のプロビジョニングステータスを確認し、仮想マシンを定期的に更新するようになりました。NIC が ProvisioningFailed 状態の場合、仮想マシンで障害が発生します。そのため、トラブルシューティングのために、問題をより適切に把握できるようになりました。(OCPBUGS-54355)

- 以前は、Administrator パースペクティブの Web コンソールの VolumeSnapshot ページで All projects オプションを選択すると 404: Page Not Found というエラーが発生していました。このリリースでは、修正により、VolumeSnapshot ページで All projects オプションを選択したときに、期待どおりの結果がページに表示され、エラーが発生しなくなりました。(OCPBUGS-54269)

- 以前は、oc-mirror プラグイン v2 の delete プラグインの --help 引数出力に誤字がありました。--generate リストに cache ではなく cahce と表示されていました。このリリースでは、--generate リストの説明にある状態 cache の誤字が修正されました。(OCPBUGS-54205)

- 以前は、oc-mirror --v2 version コマンドの出力にバージョン情報が含まれていませんでした。このリリースでは、コマンドの出力にバージョン番号が正しく表示されるようになりました。(OCPBUGS-53388)

- 以前は、IBM Cloud® Cloud Internet Services (CIS) 実装の更新により、アップストリームの Terraform プラグインが影響を受けていました。IBM Cloud® 上に外部向けクラスターを

作成しようとすると、次のエラーが発生しました。

```
ERROR Error: Plugin did not respond
ERROR
ERROR   with module.cis.ibm_cis_dns_record.kubernetes_api_internal[0],
ERROR   on cis/main.tf line 27, in resource "ibm_cis_dns_record"
"kubernetes_api_internal":
ERROR   27: resource "ibm_cis_dns_record" "kubernetes_api_internal"
```

このリリースでは、プラグインの問題が発生しなくなり、インストールプログラムを使用して OpenShift Container Platform 上に外部クラスターを作成できます。(OCPBUGS-53453)

- 以前は、ReadWriteMany (RWX) アクセスモードが設定されている場合、Google Cloud 永続ディスク (PD) の Container Storage Interface (CSI) ドライバーが、hyperdisk-balanced ボリュームタイプをサポートしていませんでした。この設定で hyperdisk-balanced ボリュームをプロビジョニングしようとすると、RWX アクセスモードが有効なボリュームをマウントできないことを示すエラーが発生しました。このリリースでは、RWX アクセスモードが有効な場合も hyperdisk-balanced ボリュームをマウントできるようになり、この問題が発生しなくなりました。マルチライターモードで Hyperdisk ボリュームを使用する場合の詳細な制限については、Google Cloud ドキュメントを参照してください。(OCPBUGS-44769)

1.9.21.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.22. RHBA-2025:3293 - OpenShift Container Platform 4.18.7 バグ修正の更新

発行日: 2025 年 4 月 3 日

OpenShift Container Platform リリース 4.18.7 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:3293 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:3295 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.7 --pullspecs
```

1.9.22.1. バグ修正

- 以前は、プロキシーが設定されると、インストールプログラムによって machineNetwork の Classless Inter-Domain Routing (CIDR) が noProxy フィールドに追加されていました。ユーザーによって machineNetwork の CIDR が noProxy に設定されていた場合、エントリーが重複していました。エントリーの重複は Ignition によって許可されていなかったため、ホストが適切に起動できないことがありました。このリリースでは、修正により、machineNetwork CIDR がすでに設定されている場合は、インストールプログラムによって noProxy に追加されなくなりました。(OCPBUGS-53183)

- 以前は、インターネット非接続環境でエージェント ISO をビルドすると、unable to read image というエラーメッセージが表示されていました。このリリースでは、このエラーメッセージは表示されません。(OCPBUGS-52515)

- 以前は、ブロックされたレジストリーからのイメージのインポートがコードによってブロックされていました。このリリースでは、レジストリーにミラーが設定されている場合でも、レジストリーからのイメージのインポートがブロックされません。(OCPBUGS-52312)

1.9.22.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.23. RHSA-2025:3066 - OpenShift Container Platform 4.18.6 のバグ修正更新とセキュリティー更新

発行日: 2025 年 3 月 25 日

OpenShift Container Platform リリース 4.18.6 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:3066 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHSA-2025:3068 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.6 --pullspecs
```

1.9.23.1. バグ修正

- 以前は、Operator Marketplace と Operator Lifecycle Manager (OLM) で、古いバージョン (v1.24) の pod-security.kubernetes.io/ ラベルが使用されていました。このリリースでは、Operator Marketplace がデプロイされている namespace で、latest とマークされた Pod Security Admission (PSA) ラベルが使用されるようになりました。(OCPBUGS-53149) (OCPBUGS-53108)

- 以前は、再起動操作中にデプロイメントがステージングの場所に移動された場合、クラスターのシャットダウン時に、競合状態により段階的な OSTree デプロイメントが完了できませんでした。このリリースでは、修正により OSTree デプロイメントから競合状態が削除され、再起動操作中でも段階的なデプロイメントを完了できるようになりました。(OCPBUGS-53111)

- 以前は、SIGTERM シグナルを処理する audit-logs コンテナーがタイムアウトしていました。SIGTERM シグナルを終了するために、Kubelet が audit-logs コンテナーにハード終了シグナル (SIGKILL) を送信する必要がありました。このリリースでは、プロセス ID (PID) エイリアスが修正され、監査ログが SIGTERM シグナルを適切に処理できるようになり、シグナルがタイムアウトすることがなくなりました。(OCPBUGS-52982)

- 以前は、apply-bootstrap コンテナーが SIGTERM シグナルを正しく処理していませんでした。このコンテナーは、シグナルを処理する前にスリープ操作が完了するのを待機していましたが、その後、Pod の termination-grace-period を超過していました。このような場合、シャットダウン操作を強制し、Pod が削除を完了できるように、SIGKILL シグナルが必要でした。このリリースでは、apply-bootstrap コンテナーがシグナル SIGTERM を正しく処理するようになりました。これにより、正常なシャットダウンの期間が正しく確保され、SIGKILLED シグナルが不要になりました。(OCPBUGS-52878)

- 以前は、ミラーからディスクへのミラーリング操作中に空のカタログをミラーリングすると、ディスクからミラーへのミラーリング操作が失敗していました。この空のカタログは、ImageSetConfiguration CR 内の無効な Operator エントリーから生成されていました。このリリースでは、空のカタログをミラーリングできなくなったため、ディスクからミラーへのミラーリング操作が正常に実行されます。(OCPBUGS-52943)

- 以前は、UEFI と互換性のないブートディスクを使用している Google Cloud クラスターをアップグレードした場合、Shielded VM のサポートを有効にできませんでした。この動作に

より、新しいマシンの作成が妨げられていました。このリリースでは、UEFI と互換性がないことがわかっているディスクに対して、Shielded VM のサポートが無効になっています。この変更は、Google Cloud マーケットプレイスイメージを使用して OpenShift Container Platform バージョン 4.12 から 4.13 にアップグレードするお客様に主に影響します。(OCPBUGS-52495)

- 以前は、OpenShift Container Platform Web コンソールのノードログが、ノードログメニューの外部をクリックしても閉じませんでした。このリリースでは、ノードログメニューの外側をクリックすると、ノードログメニューが閉じるようになりました。(OCPBUGS-52490)

- 以前は、OpenShift Container Platform Web コンソールから Developer Sandbox にログオンすると、Web コンソールは URL 内のパスを無視し、URL に詳細が記載された namespace ではなく、Developer Sandbox の all projects ビューを表示していました。このリリースでは、この動作が修正され、エラーが発生しなくなりました。(OCPBUGS-52406)

- 以前は、cluster-compare ツールの capturegroup インライン diff アルゴリズムによって、オブジェクト内のソーステキストをリファレンステンプレートの capturegroup 正規表現と一致させることができませんでした。この問題は、ソーステキストが正規表現と同様の構造を持つ場合に発生していました。このリリースでは、capturegroup のインライン diff アルゴリズムが修正され、この一致の問題が発生しなくなりました。(OCPBUGS-51306)

- 以前は、継続的インテグレーション (CI) 自動化サイクルで oc-mirror v2 を実行し、TTY 以外のコンソールで oc-mirror v2 ログを表示すると、進行状況バーの実装の問題により、出力に進行状況情報が表示されませんでした。このリリースでは、oc-mirror v2 が進行状況バーの実装を無効にし、代わりにプレーンテキストのロギングを使用して出力をリダイレクトするようになったため、情報の欠落が解消されました。(OCPBUGS-50996)

1.9.23.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.24. RHSA-2025:2705 - OpenShift Container Platform 4.18.5 のバグ修正更新とセキュリティー更新

発行日: 2025 年 3 月 18 日

OpenShift Container Platform リリース 4.18.5 が公開されました。更新に含まれるバグ修正のリス

トは、RHSA-2025:2705 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:2707 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.5 --pullspecs
```

1.9.24.1. バグ修正

- 以前は、クラスターの作成中に、IBM Cloud 上の installer-provisioned infrastructure デプロイされたクラスター内のマシンを Machine API が起動および管理していました。Machine API は、異常なコントロールプレーンノードを検出し、そのノードに削除対象のフラグを設定し、クラスターを破棄していました。このリリースでは、クラスターの作成中に、すべてのコントロールプレーンノードが復元されます。(OCPBUGS-52872)

- 以前は、managed-trust-bundle ボリュームマウントと 'trusted-ca-bundle` config map が必須コンポーネントとして導入されていました。この要件により、独自の公開鍵基盤 (PKI) を使用する場合にデプロイメントが失敗していました。OpenShift Container Platform API サーバーによって、trust-ca-bundle-managed config map が要求されていました。このリリースでは、これらのコンポーネントが任意になりました。そのため、カスタムの PKI を使用する場合に、trusted-ca-bundle-managed config map なしでクラスターを正常にデプロイできるようになりました。(OCPBUGS-52516)

- 以前は、バッチの処理に 10 ミリ秒以上かかると、etcd のコンパクションによってプロセスがブロックされていました。このリリースでは、問題が修正され、etcd のコンパクションが期待どおりに進行します。(OCPBUGS-51971)

- 以前は、Ampere ARM ベースの CPU が、他の ARM とは異なる CPU ベンダー識別子を使用していました。プラットフォームチューニングはベンダー ID とマッチしましたが、ARM ベースの CPU を搭載したマシンは識別されませんでした。このリリースでは、ARM の検出がアーキテクチャーフィールドを使用するように変更され、Ampere CPU を搭載したマシンが適切にチューニングされます。(OCPBUGS-52484)

- 以前は、openshift-install agent create pxe-files コマンドを実行すると、一時ディレクトリーが作成されていました。コマンドが完了してもこのディレクトリーは削除されませんでし

た。このリリースでは、コマンド入力時に一時ディレクトリーが削除されます。(OCPBUGS-52429)

- 以前は、oc-mirror が Operator Lifecycle Manager (OLM) のロジックを使用してカタログのフィルタリングを開始すると、パフォーマンスが低下していました。このリリースでは、この状態が解決されました。(OCPBUGS-52350)

1.9.24.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.25. RHSA-2025:2449 - OpenShift Container Platform 4.18.4 のバグ修正更新とセキュリティー更新

発行日: 2025 年 3 月 11 日

OpenShift Container Platform リリース 4.18.4 が公開されました。更新に含まれるバグ修正のリストは、RHSA-2025:2449 アドバイザリーに記載されています。更新に含まれる RPM パッケージは、RHBA-2025:2451 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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.4 --pullspecs
```

1.9.25.1. 既知の問題

- 現在、テクノロジープレビューが有効なクラスターには policy.json 内のペイロードイメージに対する Sigstore 検証がありますが、ベースイメージ内の Podman バージョンは Sigstore 設定をサポートしていないという既知の問題があります。その結果、新しいノードは利用できなくなります。

  回避策: ベースイメージ内の Podman バージョンが Sigstore をサポートしていない場合でも、ノードは実行を開始します。ベースイメージが 4.11 以前の場合は、Sigstore 検証のな

いデフォルトの policy.json ファイルを使用します。(OCPBUGS-48296)

- 現在、関連するベアメタルホストを削除した後もデータイメージが残るという既知の問題があります。

  回避策: ベアメタルホストが削除された後、データイメージが存在する場合は削除します。(OCPBUGS-45250)

1.9.25.2. バグ修正

- 以前は、制限された拡張属性を持つファイルが含まれるカタログまたはバンドルイメージは使用できませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-52173)

- 以前は、registryOverride オプションを使用して catalog Operator イメージをオーバーライドすることはできませんでした。このリリースでは、control plane Operator のロジックが更新され、問題が解決されました。(OCPBUGS-51375)

- 以前は、不安定なネットワーク経由で、または GCP サーバーに到達できない場合、インストーラーは Google Cloud Platform (GCP) タグを取得できませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-51211)

- 以前は、ノードの表示権限はあるが証明書署名要求 (CSR) の表示権限がない場合、Nodes list ページにアクセスできませんでした。このリリースでは、Nodes list ページにアクセスするために CSR の表示権限は不要になりました。(OCPBUGS-51149)

- 以前は、モニタリングに関連する特定のフラグが設定されていない限り、Web コンソールの Observe セクションにはプラグインから提供された項目が表示されませんでした。しかし、これらのフラグにより、ロギング、分散トレーシング、ネットワーク可観測性などの他のプラグインは Observe セクションに項目を追加できませんでした。このリリースでは、モニタリングフラグが削除され、他のプラグインが Observe セクションに項目を追加できるようになりました。(OCPBUGS-51086)

- 以前は、oc-mirror の収集フェーズ中に kubevirt および graphImage イメージが取得されなかった場合、イメージが欠落していても実行は成功していました。このリリースでは、イメージが見つからない場合、oc-mirror の実行は予想どおりに失敗します。(OCPBUGS-50981)

- 以前は、インストール中に Nutanix クラスターの障害ドメインに複数のサブネットを設定できないという問題がありました。このリリースにより、この問題は解決されました。(OCPBUGS-49885)

- 以前は、idle-close-on-response HAProxy 設定を管理するために、新しい Ingress Controller API (IdleConnectionTerminationPolicy) が追加されました。クラスターに IdleConnectionTerminationPolicy API フィールドがない場合、idle-close-on-response 設定は無条件に有効になります。このリリースのデフォルト値は Deferred となり、問題は解決されました。(OCPBUGS-48377)

1.9.25.3. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.26. RHBA-2025:2229 - OpenShift Container Platform 4.18.3 バグ修正の更新

発行日: 2025 年 3 月 6 日

OpenShift Container Platform リリース 4.18.3 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:2229 アドバイザリーに記載されています。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.3 --pullspecs
```

1.9.26.1. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.27. RHBA-2025:1904 - OpenShift Container Platform 4.18.2 イメージのリリース、バグ修正およびセキュリティーアドバイザリー

発行日: 2025 年 3 月 4 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.18.2 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2025:1904 アドバイザリーに記載されています。更新に含まれる RPM パッケージは RHSA-2025:1908 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

```
$ oc adm release info 4.18.2 --pullspecs
```

1.9.27.1. バグ修正

- 以前は、oc-mirror v2 コマンドで dry-run 引数を使用すると、cluster-resources ディレクトリーが誤ってクリアされていました。その結果、idms-oc-mirror.yaml や itms-oc-mirror.yaml など、以前のミラーリング操作から生成されたファイルが削除されました。このリリースでは、oc-mirror v2 コマンドに dry-run 引数を追加しても、cluster-resources ディレクトリーはクリアされなくなりました。(OCPBUGS-51185)

- 以前は、Operator Controller はプロキシー設定を持つレジストリーへのライブ更新を受け入れませんでした。コントローラー Pod を再起動しない限り、この問題により OLM v1 は間違ったイメージ URL を読み取ります。このリリースでは、Operator Controller が修正され、プロキシー設定のレジストリーへのライブ更新が受け入れられるようになり、コントローラー Pod を再起動する必要がなくなりました。(OCPBUGS-51140)

- 以前は、マルチパスデバイスにアタッチされた Internet Small Computer System Interface (iSCSI) およびファイバーチャネルデバイスは、これらのデバイスがパーティション分割されているときに正しく解決されませんでした。このリリースにより、パーティション分割されたマルチパスストレージデバイスが正しく解決できるように修正されました。(OCPBUGS-51100)

- 以前は、カタログリソースから一部の Operator をミラーリングすると、oc-mirror v1 が失敗し、ocischema.DeserializedImageIndex マニフェストファイルに問題があることを示す

エラーメッセージが表示されました。このリリースでは、oc-mirror v1 は ocischema.DeserializedImageIndex マニフェストファイルを処理できるようになり、この問題は発生しなくなりました。(OCPBUGS-51099)

- 以前は、セキュアプロキシーを有効にしてクラスターを作成し、証明書設定を configuration.proxy.trustCA に設定すると、クラスターのインストールは失敗していました。さらに、OpenShift OAuth API サーバーは、管理クラスタープロキシーを使用してクラウド API にアクセスできませんでした。このリリースでは、これらの問題を防ぐための修正が加えられてました。(OCPBUGS-51050)

- 以前は、IBM Power Virtual Server クラスターで Dynamic Host Configuration Protocol (DHCP) ネットワークを削除しても、サブリソースが残存していました。このリリースでは、DHCP ネットワークを削除すると、サブリソースも削除されます。(OCPBUGS-50870)

- 以前は、IBM Power Virtual Server クラスターで Dynamic Host Configuration Protocol (DHCP) ネットワークを削除しても、サブリソースが残存していました。このリリースでは、DHCP ネットワークを削除すると、破棄操作を続行する前にサブリソースが削除されるようになりました。(OCPBUGS-50870)

- 以前は、VMware vCenter アドレスが正しくないか見つからない場合、vmware-vsphere-csi-driver-operator Container Storage Interface (CSI) ドライバーはパニックモードになりました。このリリースでは、VMware vCenter アドレスが正しくないか見つからない場合でも、CSI ドライバーはパニックモードになりません。(OCPBUGS-50638)

- 以前は、Agent-based Installer を使用してホストにクラスターをインストールすると、Extensible Firmware Interface (EFI) デバイスである /dev/sda デバイスのマウントに失敗することがありました。このリリースでは、EFI デバイスに再試行操作が追加され、正しくマウントされるようになりました。(OCPBUGS-50621)

- 以前は、control plane Operator は、API エンドポイントの可用性をチェックするときに、設定されている _PROXY 環境変数を適用しませんでした。このリリースにより、この問題は解決されました。(OCPBUGS-50550)

- 以前は、ClusterVersion が Completed 更新を受信しなかった場合、クラスター更新中に Cluster Settings ページが正しくレンダリングされませんでした。このリリースにより、ClusterVersion が Completed 更新を受信していない場合でも、Cluster Setting ページが適切にレンダリングされるようになりました。(OCPBUGS-49921)

- 以前は、ClusterNetwork Classless Inter-Domain Routing (CIDR) のマスク値が hostPrefix 値よりも大きく、install-config.yaml ファイルに networking.ovnKubernetesConfig.ipv4.internalJoinSubnet セクションが指定されている場合、インストールプログラムは検証チェックに失敗し、Golang ランタイムエラーを返していました。このリリースにより、インストールプログラムは依然として検証チェックに失敗し、無効な hostPrefix 値を示す説明的なエラーメッセージを出力するようになりました。(OCPBUGS-49864)

- 以前は、ルーターは SHA1 リーフ証明書のみが HAProxy によって拒否されると誤って想定していました。これにより、ルーターは SHA1 中間証明書を拒否し、障害が発生しました。このリリースでは、ルーターは自己署名付き証明書以外をすべて検査し、SHA1 を使用する証明書を拒否するようになりました。SHA1 中間証明書の存在により、ルーターがクラッシュしなくなりました。自己署名付き SHA1 証明書は拒否されなくなりました。ルート CA は引き続き SHA1 を使用できます。(OCPBUGS-49389)

- 以前は、Google Cloud に、クラスターリソースを破壊する API 呼び出しに対する wait 操作は含まれていませんでした。この操作が欠落しているため、特定の状況ではインストールプログラムがバックエンドサービスを削除しませんでした。このリリースでは、Google Cloud は API 呼び出しに wait 操作を追加し、インストールプログラムがバックエンドサービスを削除できるようになりました。(OCPBUGS-49320)

- 以前は、Web コンソールの Operator Details ページに、ClusterServiceVersion (CSV) の詳細が表示されませんでした。このリリースでは、CSV の詳細が Operator Details ページでレンダリングされるようになりました。(OCPBUGS-48736)

- 以前は、Operator のインストール中に作成された Helm チャートのアノテーションに、バンドルプロパティーが伝播されない場合がありました。このリリースでは、バンドルの CSV と、metadata.yaml ファイルまたは properties.yaml ファイルの両方からプロパティーが取得されるようになったため、この問題は発生しなくなりました。(OCPBUGS-45114)

- 以前は、永続ボリューム (PV) の作成中に Local Storage Operator (LSO) が既存の Small Computer System Interface (SCSI) シンボリックリンクを無視していました。このリリースでは、PV の作成時に新規シンボリックリンクを見つける前にこれらのシンボリックリンクを収集するため、LSO はこれらのシンボリックリンクを無視しなくなりました。(OCPBUGS-51056)

- 以前は、クラスターに設定された最大転送単位 (MTU) 値よりも大きい User Datagram Protocol (UDP) パケットは、サービスを使用してパケットのエンドポイントに送信できませんでした。このリリースでは、パケットサイズにかかわらず、サービス IP アドレスの代わりに

Pod IP アドレスが使用されるため、UDP パケットをエンドポイントに送信できます。(OCPBUGS-50512)

1.9.27.2. 更新

OpenShift Container Platform 4.18 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.28. RHSA-2024:6122 - OpenShift Container Platform 4.18.1 イメージリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 2 月 25 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.18.1 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2024:6122 アドバイザリーに記載されています。更新に含まれる RPM パッケージは RHEA-2024:6126 アドバイザリーによって提供されます。

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。

以下のコマンドを実行して、このリリースでコンテナーイメージを表示できます。

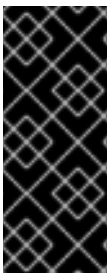
```
$ oc adm release info 4.18.1 --pullspecs
```

1.9.28.1. 更新

OpenShift Container Platform 4.17 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

第2章 その他のリリースノート

中核的な OpenShift Container Platform 4.18 リリースノート に含まれていないその他の関連コンポーネントおよび製品のリリースノートは、次のドキュメントで入手できます。



重要

以下のリリースノートは、ダウンストリームの Red Hat 製品のみを対象としています。関連製品のアップストリームまたはコミュニティーリリースノートは含まれていません。

A

AWS Load Balancer Operator

B

Builds for Red Hat OpenShift

C

cert-manager Operator for Red Hat OpenShift

Cluster Observability Operator (COO)

Compliance Operator

Custom Metrics Autoscaler Operator

D

Red Hat Developer Hub Operator

E

External DNS Operator

F

File Integrity Operator

K