OpenShift Container Platform 4.19

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 4.19 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 4.19 リリースノート **3**
1.1. このリリースについて 3
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 3
1.3. 新機能および機能拡張 4
1.4. 主な技術上の変更点 27
1.5. 非推奨の機能と削除された機能 28
1.6. バグ修正 33
1.7. テクノロジープレビュー機能のステータス 57
1.8. 既知の問題 67
1.9. 非同期エラータの更新 69

第2章 その他のリリースノート **98**

第1章 OPENSHIFT CONTAINER PLATFORM 4.19 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安全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 上に構築された 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も提供します。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-2024:11038) 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 1.32 を使用します。このトピックには、OpenShift Container Platform 4.19 に関連する新機能、変更点、既知の問題が含まれています。

OpenShift Container Platform 4.19 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。

コントロールプレーンとコンピュートマシンには RHCOS マシンを使用する必要があります。

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、すべてのサポートされているアーキテクチャーにおける OpenShift Container Platform 4.19 などの奇数リリースのサポートライフサイクルは 18 カ月です。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

以下の新機能は、OpenShift Container Platform 4.19 の IBM Power でサポートされます。

- IBM Power®11 のサポート

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. 外部 OIDC アイデンティティープロバイダーによる直接認証の有効化 (テクノロジープレビュー)

このリリースにより、外部の OpenID Connect (OIDC) アイデンティティープロバイダーとの直接統合を有効にして、認証用のトークンを発行できるようになりました。これにより、組み込みの OAuth サーバーがバイパスされ、外部アイデンティティープロバイダーが直接使用されます。

外部 OIDC プロバイダーと直接統合することで、組み込みの OAuth サーバーの機能に制限されることなく、お好みの OIDC プロバイダーの高度な機能を活用できます。組織は単一のインターフェイスからユーザーとグループを管理できるだけでなく、複数のクラスターやハイブリッド環境全体での認証を合理化できます。既存のツールやソリューションと統合することもできます。

直接認証はテクノロジープレビュー機能として利用できます。

詳細は、外部 OIDC アイデンティティープロバイダーによる直接認証の有効化 を参照してください。

1.3.1.2. ServiceAccountTokenNodeBinding Kubernetes 機能をデフォルトで有効にする

OpenShift Container Platform 4.19 では、アップストリーム Kubernetes の動作に合わせて、**ServiceAccountTokenNodeBinding** 機能がデフォルトで有効になっています。この機能により、既存のバインディングオプションに加えて、サービスアカウントトークンをノードオブジェクトに直接バインドできるようになります。この変更の利点には、バインドされたノードが削除されたときにトークンが自動的に無効化されることによるセキュリティーの強化や、異なるノード間でのトークンリプレイ攻撃に対する保護の強化などがあります。

1.3.2. ドキュメント

1.3.2.1. 統合された etcd ドキュメント

このリリースには、OpenShift Container Platform の etcd に関する既存のドキュメントをすべて統合した **etcd** セクションが含まれています。詳細は、etcd の概要 を参照してください。

1.3.2.2. チュートリアルガイド

OpenShift Container Platform 4.19 には、以前のリリースの **スタートガイド** に代わる **チュートリアル** ガイドが含まれるようになりました。既存のチュートリアルが更新され、このガイドは実践的なチュートリアルコンテンツのみに焦点を当てるようになりました。また、このガイドは、Red Hat 全体で推奨されている OpenShift Container Platform の実践的な学習リソースへの導入部としても役立ちます。

詳細は、チュートリアル 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. 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 (一般提供)

PolicyGenerator リソースと Red Hat Advanced Cluster Management (RHACM) を使用して、GitOps ZTP でマネージドクラスターのポリシーをデプロイできるようになりました。**PolicyGenerator** API は Open Cluster Management 標準の一部であり、**PolicyGenTemplate** API では不可能な、リソースにパッチを適用する一般的な方法を提供します。**PolicyGenTemplate** リソースを使用してポリシーを管理およびデプロイすることは、今後の OpenShift Container Platform リリースでは非推奨になります。

詳細は、PolicyGenerator リソースを使用したマネージドクラスターポリシーの設定 を参照してください。

1.3.3.2. ローカルアービターノードの設定 (テクノロジープレビュー)

クラスターのインフラストラクチャーコストを削減しながら高可用性 (HA) を維持するために、2 つのコントロールプレーンノードと 1 つのローカルアービターノードを使用して、OpenShift Container Platform クラスターを設定できます。この設定は、ベアメタルのインストールの場合にのみサポートされます。

ローカルアービターノードは、コントロールプレーンのクォーラム決定に参加する低コストの共存マシンです。標準のコントロールプレーンノードとは異なり、アービターノードはコントロールプレーンサービスの完全なセットを実行しません。この設定を使用すると、3 つのコントロールプレーンノードではなく 2 つの完全にプロビジョニングされたコントロールプレーンノードのみを使用して、クラスター内の HA を維持できます。

この機能を有効にするには、**install-config.yaml** ファイルでアービターマシンプールを定義し、**TechPreviewNoUpgrade** 機能セットを有効にする必要があります。

ローカルアービターノードの設定は、テクノロジープレビュー機能として利用できます。詳細は、ローカルアービターノードの設定 を参照してください。

1.3.3.3. 設定変更のための再起動の調整

このリリースにより、ZTP リファレンスに再起動ポリシーが追加されました。このポリシーは Topology Aware Lifecycle Manager (TALM) によって適用され、遅延チューニング変更などの設定変更で再起動が必要な場合に、スポーククラスターのフリート全体で再起動を調整します。再起動ポリシーが適用されると、TALM は選択したクラスター上の対象の **MachineConfigPool** オブジェクト内のすべてのノードを再起動します。

個々の変更ごとにノードを再起動する代わりに、ポリシーを通じてすべての設定の更新を適用してから、単一の調整された再起動をトリガーできます。

詳細は、設定変更のための再起動の調整 を参照してください。

1.3.4. 拡張機能 (OLM v1)

1.3.4.1. クラスター拡張機能のパーミッション事前チェック (テクノロジープレビュー)

このリリースにより、拡張機能をインストールしようとすると、Operator Controller がインストールプロセスのドライランを実行します。このドライランは、指定されたサービスアカウントに、バンドルによって定義されたロールとバインディングに必要なロールベースアクセス制御 (RBAC) ルールがあるか確認します。

サービスアカウントに必要な RBAC ルールがない場合、実際のインストールが続行される前に事前チェックが失敗し、レポートが生成されます。

詳細は、クラスター拡張機能のパーミッション事前チェック (テクノロジープレビュー) を参照してください。

1.3.4.2. 特定の namespace でのクラスター拡張機能のデプロイ (テクノロジープレビュー)

このリリースにより、**registry+v1** Operator バンドルのテクノロジープレビュー機能として、**OwnNamespace** または **SingleNamespace** インストールモードを使用し、特定の namespace に拡張機能をデプロイできます。

詳細は、特定の namespace でのクラスター拡張機能のデプロイ (テクノロジープレビュー) を参照してください。

1.3.5. ハードウェアアクセラレーター

1.3.5.1. Dynamic Accelerator Slicer Operator (テクノロジープレビュー)

このリリースにより、ノードの起動時に定義される静的にスライスされた GPU に依存するのではなく、Dynamic Accelerator Slicer (DAS) Operator を使用して OpenShift Container Platform で GPU アクセラレーターを動的にスライスすることができます。これにより、特定のワークロードの需要に基づき GPU を動的にスライスし、効率的なリソース利用を実現できます。

詳細は、Dynamic Accelerator Slicer (DAS) Operator を参照してください。

1.3.6. 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。

1.3.6.1. Red Hat OpenStack Platform (RHOSP) 17.1 上の Hosted Control Plane (テクノロジープレビュー)

RHOSP 17.1 上の Hosted Control Plane がテクノロジープレビューとしてサポートされるようになりました。

詳細は、OpenStack での Hosted Control Plane のデプロイ を参照してください。

1.3.7. IBM Power

OpenShift Container Platform 4.19 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。

- Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) のプロファイルを使用して Compliance Operator サポートを拡張します。

1.3.8. IBM Z と IBM LinuxONE

OpenShift Container Platform 4.19 の IBM Z® および IBM® LinuxONE 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 Z® および IBM® LinuxONE 上で次の機能がサポートされます。

- IBM® z17 および IBM® LinuxONE 5 のサポート

- IBM® Crypto Express (CEX) によるブートボリュームの Linux Unified Key Setup (LUKS) 暗号化

1.3.9. 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 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

表1.2 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1.3 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
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

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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
単一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
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

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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	サポート対象外
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1.4 Operators

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
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1.5 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]

機能	IBM Power®	IBM Z® および IBM® LinuxONE
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。

1.3.10. Insights Operator

1.3.10.1. Insights Runtime Extractor が一般提供される

OpenShift Container Platform 4.18 では、Insights Operator に、Red Hat がコンテナーのワークロードをより適切に理解できるようにするためのテクノロジープレビュー機能として **Insights Runtime Extractor** ワークロードデータ収集機能が導入されました。現在、バージョン 4.19 では、この機能が一般提供されています。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。

1.3.11. インストールおよび更新

1.3.11.1. IBM Cloud インストールで、Cluster API が Terraform に代わる

OpenShift Container Platform 4.19 では、インストールプログラムは、IBM Cloud へのインストール中にクラスターインフラストラクチャーをプロビジョニングするために、Terraform ではなく Cluster API を使用します。

1.3.11.2. 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** に設定されている 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。

1.3.11.3. マレーシアとタイのリージョンで AWS にクラスターをインストールする

OpenShift Container Platform クラスターを Amazon Web Services (AWS) のマレーシア (**ap-southeast-5**) およびタイ (**ap-southeast-7**) リージョンにインストールできるようになりました。

詳細は、サポートされている Amazon Web Services (AWS) リージョン を参照してください。

1.3.11.4. Microsoft Azure Stack Hub インストールで Cluster API が Terraform に置き換わる

OpenShift Container Platform 4.19 では、インストールプログラムは、Microsoft Azure Stack Hub での installer-provisioned infrastructure インストール中に、Terraform ではなく Cluster API を使用してクラスターをプロビジョニングします。

1.3.11.5. 追加の Microsoft Azure インスタンスタイプのサポートが追加される

64 ビット x86 アーキテクチャーに基づくマシンタイプ向けの追加の Microsoft Azure インスタンスタイプが、OpenShift Container Platform 4.19 でテストされました。

Dxv6 マシンシリーズでは、次のインスタンスタイプがテストされています。

- **StandardDdsv6Family**
- **StandardDldsv6Family**
- **StandardDlsv6Family**
- **StandardDsv6Family**

Lsv4 および Lasv4 マシンシリーズでは、次のインスタンスタイプがテストされています。

- **standardLasv4Family**
- **standardLsv4Family**

ND および NV マシンシリーズでは、次のインスタンスタイプがテストされています。

- **StandardNVadsV710v5Family**
- **Standard NDASv4_A100 Family**

詳細は、Azure のテスト済みインスタンスタイプ および Azure のドキュメント (Microsoft ドキュメント) を参照してください。

1.3.11.6. Microsoft Azure の仮想マシンへの送信アクセスが廃止へ

2025 年 9 月 30 日に、Microsoft Azure のすべての新しい仮想マシン (VM) のデフォルトの送信アクセス接続が廃止されます。セキュリティーを強化するために、Azure はデフォルトでセキュアなモデルへ移行しており、インターネットへのデフォルトの送信アクセスが無効化される予定です。ただし、OpenShift Container Platform の設定変更は必要ありません。デフォルトでは、インストールプログラムはロードバランサーの送信ルールを作成します。

詳細は、Azure Updates (Microsoft ドキュメント)、Azure's outbound connectivity methods (Microsoft ドキュメント)、および Azure にクラスターをインストールするための準備 を参照してください。

1.3.11.7. Google Cloud 向けの追加の Confidential Computing プラットフォーム

このリリースにより、Google Cloud で追加の Confidential Computing プラットフォームを使用できるようになります。インストール前に **install-config.yaml** ファイルで有効にしたり、マシンセットおよびコントロールプレーンマシンセットを使用してインストール後に設定したりできる、サポートされる新しいプラットフォームは次のとおりです。

- **AMDEncryptedVirtualization** は、AMD Secure Encrypted Virtualization (AMD SEV) による Confidential Computing を可能にします。

- **AMDEncryptedVirtualizationNestedPaging** は、AMD Secure Encrypted Virtualization Secure Nested Paging (AMD SEV-SNP) による Confidential Computing を可能にします。
- **IntelTrustedDomainExtensions** は、Intel Trusted Domain Extensions (Intel TDX) を使用した Confidential Computing を可能にします。

詳細は、Google Cloud のインストール設定パラメーター、マシンセットを使用した Confidential 仮想マシンの設定 (コントロールプレーン)、および マシンセットを使用した Confidential 仮想マシンの設定 (コンピュート) を参照してください。

1.3.11.8. user-provisioned DNS 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)

このリリースにより、デフォルトの cluster-provisioned DNS ソリューションの代わりに、user-provisioned ドメインネームサーバー (DNS) を有効にできます。たとえば、組織のセキュリティーポリシーにより、Google Cloud DNS などのパブリック DNS サービスの使用が許可されていない場合があります。API サーバーと Ingress サーバーの IP アドレスに対してのみ DNS を管理できます。この機能を使用する場合は、**api.<cluster_name>.<base_domain>.** および ***.apps.<cluster_name>.<base_domain>.** のレコードを含む独自の DNS ソリューションを提供する必要があります。user-provisioned DNS の有効化は、テクノロジープレビュー機能として利用できます。

詳細は、ユーザー管理 DNS の有効化 を参照してください。

1.3.11.9. 複数のディスクを持つ 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)

このリリースにより、テクノロジープレビュー機能として、複数のストレージディスクを備えた VMware vSphere にクラスターをインストールできます。これらの追加ディスクを、etcd ストレージなどのクラスター内の特別な機能に割り当てることができます。

詳細は、オプションの vSphere 設定パラメーター を参照してください。

1.3.11.10. Microsoft Azure へのインストール中にブート診断収集を有効にする

このリリースにより、Microsoft Azure にクラスターをインストールするときに、ブート診断の収集を有効にできます。ブート診断は、仮想マシンブート障害を特定するための Azure 仮想マシン (VM) のデバッグ機能です。コンピュートマシン、コントロールプレーンマシン、またはすべてのマシンの **install-config.yaml** ファイルで **bootDiagnostics** パラメーターを設定できます。

詳細は、追加の Azure 設定パラメーター を参照してください。

1.3.11.11. OpenShift Container Platform 4.18 から 4.19 に更新する際に必要な管理者の承認

OpenShift Container Platform 4.19 は、いくつかの 非推奨の API が削除された Kubernetes 1.32 を使用します。

クラスターを OpenShift Container Platform 4.18 から 4.19 に更新する前に、クラスター管理者は手動で確認を行う必要があります。これは、OpenShift Container Platform 4.19 に更新した後、クラスター上で実行されている、またはクラスターと対話しているワークロード、ツール、またはその他のコンポーネントによって、削除された API が引き続き使用されているという問題を防ぐのに役立ちます。管理者は、削除が予定されている使用中の API に対するクラスターの評価を実施し、影響を受けるコンポーネントを移行して適切な新規 API バージョンを使用する必要があります。これが完了すると、管理者による承認が可能です。

すべての OpenShift Container Platform 4.18 クラスターは、OpenShift Container Platform 4.19 に更新する前に、この管理者の承認が必要です。

詳細は、OpenShift Container Platform 4.19 への更新の準備 を参照してください。

1.3.11.12. vSphere ホストグループに対する OpenShift ゾーンのサポート (テクノロジープレビュー)

このリリースにより、OpenShift Container Platform 障害ドメインを VMware vSphere ホストグループにマップできるようになります。これにより、vSphere ストレッチクラスター設定によって提供される高可用性を活用できるようになります。この機能は、OpenShift Container Platform 4.19 でテクノロジープレビューとして利用できます。

インストール時にホストグループを設定する方法については、VMware vSphere ホストグループの有効化 を参照してください。

既存のクラスターのホストグループを設定する方法については、vSphere 上のクラスターに複数のホストグループを指定する を参照してください。

1.3.11.13. Agent-based Installer に対する Nutanix のサポート

このリリースにより、Agent-based Installer を使用して Nutanix にクラスターをインストールできるようになりました。Agent-based Installer を使用して Nutanix にクラスターをインストールするには、**install-config.yaml** ファイルで **platform** パラメーターを **nutanix** に設定します。

詳細は、Agent-based Installer のドキュメントの 必要な設定パラメーター を参照してください。

1.3.12. Machine Config Operator

1.3.12.1. 機能の新しい命名

Red Hat Enterprise Linux CoreOS (RHCOS) イメージレイヤー化は、**Image Mode for OpenShift** と呼ばれるようになりました。この変更の一環として、**クラスター上のレイヤー化** は **クラスター上のイメージモード**、**クラスター外のレイヤー化** は **クラスター外のイメージモード** と呼ばれるようになりました。

ブートイメージ更新 機能は、**ブートイメージ管理** と呼ばれるようになりました。

1.3.12.2. Image Mode for OpenShift が一般提供になる

以前はクラスター上のレイヤー化と呼ばれていた Image Mode for OpenShift が一般提供 (GA) になりました。GA への昇格に伴い、次の変更が導入されました。

- 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。

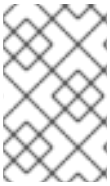
- 必要な **imageBuilderType** は **Job** になりました。以前は、必要なビルダーは **PodImageBuilder** でした。
- **renderedImagePushspec** パラメーターは **renderedImagePushSpec** になりました。
- **buildOutputs** および **currentImagePullSecret** パラメーターは不要になりました。

- **oc describe MachineOSConfig** コマンドと **oc describe MachineOSBuild** コマンドの出力には複数の違いがあります。
- **global-pull-secret-copy** は、**openshift-machine-config-operator** namespace に自動的に追加されます。
- **MachineOSConfig** オブジェクトからラベルを削除することで、カスタムのクラスター上のレイヤー化イメージをベースイメージに戻せるようになりました。
- 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。
- 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が非接続環境でサポートされるようになりました。
- クラスター上のレイヤー化が、シングルノード OpenShift (SNO) クラスターでサポートされるようになりました。

1.3.12.3. ブートイメージ管理が Google Cloud と Amazon Web Services (AWS) のデフォルトになる

以前は、ブートイメージ更新と呼ばれていたブートイメージ管理機能は、現在、Google Cloud および Amazon Web Services (AWS) クラスターのデフォルトの動作になっています。そのため、OpenShift Container Platform 4.19 に更新すると、クラスター内のブートイメージは自動的にバージョン 4.19 に更新されます。今後の更新でも、Machine Config Operator (MCO) がクラスター内のブートイメージを再び更新します。ブートイメージはマシンセットに関連付けられており、新しいノードをスケーリングするときに使用されます。更新後に作成する新しいノードはすべて、新しいバージョンに基づいています。現在のノードはこの機能の影響を受けません。

4.19 にアップグレードする前に、このデフォルトの動作をオプトアウトするか、続行する前にこの変更を承認する必要があります。詳細は、ブートイメージ管理の無効化 を参照してください。



注記

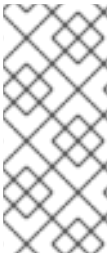
マネージドブートイメージ機能は、Google Cloud および AWS クラスターでのみ使用できます。その他のすべてのプラットフォームでは、MCO はクラスターの更新ごとにブートイメージを更新しません。

1.3.12.4. Machine Config Operator 証明書に関する変更点

インストールプログラムによって作成された Machine Config Server (MCS) CA バンドルは、**openshift-machine-config-operator** namespace の **machine-config-server-ca** config map に保存されるようになりました。バンドルは以前は **kube-system namespace** の **root-ca** configmap に保存されていました。OpenShift Container Platform 4.19 に更新されたクラスターでは、**root-ca** configmap は使用されなくなりました。この変更は、この CA バンドルが Machine Config Operator (MCO) によって管理されていることを明確にするために行われました。

MCS 署名鍵は、**openshift-machine-config-operator** namespace の **machine-config-server-ca** シークレットに保存されます。

MCS の CA および MCS 証明書は有効期間が 10 年で、MCO によって約 8 年で自動的にローテーションされます。OpenShift Container Platform 4.19 に更新すると、CA 署名鍵は存在しなくなります。その結果、MCO 証明書コントローラーが起動すると、CA バンドルは直ちに期限切れとみなされます。この有効期限により、クラスターが 10 年経過していなくても、証明書のローテーションが直ちに行われます。それ以降、次のローテーションは標準の 8 年周期で行われます。



注記

この自動証明書ローテーションは、マシンセットを使用するクラスターにのみ適用されます。vSphere user-provisioned infrastructure クラスターなどのマシンセットを使用しないクラスターの場合は、これらの証明書を手動でローテーションする必要があります。証明書の手動ローテーションの詳細は、Red Hat ナレッジベースの記事 Regenerating CA certificates for the Machine Config Server を参照してください。

MCO 証明書の詳細は、Machine Config Operator 証明書 を参照してください。

1.3.13. マシン管理

1.3.13.1. Cluster API と Machine API 間のリソースの移行 (テクノロジープレビュー)

このリリースにより、テクノロジープレビュー機能として、Amazon Web Services (AWS) 上の Cluster API と Machine API 間で一部のリソースを移行できます。詳細は、Machine API リソースの Cluster API リソースへの移行 を参照してください。

この機能をサポートするために、OpenShift Container Platform Cluster API ドキュメントに AWS クラスターの追加設定の詳細が含まれるようになりました。

1.3.13.2. コントロールプレーンマシン名のカスタム接頭辞

このリリースにより、コントロールプレーンマシンセットによって作成されたマシンのマシン名の接頭辞をカスタマイズできます。この機能は、**ControlPlaneMachineSet** カスタムリソースの **spec.machineNamePrefix** パラメーターを変更することで有効になります。

詳細は、コントロールプレーンマシン名へのカスタム接頭辞の追加 を参照してください。

1.3.13.3. Amazon Web Services クラスターでの Capacity Reservations の設定

このリリースにより、On-Demand Capacity Reservations および Capacity Blocks for ML などの Capacity Reservations を使用するマシンを Amazon Web Services クラスターにデプロイできます。

これらの機能は、コンピュート および コントロールプレーン マシンセットで設定できます。

1.3.13.4. 複数の VMware vSphere データディスクのサポート (テクノロジープレビュー)

このリリースにより、テクノロジープレビュー機能として、vSphere クラスターの仮想マシン (VM) コントローラーに最大 29 個のディスクを追加できるようになりました。この機能は、コンピュート および コントロールプレーン マシンセットで利用できます。

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。

- Alertmanager 0.28.1 への更新
- Prometheus 3.2.1 への更新
- Prometheus Operator 0.81.0 への更新
- Thanos 0.37.2 への更新
- kube-state-metrics 2.15.0 への更新
- node-exporter 1.9.1 への更新

1.3.14.2. アラートルールの変更

注記

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

- Prometheus v3 では、クラシックなヒストグラムの **le** ラベルやサマリーの **quantile** ラベルの値が浮動小数点数であることを考慮せず、制限が強すぎる可能性のあるセレクターを PromQL クエリーやメトリクスのラベルの再設定で使用している場合にユーザーに警告するために、**PrometheusPossibleNarrowSelectors** アラートが追加されました。詳細は、「Prometheus v3 アップグレード」セクションを参照してください。

1.3.14.3. Prometheus v3 アップグレード

このリリースにより、v2 から v3 へと移行する Prometheus コンポーネントに大規模な更新が導入されました。モニタリングスタックとその他のコアコンポーネントには、スムーズにアップグレードするために必要な調整がすべて含まれています。ただし、一部のユーザー管理設定では変更が必要になる場合があります。主な変更点は次のとおりです。

- クラシックヒストグラムの **le** ラベルとサマリーの **quantile** ラベルの値は、取り込み時に正規化されます。たとえば、**example_bucket{le="10"}** メトリクスセレクターは、**example_bucket{le="10.0"}** として取り込まれます。その結果、ラベル値を整数として参照するアラート、記録ルール、ダッシュボード、およびラベルの再設定 (例: **le="10"**) が意図したとおりに機能しなくなる可能性があります。
  問題を軽減するには、セレクターを更新します。
  - クエリーで Prometheus のアップグレード前とアップグレード後の両方のデータを対象とする必要がある場合は、両方の値が考慮されるようにします。たとえば、正規表現 **example_bucket{le=~"10(.0)?"}** を使用します。
  - アップグレード後のデータのみを対象とするクエリーの場合は、浮動小数点値 (例: **le="10.0"**) を使用します。

- Alertmanager v1 API を使用し、**additionalAlertmanagerConfigs** を通じて追加の Alertmanager インスタンスにアラートを送信する設定はサポートされなくなりました。この問題を軽減するには、影響を受ける Alertmanager インスタンスをアップグレードして、Alertmanager **v0.16.0** 以降でサポートされている v2 API をサポートし、モニタリング設定を更新して v2 スキームを使用します。

Prometheus v2 と v3 の間の変更の詳細は、Prometheus 3.0 migration guide を参照してください。

1.3.14.4. メトリクス収集プロファイルが一般提供される

OpenShift Container Platform 4.13 では、デフォルトのプラットフォームモニタリングのメトリクス収集プロファイルを設定して、デフォルトの量のメトリクスデータまたは最小量のメトリクスデータを収集する機能が導入されました。OpenShift Container Platform 4.19 では、メトリクス収集プロファイルが一般提供されました。

詳細は、メトリクス収集プロファイルについて および メトリクス収集プロファイルの選択 を参照してください。

1.3.14.5. 外部 Alertmanager インスタンス用のクラスタープロキシーサポートが追加される

このリリースにより、外部 Alertmanager インスタンスは通信にクラスター全体の HTTP プロキシー設定を使用するようになりました。Cluster Monitoring Operator (CMO) は、クラスター全体のプロキシー設定を読み取り、Alertmanager エンドポイントに適切なプロキシー URL を設定します。

1.3.14.6. Cluster Monitoring Operator の厳密な検証が改善される

このリリースにより、OpenShift Container Platform 4.18 で導入された厳密な検証が改善されました。エラーメッセージに影響を受けたフィールドが明確に示されるようになり、検証は大文字と小文字を区別するようになったため、より正確で一貫性のある設定が可能になりました。

詳細は、(OCPBUGS-42671) および (OCPBUGS-54516) を参照してください。

1.3.15. ネットワーク

1.3.15.1. Border Gateway Protocol (BGP) を使用したクラスターユーザー定義ネットワーク (CUDN) のルートアドバタイズメントのサポート

ルートアドバタイズメントを有効にすると、OVN-Kubernetes ネットワークプラグインが、クラスターユーザー定義ネットワーク (CUDN) に関連付けられた Pod とサービスのルートを、プロバイダーネットワークに直接アドバタイズできるようになります。この機能により、次のような利点がいくつか得られます。

- Pod へのルートを動的に学習する
- ルートを動的にアドバタイズする
- Gratuitous ARP に基づくレイヤー 2 の通知に加えて、EgressIP フェイルオーバーのレイヤー 3 通知を有効にする
- 外部のルートリフレクターをサポートし、大規模なネットワークで必要な BGP 接続の数を削減する

詳細は、ルートアドバタイズメントについて を参照してください。

1.3.15.2. 外部管理証明書を使用したルートの作成 (一般提供)

このリリースにより、ルート API の **.spec.tls.externalCertificate** フィールドを利用して、サードパーティーの証明書管理ソリューションで OpenShift Container Platform ルートを設定できるようになりました。これにより、シークレットを介して外部で管理されている TLS 証明書を参照できるようになり、手動による証明書管理が不要になり、プロセスが合理化されます。外部で管理される証明書を使用することで、エラーが削減され、証明書の更新プロセスがスムーズになり、OpenShift ルーターが更新された証明書を迅速に提供できるようになります。詳細は、外部管理証明書を使用したルートの作成 を参照してください。

1.3.15.3. BGP ルーティングプロトコルのサポート

Cluster Network Operator (CNO) が、Border Gateway Protocol (BGP) ルーティングの有効化をサポートするようになりました。BGP を使用すると、基盤となるプロバイダーネットワークへのルートをインポートおよびエクスポートしたり、マルチホーミング、リンク冗長性、高速コンバージェンスを使用したりできます。BGP 設定は、**FRRConfiguration** カスタムリソース (CR) を使用して管理されます。

MetalLB Operator をインストールした以前のバージョンの OpenShift Container Platform からアップグレードする場合は、カスタムの frr-k8s 設定を **metallb-system** namespace から **openshift-frr-k8s** namespace に手動で移行する必要があります。これらの CR を移動するには、次のコマンドを入力します。

1. **openshift-frr-k8s** namespace を作成するには、次のコマンドを入力します。

```
$ oc create namespace openshift-frr-k8s
```

2. 移行を自動化するには、次の内容の **migrate.sh** ファイルを作成します。

```
#!/bin/bash
OLD_NAMESPACE="metallb-system"
NEW_NAMESPACE="openshift-frr-k8s"
FILTER_OUT="metallb-"
oc get frrconfigurations.frrk8s.metallb.io -n "${OLD_NAMESPACE}" -o json |\
  jq -r '.items[] | select(.metadata.name | test("""${FILTER_OUT}""") | not)' |\
  jq -r '.metadata.namespace = """${NEW_NAMESPACE}"""' |\
  oc create -f -
```

3. 移行スクリプトを実行するには、次のコマンドを入力します。

```
$ bash migrate.sh
```

4. 移行が成功したことを確認するには、次のコマンドを入力します。

```
$ oc get frrconfigurations.frrk8s.metallb.io -n openshift-frr-k8s
```

移行が完了したら、**metallb-system** namespace から **FRR-K8s** カスタムリソースを削除できます。

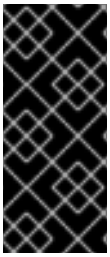
詳細は、BGP ルーティングについて を参照してください。

1.3.15.4. Gateway API を使用してクラスター Ingress トラフィックを設定するためのサポート (一般提供)

このリリースにより、Gateway API リソースを使用して Ingress クラスタートラフィックを管理するためのサポートが一般提供されます。Gateway API は、標準化されたオープンソースエコシステムを使用

して、OpenShift Container Platform クラスターのトランスポート層 (L4) とアプリケーション層 (L7) 内で堅牢なネットワークソリューションを提供します。

詳細は、OpenShift Container Platform ネットワークを使用した Gateway API を参照してください。



重要

Gateway API リソースは、サポートされている OpenShift Container Platform API サーフェスに準拠する必要があります。つまり、OpenShift Container Platform の Gateway API 実装では、Istio の VirtualService などの別のベンダー固有のリソースを使用することはできません。詳細は、OpenShift Container Platform の Gateway API 実装 を参照してください。

1.3.15.5. Gateway API カスタムリソース定義 (CRD) ライフサイクルの管理のサポート

このリリースにより、OpenShift Container Platform が Gateway API CRD のライフサイクルを管理するようになりました。つまり、Ingress Operator は必要なバージョン管理とリソースの管理を処理します。以前の OpenShift Container Platform バージョンで作成された Gateway API リソースは、Ingress Operator に必要な仕様に準拠するように再作成および再デプロイする必要があります。

詳細は、Ingress Operator による Gateway API 管理継承の準備 を参照してください。

1.3.15.6. Gateway API カスタムリソース定義 (CRD) の更新

OpenShift Container Platform 4.19 では、Red Hat OpenShift Service Mesh がバージョン 3.0.2 に、Gateway API がバージョン 1.2.1 に更新されます。詳細は、Service Mesh 3.0.0 リリースノート および Gateway API 1.2.1 changelog を参照してください。

1.3.15.7. API および Ingress ロードバランサーを特定のサブネットに割り当てる

このリリースにより、AWS に OpenShift Container Platform クラスターをインストールするときに、ロードバランサーを割り当ててデプロイメントをカスタマイズできるようになりました。この機能により、最適なトラフィック分散、高いアプリケーション可用性、中断のないサービス、ネットワークのセグメンテーションが確保されます。

詳細は、AWS のインストール設定パラメーター および 特定のサブネットへのロードバランサーの割り当て を参照してください。

1.3.15.8. PTP 通常クロックの冗長性を向上させるデュアルポート NIC (テクノロジープレビュー)

このリリースにより、デュアルポートネットワークインターフェイスコントローラー (NIC) を使用して、Precision Time Protocol (PTP) の通常クロックの冗長性を向上させることができます。テクノロジープレビューとして利用可能な通常クロックのデュアルポート NIC 設定では、1 つのポートに障害が発生した場合、スタンバイポートが引き継ぎ、PTP タイミング同期を維持します。

注記

PTP の通常クロックは、冗長性を追加して設定することができますが、これはデュアルポート NIC を搭載した **x86** アーキテクチャーのノードに限られます。

詳細は、デュアルポート NIC を使用して PTP 通常クロックの冗長性を向上させる を参照してください。

1.3.15.9. SR-IOV Network Operator での条件付き Webhook マッチングのサポート

SriovOperatorConfig オブジェクトで **featureGates.resourceInjectorMatchCondition** 機能を有効にして、Network Resources Injector Webhook の範囲を制限できるようになりました。この機能を有効にすると、Webhook はセカンダリーネットワークアノテーション **k8s.v1.cni.cncf.io/networks** を持つ Pod にのみ適用されます。

この機能が無効になっている場合、Webhook の **failurePolicy** はデフォルトで **Ignore** に設定されます。この設定により、Webhook が利用できない場合に、SR-IOV ネットワークを要求する Pod が必要なリソース注入なしでデプロイされる可能性があります。この機能が有効になっていて、Webhook が利用できない場合でも、アノテーションのない Pod はデプロイされ、他のワークロードへの不要な中断が阻止されます。

詳細は、Network Resources Injector について を参照してください。

1.3.15.10. DPU Operator による DPU デバイス管理の有効化

このリリースでは、OpenShift Container Platform に Data Processing Unit (DPU) Operator が導入され、Operator を使用して DPU デバイスを管理できるようになりました。DPU Operator は、データネットワーク、ストレージ、セキュリティーワークロードのオフロードを有効にするなど、DPU が設定されたコンピュートノード上のコンポーネントを管理します。DPU デバイス管理を有効にすると、クラスターのパフォーマンスが向上し、レイテンシーが短縮され、セキュリティーが強化され、全体的にクラスターインフラストラクチャーの効率が向上します。詳細は、DPU および DPU Operator について を参照してください。

1.3.15.11. ユーザー定義ネットワークの Localnet トポロジー (一般提供)

管理者は、**ClusterUserDefinedNetwork** カスタムリソースを使用して、**Localnet** トポロジーにセカンダリーネットワークをデプロイできるようになりました。この機能により、localnet ネットワークに接続された Pod と仮想マシンが物理ネットワークに Egress できるようになります。詳細は、Localnet トポロジー用の ClusterUserDefinedNetwork CR の作成 を参照してください。

1.3.15.12. Linux ブリッジ NAD のポート分離を有効にする (一般提供)

Linux ブリッジ Network Attachment Definition (NAD) のポート分離を有効にすると、同じ仮想 LAN (VLAN) 上で実行される仮想マシン (VM) または Pod が相互に分離して動作できるようになります。詳細は、Linux ブリッジ NAD のポート分離の有効化 を参照してください。

1.3.15.13. Whereabouts IPAM CNI プラグインの高速 IPAM 設定 (テクノロジープレビュー)

特にクラスター内のノードが大量の Pod を実行している場合に、Whereabouts のパフォーマンスを向上させるために、Fast IP Address Management (IPAM) 機能を有効化できるようになりました。Fast IPAM 機能は、Whereabouts Controller によって管理される **nodeslicepools** を使用して、ノードの IP アドレスの割り当てを最適化します。詳細は、Whereabouts IPAM CNI プラグインの高速 IPAM 設定 を参照してください。

1.3.15.14. 番号のない BGP ピアリング (テクノロジープレビュー)

このリリースにより、OpenShift Container Platform に番号のない BGP ピアリングが導入されました。これは、テクノロジープレビュー機能として利用可能です。BGP ピアカスタムリソースの **spec.interface** フィールドを使用して、番号のない BGP ピアリングを設定できます。

1.3.15.15. DNS 接続の問題を解決するためにカスタム DNS ホスト名を作成する

外部 DNS サーバーに到達できない非接続環境では、**NMState** カスタムリソース定義 (CRD) にカスタム DNS ホスト名を指定することで、Kubernetes NMState Operator のヘルスプローブの問題を解決できます。詳細は、DNS 接続の問題を解決するためのカスタム DNS ホスト名の作成 を参照してください。

1.3.15.16. PTP イベント REST API v1 およびイベントコンシューマーアプリケーションサイドカーの削除

このリリースでは、PTP イベント REST API v1 およびイベントコンシューマーアプリケーションサイドカーのサポートが削除されました。

代わりに、O-RAN 準拠の PTP イベント REST API v2 を使用する必要があります。

詳細は、REST API v2 を使用した PTP イベントコンシューマーアプリケーションの開発 を参照してください。

1.3.15.17. RouteExternalCertificate フィーチャーゲートを有効にして、以前に削除されたシークレットを再度追加する

クラスターの **RouteExternalCertificate** フィーチャーゲートを有効にした場合、以前に削除されたシークレットを再度追加できるようになりました。(OCPBUGS-33958)

1.3.16. OpenShift CLI (oc)

1.3.16.1. oc-mirror プラグイン v2 でのイメージ署名のミラーリングと検証

OpenShift Container Platform 4.19 以降、oc-mirror プラグイン v2 は、コンテナーイメージに対する cosign のタグベース署名のミラーリングおよび検証をサポートします。

1.3.17. Operator の開発

1.3.17.1. サポートされる Operator のベースイメージ

Operator プロジェクトの以下のベースイメージは、OpenShift Container Platform 4.19 との互換性のために更新されます。これらのベースイメージのランタイム機能と設定 API は、バグ修正と CVE への対応のためにサポートされます。

- Ansible ベースの Operator プロジェクトのベースイメージ
- Helm ベースの Operator プロジェクトのベースイメージ

詳細は、Updating the base image for existing Ansible- or Helm-based Operator projects for OpenShift Container Platform 4.19 and later (Red Hat ナレッジベース) を参照してください。

1.3.18. インストール後の設定

1.3.18.1. Bare Metal as a Service の使用 (テクノロジープレビュー)

OpenShift Container Platform 4.19 では、Bare Metal as a Service (BMaaS) を使用して、OpenShift Container Platform 以外のノードをデプロイできます。BMaaS ノードは、コンテナー化や仮想化に適さない可能性のあるワークロードを実行できます。たとえば、ハードウェアへの直接アクセスを必要とするアプリケーション、高性能コンピューティングタスクを実行するアプリケーション、またはレガシーアプリケーションでクラスターから独立して動作するアプリケーションなどのワークロードは、BMaaS を使用したデプロイメントに適しています。

詳細は、ベアメタルをサービスとして使用する を参照してください。

1.3.19. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.19.1. RHCOS が RHEL 9.6 を使用

RHCOS は、OpenShift Container Platform 4.19 で Red Hat Enterprise Linux (RHEL) 9.6 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。

1.3.20. スケーラビリティーおよびパフォーマンス

1.3.20.1. パフォーマンスプロファイルカーネルページサイズ設定

この更新により、リアルタイムカーネルが無効になっている ARM インフラストラクチャーノードで、メモリーを大量に消費する高パフォーマンスのワークロードのパフォーマンスを向上させるために、より大きなカーネルページサイズを指定できるようになりました。詳細は、カーネルページサイズの設定 を参照してください。

1.3.20.2. クラスター比較プラグインの更新

このリリースには、**cluster-compare** プラグインに対する次の使いやすさと機能の更新が含まれています。

- キャプチャーグループのより効果的な一致: キャプチャーグループの処理が改善され、テンプレート全体およびテンプレート間の一致をより正確に行うことができるようになりました。
- JUnit 出力の生成: **-o junit** フラグを使用すると結果を **junit** 形式で出力できるため、テストや CI/CD システムとの統合が容易になります。
- **sprig** 関数のサポート: **cluster-compare** プラグインは、**env** と **expandenv** 関数を除くすべての **sprig** ライブラリー関数をサポートします。sprig ライブラリー関数の完全なリストについては、Sprig Function Documentation を参照してください。

利用可能なテンプレート関数の完全なリストについては、テンプレート関数のリファレンス を参照してください。

1.3.20.3. パフォーマンスプロファイルを使用して Hosted Control Plane をチューニングする

この更新により、パフォーマンスプロファイルを適用して、Hosted Control Plane のノードを低レイテンシーに調整できるようになりました。詳細は、Hosted Control Plane のパフォーマンスプロファイルの作成 を参照してください。

1.3.21. セキュリティー

1.3.21.1. コントロールプレーンが TLS 1.3 と Modern TLS セキュリティープロファイルをサポートするようになる

このリリースにより、コントロールプレーンは TLS 1.3 をサポートします。コントロールプレーンに **Modern** TLS セキュリティープロファイルを使用できるようになりました。

詳細は、コントロールプレーンの TLS セキュリティープロファイルの設定 を参照してください。

1.3.21.2. External Secrets Operator for Red Hat OpenShift (テクノロジープレビュー)

このリリースでは、External Secrets Operator for Red Hat OpenShift を使用して外部シークレットストアで認証し、シークレットを取得し、取得したシークレットをネイティブ Kubernetes シークレットに注入できるようになりました。External Secrets Operator for Red Hat OpenShift は、テクノロジープレビューとして利用可能です。

詳細は、External Secrets Operator for Red Hat OpenShift の概要 を参照してください。

1.3.22. ストレージ

1.3.22.1. 非接続環境での Secrets Store CSI ドライバーのサポート

このリリースにより、Secrets Store CSI ドライバーを使用することで、非接続クラスターでもシークレットストアプロバイダーのサポートが可能になりました。

詳細は、非接続環境のサポート を参照してください。

1.3.22.2. Azure File のクロスサブスクリプションサポートが一般提供される

クロスサブスクリプションサポートにより、1 つの Azure サブスクリプションに OpenShift Container Platform クラスターを配置し、Azure File Container Storage Interface (CSI) ドライバーを使用して、別の Azure サブスクリプションに Azure ファイル共有をマウントできるようになります。サブスクリプションは同じテナント内にある必要があります。

OpenShift Container Platform 4.19 では、この機能が一般提供されています。

詳細は、AWS EFS CSI クロスアカウントのサポート を参照してください。

1.3.22.3. Volume Attributes Classes (テクノロジープレビュー)

Volume Attributes Classes は、管理者が提供するストレージの "クラス" を記述する手段を提供するものです。それぞれのクラスを別々のサービス品質レベルに対応させることができます。

OpenShift Container Platform 4.19 の Volume Attributes Classes は、AWS Elastic Block Storage (EBS) および Google Cloud Platform (GCP) Persistent Disk (PD) Container Storage Interface (CSI) でのみ利用できます。

Volume Attributes Classes を永続ボリューム要求 (PVC) に適用できます。クラスターで新しい Volume Attributes Classes が使用可能になった場合は、必要に応じて新しい Volume Attributes Classes で PVC を更新できます。

Volume Attributes Classes には、それに属するボリュームを記述するパラメーターがあります。パラメーターを省略すると、ボリュームのプロビジョニング時にデフォルトが使用されます。ユーザーが、パラメーターを省略した異なる Volume Attributes Class を持つ PVC を適用すると、CSI ドライバーの実装に応じてパラメーターのデフォルト値が使用される場合があります。詳細は、関連する CSI ドライバーのドキュメントを参照してください。

Volume Attributes Classes は、OpenShift Container Platform 4.19 ではテクノロジープレビューのステータスで提供されます。

詳細は、Volume Attributes Classes を参照してください。

1.3.22.4. PVC の使用状況を表示する新しい CLI コマンド (テクノロジープレビュー)

OpenShift Container Platform 4.19 では、永続ボリューム要求の使用状況を表示するための新しいコマンドが導入されました。この機能はテクノロジープレビューです。

詳細は、PVC 使用状況の統計情報の表示 を参照してください。

1.3.22.5. CSI ボリュームのサイズ変更リカバリーが一般提供される

以前は、永続ボリューム要求 (PVC) を、基盤となるストレージプロバイダーでサポートされていないサイズまで拡張することがありました。この場合、拡張コントローラーは通常、ボリュームの拡張を永久に試行し、失敗し続けます。

この新機能を使用すると、PVC を回復し、別のサイズ変更値を提供できます。サイズ変更のリカバリーは、OpenShift Container Platform 4.19 で一般提供としてサポートされています。

ボリュームのサイズ変更の詳細は、永続ボリュームの拡張 を参照してください。

ボリュームのサイズ変更時の回復の詳細は、ボリュームの拡張時の障害からの回復 を参照してください。

1.3.22.6. vSphere のツリー内移行ボリュームのサイズ変更のサポートが一般提供される

以前は、ツリー内から Container Storage Interface (CSI) に移行された VMware vSphere 永続ボリュームのサイズを変更できませんでした。OpenShift Container Platform 4.19 では、移行されたボリュームのサイズ変更がサポートされています。この機能は一般提供されています。

ボリュームのサイズ変更の詳細は、永続ボリュームの拡張 を参照してください。

1.3.22.7. vSphere でのストレージの無効化と有効化が一般提供される

場合によって、クラスター管理者は Day 2 運用として VMware vSphere Container Storage Interface (CSI) ドライバーを無効にし、vSphere CSI ドライバーが vSphere セットアップと接続されないようにする必要があります。

この機能は、OpenShift Container Platform 4.17 でテクノロジープレビューのステータスで導入されました。この機能は、OpenShift Container Platform 4.19 で一般提供としてサポートされるようになりました。

詳細は、vSphere でのストレージの無効化と有効化 を参照してください。

1.3.22.8. vSphere のノードあたりのボリュームの最大数の増加 (テクノロジープレビュー)

VMware vSphere バージョン 7 の場合、OpenShift Container Platform ではノードあたりのボリュームの最大数が 59 に制限されます。

ただし、OpenShift Container Platform 4.19 for vSphere バージョン 8 以降では、ノードあたりの許容ボリューム数を最大 255 まで増やすことができます。それ以外の場合、デフォルト値は 59 のままになります。

この機能はテクノロジープレビューです。

詳細は、vSphere のノードあたりの最大ボリュームの増加 を参照してください。

1.3.22.9. vSphere のデータストア間での CNS ボリュームの移行が完全にサポートされる

現在のデータストアの容量が不足している場合、またはよりパフォーマンスの高いデータストアに移行する場合は、VMware vSphere Cloud Native Storage (CNS) ボリュームをデータストア間で移行できます。これは、接続されたボリュームと切断されたボリュームの両方に適用されます。

OpenShift Container Platform は、vCenter UI を使用した CNS ボリュームの移行を完全にサポートするようになりました。移行されたボリュームは期待どおりに動作し、永続ボリュームが機能しなくなることはありません。CNS ボリュームは、Pod によって使用されている間にも移行できます。

この機能は OpenShift Container Platform 4.17 で開発プレビューとして導入されましたが、4.19 では完全にサポートされるようになりました。

データストア間で CNS ボリュームを移行するには、VMware vSphere 8.0.2 以降または vSphere 7.0 Update 3o 以降が必要です。

詳細は、vSphere のデータストア間での CNS ボリュームの移行 を参照してください。

1.3.22.10. Filestore ストレージクラスの NFS エクスポートオプションが一般提供される

デフォルトでは、Filestore インスタンスは、同じ Google Cloud プロジェクトと Virtual Private Cloud (VPC) ネットワークを共有するすべてのクライアントにルートレベルの読み取り/書き込みアクセス権を付与します。ネットワークファイルシステム (NFS) エクスポートオプションを使用すると、Filestore インスタンスの特定の IP 範囲と特定のユーザー/グループ ID へのアクセスを制限できます。ストレージクラスを作成するときに、**nfs-export-options-on-create** パラメーターを使用して、これらのオプションを設定できます。

NFS エクスポートオプションは、OpenShift Container Platform 4.19 で一般提供としてサポートされています。

詳細は、NFS エクスポートオプション を参照してください。

1.3.23. Web コンソール

OpenShift Container Platform 4.19 以降、Web コンソールのパースペクティブが統合されました。これにより、ナビゲーションの簡素化、コンテキストの切り替えの軽減、タスクの効率化、より統一された OpenShift Container Platform エクスペリエンスのユーザーへの提供が実現されました。

この統合された設計により、デフォルトビューに **Developer** パースペクティブは表示されなくなりましたが、**すべて** の OpenShift Container Platform Web コンソール機能は、すべてのユーザーによって検出できるようになりました。クラスターの所有者でない場合は、クラスターの所有者に特定の機能に対するパーミッションを要求する必要がある場合があります。必要に応じて、**Developer** パースペクティブを引き続き手動で有効にすることもできます。

Web コンソールの **Getting Started** ペインには、コンソールのツアー、クラスターのセットアップに関する情報、**Developer** パースペクティブを有効にするためのクイックスタート、新しい機能を調べるためのリンクなどのリソースが提供されます。

1.3.23.1. Patternfly 6 のアップグレード

Web コンソールでは Patternfly 6 が使用されるようになりました。Web コンソールでの Patternfly 4 のサポートは利用できなくなりました。

このリリースにより、Web コンソールに次の更新も導入されています。次のアクションを実行できるようになりました。

- **.spec.customization.logos** 設定の **logos** フィールドを使用して、ライトテーマとダークテーマの両方に異なるコンソールロゴを指定し、より包括的なブランド化を可能にします。

- Web コンソールから直接アイデンティティープロバイダー (IDP) を簡単に削除できるため、YAML ファイルを手動で編集することなく認証設定を合理化できます。
- デフォルトの **StorageClass** を Web コンソールで直接簡単に設定できます。
- 作成日時別に **Created** 列を並べ替えることで、Web コンソールで特定のジョブをすばやく見つけることができます。

1.4. 主な技術上の変更点

1.4.1. readOnlyRootFilesystem を true に設定して Pod がデプロイされる

このリリースにより、Cloud Credential Operator Pod は、**readOnlyRootFilesystem** セキュリティーコンテキスト設定を **true** に設定してデプロイされるようになりました。これにより、コンテナーのルートファイルシステムが読み取り専用としてマウントされるようになり、セキュリティーが強化されます。

1.4.2. 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。

1.4.3. Readiness プローブは etcd チェックを除外する

API サーバーの Readiness プローブは、etcd チェックを除外するように変更されました。これにより、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のを防ぎます。つまり、クライアント接続は短時間の etcd の利用不能状態でも維持され、一時的な API サーバーの停止が最小限に抑えられます。

1.4.4. 残存する Cloud Native Storage (CNS) ボリュームをインストーラーが自動的に削除する

OpenShift インストールプログラムは、クラスターを削除すると、VMware vSphere 上に残存する永続ストレージボリュームを自動的に検出して削除するようになりました。これにより、孤立したボリュームがディスク領域を消費したり、vCenter で不要なアラートを作成したりすることが阻止されます。

1.4.5. Red Hat Enterprise Linux CoreOS (RHCOS) のバージョン管理で、OpenShift Container Platform ではなく Red Hat Enterprise Linux (RHEL) が使用される

Image Mode for RHEL への対応の一環として、RHCOS が、共通の RHEL ベースイメージ上のレイヤーとして構築されるようになりました。ユーザーにとって最も明らかな変更点は、バージョン管理に関するものです。たとえば、**/etc/os-release** の **VERSION_ID** は、OpenShift Container Platform 4.19 などの OpenShift Container Platform のバージョンではなく、RHEL 9.6 などの RHEL のバージョンを反映するようになりました。このバージョンの変更は、コマンド **rpm-ostree status** の出力やブートローダーのエントリーなど、他の場所にも現れる可能性があります。ノードイメージ上の **/etc/os-release** 内の **OPENSHIFT_VERSION** は、引き続き OpenShift Container Platform のバージョンを使用するため、この変更の影響を受けません。

RHCOS は現在 RHEL ベースイメージを使用しています。そのため、このベースイメージに追加される新しいオペレーティングシステム機能は、通常、このベースイメージを使用するすべての OpenShift Container Platform リリースに継承されます。

1.4.6. 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. 非推奨の機能と削除された機能

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 4.19 内で非推奨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	4.17	4.18	4.19
Bare Metal Event Relay Operator	削除済み	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	4.17	4.18	4.19
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	4.17	4.18	4.19
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	削除済み
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. ネットワーキングに関する非推奨機能と削除された機能

表1.9 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	4.17	4.18	4.19
iptables	非推奨	非推奨	非推奨

1.5.5. ノードに関する非推奨機能と削除された機能

表1.10 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	4.17	4.18	4.19
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	削除済み

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

表1.11 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	4.17	4.18	4.19
oc-mirror plugin v1	一般提供	非推奨	非推奨

1.5.7. 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1.12 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	4.17	4.18	4.19
Operator SDK	非推奨	非推奨	削除済み
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	削除済み
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	削除済み
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	削除済み
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	削除済み	削除済み
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	削除済み	削除済み
Operator カタログの SQLite データベース形式	非推奨	非推奨	非推奨

1.5.8. ストレージに関する非推奨機能と削除された機能

表1.13 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	4.17	4.18	4.19
FlexVolume を使用した永続ストレージ	非推奨	非推奨	非推奨
AliCloud Disk CSI Driver Operator	削除済み	削除済み	削除済み
Shared Resources CSI Driver Operator	非推奨	削除済み	削除済み

1.5.9. クラスターの更新に関する非推奨機能と削除された機能

表1.14 クラスターの更新に関する非推奨および削除されたトラッカー

機能	4.17	4.18	4.19

1.5.10. Web コンソールに関する非推奨機能と削除された機能

表1.15 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	4.17	4.18	4.19
動的プラグイン SDK の **useModal** フック	一般提供	一般提供	非推奨
Patternfly 4	非推奨	非推奨	削除済み

1.5.11. ワークロードに関する非推奨機能と削除された機能

表1.16 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	4.17	4.18	4.19
DeploymentConfig オブジェクト	非推奨	非推奨	非推奨

1.5.12. 非推奨の機能

1.5.12.1. **oc adm pod-network** コマンドが非推奨になる

OpenShift SDN マルチテナントモードを使用する **oc adm pod-network** コマンドが **oc adm --help** 出力から削除されました。**oc adm pod-network** コマンドが使用される場合、非推奨であることを示すエラーメッセージがユーザーに表示されます。

1.5.12.2. 動的プラグイン SDK の useModal フック

このリリースでは、動的プラグインの **useModal** フックのサポートが非推奨になりました。

このリリース以降、**useOverlay** API フックを使用してモーダルを起動します。

1.5.12.3. 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。

1.5.13. 削除された機能

1.5.13.1. cgroup v1 が削除される

OpenShift Container Platform 4.16 で非推奨化された cgroup v1 はサポートされなくなり、OpenShift Container Platform から削除されました。クラスターで cgroup v1 を使用している場合は、OpenShift Container Platform 4.19 にアップグレードする前に cgroup v2 を設定する必要があります。すべてのワークロードは cgroup v2 と互換性がある必要があります。

クラスターで cgroup v2 を設定する方法は、OpenShift Container Platform バージョン 4.18 ドキュメントの Linux cgroup の設定 を参照してください。

cgroup v2 の詳細は、Linux cgroup バージョン 2 について および Red Hat OpenShift ワークロードのコンテキストにおける Red Hat Enterprise Linux 9 の変更点 (Red Hat ブログ) を参照してください。

1.5.13.2. パッケージベースの RHEL コンピュートマシン

このリリースにより、パッケージベースの RHEL ワーカーノードのインストールのサポートが削除されました。

RHCOS イメージレイヤー化により、この機能が置き換えられ、ワーカーノードのベースオペレーティングシステムへの追加パッケージのインストールがサポートされます。

クラスター内の RHEL ノードを識別して削除する方法は、OpenShift Container Platform 4.18 から新しいバージョンへの更新の準備 を参照してください。イメージレイヤー化の詳細は、RHCOS イメージレイヤー化 を参照してください。

1.5.13.3. Kubernetes 1.32 から削除された API

Kubernetes 1.32 では、以下の非推奨 API が削除されたため、マニフェストと API クライアントを移行して、適切な API バージョンを使用する必要があります。削除された API の移行の詳細は、Kubernetes のドキュメント を参照してください。

表1.17 Kubernetes 1.32 から削除された API

リソース	削除された API	移行先	大きな変更
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta3**	**flowcontrol.apiserver.k8s.io/v1**	いいえ
PriorityLevelConfiguration	**flowcontrol.apiserver.k8s.io/v1beta3**	**flowcontrol.apiserver.k8s.io/v1**	はい

1.5.13.4. Operator SDK CLI および関連するスキャフォールディングとテストツール

このリリースにより、Operator プロジェクトの関連するスキャフォールディングおよびテストツールを含む、Red Hat がサポートするバージョンの Operator SDK CLI ツールが OpenShift Container Platform でリリースされなくなりました。

Red Hat は、OpenShift Container Platform 4 の製品ライフサイクル (Red Hat カスタマーポータル) に従って、OpenShift Container Platform の以前のバージョンでリリースされた Operator SDK のバージョンに対してバグ修正とサポートを提供します。

既存の Operator プロジェクトを含む Operator の作成者は、OpenShift Container Platform 4.18 でリリースされた Operator SDK CLI ツールのバージョン を使用してプロジェクトを維持し、OpenShift Container Platform の新しいバージョンを対象とする Operator リリースを作成できます。詳細は、Updating the base image for existing Ansible- or Helm-based Operator projects for OpenShift Container Platform 4.19 and later (Red Hat ナレッジベース) を参照してください。

コミュニティーによって管理されているサポート対象外の Operator SDK のバージョンは、Operator SDK (Operator Framework) 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、**machineconfiguration.openshift.io** グループからの **MachineConfig** および **ControllerConfig** リソースの内容は、監査ログから除外されませんでした。このリリースにより、これらにはシークレットが含まれている可能性があるため、監査ログから除外されます。(OCPBUGS-55709)

- 以前は、kube-apiserver のサービスレベル目標 (SLO) アラート式は、合計リクエスト数とは無関係に、読み取りおよび書き込みの成功率を誤って合算していました。このため、障害発生時に誤解を招くバーンレートの計算が行われていました。このリリースでは、成功率の計算において総リクエスト数に応じて適切に重み付けされるよう修正が加えられています。これにより、実際の成功リクエストの割合に基づいた正確で信頼性の高いアラートが可能になります。(OCPBUGS-49764)

- 以前は、etcd アクセスが失われた場合にクラスターブートストラップを削除すると kube-apiserver の Readiness が失われ、ダウンタイムが発生する可能性がありました。このリリースでは、各 kube-apiserver には、ロールアウト中に可用性を維持するブートストラップを削除する前に 2 つの安定した etcd エンドポイントがあります。(OCPBUGS-48673)

- 以前は、Static Pod Operator API が、**currentRevision** が設定されておらず、**targetRevision** に複数のゼロ以外のエントリーがあるという無効なノードステータスを許容していたため、ノードコントローラーやインストーラーコントローラーで障害が発生していました。このリリースにより、安定性と一貫性のある静的 Pod ステータスの処理を確保するために、正しいリビジョンフィールドを適用するための新しい検証ルールが追加されました。(OCPBUGS-46380)

- 以前は、ノードコントローラーがリスターから取得した古い **NodeStatus** データを適用して、他のコントローラーによる最新の更新内容を意図せず上書きしていました。このリリースでは、修正によりマネージドフィールドを使用して、コントローラーが競合せずに個別のエントリーを更新できるようになり、正確かつ同時並行的なノードステータスの更新が維持されます。(OCPBUGS-46372)

- 以前は、etcd ブートストラップメンバーの削除に設定された固定の 5 分タイムアウトが早すぎるタイミングで開始されていました。これにより、全体としては十分な時間があったにもかかわらず、HA クラスターで早期に障害が発生していました。このリリースにより、短いタイムアウト設定が削除され、代わりにブートストラップ全体の進行状況に基づいて処理が行われるようになり、etcd のブートストラップ削除がより確実かつクォーラムを保った形で実行されるようになりました。(OCPBUGS-46363)

- 以前は、ブートストラップインスタンスを含む 2 つの kube-apiserver エンドポイントが検出されると、ブートストラップが解除されていました。その結果、永続インスタンスが 1 つしか存在しない状態でロールアウトが行われ、可用性が 0% になる期間が発生していました。このリリースにより、複数の永続インスタンスの準備が整うまで破棄が遅延するようになりました。これにより、ロールアウト時に継続的な kube-apiserver の可用性が確保されます。(OCPBUGS-46010)

- 以前は、一時的なコントロールプレーンがダウンした場合に、**networkConfig.status.ServiceNetwork** は設定されず、生成された証明書に SAN の Kubernetes サービス IP がない場合、クライアントはデフォルトの kubernetes サービスを介し

た kube-apiserver への接続に失敗していました。このリリースにより、**networkConfig.status.ServiceNetwork** が nil の場合、証明書の生成をスキップするガードが追加されました。クライアント接続は安定し、有効になります。(OCPBUGS-45943)

- 以前は、etcd メンバーが削除される前にインストーラーによってブートストラップマシンが削除されていました。これにより、HA クラスターでクォーラム損失が発生しました。このリリースにより、SNO からのチェックがすべてのトポロジーに拡張され、etcd Operator の状態を安全な削除のサインとして使用するようになりました。これにより、ブートストラップの終了処理中も etcd クラスターの安定性が確保されます。(OCPBUGS-45482)

- 以前は、CRD 要求の処理中に image および error フィールドの両方が未設定の場合、openshift-apiserver がパニックを起こす可能性がありました。この問題により、特定の条件下で API サーバーがランタイムクラッシュを起こし、不安定になることがありました。このリリースにより、両方のフィールドが設定されていない場合に、ケースを安全に処理することでパニックが発生しないようにガードが追加され、CRD 要求をクラッシュすることなく堅牢で安定して処理できるようになりました。(OCPBUGS-45861)

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、Ironic Python Agent (IPA) からの NetworkManager ログは ramdisk ログに含まれていませんでしたが、代わりに **dmesg** ログのみが ramdisk ログに含まれていました。このリリースにより、metal3 Pod の **metal3-ramdisk-logs** コンテナーに存在する ramdisk ログに、**dmesg** ログと IPA ではなく、ホストからのジャーナル全体が含まれるようになりました。(OCPBUGS-56042)

- 以前は、ramdisk ログには明確なファイル区切りが含まれていなかったため、あるファイルの内容が別のファイルのランダムな行にマージされていました。この問題により、どのコンテンツがどのファイルに属するかを区別することが困難でした。このリリースにより、ファイルの内容を ramdisk ログファイルにマージする際に、それぞれのファイルが明確に区別できるようにファイル区切りが追加されました。(OCPBUGS-55743)

- 以前は、Baseboard Management Console (BMC) URL に **redfish://host/redfish/v1/Self** ではなく **redfish://host/redfish/v1/** のような Redfish システム ID を含めることを忘れた場合、JSON 解析の問題が Ironic に存在していました。このリリースにより、JSON 解析の問題が発生することなく、BMO が Redfish システム ID なしで URL を有効なアドレスとして処理できるようになりました。(OCPBUGS-56026)

- 以前は、プロビジョニング中に競合状態が存在し、DHCP 応答が遅いと、マシンオブジェクトとノードオブジェクトに異なるホスト名が使用される可能性がありました。これにより、ワーカーノードの CSR が自動承認されなくなる可能性がありました。このリリースにより、競合状態が修正され、ワーカーノードの CSR が適切に承認されるようになりました。(OCPBUGS-55315)

- 以前は、**ars-111gl-nhr** などの SuperMicro マシンの特定のモデルは、他の SuperMicro マシンとは異なる仮想メディアデバイス文字列を使用していたため、これらのサーバーで仮想メディアの起動に失敗する可能性がありました。このリリースにより、影響を受ける特定のモデルをチェックし、それに応じて動作を調整するための追加の条件チェックが追加され、ars-111gl-nhr などの SuperMicro モデルが仮想メディアから起動できるようになりました。(OCPBUGS-56639)

- 以前は、関連する **DataImage** を持つ **BaremetalHost** を削除した後、**DataImage** が引き続き存在していました。このリリースにより、**DataImage** は、**BaremetalHost** が削除された後も存在する場合は削除されます。(OCPBUGS-51294)

1.6.3. クラウドコンピュート

- UEFI と互換性のないブートディスクを使用する Google Cloud クラスターをアップグレードする場合、Shielded VM サポートは有効化できません。以前は、これにより新規コンピュートマシンの作成ができませんでした。このリリースにより、既知の UEFI 非互換性があるディスクに対して、Shielded VM のサポートが無効化されました。これは主に、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影響します。(OCPBUGS-17079)

- 以前は、接続されたネットワークインターフェイスコントローラー (NIC) が **ProvisioningFailed** 状態であったため、Azure で実行されたクラスター内の仮想マシンが失敗していました。このリリースにより、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して問題を回避するようになりました。(OCPBUGS-31515)

- 以前は、証明書署名要求 (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、関連性のない未承認の CSR を合計に含め、それ以上の承認が妨げられていました。このリリースにより、CSR 承認者は **signerName** プロパティーをフィルターとして使用し、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-36404)

- 以前は、Machine API コントローラーはゾーン番号のみを読み取り、マシンゾーン情報を入力していました。可用性セットのみをサポートする Azure リージョンのマシンの場合、セット数はゾーンを表すため、Machine API コントローラーはゾーン情報を設定しませんでした。このリリースにより、Machine API コントローラーは Azure 障害ドメインプロパティーを参照します。このプロパティーは可用性セットとアベイラビリティーゾーンで機能するため、コントローラーはそれぞれのケースの障害ドメインを正しく読み取り、マシンは常にゾーンを報告します。(OCPBUGS-38570)

- 以前は、Google Cloud ゾーン API のエラーメッセージが詳細化されたことで、マシンコントローラーが一部の無効な設定のマシンを一時的なクラウドエラーとして誤って有効と判定してしまっていました。この動作により、無効なマシンが failed 状態に移行することができませんでした。このリリースにより、マシンコントローラーがより詳細なエラーメッセージを正しく処理するようになったため、無効なゾーンまたはプロジェクト ID を持つマシンは正しく障害状態に移行します。(OCPBUGS-43531)

- 以前は、リンクされたアクションに必要な一部のパーミッションが欠落していました。リンクされたアクションは、クラウドコントローラーマネージャーおよび OpenShift Container Platform が必要とする他の Azure リソースに必要なサブリソースを作成します。このリリースにより、Azure のクラウドコントローラーマネージャーには、リンクされたアクションに対する次のパーミッションがあります。

  - **Microsoft.Network/applicationGateways/backendAddressPools/join/action**
  - **Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action**
  - **Microsoft.Network/applicationSecurityGroups/joinNetworkSecurityRule/action**
  - **Microsoft.Network/ddosProtectionPlans/join/action**
  - **Microsoft.Network/gatewayLoadBalancerAliases/join/action**
  - **Microsoft.Network/loadBalancers/backendAddressPools/join/action**
  - **Microsoft.Network/loadBalancers/frontendIPConfigurations/join/action**
  - **Microsoft.Network/loadBalancers/inboundNatRules/join/action**

- **Microsoft.Network/networkInterfaces/join/action**
- **Microsoft.Network/networkSecurityGroups/join/action**
- **Microsoft.Network/publicIPAddresses/join/action**
- **Microsoft.Network/publicIPPrefixes/join/action**
- **Microsoft.Network/virtualNetworks/subnets/join/action**

(OCPBUGS-44126)

- 以前は、リンクされたアクションに必要な一部のパーミッションが欠落していました。リンクされたアクションは、Machine API および OpenShift Container Platform が必要とする他の Azure リソースに必要なサブリソースを作成します。このリリースにより、Azure の Machine API プロバイダーには、リンクされたアクションに対する次のパーミッションがあります。
  - **Microsoft.Compute/disks/beginGetAccess/action**
  - **Microsoft.KeyVault/vaults/deploy/action**
  - **Microsoft.ManagedIdentity/userAssignedIdentities/assign/action**
  - **Microsoft.Network/applicationGateways/backendAddressPools/join/action**
  - **Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action**
  - **Microsoft.Network/applicationSecurityGroups/joinNetworkSecurityRule/action**
  - **Microsoft.Network/ddosProtectionPlans/join/action**
  - **Microsoft.Network/gatewayLoadBalancerAliases/join/action**
  - **Microsoft.Network/loadBalancers/backendAddressPools/join/action**
  - **Microsoft.Network/loadBalancers/frontendIPConfigurations/join/action**
  - **Microsoft.Network/loadBalancers/inboundNatPools/join/action**
  - **Microsoft.Network/loadBalancers/inboundNatRules/join/action**
  - **Microsoft.Network/networkInterfaces/join/action**
  - **Microsoft.Network/networkSecurityGroups/join/action**
  - **Microsoft.Network/publicIPAddresses/join/action**
  - **Microsoft.Network/publicIPPrefixes/join/action**
  - **Microsoft.Network/virtualNetworks/subnets/join/action**

  (OCPBUGS-44130)

- 以前は、コンピュートマシンセット CR の **publicIp** パラメーターが **false** に設定されている場合、既存のサブネット上の特定の環境での AWS クラスターのインストールが失敗していました。このリリースにより、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際に、**publicIp** に設定された設定値が問題を引き起こさないよう修正されました。(OCPBUGS-44373)

- 以前は、UEFI 以外のディスクを使用する Google Cloud クラスターのロードに失敗していました。このリリースにより、セキュアブートなどの UEFI を必要とする機能を有効にする前に、ディスクが UEFI と互換性があることを確認するチェックが追加されました。この変更により、**compute.images.get** および **compute.images.getFromFamily** パーミッションの要件が追加されます。その結果、これらの機能が必要ない場合は、UEFI 以外のディスクを使用できます。(OCPBUGS-44671)

- 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 **DHCPOptionSet** パラメーター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。このリリースにより、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は、作成される Kubernetes オブジェクト名が有効になるように末尾のピリオドをトリミングします。このパラメーターの末尾のピリオドが原因でインストールが失敗することはなくなりました。(OCPBUGS-45306)

- 以前は、Azure 可用性セットの障害ドメインの数は、固定値の **2** を使用していました。障害ドメイン数は通常 2 以上であるため、この設定はほとんどの Azure リージョンで機能します。ただし、この設定は **centraluseuap** および **eastusstg** リージョンで失敗しました。このリリースにより、リージョン内の可用性セット障害ドメインの数が動的に設定されるようになりました。(OCPBUGS-45663)

- 以前は、一時的な API サーバーの切断が発生した場合に、Azure クラウドコントローラーマネージャーはパニックを起こしました。このリリースにより、Azure クラウドコントローラーマネージャーは一時的な切断から正しく回復します。(OCPBUGS-45859)

- 以前は、アノテーションが間違っているか、欠落しているために、一部のサービスが保留状態のままになりました。このリリースにより、Azure **service.beta.kubernetes.io/azure-load-balancer-tcp-idle-timeout** および Google Cloud **cloud.google.com/network-tier** アノテーションに検証が追加され、問題が解決されました。(OCPBUGS-48481)

- 以前は、AWS からプロバイダー ID を取得するために使用される方法では、必要に応じてこの値を kubelet に提供することができませんでした。その結果、マシンは異なる状態でスタックし、初期化を完了できない場合がありました。このリリースにより、kubelet の起動時にプロバイダー ID が一貫して設定されるようになりました。(OCPBUGS-50905)

- 以前は、Azure クラウドコントローラーマネージャーのエンドポイントが正しくないため、Microsoft Azure Government Cloud へのインストールが失敗していました。この問題はこのリリースで解決されています。(OCPBUGS-50969)

- 以前は、Machine API は、IBM Cloud でのクラスター作成時に異常なコントロールプレーンノードを検出し、ノードの置き換えを試みることがありました。これにより、クラスターが事実的に破棄されました。このリリースにより、Machine API はクラスターの作成中に異常なコンピュートノードのみを置き換えようとし、異常なコントロールプレーンノードを置き換えようとはしません。(OCPBUGS-51864)

- 以前は、ノードが準備完了になる前に削除された Azure スポットマシンが、**provisioned** 状態のままになることがありました。このリリースにより、Azure スポットインスタンスで削除エビクションポリシーが使用されるようになりました。このポリシーにより、プリエンプション時にマシンが **failed** 状態に正しく移行するようになります。(OCPBUGS-54617)

- 以前、バグ修正により可用性セットの設定が変更されました。その際に、障害ドメイン数が固定値の **2** ではなく、利用可能な最大値を使用するように変更されました。これにより、バグ修正前に作成されたコンピュートマシンセットでスケーリングの問題が発生しました。これはコ

ントローラーがイミュータブルな可用性セットの変更を試みることが原因でした。このリリースにより、可用性セットが作成後に変更されなくなり、影響を受けるコンピュートマシンセットが適切にスケーリングできるようになりました。(OCPBUGS-56653)

- 以前は、**openshift-cnv** namespace コンポーネントには **openshift.io/required-scc** アノテーションがありませんでした。ワークロードは、必要な Security Context Constraints (SCC) を要求していませんでした。このリリースにより、ワークロードが必要な SCC を要求できるように、**openshift.io/required-scc** アノテーションが **openshift-cnv** namespace コンポーネントに追加されました。(OCPBUGS-49657)

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-41727)

1.6.5. Cluster Autoscaler

- 以前は、Machine Set がスケールダウンされ、最小サイズに達すると、Cluster Autoscaler が最後に残ったノードに NoSchedule taint を付与してしまい、そのノードが利用できなくなることがありました。この問題は、Cluster Autoscaler のカウントエラーが原因で生じました。このリリースにより、カウントエラーが修正され、Machine Set がスケールダウンし、最小サイズに達したときに Cluster Autoscaler が想定どおりに機能するようになりました。(OCPBUGS-54231)

- 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-25852)

- 以前は、マシンセットのマシンが失敗するため、Cluster Autoscaler はスケーリングを停止する可能性がありました。この状況は、Cluster Autoscaler がさまざまな非実行フェーズのマシンをカウントする方法が不正確なために発生しました。このリリースにより、不正確さが修正され、Cluster Autoscaler がマシンを正確にカウントするようになりました。(OCPBUGS-11115)

1.6.6. Cluster Resource Override Admission Operator

- 以前は、Cluster Resource Admission Override Operator は OpenShift Container Platform 4.16 から OpenShift Container Platform 4.17 へのアップグレード時に、古いシークレットを削除できませんでした。この状況では、Cluster Resource Override Admission Operator Webhook が機能しなくなり、Cluster Resource Override Admission Operator が有効化された namespace で Pod が作成されなくなっていました。このリリースにより、古いシークレットが削除され、Cluster Resource Override Admission Operator のエラーハンドリングが改善され、namespace 内での Pod 作成に関する問題が解決されました。(OCPBUGS-54886)

- 以前は、**clusterresourceoverride-operator** サービスを削除するか、Cluster Resource Admission Override Operator をアンインストールすると、**v1.admission.autoscaling.openshift.io** API サービスに到達できず、クラスターに他の Operator をインストールするなど、必要なクラスター機能が阻止されていました。このリリースにより、Cluster Resource Admission Override Operator がアンインストールされた場合は、**v1.admission.autoscaling.openshift.io** API サービスも削除されるように修正され、クラスター機能に影響を及ぼすことがなくなります。(OCPBUGS-48115)

- 以前は、**ClusterResourceOverride** CR で **forceSelinuxRelabel** パラメーターを指定してから、そのパラメーターを別の値に変更した場合、変更された値は **clusterresourceoverride-**

configuration Config Map に反映されませんでした。この Config Map は、クラスターに selinux のラベルの再設定回避策機能を適用するために必要です。このリリースにより、この問題が修正され、**forceSelinuxRelabel** パラメーターが変更されると、**clusterresourceoverride-configuration** Config Map が更新を受け取るようになりました。(OCPBUGS-44649)

1.6.7. Cluster Version Operator

- 以前は、**ClusterVersion** 条件のステータスが **ImplicitlyEnabled** から **ImplicitlyEnabledCapabilities** に変更される可能性がありました。このリリースにより、**ClusterVersion** 条件タイプが修正され、**ImplicitlyEnabled** から **ImplicitlyEnabledCapabilities** に変更されました。(OCPBUGS-56771)

- 以前は、カスタム Security Context Constraint (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-31462)

- 以前は、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-23514)

1.6.8. etcd

- この更新前は、etcd 3.5.19 から 3.6 リリースへのローリングクラスター更新中に、間違ったメンバーシップデータが新しいメンバーに伝播されることがありました。その結果、クラスター内の learner メンバーが多すぎることを示すエラーが発生し、クラスターの更新が失敗していました。このリリースでは etcd が 3.5.24 に更新され、そこに含まれる修正により、メンバーシップ関連のエラーが発生しなくなりました。(OCPBUGS-63473)

1.6.9. ImageStreams

- 以前は、ミラーレジストリーがセットアップされている場合でも、**NeverContactSource** に設定されたレジストリーが存在すると、イメージのインポートが失敗するレジストリーをブロックしていました。この更新により、レジストリーにミラーが設定されている場合にイメージのインポートがブロックされなくなりました。これにより、**ImageDigestMirrorSet** または **ImageTagMirrorSet** リソースで元のソースが **NeverContactSource** に設定されている場合でも、イメージのインポートが成功するようになります。(OCPBUGS-44432)

1.6.10. インストーラー

- 以前は、最小限の特権で Amazon Web Services (AWS) クラスターをインストールしようとし、**install-config.yaml** ファイルでインスタンスタイプを指定しなかった場合、クラスターのインストールは失敗していました。この問題は、インストールプログラムが、サポート対象のアベイラビリティーゾーンでクラスターが使用できるサポート対象のインスタンスタイプを見つけられなかったために発生しました。たとえば、**m6i.xlarge** デフォルトインスタンスタイプは、**ap-southeast-4** および **eu-south-2** アベイラビリティーゾーンでは使用できませんでした。このリリースにより、**openshift-install** プログラムでは、**ec2:DescribeInstanceTypeOfferings** AWS パーミッションが必要になりました。これ

は、サポート対象のアベイラビリティーゾーンで **m6i.xlarge** または別のサポート対象インスタンスタイプが利用できない状況で、クラスターのインストールが失敗しないようにするために必要になりました。(OCPBUGS-46596)

- 以前は、インストールプログラムは、ユーザーがベアメタル上にシングルノードクラスターをインストールしようとするのを阻止せず、インストール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、サポートされていないプラットフォームでのシングルノードクラスターのインストールを防止します。(OCPBUGS-56811)

- 以前は、VMware vSphere の **openshift-install destroy cluster** コマンドの実行に関連する問題を診断したときに、ログ情報で提供される詳細が不十分でした。その結果、クラスターが仮想マシン (VM) から削除されない理由が不明でした。このリリースにより、クラスターを破棄するときに、拡張デバッグロギングが提供され、問題が解決されました。(OCPBUGS-56372)

- 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のアベイラビリティーゾーン情報が一致するようになり、問題が解決されました。(OCPBUGS-55492)

- 以前は、**OVNKubernetes** ネットワークプラグインを使用してクラスターをインストールするときに、プラグインが小文字の "k" で **OVNkubernetes** として指定されていると、インストールが失敗する可能性がありました。この更新により、インストールプログラムは大文字と小文字に関係なく、プラグイン名を正しく解釈するようになりました。(OCPBUGS-54606)

- プロキシーが設定されると、インストールプログラムは **machineNetwork** CIDR を **noProxy** フィールドに追加します。以前は、**machineNetwork** CIDR が **noProxy** フィールドのユーザーによっても設定されていた場合、重複エントリーが発生し、Ignition では許可されず、ホストが適切に起動できなくなる可能性がありました。このリリースでは、**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はそれを **noProxy** フィールドに追加しません。(OCPBUGS-53183)

- 以前は、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 が自動的に割り当てられていました。この動作は意図されたものではありませんでした。現在、API および Ingress 仮想 IP は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** ファイルで明示的に設定されていない場合、インストールはエラーで失敗し、ユーザーは値を指定するよう求められます。(OCPBUGS-53140)

- 以前は、Agent-based Installer を使用する場合、ハードウェア検出中にファイバーチャネル (FC) マルチパスボリュームの WWN は検出されませんでした。その結果、**wwn** ルートデバイスヒントが指定されると、すべてのマルチパス FC ボリュームがそれによって除外されました。このリリースにより、マルチパス FC ボリュームに対して WWN が収集されるようになったため、複数のマルチパスボリュームが存在する場合でも、ユーザーは **wwn** ルートデバイスヒントを使用してそれらのボリュームを選択できるようになりました。(OCPBUGS-52994)

- 以前は、Azure 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に NVMe または SCSI のサポートが含まれていなかったため、それらを必要とする仮想マシンインスタンスファミリーを使用できませんでした。この更新により、インストールプログラムは、NVMe または SCSI サポートを必要とする仮想マシンインスタンスファミリーを利用できるようになります。(OCPBUGS-52658)

- 以前は、ユーザー提供の暗号化鍵を使用して Google Cloud にクラスターをインストールする

際、インストールプログラムがキーリングを見つけられないことがありました。この更新により、インストールプログラムはユーザー提供の暗号鍵リングを見つけるようになり、インストールが失敗しなくなりました。(OCPBUGS-52203)

- 以前は、Google Cloud にクラスターをインストールする場合、ネットワークの不安定性によりインストール中に Google Cloud タグを取得できなかった場合、インストールが失敗する可能性がありました。この更新により、インストールプログラムが改善され、インストール中のネットワークの不安定さを許容できるようになりました。(OCPBUGS-50919)

- 以前は、インストーラーは VMware vSphere クラスター内で電源がオフになっている ESXi ホストをチェックしていなかったため、OVA をアップロードできず、インストールが失敗していました。このリリースにより、インストーラーが各 ESXi ホストの電源状態をチェックし、電源がオフになっているホストをスキップするようになりました。これにより問題が解決され、OVA を正常にインポートできるようになりました。(OCPBUGS-50649)

- 以前は、Agent-based Installer を使用する場合、非接続環境で Agent ISO イメージを構築すると、**unable to read image** というエラーメッセージが誤って出力されていました。このリリースにより、これらの誤ったメッセージは削除され、表示されなくなりました。(OCPBUGS-50637)

- 以前は、Azure にクラスターをインストールするときに、IP アドレスの可用性を確認するための適切なパーミッションがない場合、インストールプログラムがセグメンテーションフォールトエラーでクラッシュしていました。この更新により、インストールプログラムは不足しているパーミッションを正しく識別し、正常に失敗するようになりました。(OCPBUGS-50534)

- 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-49784)

- 以前は、IBM Cloud® にクラスターをインストールする場合、**ca-mon** リージョンが使用可能であるにもかかわらず、インストールプログラムはそのリージョンへのインストールに失敗していました。この更新により、インストールプログラムは最新の IBM Cloud® の利用可能なリージョンに対応しました。(OCPBUGS-49623)

- 以前は、ユーザー提供のパブリック IPv4 プールを持つ既存の VPC に最小限のパーミッションで AWS にクラスターをインストールした後、パーミッションが不足しているためにクラスターを破棄できませんでした。この更新により、インストールプログラムは **ec2:ReleaseAddress** パーミッションを伝播し、クラスターを破棄できるようになります。(OCPBUGS-49594)

- 以前は、VMware vSphere のインストーラーは、障害ドメインの **install-config.yaml** で提供されるネットワークの数を検証していませんでした。このため、最大数の 10 を超えるネットワークが指定された場合、エラーは表示されずに、サポートされていない設定でインストールが続行されていました。このリリースにより、インストーラーが設定されたネットワークの数を検証するようになり、最大制限を超える設定の使用を防ぐことで問題が解決されました。(OCPBUGS-49351)

- 以前は、Local Zone または Wavelength Zone の既存のサブネット (BYO VPC) を使用して AWS にクラスターをインストールすると、エッジサブネットリソースに **kubernetes.io/cluster/<InfraID>:shared** タグがありませんでした。このリリースにより、**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付与されるように修正が加えられました。(OCPBUGS-48827)

- 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。この問題はこのリリースで解決されています。(OCPBUGS-49885)

- 以前は、AWS にクラスターをインストールする場合、このリージョンが OpenShift Container Platform でサポートされていたにもかかわらず、インストールプログラムサーベイで **ap-southeast-5** リージョンは使用できませんでした。この更新により、**ap-southeast-5** リージョンが利用可能になりました。(OCPBUGS-47681)

- 以前は、Google Cloud にインストールされたクラスターを破棄するときに、インストールプログラムがすべての破棄操作が正常に完了するまで待機しなかったため、一部のリソースが残されることがありました。この更新により、destroy API はすべてのリソースが適切に削除されたことを確認するために待機するようになりました。(OCPBUGS-47489)

- 以前は、**us-east-1** リージョンの AWS にクラスターをインストールする場合、**use1-az3** ゾーンは OpenShift Container Platform でサポートされるインスタンスタイプをいずれもサポートしていないため、**install-config.yaml** ファイルにゾーンが指定されていないと、インストールが失敗する可能性がありました。この更新により、インストール設定ファイルでゾーンが指定されていない場合、インストールプログラムは **use1-az3** ゾーンの使用を阻止します。(OCPBUGS-47477)

- 以前は、Google Cloud にクラスターをインストールする際に、プロジェクトで **constraints/compute.vmCanIpForward** 制約を有効にした場合、インストール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この制約が有効になっている場合はそれを無効にし、インストールが正常に実行できるようにします。(OCPBUGS-46571)

- 以前は、Google Cloud にクラスターをインストールするときに、ユーザーが存在しない暗号鍵リングを指定した場合、インストールプログラムはそれを検出できず、インストール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ユーザーが提供する暗号鍵リングの存在を正しく検証し、失敗を阻止します。(OCPBUGS-46488)

- 以前は、Microsoft Azure にインストールされたクラスターを破棄しても、ブートストラップノードの受信 NAT ルールとセキュリティーグループは削除されませんでした。この更新により、正しいリソースグループにより、クラスターが破棄されたときにすべてのリソースが削除されるようになります。(OCPBUGS-45429)

- 以前は、AWS の **ap-southeast-5** リージョンにクラスターをインストールすると、ロードバランサーのホスト名の形式が正しくないためにインストールが失敗する可能性がありました。この更新により、インストールプログラムが改善され、正しいホスト名が形成されるようになったため、インストールが成功するようになりました。(OCPBUGS-45289)

- 以前は、Google Cloud にクラスターをインストールするときに、Google のサーバー上でサービスアカウントをアクティブ化する際の遅延が原因で、インストールプログラムが作成したサービスアカウントを見つけられないことがありました。この更新により、インストールプログラムは、作成されたサービスアカウントの使用を試みる前に適切な時間待機するようになりました。(OCPBUGS-45280)

- 以前は、AWS にクラスターをインストールするときに、エッジマシンプールを指定してもインスタンスタイプを指定しないと、インストールが失敗する可能性がありました。この更新により、インストールプログラムではエッジマシンプールにインスタンスタイプを提供する必要があります。(OCPBUGS-45218)

- 以前は、Google Cloud にインストールされたクラスターを破棄しても、**kubernetes-io-cluster-<cluster-id>: owned** のラベルが付いた PVC ディスクは削除されませんでした。この更新により、クラスターが破棄されたときに、インストールプログラムはこれらのリソースを正しく見つけて削除するようになりました。(OCPBUGS-45162)

- 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-44938)

- 以前は、AWS にクラスターをインストールするときに、**publicIPv4Pool** パラメーターが設定されているが **ec2:AllocateAddress** パーミッションが存在しない場合は、インストール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では、このパーミッションが存在する必要があります。(OCPBUGS-44925)

- 以前は、共有 Virtual Private Cloud (VPC) のインストール時に、インストーラーは、クラスターのプライベート DNS ゾーンにレコードを追加するのではなく、インストーラー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、インストーラー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** ファイルによって提供され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、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はそれらをサポートしませんでした。この状況では、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出力していました。このリリースにより、AWS タグの正規表現は、空白のあるタグ名を検証するようになり、インストールプログラムがこれらのタグを受け入れ、空白が原因であるエラーを出力しなくなりました。(OCPBUGS-44199)

- 以前は、Google Cloud にインストールされていたクラスターを破棄すると、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ず、エラーが発生していました。この更新により、クラスターが破棄されるとすべてのリソースが削除されます。(OCPBUGS-43779)

- 以前は、Microsoft Azure にクラスターをインストールするときに、**Standard_M8-4ms** インスタンスタイプを指定すると、そのインスタンスタイプがメモリーを整数形式ではなく小数形式で指定するため、エラーが発生しました。この更新により、インストールプログラムはメモリー値を正しく解析するようになりました。(OCPBUGS-42241)

- 以前は、VMware vSphere にクラスターをインストールするときに、API および Ingress サーバーの仮想 IP がマシンネットワークの外部にあるとインストールが失敗する可能性がありました。この更新により、インストールプログラムには、マシンネットワーク内の API および Ingress サーバーの仮想 IP がデフォルトで含まれるようになりました。API および Ingress サーバーの仮想 IP を指定する場合は、それらがマシンネットワーク内にあることを確認してください。(OCPBUGS-36553)

- 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、イメージのインポートエラーのため、Madrid ゾーンを選択した場合はインストール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が変更され、正しいストレージバケット名が使用され、インストールが正常に続行されるようになりました。(OCPBUGS-50899)

- 以前は、IBM Power Virtual Server にインストールされたクラスターを破棄しても、ネットワークサブネットを含む一部のリソースが削除されませんでした。この更新により、クラスターが破棄されるとすべてのネットワークリソースが削除されます。(OCPBUGS-50657)

- 以前は、Assisted Installer を使用してクラスターをインストールすると、イメージのプル時にタイムアウトが発生し、インストールが失敗する可能性がありました。この更新により、タイムアウトが延長され、インストールプログラムがイメージのプルを完了できるようになりました。(OCPBUGS-50655)

- 以前は、一部の低速な PrismCentral 環境では、prism-api 呼び出しが RHCOS イメージをロードすると、インストールプログラムがタイムアウトで失敗していました。以前のタイムアウト

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 **platform.nutanix.prismAPICallTimeout** として **install-config.yaml** ファイル内の設定可能なパラメーターで、デフォルト値は 10 分です。(OCPBUGS-48570)

- 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。この問題はこのリリースで解決されています。(OCPBUGS-48044)

- 以前は、installer-provisioned infrastructure を使用して IBM Power Virtual Server 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、ユーザーが提供したネットワークを使用する代わりに、ランダムなマシンネットワークを選択していました。この更新により、インストールプログラムは、ユーザーが提供するマシンネットワークを使用します。(OCPBUGS-45286)

- 以前は、**openshift-install agent create pxe-files** コマンドの実行時に作成された一時ディレクトリーは、コマンドの完了後に削除されませんでした。このリリースにより、コマンドの完了後に一時ディレクトリーが適切に削除されるようになりました。(OCPBUGS-39583)

1.6.11. Machine Config Operator

- 以前は、**ContainerRuntimeConfig** は **runc** ランタイムの **--root** パスを誤って設定していました。これにより、コンテナーが誤ったルートパスで実行され、コンテナー操作に問題が発生しました。このリリースにより、コンテナーランタイムの **--root** パスは適切となり、指定されたランタイムと一致し、一貫した操作が提供されるようになりました。(OCPBUGS-47629)

- 以前は、クラスターに OpenShift Container Platform 4.19 以降ではサポートされなくなった Red Hat Enterprise Linux (RHEL) ワーカーノードが含まれていた場合、ユーザーには警告が表示されませんでした。このリリースにより、Machine Config Operator は RHEL ノードを検出し、OpenShift Container Platform 4.19 と互換性のないユーザーに通知します。(OCPBUGS-54611)

- 以前は、Machine Config Operator (MCO) が、更新をステージングした後すぐにノードを再起動すると、更新は失敗していました。このリリースにより、MCO はステージング操作が完了するのを待ってからシステムを再起動するようになり、更新を完了できるようになりました。(OCPBUGS-51150)

- 以前は、**MachineOSConfig** オブジェクトを削除した後、関連付けられた **MachineOSBuild** オブジェクトは期待どおりに削除されませんでした。これは、**MachineOSBuild** オブジェクトの所有権が設定されていなかったためです。このリリースにより、ビルド用にすべてのオブジェクトが作成され、**MachineOSConfig** オブジェクトが削除されると、関連するすべてのオブジェクトが削除されるようになりました。(OCPBUGS-44602)

1.6.12. 管理コンソール

- 以前は、**Developer パースペクティブ** の **Projects details** にパンくずリストが誤って含まれていませんでした。このリリースにより、パンくずリストが追加されました。(OCPBUGS-52298)

- 以前は、Web ターミナルを開いた状態で **Project** ドロップダウンリストを開くと、視覚的な表示の乱れが発生していました。この更新後、表示の乱れが修正され、Web ターミナルが開いているときに **Project** ドロップダウンリストを使用できるようになりました。(OCPBUGS-45325)

- 以前は、リゾルバーを使用する **PipelineRuns** CR を OpenShift Container Platform Web コンソールで再実行できませんでした。CR を再実行しようとすると、"Invalid **PipelineRun**

configuration, unable to start Pipeline" が生成されました。このリリースにより、この問題が発生することなく、リゾルバーを使用する **PipelineRuns** CR を再実行できるようになりました。(OCPBUGS-44265)

- 以前は、OpenShift Container Platform Web コンソールで **Form View** を使用して **Deployment** または **DeploymentConfig** API オブジェクトを編集すると、どちらかのオブジェクトの YAML 設定に重複した **ImagePullSecrets** パラメーターが追加されていました。このリリースにより、どちらのオブジェクトにも重複した **ImagePullSecrets** パラメーターが自動的に追加されないように修正されました。(OCPBUGS-41974)

- 以前は、特定の **Pipelinerun** の **TaskRun** は、**PipelineRun** 名に基づいて取得されていました。2 つの **PipelineRuns** の名前が同じ場合、両方の **PipelineRuns** の **TaskRun** が取得されて表示されていました。このリリースにより、特定の **PipelineRun** の **TaskRun** が、**PipelineRun** 名ではなく **PipelineRun** UID に基づいて取得されるようになりました。(OCPBUGS-36658)

- 以前は、Pod が実行されていない場合、**Test Serverless 機能** ボタンは応答しませんでした。この更新により、Pod が実行されていない場合はボタンは無効になります。(OCPBUGS-32406)

- 以前は、失敗した **TaskRun** の結果は UI に表示されませんでした。この更新により、失敗に関係なく、**TaskRun** の結果が常に利用できるようになります。(OCPBUGS-23924)

- 以前は、コントロールプレーンのみの更新を実行する場合、コンソールで、コンピュートノードを 60 日以内に更新する必要があるというアラートがユーザーに表示されていました。このリリースにより、コンソールにこの無効なアラートが表示されなくなりました。(OCPBUGS-56077)

- 以前は、**Notification Drawer** の **Critical Alerts** セクションを折りたたむことができませんでした。このリリースにより、セクションを折りたたむことができます。(OCPBUGS-55702)

- 以前は、インストール済みの Operator のリストを表示した際に、コピーされた CSV が Operator Lifecycle Manager (OLM) で無効になっている場合、選択中のプロジェクトが Operator のデフォルトの namespace と一致していると、Operator がリストに 2 回表示されていました。このリリースにより、このような場合に Operator は 1 回だけ表示されます。(OCPBUGS-54601)

- 以前は、**Installed Operators** ページの **OperatorHub** へのリンクがハードリロードをトリガーすることがありました。このリリースにより、このリンクによってハードリロードがトリガーされなくなりました。(OCPBUGS-54536)

- 以前は、**Create VolumeSnapshot** ページでプロジェクトのピッカーから **All Projects** を選択すると、page not found エラーが発生していました。このリリースにより、VolumeSnapshot リストページが正しく表示されるようになりました。(OCPBUGS-53227)

- 以前は、Pod コンテナーの数を計算するロジックが間違っていたため、計算結果が不正確になっていました。このリリースにより、カウントロジックに **Ready** および **Started** ステータスが追加され、**oc** CLI と一致する正しい Pod コンテナー数が表示されるようになりました。(OCPBUGS-53118)

- 以前は、**Select** メニューのトグルが再度クリックされたか、または Select メニューの項目の 1 つがクリックされていない限り、**Node Logs** セクションの上にある **Select** メニューは閉じられませんでした。このリリースにより、メニューの外側をクリックするか、キーボードの適切なキーを押すと、**Select** メニューが閉じます。(OCPBUGS-52316)

- 以前は、共有タイムスタンプコンポーネントは、相対時刻を計算する際に未定義のプロパ

ティーを参照していました。そのため、コンソールに表示される時刻のほとんどが、**Just now** や **Less than a minute ago** といった相対的な文字列を正しく表示できていませんでした。このリリースにより、問題が修正され、相対時間の文字列がコンソールに正しく表示されるようになりました。(OCPBUGS-51202)

- 以前は、**Observe** メニューは、モニタリング用の現在のユーザーおよびコンソール設定に基づいてのみ表示されていました。これにより、可観測性プラグインによって追加された他の項目が非表示になりました。このリリースにより、**Observe** メニューにさまざまな監視プラグインの項目も表示されるようになりました。(OCPBUGS-50693)

- 以前は、コンソールに初めてログインすると、自動パースペクティブ検出により、ユーザーがコンソールにアクセスするためにクリックした特定の URL パスが無視され、代わりに別のページが読み込まれていました。このリリースにより、現在のパスが適用されます。(OCPBUGS-50650)

- 以前は、Web コンソールにある水平ナビゲーションで新しいタブをプラグインから作成すると、問題が発生していました。このリリースにより、プラグインを使用して、Web コンソールの水平ナビゲーションにタブを作成できるようになりました。(OCPBUGS-49996)

- 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-49839)

- 以前は、CLI downloads ページのリンクはオペレーティングシステムによってソートされませんでした。このリリースにより、リンクはオペレーティングシステムごとにアルファベット順に並べられます。(OCPBUGS-48413)

- 以前は、**OperatorHub** モーダルのプライマリー **Action** ボタンに複数の外部リンクアイコンが表示される可能性がありました。このリリースにより、外部リンクアイコンが 1 つだけ表示されます。(OCPBUGS-46555)

- 以前は、Red Hat OpenShift Lightspeed モーダルで **Don't show again** のリンクをクリックしても、他の **User Preference** タブのいずれかが表示されている場合は、一般的な **User Preference** タブに正しく移動されませんでした。この更新後、**Don't show again** リンクをクリックすると、一般的な **User Preference** タブに移動します。(OCPBUGS-46511)

- 以前は、**Console plugin enablement** モーダルで、コンソールプラグインが複数回有効化される可能性があったため、Console Operator Configuration を表示するプラグインに複数のエントリーが発生していました。このリリースにより、すでに有効になっているプラグインを有効にすることはできなくなりました。(OCPBUGS-44595)

- 以前は、OpenShift Container Platform Web コンソールのログインページでは、常に **Login** ボタンをクリックできました。ユーザー名やパスワードが入力されていない場合、あるいは **Login** ボタンがすでにクリックされた場合でも、クリックできました。このリリースでは、ユーザー名やパスワードが入力されていない場合に **Login** ボタンをクリックできないようにするため、**Login** ボタンは無効化されています。(OCPBUGS-43610)

- 以前は、**Operator installation** ステータスページで、名前のみで **PackageManifest** が選択されていました。場合によっては、名前の衝突が発生する可能性があるため、ロゴやプロバイダーの表示に誤った **PackageManifest** が使用されることがありました。このリリースにより、**PackageManifests** は名前とラベルセレクターによって選択され、現在のインストールに対して正しいものが選択されるようにします。その結果、Operator のインストールステータスページには、常に正しいロゴとプロバイダーが表示されます。(OCPBUGS-21755)

1.6.13. モニタリング

- 以前は、スクレイプが失敗すると、Prometheus は誤って次のスクレイプのサンプルを重複と見なし、破棄していました。この問題は、失敗直後のスクレイプにのみ影響し、その後のスクレイプは正しく処理されました。このリリースにより、失敗後のスクレイプが正しく処理されるようになり、有効なサンプルが誤って破棄されることがなくなりました。(OCPBUGS-53025)

1.6.14. ネットワーク

- 以前は、Pod が他の CNI プラグインと組み合わせて DHCP アドレスの割り当てに 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ている可能性がありました。その結果、Pod の DHCP リースの有効期限が切れると、新しいリースを再作成しようとして 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した。このリリースにより、ネットワークインターフェイスが存在しない場合に DHCP リースのメンテナンスが終了します。これにより、インターフェイスの削除は正常に処理され、ノードの安定性が確保されます。(OCPBUGS-45272)

- 以前は、**pluginPort** テンプレートの問題が原因で、Kubernetes NMState Operator は **nmstate-console-plugin** Pod を作成しませんでした。このリリースにより、テンプレートへの修正により、Operator が **nmstate-console-plugin** Pod を正常に作成できるようになりました。(OCPBUGS-54295)

- 以前は、Whereabouts リコンサイラーの Pod コントローラーは、リーダー選出機能に namespace を渡していなかったため、Pod コントローラーは孤立した割り当てを削除していませんでした。これにより、ログメッセージが繰り返されました。このリリースでは、namespace が渡され、孤立した割り当てが適切に削除されます。(OCPBUGS-53397)

- 以前は、**SriovOperatorConfig** Operator は、**SriovOperatorConfig** リソース内のデフォルト値を持つパラメーターをすべて削除していました。この状況が原因で、リソースの出力から特定の情報が欠落していました。このリリースにより、Operator が API サーバーに対して PATCH メソッドを使用するようになり、デフォルト値を持つパラメーターが保持されるため、リソースの出力に情報が欠落しなくなりました。(OCPBUGS-53346)

- 以前は、**SriovNetworkNodePolicy** オブジェクトリコンサイラーは、すべてのノードリソース更新で実行されていました。この結果、SR-IOV Operator の Pod が過剰にリソースを消費し、ログエントリーも大量に出力されるようになっていました。このリリースでは、ノードラベルが変更された場合にのみリコンサイラーが実行されるように動作が変更され、リソースの消費とログエントリーの生成が削減されます。(OCPBUGS-52955)

- 以前は、OpenShift Container Platform の最新バージョンにアップグレードする際に、同じ IP アドレスファミリーの複数のネットワークをリストした **clusterNetwork** パラメーターを持つクラスターが **crashloopbackoff** 状態になっていました。このリリースでは、修正により、この設定のクラスターがクラスタアップグレード時に **crashloopbackoff** 状態に陥らなくなりました。(OCPBUGS-49994)

- 以前は、**resolv-prepender** サービスが想定よりも早いタイミングでトリガーされていました。この状況によりサービスが失敗し、ホスト DNS は正しく設定されませんでした。このリリースにより、**resolv-prepender** サービスの設定が更新され、サービスが予想より早く起動してもホストの DNS 設定が誤って設定されることがなくなりました。(OCPBUGS-49436)

- 以前は、**nmstate-configuration** サービスは、**platform** パラメーターが **baremetal** に設定されたデプロイメントに対してのみ有効になっています。しかし、Assisted Installer を使用して、**platform** パラメーターを **None** に設定することにより、ベアメタルデプロイメントを設定することもできますが、NMState **br-ex** ネットワークブリッジ作成機能はこのインストール方法では機能しませんでした。このリリースにより、**nmstate-configuration** サービスがクラス

ターインストールパスのベースディレクトリーに移動され、**None** に設定された **platform** パラメーターで設定されたデプロイメントが、NMState **br-ex** ネットワークブリッジ作成機能に影響しないようになりました。(OCPBUGS-48566)

- 以前は、ゲートウェイモードが **local** に設定されているレイヤー 2 またはレイヤー 3 トポロジーネットワークでは、OVN-Kubernetes の再起動時に問題が発生していました。この問題により、Egress IP がネットワークのプライマリー IP アドレスとして選択されました。このリリースでは、修正によりこの動作が発生しなくなりました。(OCPBUGS-46585)

- 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、大文字で DNS 名を含むファイアウォールルールの作成が行われるようになります。(OCPBUGS-46564)

- 以前は、IPv6 プロトコル上の Egress 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、Pod はデュアルスタッククラスター内の OVN-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 アドレスファミリーのトラフィックがドロップされました。このリリースにより、Egress IP が適用された IP アドレスファミリーの 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-46543)

- 以前は、マニフェストオブジェクトのカスタマイズされた **br-ex** ネットワークブリッジ設定で静的 IP アドレスを使用すると、競合状態が追加され、クラスターのデプロイメントがさらに影響を受けるノードの再起動操作が発生していました。このリリースで、**nodeip-configuration** サービスが **br-ex** ネットワークブリッジの起動後に起動されるようになり、競合状態とノードの再起動が阻止されるようになりました。(OCPBUGS-46072)

- 以前は、HAProxy ルーターは、SHA1 リーフ証明書のみが HAProxy によって拒否されたと誤って想定し、SHA1 中間証明書を拒否しないことで失敗していました。この更新により、ルーターは自己署名以外の SHA1 証明書すべてを検査および拒否するようになりました。これにより、クラッシュが回避され、クラスターの安定性が向上します。(OCPBUGS-45290)

- 以前は、ノードが **openvswitch** デーモンを再起動すると、**nmstate-handler** コンテナーは OpenVSwitch (OVS) データベースにアクセスできず、すべての OVS 関連の NNCP 設定が失敗する原因となっていました。このリリースにより、この問題は修正されました。**nmstate-handler** コンテナーは、ノードで OVS プロセスを再起動した後でも、OVS データベースにアクセスできます。**nmstate-handler** では、手動の再起動が不要になりました。(OCPBUGS-44596)

- 以前は、クラスター設定で **protocol** パラメーターが指定されていても **port** パラメーターが指定されていない場合、**MultiNetworkPolicy** API は適用されませんでした。この状況では、すべてのネットワークトラフィックがクラスターに到達しました。このリリースにより、**MultiNetworkPolicy** API ポリシーは、特定のトラフィックのみがクラスターに到達するように、**protocol** パラメーターで指定されたポートとの間の接続のみを許可するようになりました。(OCPBUGS-44354)

- 以前は、HAProxy が設定をリロードした際、アイドル接続が開いたままになっており、クライアントがそのアイドル接続を使ってリクエストを送信するか、**hard-stop-after** の期間が経過するまで接続が終了しませんでした。このリリースでは、リロード中のアイドル接続の HAProxy 動作を制御するための新しい **IdleConnectionTerminationPolicy** API フィールドが追加されました。新しいデフォルト設定は **Immediate** です。これは、設定を再読み込みすると、HAProxy がアイドル状態の接続をすぐに終了することを意味します。以前の動作は、**IdleConnectionTerminationPolicy** の **Deferred** 設定を使用して指定できます。(OCPBUGS-43745)

- 以前は、ネットワーク MTU より大きい UDP パケットの送信中にアプリケーションが Path MTU 検出 (PMTUD) メカニズムを使用しなかった場合、**OVN** パッケージの問題により、パケットの断片化中にパケットがドロップされていました。このリリースにより、**OVN** パッケージが修正され、大規模な UDP パケットが適切に断片化されて、ネットワーク経由で送信されるようになりました。(OCPBUGS-43649)

- 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-43004)

- 以前は、実行中のクラスターに特定のネットワーク変更が加えられると、**ovs-configuration** サービスにより **NetworkManager** 接続プロファイルが永続的に作成され、プロファイルはストレージに誤って保存されていました。このプロファイルファイルは再起動後も保持され、**ovs-configuration** サービスが失敗する原因となっていました。このリリースでは、**ovs-configuration** のクリーンアッププロセスが更新され、不要なファイルが削除され、再起動後にこのようなファイルが原因となる問題が発生しなくなりました。(OCPBUGS-41489)

- 以前は、**parseIPList** 関数は、有効および無効な IP アドレスまたは CIDR 範囲を含む IP アドレスリストを処理できませんでした。この状況により、関数は無効なエントリーに遭遇した際に空の文字列を返し、有効なエントリーの処理を省略していました。このリリースにより、**haproxy.router.openshift.io/ip_allowlist** ルートアノテーションが無効な IP アドレスまたは CIDR 範囲を省略し、**parseIPList** 関数がリスト表示されるすべてのエントリーを処理できるようになりました。(OCPBUGS-39403)

- 以前は、HAProxy ルーターには **router.openshift.io/haproxy.health.check.interval** アノテーションの範囲外の検証がありませんでした。HAProxy ルーターが処理できる最大値を超える値を設定した場合、**router-default** Pod は **Ready** 状態になることができませんでした。このリリースにより、ルーターはアノテーションの値を検証し、範囲外の値を除外するようになりました。ルーターは期待どおりに機能するようになりました。(OCPBUGS-38078)

- 以前は、特定の状況では、ノードのゲートウェイ IP アドレスが変更され、クラスターサブネットへの静的ルートを管理する **OVN** クラスタールーターは、元の IP アドレスを削除せずに、新しいゲートウェイ IP アドレスを持つ新しい静的ルートを追加していました。その結果、古いルートが引き続きスイッチサブネットを指し、これにより Egress トラフィックの転送中に断続的なドロップが発生していました。このリリースでは、**OVN** クラスタールーターに適用されたパッチにより、ゲートウェイ IP アドレスが変更された場合に、**OVN** クラスタールーターは新しいゲートウェイ IP アドレスを使用して既存の静的ルートを更新するようになりました。古いルートは **OVN** クラスタールーターを指さなくなり、Egress トラフィックフローがドロップされなくなりました。(OCPBUGS-32754)

- 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、変換に失敗したエラーがログに記録されるようになりました。(OCPBUGS-29354)

- 以前は、PowerVS インストーラーは、サポートされているマシンタイプのハードコーディングされたリストを使用していました。ただし、このリストは、新しいタイプが追加されても常に更新されるわけではありませんでした。このリリースにより、データセンターがクエリーされ、サポートされているタイプの現在のリストを取得できるようになりました。(OCPBUGS-49940)

- 以前は、RootDiskHint が定義され、インストールが **Requested installation disk is not part**

of the host's valid disks エラーで失敗した場合、ヒントとして使用できる有効なディスク名を判断することが困難でした。このリリースにより、受け入れ可能なディスクのリストにロギングが追加され、ユーザーはルートディスクヒントを迅速に判別できるようになりました。(OCPBUGS-43578)

- 以前は、API サーバーの中断または一時的な接続の問題がある場合に、**oc adm node-image monitor** コマンドは EOF エラーを返していました。これにより、コマンドが終了しました。このリリースにより、このコマンドは API サーバーの中断および一時的な接続の問題を検出し、コマンドを終了することなく API サーバーに再接続するようになりました。(OCPBUGS-38975)

- 以前は、仮想マシン (VM) を作成し、IP プールに IP アドレスが存在しなかった場合は、仮想マシンは起動しませんでした。**virt-launcher-<vm_name>** Pod でエラーメッセージが生成されましたが、このメッセージは問題の原因を明確に説明していませんでした。このリリースにより、IP プールに IP アドレスが存在しないという状況の場合、**virt-launcher-<vm-name>** Pod には、次の例のような明確なエラーメッセージが含まれます。

> Warning ErrorAllocatingPod 4s (x7 over 79s) ovnk-controlplane failed to update pod localnet-ipam/virt-launcher-vmb-localnet-ipam-hlnmf: failed to assign pod addresses for localnet-ipam/ipam-localnet-nad/localnet-ipam/virt-launcher-vmb-localnet-ipam-hlnmf: failed to allocate new IPs for tenantblue-network: subnet address pool exhausted

(OCPBUGS-54245)

1.6.15. ノード

- 以前は、クラスターが Zscaler を使用してすべての転送をスキャンした場合、イメージをプルするときにタイムアウトが発生することがありました。この問題は、イメージプルのハードコーディングされたタイムアウト値が原因でした。CRI-O のプル進捗タイムアウトが 30 秒に増えました。その結果、これまで影響を受けていたクラスターでタイムアウトは発生しなくなります。(OCPBUGS-54662)

- 以前は、**container_logreader_t** SELinux ドメインを使用して **/var/log** の場所にあるホスト上のコンテナーログを監視したコンテナーは、ログにアクセスできませんでした。この動作は、**var/log/containers** の場所のログがシンボリックリンクであるために発生しました。この修正により、コンテナーは予想通りにログを監視できます。(OCPBUGS-48555)

- 以前は、ファイルがループ操作にあるときに、**json.NewDecoder** ファイルで end-of-file エラーが発生しました。このエラーにより、複数の namespace に存在する namespace ポリシーへのアプリケーションの更新が一貫性のない状態になっていました。この問題は、クラスターにセキュリティー上の脆弱性を引き起こす可能性がありました。このリリースでは、各ループ操作に入る際に新しいポリシーバッファーが **json.NewDecoder** ファイルに追加され、複数の namespace にテストケースが追加されました。その結果、ポリシーバッファーは JSON ポリシーファイルに対して堅牢なデコードプロセスを提供するため、namespace ポリシーは問題なく更新を受け取ることができます。(OCPBUGS-48195)

- 以前は、イメージ参照ダイジェストの計算に問題があり、**schemaVersion 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。この問題により、新しいデプロイメントを作成できませんでした。このリリースにより、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-42844)

- 以前は、**policy.json** ファイル内のペイロードイメージの Sigstore 検証を使用するテクノロジープレビュー対応クラスターの場合、ベースイメージの Podman バージョンは Sigstore 設定をサポートしていませんでした。このサポートがないため、新規ノードが使用できなくなりま

した。このリリースにより、問題が修正され、ノードが使用可能になりました。(OCPBUGS-38809)

- 以前は、ノードに最後に割り当てられた Guaranteed Pod の CPU が、その Pod の削除後も残っていました。この動作により、スケジューリングドメインの不整合が発生していました。このリリースにより、保証された Pod に割り当てられた CPU が期待どおりに使用可能な CPU リソースのプールに戻り、後続の Pod が正しく CPU スケジューリングされるようになります。(OCPBUGS-17792)

1.6.16. Node Tuning Operator (NTO)

- 以前は、パフォーマンスプロファイルをノードに適用する際に、OpenShift Container Platform はノード上の CPU ユニットのベンダー識別子に基づいて、適切なプロファイルを選択していました。このため、認識されない別のベンダー識別子が CPU で使用されている場合、OpenShift Container Platform は適切なプロファイルを組み込むことができませんでした。たとえば、識別子には ARM ではなく APM が含まれる場合がありました。この修正により、ARM アーキテクチャーを使用する CPU の場合、Operator はベンダー識別子ではなく、アーキテクチャーのみに基づいてプロファイルを選択するようになりました。その結果、正しいプロファイルが適用されるようになりました。(OCPBUGS-52352)

1.6.17. 可観測性

- 以前は、**Silence details** ページには **namespace** パラメーターが欠落している誤ったリンク URL があり、これにより、ユーザーは特定バージョンの dev コンソールで特定のアラートをサイレンスにできませんでした。その結果、アラート管理が不十分になりました。このリリースにより、**SilencedAlertsList** の未定義のリンクがアクティブな namespace を使用して修正されました。その結果、'No Alert found' というエラーが解決され、OpenShift Container Platform Monitoring の **Alert details** ページに正しく移動できるようになりました。(OCPBUGS-48142)

- 以前は、コンソールの更新により PatternFly 4 が非推奨となった結果、モニタリングプラグインのテーブルレイアウトが正しくレンダリングされなくなっていました。このリリースにより、テーブルとスタイルが PatternFly 5 にアップグレードされ、正しくレンダリングされるようになりました。(OCPBUGS-47535)

- 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-45896)

- 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** チェックがなくなっていました。チェックが欠落していたために、**Show all Series** と **Hide all Series** 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-45816)

- 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。この問題のため、Web コンソールで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-45801)

- 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-45174)

1.6.18. oc-mirror

- 以前は、oc-mirror プラグイン v2 では、ローカルキャッシュの作成フェーズ中に進行状況の出力が表示されていませんでした。多数のイメージが関係するミラー設定の場合、これによりプロセスが応答しなくなったり、停止したりする可能性があります。この更新により、キャッシュの作成ステータスを示す進行状況バーが追加され、ユーザーはキャッシュ作成における最新の進行状況を確認できるようになりました。(OCPBUGS-56563)

- 以前は、oc-mirror プラグイン v2 を使用して Operator をミラーリングする場合、チャネルグラフ内に **skips** および **replaces** エントリーの長いリストを持つ一部のコミュニティー Operator によって、ミラーリングプロセスでメモリー不足が発生し、失敗していました。この更新により、oc-mirror プラグイン v2 は、複数の **skips** および **replaces** スタンザで参照されるエントリーの繰り返の評価を回避することでフィルタリングロジックを改善し、Operator ミラーリング中のメモリー処理が改善されました。(OCPBUGS-52471)

- 以前は、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、以前の実行からの既存の **tar** アーカイブファイルは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。この更新により、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、作業ディレクトリーに現在の実行からのアーカイブのみが含まれるようにします (OCPBUGS-56433)。

- 以前は、イメージのコピー中にソースレジストリーが、502、503、504 のいずれかの HTTP ステータスコードで応答した場合、oc-mirror プラグイン v2 はエラーで終了していました。この更新により、oc-mirror プラグイン v2 は、これらの一時的なサーバーエラーが発生すると、コピー操作を自動的に再試行します。(OCPBUGS-56185)

- 以前は、参照にタグとダイジェストの両方が含まれるコンテナーイメージを含む Helm チャートをミラーリングすると、oc-mirror プラグイン v2 は次のエラーで失敗していました。

  > Docker references with both a tag and digest are currently not supported.

  この更新により、oc-mirror プラグイン v2 は、タグとダイジェストの両方を使用してイメージを参照する Helm チャートをサポートするようになりました。このツールは、ダイジェストをソースとして使用してイメージをミラーリングし、宛先にタグを適用します。(OCPBUGS-54891)

- 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-54653)

- 以前は、**ImageSetConfiguration** ファイルで無効な Operator が指定されている場合、mirror-to-disk (m2d) フェーズ中に空のカタログをミラーリングすることが可能でした。これにより、後続の disk-to-mirror (d2m) フェーズで障害が発生しました。このリリースにより、oc-mirror プラグイン v2 は、設定で Operator 参照を検証することで空のカタログのミラーリングを阻止し、ミラーリングプロセスの信頼性を高めます。(OCPBUGS-52588)

- 以前は、**--dry-run** フラグを使用して oc-mirror プラグイン v2 を使用すると、作業ディレクトリー内の **cluster-resources** フォルダーがクリアされていました。その結果、**idms-oc-mirror.yaml** や **itms-oc-mirror.yaml** などの以前に生成されたファイルが削除されました。この

リリースにより、ドライラン操作中に **cluster-resources** フォルダーがクリアされなくなり、以前に生成された設定ファイルが保持されるようになりました。(OCPBUGS-50963)

- 以前は、oc-mirror プラグイン v2 は、ミラーリングエラーが発生した場合でも、終了ステータス **0** (成功) を返していました。その結果、自動化されたワークフローでの oc-mirror プラグイン v2 の実行失敗が検出されない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 が更新され、ミラー障害が発生したときに **0** 以外の終了ステータスを返すようになりました。この修正が適用されていても、自動化されたワークフローにおいては終了ステータスのみに依存すべきではありません。潜在的な問題を特定するために、oc-mirror プラグイン v2 によって生成された **mirroring_errors_XXX_XXX.txt** ファイルをユーザーが手動で確認することが推奨されます。(OCPBUGS-49880)

- 以前は、宛先または **--from** パスフラグで **release-images** などの内部 oc-mirror 予約キーワードを使用してミラーリングすると、操作が失敗したり、予期しない動作を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、宛先パスまたはソースパスで使用される予約キーワードを正しく処理します。(OCPBUGS-42862)

1.6.19. OpenShift CLI (oc)

- 以前は、**oc adm node-image** コマンドを使用して非接続環境にノードを追加しようとすると、プライベートレジストリーイメージがコマンドにアクセスできず、ノードの追加が失敗していました。このエラーは、クラスターが最初に (mirror.openshift.com) からダウンロードされたインストーラーバイナリーを使用してインストールされた場合にのみ発生しました。このリリースにより、非接続環境でイメージのプルとノードの作成を正常に実行できる修正が実装されました。(OCPBUGS-53106)

- 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** が大きすぎて処理できず、ノードの追加に失敗しました。このリリースにより、**additionalTrustBundle** の生成時に組み込み証明書が除外されるため、明示的にユーザーが設定した証明書のみが含まれ、ノードを正常に追加できるようになります。(OCPBUGS-43990)

- 以前は、**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-44857)

- 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-45311)

1.6.20. Operator Lifecycle Manager (OLM)

- 以前は、Operator に必要な **olm.managed=true** ラベルがない場合、Operator は失敗し、**CrashLoopBackOff** 状態になる可能性がありました。この現象が発生すると、ログにはステータスがエラーとして報告されませんでした。その結果、障害の診断が困難になりました。この更新により、このタイプの障害はエラーとして報告されます。(OCPBUGS-56034)

- 以前は、Machine Config Operator (MCO) は、イメージのマウントに必要な証明書を **/etc/docker/certs.d** ディレクトリーで検索しませんでした。その結果、Operator Controller と catalogd は、このディレクトリーにホストされている証明書にアクセスできなかったため、起動に失敗しました。この更新により、この問題は解決されました。(OCPBUGS-54175)

- このリリース前は、クラスター拡張機能の更新が、**CRDUpgradeCheck** リソースからの **unknown change, refusing to determine that change is safe** というエラーで失敗することがありました。このエラーは、OLM v1 がバージョンスキーマ間の差異を計算する方法が原因で発生しました。この更新でこの問題が修正されています。(OCPBUGS-53019)

- 以前は、Operator Controller が CA 証明書を適切にマウントできない場合がありました。その結果、Operator Controller は TLS 証明書検証エラーのために catalogd への接続に失敗しました。この更新でこの問題が修正されています。(OCPBUGS-49860)

- 以前は、OLM v1 は、Operator Controller と catalogd Pod をマウントする前に、証明書が ready 状態になるまで待機しませんでした。これらの更新により、この問題は修正されます。OCPBUGS-48830 および (OCPBUGS-49418)

- 以前は、OLM v1 では、Operator バンドル内のクラスター拡張機能の作成者によって提供されたすべてのメタデータが適用されませんでした。その結果、OLM v1 では、**metadata/properties.yaml** ファイルで指定された更新制約などのプロパティーは適用されませんでした。この更新でこの問題が修正されています。(OCPBUGS-44808)

1.6.21. Operator Controller Manager

- 以前は、デフォルトのプロキシー設定に関係なく、ビルドコンテナーに **HTTP_PROXY**、**http_proxy**、**HTTPS_PROXY**、**https_proxy**、**NO_PROXY**、および **no_proxy** 変数が設定されていました。このリリースにより、変数は、デフォルトで定義され、null でない場合にのみ追加されます。(OCPBUGS-55642)

- 以前は、内部 Image Registry 用に生成されたイメージプルシークレットは、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は短い間無効になっていました。このリリースにより、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-50507)

- 以前は、OLM v1 はイメージのマウントに必要な証明書を **/etc/docker/** ディレクトリーで検索していませんでした。その結果、OLM v1 はカスタム証明書をマウントできませんでした。この更新でこの問題が修正されています。(OCPBUGS-48795)

- 以前は、OLM v1 は、リーダー選出などの定期的なクラスターメンテナンス中に発生する一時的な停止時にエラーメッセージを送信していました。この更新でこの問題が修正されています。(OCPBUGS-48765)

- 以前は、Operator Lifecycle Manager (OLM) Classic は、同じ namespace で Operator を同時に調整しようとしたときに、**Subscription** リソースに誤って障害を報告していました。この問題が発生すると、Operator のインストールが失敗しました。この更新でこの問題が修正されています。(OCPBUGS-48486)

- 以前は、OLM (Classic) は、サブスクリプションを調整するときに、インストールされているすべての Operator のカタログソースのスナップショットを取得していました。この動作により、CPU 使用率が高くなっていました。この更新により、OLM (Classic) はカタログソースをキャッシュし、gRPC Remote Procedure Calls (gRPC) サーバーへの呼び出しを制限して問題を解決します。(OCPBUGS-48468)

1.6.22. Performance Addon Operator

- 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-45264)

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。

- 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-44372)

1.6.23. Samples Operator

- 以前は、条件が変更されていない場合でも、Samples Operator は **Progressing** 条件の **lastTransitionTime** 仕様を更新していました。これにより、Operator は実際よりも不安定に表示されました。このリリースにより、**lastTransitionTime** 仕様は **Progressing** 条件が変更された場合にのみ更新されます。(OCPBUGS-54591)

- 以前は、**Progressing** 状態のイメージストリーム名がソートされていなかったため、不要な更新が発生していました。これにより、ユーザーが過度に更新され、システムパフォーマンスを低下させる原因となっていました。このリリースでは、**activeImageStreams** 関数が失敗したイメージのインポートをソートするようになりました。このアクションにより、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す。(OCPBUGS-54590)

- 以前は、Samples Operator はすべてのクラスター Operator の監視を確立し、いずれかの Operator が変更されると Samples Operator の同期ループが実行されていました。このリリースにより、Samples Operator は監視する必要がある Operator のみを監視します。(OCPBUGS-54589)

1.6.24. ストレージ

- 以前は、**oc adm top pvc** コマンドを使用しても、プロキシーを含むクラスターや非接続環境内のクラスターなど、ネットワーク設定が制限されているクラスターの永続ボリューム要求 (PVC) の使用状況統計は表示されませんでした。このリリースにより、これらの環境内のクラスターの使用状況の統計情報を取得できるようになります。(OCPBUGS-54168)

- 以前は、vCenter アドレスが正しくない場合、VMware vSphere CSI ドライバー Operator がパニックモードになりました。このリリースにより、この問題は解決されました。(OCPBUGS-43273)

- 以前は、C3-standard-2、C3-standard-4、N4-standard-2、N4-standard-4 ノードを含む Google Cloud Persistent Disk クラスターが、接続可能なディスクの最大数 (16) を誤って超過することがあり、その結果、ボリュームを Pod に正常に作成またはアタッチできなくなる可能性がありました。このリリースにより、上限を超えることがなくなり、その結果、ボリュームの作成や Pod へのアタッチが正常に行えるようになりました。(OCPBUGS-39258)

- 以前は、永続ボリューム (PV) が削除されると、Local Storage Operator (LSO) はシンボリックリンクを確実に再作成しませんでした。このリリースにより、PV を作成するときに、新しいシンボリックリンクを見つける前に、以前に指定されたシンボリックリンクが選択されます。(OCPBUGS-31059)

- 以前は、Cloud Credential Operator (CCO) が Container Storage Interface (CSI) ドライバー Operator に認証情報を提供しなかった場合、CSI ドライバー Operator は無期限で **Progressing=true** のままとなり、**operator is waiting for deployment/unavailable** というメッセージが表示されていました。このリリースにより、Progressing の状態が 15 分以上になると、Operator は **Degraded=True** に変更されます。(OCPBUGS-24588)

- 以前は、名前が 53 文字のコンピュートノードと、hostpath Container Storage Interface (CSI) ドライバーを使用する場合、external-provisioner で **--enable-node-deployment flag** を使用するとボリュームのプロビジョニングが失敗していました。このリリースにより、この問題は解決され、コンピュートノード名の長さに制限がなくなりました。(OCPBUGS-49805)

- 以前は、Azure Red Hat OpenShift で Hosted Control Plane を使用してホステッドクラスターを作成すると、Azure Disk Container Storage Interface (CSI) ドライバーはボリュームを正常にプロビジョニングしませんでした。このリリースにより、この問題は解決され、Azure Disk CSI ドライバーはボリュームを正常にプロビジョニングできるようになりました。(OCPBUGS-46575)

- 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-46038)

- 以前は、指定されたラベルを使用してホステッドクラスターを作成すると、AWS EBS ドライバー、Driver Operator、スナップショットコントローラー、およびスナップショット Webhook Pod には、これらの指定されたラベルが伝播されませんでした。このリリースにより、指定されたラベルが伝播されます。(OCPBUGS-45073)

- 以前は、Manila Container Storage Interface (CSI) ドライバーのサービスが意図しないホストで実行されていました。これは、Manila CSI ドライバーがコントローラーとノード (ワーカー) サービスの両方に、単一のバイナリーを使用するために発生しました。このリリースにより、CSI ドライバーコントローラー Pod はコントローラーサービスのみを実行し、CSI ドライバーノード Pod はノードサービスのみを実行します。(OCPBUGS-54447)

- 以前は、Container Storage Interface (CSI) Operator は、将来的に致命的となる欠落項目に関する警告をログに発行していました。このリリースにより、警告は発行されなくなりました。(OCPBUGS-44374)

- 以前は、vCenter アドレスが正しくない場合、VMWare vSphere CSI ドライバー Operator がパニックを起こしていました。このリリースにより、この問題は解決されました。(OCPBUGS-43273)

1.6.25. Red Hat Enterprise Linux CoreOS (RHCOS)

- 以前は、**GRUB** ブートローダーは RHCOS ノード上で自動的に更新されませんでした。その結果、ノードが RHEL 8 に作成され、その後 RHEL に更新された場合、**GRUB** は古い **GRUB** バージョンでサポートされていない形式を使用するため、カーネルを読み込むことができませんでした。このリリースにより、OpenShift Container Platform 4.18 への更新中に **GRUB** ブートローダーの更新がノード上で強制されるため、この問題は OpenShift Container Platform 4.19 では発生しません。(OCPBUGS-55144)

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**
- **削除済み**

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	4.17	4.18	4.19
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
外部 OIDC アイデンティティープロバイダーを使用した直接認証	利用不可	利用不可	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	4.17	4.18	4.19
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

機能	4.17	4.18	4.19
TPM と PCR の保護によるディスク暗号化の有効化	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
ローカルアービターノードの設定	利用不可	利用不可	テクノロジープレビュー

1.7.3. 拡張機能のテクノロジープレビュー機能

表1.20 拡張機能のテクノロジープレビュートラッカー

機能	4.17	4.18	4.19
Operator Lifecycle Manager (OLM) v1	テクノロジープレビュー	一般提供	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	テクノロジープレビュー	テクノロジープレビュー
クラスター拡張機能の OLM v1 パーミッション事前チェック	利用不可	利用不可	テクノロジープレビュー
指定された namespace にクラスター拡張機能をデプロイする OLM v1	利用不可	利用不可	テクノロジープレビュー

1.7.4. インストールのテクノロジープレビュー機能

表1.21 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	4.17	4.18	4.19
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	一般提供	一般提供	一般提供
Google Cloud のユーザー定義ラベルとタグ	一般提供	一般提供	一般提供

機能	4.17	4.18	4.19
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
機密仮想マシンを使用して Microsoft Azure にクラスターをインストールする	利用不可	テクノロジープレビュー	一般提供
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
vSphere ホストグループに対する OpenShift ゾーンのサポート	利用不可	利用不可	テクノロジープレビュー
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	一般提供	一般提供	一般提供
Google Cloud で user-provisioned DNS を有効にする	利用不可	利用不可	テクノロジープレビュー
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	テクノロジープレビュー	テクノロジープレビュー
Bare Metal as a Service の使用	利用不可	利用不可	テクノロジープレビュー

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

表1.22 Machine Config Operator のテクノロジープレビュートラッカー

機能	4.17	4.18	4.19
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
Image Mode for OpenShift/クラスター上の RHCOS イメージレイヤー化	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

機能	4.17	4.18	4.19
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	一般提供[1]

1. この機能は、OpenShift Container Platform 4.19.12 から GA になります。以前の 4.19.x バージョンはテクノロジープレビューのままです。

1.7.6. マシン管理のテクノロジープレビュー機能

表1.23 マシン管理のテクノロジープレビュートラッカー

機能	4.17	4.18	4.19
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	テクノロジープレビュー	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
ベアメタル向け Cluster API を使用したマシンの管理	利用不可	利用不可	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	テクノロジープレビュー	テクノロジープレビュー

機能	4.17	4.18	4.19
マシンセットを使用して Microsoft Azure 仮想マシンの Trusted Launch を設定する	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
マシンセットを使用した Azure 機密仮想マシンの設定	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

1.7.7. モニタリングのテクノロジープレビュー機能

表1.24 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	4.17	4.18	4.19
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	一般提供

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	4.17	4.18	4.19
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
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	テクノロジープレビュー	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	4.17	4.18	4.19
eBPF マネージャー 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
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	一般提供
SR-IOV VF のホストネットワーク設定	一般提供	一般提供	一般提供
MetalLB と FRR-K8 のインテグレーション	一般提供	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	一般提供	一般提供	一般提供
PTP イベント REST API v2	一般提供	一般提供	一般提供
ベアメタル上の OVN-Kubernetes の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
vSphere と RHOSP 上の OVN-Kubernetes のカスタマイズされた **br-ex** ブリッジ	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
OpenShift SDN から OVN-Kubernetes へのライブマイグレーション	一般提供	利用不可	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	テクノロジープレビュー	一般提供	一般提供

機能	4.17	4.18	4.19
Dynamic Configuration Manager	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
Intel C741 Emmitsburg Chipset の SR-IOV Network Operator 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
ARM アーキテクチャーでの SR-IOV Network Operator のサポート	利用不可	一般提供	一般提供
Ingress 管理用の Gateway API と Istio	利用不可	テクノロジープレビュー	一般提供
PTP 通常クロック用デュアルポート NIC	利用不可	利用不可	テクノロジープレビュー
DPU Operator	利用不可	利用不可	テクノロジープレビュー
Whereabouts IPAM CNI プラグイン用の高速 IPAM	利用不可	利用不可	テクノロジープレビュー
番号のない BGP ピアリング	利用不可	利用不可	テクノロジープレビュー

1.7.10. ノードの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	4.17	4.18	4.19
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	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

1.7.11. 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	4.17	4.18	4.19
oc-mirror プラグイン v2	テクノロジープレビュー	一般提供	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	一般提供	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	一般提供	一般提供

1.7.12. 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機能

表1.29 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	4.17	4.18	4.19
Operator Lifecycle Manager (OLM) v1	テクノロジープレビュー	一般提供	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	削除済み	削除済み
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	削除済み	削除済み

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

表1.30 RHOSP のテクノロジープレビュートラッカー

機能	4.17	4.18	4.19
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	一般提供	一般提供	一般提供

機能	4.17	4.18	4.19
RHOSP 17.1 上の Hosted Control Plane	利用不可	利用不可	テクノロジープレビュー

1.7.14. 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機能

表1.31 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	4.17	4.18	4.19
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	一般提供
NUMA 対応スケジューリングが Hosted Control Plane でサポートされる	利用不可	利用不可	テクノロジープレビュー

1.7.15. ストレージのテクノロジープレビュー機能

表1.32 ストレージのテクノロジープレビュートラッカー

機能	4.17	4.18	4.19
AWS EFS ストレージ CSI 使用状況メトリクス	一般提供	一般提供	一般提供

機能	4.17	4.18	4.19
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	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 のクロスサブスクリプションサポート	利用不可	利用不可	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
Secrets Store CSI Driver Operator	テクノロジープレビュー	一般提供	一般提供
CIFS/SMB CSI Driver Operator	テクノロジープレビュー	一般提供	一般提供
VMware vSphere 複数 vCenter のサポート	テクノロジープレビュー	一般提供	一般提供
vSphere でのストレージの無効化/有効化	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
vSphere のノードあたりのボリュームの最大数の増加	利用不可	利用不可	テクノロジープレビュー
RWX/RWO SELinux マウント	開発者プレビュー	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	開発者プレビュー	開発者プレビュー	一般提供
CSI ボリュームグループスナップショット	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
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	一般提供	一般提供
GCP Filestore による Workload Identity のサポート	一般提供	一般提供	一般提供

機能	4.17	4.18	4.19
OpenStack Manila による CSI サイズ変更のサポート	利用不可	一般提供	一般提供
Volume Attribute Classes	利用不可	利用不可	テクノロジープレビュー

1.7.16. Web コンソールのテクノロジープレビュー機能

表1.33 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	4.17	4.18	4.19
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

1.8. 既知の問題

- OpenShift Container Platform 4.19 では、ネットワーク暗号化に IPsec を使用するクラスターで、Pod 間の接続が断続的に失われる可能性があります。これにより、特定のノード上の一部の Pod が他のノード上のサービスに到達できなくなり、接続タイムアウトが発生します。内部テストでは、120 ノード以下のクラスターではこの問題を再現できませんでした。この問題に対する回避策はありません。(OCPBUGS-55453)

- メキシコ中部リージョン (**mx-central-1**) の AWS にインストールされている OpenShift Container Platform クラスターは、破棄できません。(OCPBUGS-56020)

- Azure にクラスターをインストールするときに、**compute.platform.azure.identity.type**、**controlplane.platform.azure.identity.type**、または **platform.azure.defaultMachinePlatform.identity.type** フィールド値のいずれかを **None** に設定すると、クラスターは Azure Container Registry からイメージをプルできません。この問題は、ユーザーが割り当てたアイデンティティーを提供するか、アイデンティティーフィールドを空白のままにすることで回避できます。どちらの場合も、インストールプログラムはユーザーが割り当てたアイデンティティーを生成します。(OCPBUGS-56008)

- 以前は、kubelet は、定期的に Pod の状態をチェックし、通常のプローブ期間外で Readiness プローブを実行する **syncPod** メソッドで実行されたプローブを考慮していませんでした。このリリースにより、kubelet が **readinessProbe** 期間を誤って計算するバグが修正されました。ただし、Pod 作成者は、Readiness プローブが設定された Pod の Readiness レイテンシーが増加する可能性があることに気付く場合があります。この動作は、設定されたプローブに対してより正確です。詳細は、(OCPBUGS-50522) を参照してください。

- 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)

- AWS にクラスターをインストールするときに、**openshift-install create** コマンドを実行する前に AWS 認証情報を設定しないと、インストールプログラムは失敗します。(OCPBUGS-56658)

- **must-gather** ツールは、OpenShift Container Platform 4.14 からアップグレードされたクラスターの IPsec 情報を収集しません。この問題は、**networks.operator.openshift.io cluster** CR の **ipsecConfig** 設定に空のコンストラクト **{}** があるために発生します。空のコンストラクトは、OpenShift Container Platform のアップグレードされたバージョンに渡されます。この問題を回避するには、Cluster Network Operator (CNO) CR で次の **ipsecConfig** 設定を使用して、以下のコマンドを実行します。

```
$ oc patch networks.operator.openshift.io cluster --type=merge -p \
  '{
  "spec":{
    "defaultNetwork":{
      "ovnKubernetesConfig":{
        "ipsecConfig":{
          "mode":"Full"
        }}}}}'
```

  コマンドを実行すると、CNO は検査可能な **must-gather** ログを収集します。

  (OCPBUGS-52367)

- Gateway API と Amazon Web Services (AWS)、Google Cloud、Microsoft Azure プライベートクラスターには既知の問題があります。ゲートウェイにプロビジョニングされるロードバランサーは常に外部として設定されるため、エラーや予期しない動作が発生する可能性があります。

  - AWS プライベートクラスターでは、ロードバランサーが **pending** 状態のままになり、**Error syncing load balancer: failed to ensure load balancer: could not find any suitable subnets for creating the ELB** というエラーを報告します。

  - Google Cloud および Azure プライベートクラスターでは、ロードバランサーは外部 IP アドレスを持つべきではないにもかかわらず、外部 IP アドレス付きでプロビジョニングされます。

  この問題に対して、サポートされている回避策はありません。(OCPBUGS-57440)

- クラッシュが発生した場合、**mlx5_core** NIC ドライバーによってメモリー不足の問題が発生し、**kdump** は **vmcore** ファイルを **/var/crash** に保存しません。**vmcore** ファイルを保存するには、**crashkernel** 設定を使用して、**kdump** カーネル用に 1024 MB のメモリーを予約します。(OCPBUGS-54520、RHEL-90663)

- 第 4 世代 Intel Xeon プロセッサーには、既知のレイテンシーの問題があります。(OCPBUGS-42495)

- 現在、**guaranteed** QoS クラスを使用し、CPU 全体を要求する Pod は、ノードの再起動または kubelet の再起動後に自動的に再起動しない可能性があります。この問題は、静的 CPU Manager ポリシーが設定され、**full-pcpus-only** 仕様を使用しているノードで発生する可能性があるほか、ノード上の CPU のほとんどまたはすべてがこのようなワークロードによってすでに割り当てられている場合に発生する可能性があります。回避策として、影響を受ける Pod を手動で削除して再作成します。(OCPBUGS-43280)

- 現在、特定の AArch64 マシンで **irqbalance** サービスを実行すると、バッファーオーバーフローの問題によりサービスがクラッシュする可能性があります。その結果、レイテンシーの影

響を受けやすいワークロードは、CPU 間で適切に分散されていない未管理の割り込みの影響を受け、パフォーマンスの低下を招く可能性があります。現在、この問題に対する回避策はありません。(RHEL-89986)

- 現在、SR-IOV ネットワーク Virtual Function が設定されているクラスターでは、ネットワークデバイスの名前変更をするシステムサービスと、Node Tuning Operator によって管理される TuneD サービスの間で競合状態が発生する可能性があります。その結果、ノードの再起動後に TuneD プロファイルが degraded 状態となり、パフォーマンスが低下する可能性があります。回避策として、TuneD Pod を再起動してプロファイルの状態を復元します。(OCPBUGS-41934)

- RHEL-83435 により、VMware vSAN ファイルからエクスポートされる NFS ボリュームは、OpenShift Container Platform 4.19 を実行しているクラスターではマウントできません。この問題を回避するには、VMware ESXi および vSAN が 8.0 P05 以降の最新のパッチバージョンで実行されていることを確認してください。(OCPBUGS-55978)

1.9. 非同期エラータの更新

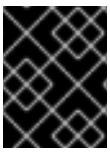
OpenShift Container Platform 4.19 のセキュリティー、バグ修正、機能拡張の更新は、Red Hat Network を通じて非同期エラータとしてリリースされます。すべての OpenShift Container Platform 4.19 エラータは、Red Hat カスタマーポータルから入手できます。非同期エラータは、OpenShift Container Platform ライフサイクル を参照してください。

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 4.19 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 4.19.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-2025:22278 - OpenShift Container Platform 4.19.20 のバグ修正アドバイザリー

発行日: 2025 年 12 月 2 日

OpenShift Container Platform リリース 4.19.20 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:22278 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-2025:22276 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 4.19.20 --pullspecs
```

1.9.2. バグ修正

このリリースでは次のバグが修正されました。

- この更新前は、NMState が管理する **br-ex** インターフェイスを持つノードで NetworkManager が再起動またはクラッシュすると、ノードがネットワーク接続を失っていました。このリリースでは、ディスパッチャースクリプトにフォールバックチェックが追加されました。これにより、標準の **br-ex** ブリッジ ID が見つからない場合に **br-ex-br** ブリッジ ID をチェックすることで、NMState が管理する **br-ex** インターフェイスを検出できます。その結果、NetworkManager が再起動またはクラッシュしても、このタイプのインターフェイスを持つノードがネットワーク接続を失うことがなくなりました。(OCPBUGS-62168)

- この更新前は、ミラー操作中に、**oc-mirror** が実行可能プログラムコードまたはスクリプトを含まない一部の同期ファイルに実行可能プログラムフラグを誤って設定し、予期しない実行が発生する可能性がありました。このリリースでは、同期ファイルから意図しない実行可能プログラムフラグが削除されました。その結果、正しいファイル権限が設定され、同期ファイルの意図しない実行が防止されます。(OCPBUGS-64683)

- この更新前は、Web コンソールの動的プラグインによって作成されたページに直接移動すると、Web コンソールが別の URL にリダイレクトされる可能性がありました。このリリースでは、URL リダイレクトが削除されました。(OCPBUGS-64834)

- この更新前は、**ccoctl** ユーティリティーは **CloudFront** ディストリビューションの取得時にページ区切りをサポートしませんでした。その結果、削除対象のディストリビューションが最初の結果バッチに含まれていなければ、**ccoctl** Amazon Web Services (AWS) の削除操作中に、**CloudFront** ディストリビューションとそれに関連付けられたオリジンアクセスアイデンティティーを正常に削除できませんでした。このリリースでは、**CloudFront** ディストリビューションの取得時に **ccoctl** ユーティリティーにページ区切りのサポートが追加され、ディストリビューションを適切に見つけて削除できるようになりました。(OCPBUGS-65478)

- この更新前は、Redfish Power インターフェイスの競合状態により、同時アクセス中に電源操作が失敗していました。その結果、ユーザーは電源状態を確実に管理できませんでした。このリリースでは、Redfish Power インターフェイスの競合状態が解決され、電源操作が正常に実行されるようになりました。その結果、ユーザーは電源状態を確実に管理できるようになりました。(OCPBUGS-65572)

- この更新前は、Pod のノードアフィニティーがコントロールプレーンノードのみを受け入れたため、**--node-name** 引数が使用された場合に **must-gather** Pod を特定のワーカーノードにスケジュールできませんでした。このリリースでは、**--node-name** 引数が設定されている場合にノードアフィニティーが設定されないように **must-gather** ロジックが更新されました。(OCPBUGS-65594)

1.9.3. 更新

OpenShift Container Platform 4.19 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-2025:21363 - OpenShift Container Platform 4.19.19 のバグ修正アドバイザリー

発行日: 2025 年 11 月 19 日

OpenShift Container Platform リリース 4.19.19 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:21363 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-2025:21361 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 4.19.19 --pullspecs
```

1.9.5. バグ修正

このリリースでは次のバグが修正されました。

- この更新前は、ロケールの不一致により、フランスのユーザーにスペイン語のログイン画面が表示されていました。その結果、ユーザーインターフェイスにはフランス語ではなくスペイン語という誤った言語が表示されました。このリリースでは、フランス語ユーザー向けログイン画面の言語が修正されました。その結果、フランスのユーザー向けにはログイン画面がフランス語で表示され、ローカリゼーションが改善しました。(OCPBUGS-58892)

- この更新前は、ボンディングされたネットワーク設定により **bootMACAddress** 設定がないという設定エラーが発生し、Ironic API サービスへのホスト登録ができませんでした。その結果、設定が不足しているため、ユーザーは Ironic サービスにホストを登録できませんでした。このリリースでは、Ironic サービスエージェント登録のボンディングされたネットワーク MAC の一貫性が復元されました。その結果、ボンディングされたネットワーク MAC の一貫性が正常になり、Assisted Installer でのホスト登録が成功します。(OCPBUGS-62441)

- この更新前は、Control Plane Operator (CPO) が Cluster Version Operator (CVO) のオーバーライドされたイメージを誤って使用していました。その結果、ユーザーは CVO のデプロイメントに間違ったイメージを使用していました。このリリースでは、CVO は CVO のイメージオーバーライドを正しく使用します。その結果、CVO のデプロイメントには正しいイメージが使用されます。(OCPBUGS-62959)

- この更新前は、**AlertmanagerConfig** カスタムリソース定義内の Secret 参照オブジェクトが適切ではなかったため、User Workload Monitoring Prometheus Operator が Kubernetes API に過度にアクセスしていました。その結果、User Workload Monitoring によって Kubernetes API が過負荷になり、プライマリーノードの CPU 使用率が増加しました。このリリースでは、User Workload Monitoring Prometheus Operator での過剰な Secret オブジェクト **GET** 要求が削減されました。その結果、プライマリーノード上の API 負荷が最適化されました。(OCPBUGS-63197)

- この更新前は、不正アクセスにより、証明書のローテーション後に kubelet サーバー証明書が更新されませんでした。その結果、ローテーション後の不正アクセスにより、クラスターは正常な状態で起動できませんでした。このリリースでは、kubelet サーバー証明書がローテーション後に更新されます。その結果、OpenShift Container Platform クラスター内の証明書のローテーションが成功し、セキュアな通信と正常なクラスター状態が確保されます。(OCPBUGS-63342)

- この更新前は、Azure Stack 上に仮想マシンが作成されても、MachineSet カスタムリソース定

義 (CRD) のデータディスク設定が **StorageProfile** オブジェクトに渡されませんでした。このアクションにより設定が無視されました。その結果、ユーザーのカスタムディスク設定が仮想マシンに適用されました。このリリースでは、MachineSet CRD のデータディスク設定が **StorageProfile** オブジェクトに渡され、Azure Stack での一貫した処理が確実になります。その結果、データディスク設定が **StorageProfile** オブジェクトに渡され、Azure Stack で確実かつ適切にセットアップされるようになり、仮想マシンの作成が改善されました。(OCPBUGS-63578)

- この更新前は、サービス接続が欠落していたため、通信マトリックスプロジェクトはプライマリーノード上の開いているポート 9193 および 9194 のエンドポイントスライス EndPointSlice オブジェクトを作成できませんでした。その結果、開いているポートにエンドポイントスライスが存在せず、通信マトリックスが不正確になりました。このリリースでは、サービスが開いているポート 9193 および 9194 に接続され、エンドポイントスライスの欠落が解決され、OpenShift Container Platform ユーザーは正確な通信マトリックスを使用できます。(OCPBUGS-63586)

- この更新前は、大きなジャーナルのダウンロードにより、ノードログビューアーでブラウザーがクラッシュしていました。その結果、ジャーナルログが過負荷になり、ログビューアーがクラッシュし、ユーザーエクスペリエンスに影響が出ました。このリリースでは、ログのダウンロードサイズが制限されたことでブラウザーのクラッシュが防止され、ログビューアーにジャーナル行が表示されます。(OCPBUGS-63607)

- この更新前は、拒否リストメトリクスにより Kubernetes カスタムリソースの正規表現が誤ってフォーマットされ、**annotations** フィールドが省略されていました。そのため、拒否リストの誤設定によりメトリクスが欠落していました。このリリースでは、メトリクス拒否リストから不要なエントリーが削除されました。その結果、欠落していたアノテーションがレジストリーメトリクスに含まれ、データ精度が向上しました。(OCPBUGS-64578)

- この更新前は、ノードは taint を持つノードに特定の tolerance を持たない Pod をスケジュールしていました。その結果、must-gather Pod は利用できないノードにスケジュールされ、ログ収集が失敗していました。このリリースでは、Pod にスケジュール先のノードが持つ taint に対する tolerance がある場合にのみ、その Pod を taint を持つノード上にスケジュールします。(OCPBUGS-64585)

1.9.6. 更新

OpenShift Container Platform 4.19 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. RHBA-2025:19301 - OpenShift Container Platform 4.19.18 イメージのリリースおよびバグ修正アドバイザリー

発行日: 2025 年 11 月 5 日

OpenShift Container Platform リリース 4.19.18 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:19301 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-2025:19299 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 4.19.18 --pullspecs
```

1.9.7.1. バグ修正

- この更新前は、DNS レコードが **external-dns** Operator に登録されていない場合、プライベートルーターは **OAuth** ルートを受け入れませんでした。このアクションにより URL が適切に解決されず、コンソールは **OAuth** ルートにアクセスできませんでした。その結果、**Console ClusterOperator** がスタックしました。このリリースでは、ホストされたクラスター内の **OAuth** ルートアドミッションと URL 解決の問題が修正されました。その結果、**OAuth** ルートへのアクセスが可能になり、コンソールアクセスが承認されます。(OCPBUGS-61407)

- このリリースの前は、Azure ファイル CSI ドライバーによってプロビジョニングされた永続ボリュームの **VolumeSnapshot** オブジェクトを削除すると、基礎となるファイル共有も削除され、データが失われていました。このリリースでは、スナップショットのみが削除されるようにドライバーが更新され、この問題は修正されました。ソースファイル共有は保持されます。(OCPBUGS-62911)

- この更新前は、ホストされたクラスターの namespace 内でストレージクラスの順序に一貫性がなく、そのために発生した頻繁なドライバー設定の更新により、**ConfigMap** コンテンツのフラップが発生していました。この問題により、ストレージクラスの適用に一貫性がなくなり、ユーザーエクスペリエンスに影響が出ました。このリリースでは、**ConfigMap** ドライバー設定が安定化され、ストレージクラスのフラッピングが防止され、**ConfigMap** ドライバー設定の安定性が向上し、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順序の頻繁なフラッピングが防止されます。(OCPBUGS-62807)

- この更新前は、**metal3-ironic** コンテナーログの **eTag** フィールドが空であるため、シングルノードの OpenShift ノードでの Redfish トランザクションが失敗していました。その結果、シングルノードの OpenShift ノードで Redfish トランザクションが失敗しました。このリリースでは、Redfish トランザクションの **eTag** フィールドの問題が解決され、**eTags** が正常になりました。その結果、Redfish トランザクションは失敗せず、通信会社はシングルノードの OpenShift ノードで **HostFirmwareSettings** パラメーターを使用できます。(OCPBUGS-62961)

- この更新前は、200% を超える過度の CPU オーバーコミットにより、10 分後に **KubeCPUOvercommit** アラートのトリガーが停止していました。その結果、アラートがなかったため、ユーザーは CPU のオーバーコミットメントに気付きませんでした。このリリースでは、CPU 制限のオーバーコミットにより **KubeCPUOvercommit** アラートが正しくトリガーされ、タイムリーなリソース管理とクラスターの安定性の向上が確実になりました。(OCPBUGS-62965)

- この更新前は、メモリー消費の急増が許容制限内で発生すると、小規模なマルチノードクラスターで **KubeMemoryOvercommit** アラートが誤ってトリガーされていました。このリリースでは、アラート式が調整され、小規模のマルチノードクラスターが正しく考慮されるようになりました。その結果、これらのインスタンスの後に **KubeMemoryOvercommit** アラートが誤ってトリガーされなくなりました。(OCPBUGS-62966)

- この更新前は、コントローラーが Pod の作成に失敗した場合に、無効な Pod 仕様に対して Kubernetes **StatefulSet** ステータスレプリカアラートがアクティブになりませんでした。その結果、**StatefulSet** で必要な数のレプリカの作成に失敗しても、ユーザーには正しく伝わりませんでした。このリリースでは、Pod の作成が失敗すると、Kubernetes **StatefulSet** レプリカカウントアラートがトリガーされます。その結果、**StatefulSet** レプリカと設定されている数が一致しない場合は、アラートが正しく表示されます。(OCPBUGS-62967)

- この更新前は、インスタンス全体のエラーの合計数に基づいて **KubeAggregatedAPIErrors** アラートがトリガーされ、API の複数のインスタンスに対して機密性の高いユーザーアラートが発生していました。このリリースでは、**KubeAggregatedAPIErrors** アラートのアラート機能

がインスタンスレベルで動作するように変更され、複数のインスタンスを持つ API の間違ったアラートが減少しました。(OCPBUGS-62968)

- この更新前は、cordon 状態のノードに対してアラートがフィルタリングされていなかったため、メンテナンス中のノードの誤検知が発生していました。その結果、アラート内の cordon 状態のノードのフィルタリングにより、ユーザーは誤検知を経験しました。このリリースでは、メンテナンス中の誤検知を減らすために、cordon 状態のノードがアラートからフィルタリングされます。その結果、メンテナンスアラートが正常になり、cordon 状態のノードに対する誤検知が減少しました。(OCPBUGS-62969)

- この更新前は、Google Cloud 上の OpenShift Container Platform クラスターを破棄すると、**waitFor** メソッドでの null ポインター参照のキャンセルによりパニックエラーが発生しました。これは、Google Cloud API 呼び出しが失敗したか、クライアントが初期化されていないことが原因でした。その結果、Google Cloud でのクラスターの破棄中にパニックエラーが発生しました。このリリースでは、クラスターアンインストーラーの null ポインターの問題が修正され、Google Cloud の破棄中にパニックエラーが発生しなくなりました。その結果、Google Cloud でのクラスター破棄時のパニックエラーが解決され、リソースをスムーズに削除できるようになりました。(OCPBUGS-62981)

- この更新前は、単一の namespace ロールを持つ管理ユーザーが Pod を作成すると、URL のパースペクティブが正しくなかったためにメトリクスの表示時に空白ページが発生していました。その結果、ユーザーは CPU 使用率メトリクスを表示できませんでした。このリリースでは、管理ユーザーは開発者パースペクティブで Pod メトリクスを表示でき、ユーザーは CPU 使用率メトリクスを表示できます。(OCPBUGS-62999)

- この更新前は、Oracle Container Storage Interface (CSI) ノードレジストラーコンテナーが 10 秒ごとに **gRPC** 接続チェックをログに記録し、Elasticsearch 領域を過剰に占有していました。この急速なログの増加により、ユーザーコストが増加しました。このリリースでは、**csi-node-registrar** コンテナー内での **gRPC** 接続チェックのログ記録頻度が減少しました。その結果、Elasticsearch のログ容量が増加し、コストが削減され、パフォーマンスが向上します。(OCPBUGS-63193)

- この更新前は、ユーザーが適切な IP アドレスを持つゲートウェイノード間で EgressIP フェイルオーバーを定義しなかった場合、再起動後に EgressIP アドレスが 2 つめのゲートウェイノードに再割り当てされませんでした。その結果、Pod と外部システム間の通信に失敗していました。このリリースでは、デュアルスタック環境の EgressIP フェイルオーバーロジックが改善され、再起動後に EgressIP アドレスが利用可能なゲートウェイノードに適切に再割り当てされるようになりました。ゲートウェイノードの再起動後、Pod と外部システム間の通信は中断されません。(OCPBUGS-63234)

- この更新前は、OpenShift Container Platform 4.18.24 にアップグレードすると、**ocp-tuned-one-shot** サービスの問題によりプライマリーノードで kubelet 障害が発生していました。その結果、アップグレード中に kubelet がプライマリーノードで起動できなくなりました。このリリースでは、**ocp-tuned-one-shot** サービスを修正することで kubelet の問題が解決されました。その結果、アップグレード後に kubelet がプライマリーノードで起動します。(OCPBUGS-63418)

1.9.7.2. 更新

OpenShift Container Platform 4.19 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-2025:18233 - OpenShift Container Platform 4.19.17 イメージのリリースおよびバグ修正アドバイザリー

発行日: 2025 年 10 月 22 日

OpenShift Container Platform リリース 4.19.17 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-2025:18233 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-2025:18201 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 4.19.17 --pullspecs
```

1.9.8.1. バグ修正

- 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、HyperShift およびホストされたクラスターが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 HyperShift およびホストされたクラスター上で回復されます。(OCPBUGS-62868)

- この更新前は、インストールプログラムでは、**None** または **External** として指定されたプラットフォーム上での IPv6 プライマリーデュアルスタックのインストールは許可されませんでした。その結果、これらのプラットフォームタイプでデュアルスタックのインストールを続行すると、エラーまたは設定ブロックが発生しました。このリリースでは、**None** および **External** プラットフォームに IPv6 プライマリーデュアルスタック設定を正常にインストールできます。(OCPBUGS-62911)

1.9.8.2. 更新

OpenShift Container Platform 4.19 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. RHBA-2025:17663 - OpenShift Container Platform 4.19.16 イメージのリリースおよびバグ修正アドバイザリー

発行日: 2025 年 10 月 14 日

OpenShift Container Platform リリース 4.19.16 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:17663 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-2025:17660 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 4.19.16 --pullspecs
```

1.9.9.1. バグ修正

- この更新前は、1 つの etcd メンバーでタイムアウトが発生すると、コンテキストのデッドライン超過が引き起こされていました。その結果、一部のメンバーは到達可能であったにもかかわ

らず、すべてのメンバーが異常であると宣言されていました。このリリースにより、1つのメンバーがタイムアウトしても、他のメンバーが誤って異常とマークされることはなくなりました。(OCPBUGS-60941)

- この更新前は、OVN-Kubernetes ローカルネットワーク (br-ex ブリッジにマッピング) 内のセカンダリーインターフェイスを持つ Pod は、ローカルネットワーク 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、接続にデフォルトネットワークを使用する同じノード上の Pod と通信できました。このリリースでは、任意のサブネットからローカルネットワーク IP アドレスを抽出できます。この一般的なケースでは、クラスター外の外部ルーターがローカルネットワークサブネットをホストネットワークに接続すると予想されます。(OCPBUGS-61454)

- この更新前は、外部のアクターが、Machine Config Operator (MCO) が drain 中のノードを uncordon することができました。その結果、MCO とスケジューラーは同時に Pod のスケジュールとスケジュール解除を行うことになり、drain プロセスが長引いていました。この修正により、drain プロセス中に外部アクターがノードを uncordon した場合、MCO はそのノードを再度 cordon 状態にしようと試みます。その結果、MCO とスケジューラーは同時に Pod をスケジュールおよび削除しなくなりました。(OCPBUGS-62003)

- この更新前は、**oc-mirror** 出力でバイナリーバージョンが表示されなかったためデバッグが妨げられ、必要な修正の特定が遅れ、ユーザーエクスペリエンスが低下していました。このリリースでは、デバッグを容易にするために、**oc-mirror** の出力にバージョンが表示されます。その結果、エンドユーザーは **oc-mirror** バージョンを簡単に識別して速やかにデバッグできます。(OCPBUGS-62311)

- この更新前は、モニタリングスタックがまだ UTF-8 を完全にサポートしていないにもかかわらず、プラットフォーム監視用とユーザーワークロード監視用の両方の Prometheus が UTF-8 メトリクスをネゴシエートして受け入れていました。このリリースでは、Prometheus は UTF-8 メトリクスを受け入れなくなりました。(OCPBUGS-62429)

- この更新前は、永続ボリューム要求 (PVC) を作成した直後に、あまりにもすばやくサイズ変更すると、競合状態が原因で、flake と呼ばれる断続的な障害が時折発生していました。その結果、バインドされた永続ボリューム (PV) が見つからないという誤った報告がシステムから出力されるエラーが発生しました。このリリースにより、タイミングの問題が修正され、PVC を作成した直後にサイズ変更できるようになりました。(OCPBUGS-62468)

1.9.9.2. 更新

OpenShift Container Platform 4.19 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.10. RHBA-2025:17237 - OpenShift Container Platform 4.19.15 イメージのリリースおよびバグ修正アドバイザリー

発行日: 2025 年 10 月 7 日

OpenShift Container Platform リリース 4.19.15 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-2025:17237 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-2025:17235 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 4.19.15 --pullspecs
```

1.9.10.1. バグ修正

- このリリースでは、**oc-mirror** v1 の非推奨化プロセスの一環として、**--v1** または **--v2** フラグが必須であることを示す警告メッセージが表示されます。その結果、これらのフラグを指定しないと **oc-mirror** が失敗します。(OCPBUGS-62062)

- この更新前は、**/auth/error** ページが正しくレンダリングされませんでした。その結果、ページが空になり、エラーの詳細が表示されませんでした。このリリースでは、フロントエンドエラーページの内容が **/auth/error** ページに表示されます。(OCPBUGS-62083)

1.9.10.2. 更新

OpenShift Container Platform 4.19 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.11. RHBA-2025:16693 - OpenShift Container Platform 4.19.14 イメージのリリースおよびバグ修正アドバイザリー

発行日: 2025 年 9 月 30 日

OpenShift Container Platform リリース 4.19.14 が公開されました。更新に含まれるバグ修正のリストは、RHBA-2025:16693 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-2025:16691 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 4.19.14 --pullspecs
```

1.9.11.1. バグ修正

- この更新前は、Ignition サーバーのデプロイメントでグローバルの **mirroredReleaseImage** 状態が使用されていました。この状態が同時イメージ検索操作によって変更されると、競合状態が発生していました。その結果、環境変数 **MIRRORED_RELEASE_IMAGE** が元のイメージとそのミラーレジストリーの間で頻繁に切り替わり、デプロイメントの再生成が継続的に発生していました。このリリースでは、グローバルのミラー状態がイメージ固有の検索ロジックに置き換えられました。ミラーの解決が確定的になり、空のレジストリーエントリーに対する防御的なフィルタリングが不要になりました。その結果、**MIRRORED_RELEASE_IMAGE** の値が一定になり、Ignition サーバーのデプロイメントが安定した状態を保つようになりました。これにより、不要な Pod の再起動やデプロイメントの頻繁な変更が排除されました。(OCPBUGS-61677)

- この更新前は、Web コンソールの **Pod** および **Node logs** ページの **Expand** ボタンが正しく機能していませんでした。その結果、ターミナルのプロンプトに入力することができませんでした。このリリースでは、**Expand** ボタンをクリックするとブラウザーが全画面に設定されます。そのため、ターミナルで入力を正常に行うことができます。(OCPBUGS-61821)

- この更新前は、ベアメタルおよび複数ネットワークインターフェイスコントローラー (NIC) 環境における **NetworkManager-wait-online** 依存関係の問題が原因で、OpenShift Container Platform デプロイメントで **NMState** サービスの障害が発生していました。その結果、不適切なネットワーク設定によりデプロイメントの失敗が発生していました。このリリースでは、ベ

アメタルデプロイメントの **NetworkManager-wait-online** 依存関係が更新されました。これにより、デプロイメントの失敗が減り、**NMState** サービスの安定性が確保されました。(OCPBUGS-61835)

1.9.11.2. 更新

OpenShift Container Platform 4.19 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. RHBA-2025:16148 - OpenShift Container Platform 4.19.13 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 9 月 23 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.13 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-2025:16148 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-2025:16146 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 4.19.13 --pullspecs
```

1.9.12.1. バグ修正

- この更新前は、コード内にロギングステートメントがなかったため、**config-sync-controller** が結果をログに記録しませんでした。その結果、ユーザーに **config-sync-controller** でサイレント障害が発生していました。このリリースでは、**config-sync-controller** が結果をログに記録するようになり、ユーザー向けのエラー診断が強化されました。(OCPBUGS-56788)

- この更新前は、タグ付けされたイメージ名を使用してイメージマニフェストとメタデータを取得する呼び出しで、検索の結果がキャッシュされませんでした。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、名前付きタグまたは正規名を使用する Hosted Control Plane 内のイメージが 12 時間キャッシュされます。その結果、Hosted Control Plane のメモリー使用量が最適化されます。(OCPBUGS-59933)

- 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-61313)

- この更新前は、リモートエンドポイントがデータをまったく受信しなかった場合も、**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-61486)

- 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-61488)

- この更新前は、Web コンソールの **Operand details page** で、3 番目の列に追加のステータス項目が表示されていました。これにより、コンテンツがつぶれたように表示されていました。この更新により、不具合が修正され、詳細ページに 2 つの列だけが表示されるようになりました。(OCPBUGS-61781)

1.9.12.2. 更新

OpenShift Container Platform 4.19 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.13. RHBA-2025:15694 - OpenShift Container Platform 4.19.12 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 9 月 16 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.12 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2025:1694 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-2025:15692 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 4.19.12 --pullspecs
```

1.9.13.1. 機能拡張

- この更新により、**cluster-etcd-operator** Operator に、etcd ストレージクォータをプロアクティブに管理するための **etcdDatabaseQuotaLowSpace** アラートのマルチステージ通知システムが実装されました。この機能拡張により、データベース容量不足の警告を早期に提供することで、API サーバーの不安定化を防止できます。etcd ディスク領域の使用率が 65%、75%、および 85% に達すると、重大度が情報提供、警告、または重大のアラートが管理者に届くようになりました。(OCPBUGS-60443)

- この更新により、Kubernetes 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-61485)

- この更新により、マシン設定ノードのカスタムリソースが一般提供になりました。これを使用すると、ノードに対するマシン設定の更新の進行状況を監視できます。一般提供への昇格により、コントロールプレーンとワーカープールに加えて、カスタムのマシン設定プールの更新ステータスを確認できるようになりました。この機能そのものは変更されていません。ただし、コマンドの出力および **MachineConfigNode** オブジェクトのステータスフィールドの情報が一部更新されています。Machine Config Operator 用の **must-gather** には、クラスター内のすべての **MachineConfigNodes** オブジェクトが含まれます。詳細は、マシン設定ノードのステータスの確認について を参照してください。

- この更新により、**PinnedImageSet** オブジェクトが一般提供になりました。これを使用すると、実際に必要になる前に、コンテナーイメージを事前に取得できます。このイメージはマシン設定プールに関連付けることができます。イメージレジストリーへの接続が遅く、信頼性が低いクラスターでは、イメージをピン留めすることで、必要なときにイメージを利用できるよ

うになります。Machine Config Operator 用の **must-gather** には、クラスター内のすべての **PinnedImageSet** オブジェクトが含まれるようになりました。詳細は、ノードへのイメージのピニング を参照してください。

1.9.13.2. バグ修正

- この更新前は、SSH 鍵なしでクラスターを作成した場合、**99-worker-ssh** というマシン設定が存在しないために、**oc adm node-image create** コマンドによるノードイメージの作成が失敗していました。これにより、ワーカーノード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、**worker-ssh** の **machineConfig** が作成されるようになり、ノードイメージの作成が可能になりました。その結果、ワーカーノードのノードイメージの作成が成功するようになりました。(OCPBUGS-60832)

- この更新前は、Amazon Web Services (AWS) プラットフォームと **--create-private-s3-bucket** パラメーターの使用中に **ccoctl** を複数回実行すると、OpenID Connect (OIDC) 発行者に間違った URL が設定されていました。その結果、一部のクラスター Operator が AWS API に対して認証できませんでした。このリリースでは、**ccoctl** が OIDC 発行者の正しい URL を適切に設定します。その結果、クラスター Operator が期待どおりに認証を継続します。(OCPBUGS-60970)

- この更新前は、**MachineHealthCheck** カスタムリソース (CR) に **maxUnhealthy** フィールドのデフォルト値が表示されませんでした。このリリースでは、値が設定されていない場合にデフォルトで適用される値が CR に記録されるようになりました。(OCPBUGS-61096)

- この更新前は、**multus-networkpolicy** DaemonSet に更新を適用するのにかかる時間が、ノード数に応じて直線的に増加していました。このリリースでは、DaemonSet が更新され、10% の **maxUnavailable** が許容されるようになったため、10 ノードを超えるクラスターでも DaemonSet が即座に更新されるようになりました。(OCPBUGS-61460)

1.9.13.3. 更新

OpenShift Container Platform 4.19 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-2025:15293 - OpenShift Container Platform 4.19.11 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 9 月 9 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.11 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-2025:15293 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-2025:15291 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 4.19.11 --pullspecs
```

1.9.14.1. 機能拡張

- この更新により、Kubernetes API サーバーの分散が最適化され、クォーラムが再確立された後にすべてのプライマリーノード間で負荷が均等に分散されるようになりました。これにより、

単一の API サーバーがライブ接続の大部分を受信し、CPU 使用率が高くなるという問題が解決されます。リソース使用率が向上し、プライマリーノードまたは API サーバー再起動時の CPU 使用率の急増が減少します。(OCPBUGS-60121)

1.9.14.2. バグ修正

- この更新前は、OpenShift イメージレジストリーを無効にすると、従来のプルシークレットファイナライザーが保持され、レジストリーの削除中にシークレットの削除がハングしていました。この問題によりクラスターの削除がブロックされていました。このリリースでは、レジストリーが無効になっている場合でも、シークレットファイナライザーが namespace の削除をブロックせず、クラスターの削除を確実に実行します。(OCPBUGS-56614)

- この更新前は、**noexec-mounted /tmp** ディレクトリーを持つ RHEL 8 システムで **oc mirror** コマンドが失敗していました。このコマンドにより、一時ファイルまたはスクリプトを起動できなかったためです。その結果、イメージのミラーリングが防げられていました。このリリースでは、**oc mirror** コマンドに **noexec-mounted /tmp** ディレクトリーの例外が組み込まれており、RHEL 8 システムでのミラーリングが成功するようになりました。その結果、**oc mirror** コマンドにより、**noexec-mounted /tmp** ディレクトリーを持つ RHEL 8 システム上の出力およびミラーコンテナーイメージがリスト表示されるようになりました。(OCPBUGS-59760)

- この更新前は、**apiserver** の一時的なダウンタイムが原因で、**openshift-etcd** namespace が存在しないという誤った報告が **cluster-etcd-operator** によって行われていました。その結果、ダウンタイム中に、namespace が見つからないという誤ったメッセージがユーザーに表示されました。このリリースでは、etcd namespace が見つからない場合のエラーメッセージを改善するための修正が実装されました。その結果、エラーメッセージが修正され、**apiserver** の一時的なダウンタイム中に **cluster-etcd-operator** のステータスが問題を正確に反映するようになりました。(OCPBUGS-59802)

- この更新前は、**Quickstarts** ページの重複したリンクボタンが **/quickstart** パスにのみ表示され、ユーザーを混乱を招いていました。このリリースでは、**Quickstart** リンクボタンが正しく表示され、重複が排除されました。(OCPBUGS-60420)

- この更新前は、Hosted Control Plane クラスターが、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 Hosted Control Plane クラスターで複数の SAN ホスト名を持つ証明書をデプロイする際にエラーが発生していました。このリリースでは、Hosted Control Plane クラスターで、複数の SAN エントリーに対応した証明書検証がサポートされるようになりました。その結果、複数の SAN エントリーを持つ証明書が受け入れられるようになり、Hosted Control Plane クラスターのデプロイが改善されました。(OCPBUGS-60483)

- この更新前は、マシン削除処理が不適切だったため、スケールダウンプロセス中に最後のノードに **ToBeDeletedByClusterAutoscaler** taint が残っていました。その結果、最後のノードがクラスターの自動スケーリングの効率に影響を与えていました。このリリースでは、スケールダウン後の最後のノードから **ToBeDeletedByClusterAutoscaler** taint が削除されます。最後のノードに不要な taint が残らず、クラスターの安定性が向上しました。(OCPBUGS-60900)

- このリリースより前では、DNS Egress ファイアウォールルールに対応する **address_set** 設定要素内の古い IP アドレスエントリーが削除されていませんでした。その結果、**address_set** が増加し、メモリーリークの問題が発生していました。このリリースでは、IP アドレスの Time to Live (TTL) の有効期限が切れた後の 5 秒間の猶予期間後に、**address_set** から IP アドレスを削除することで、この問題が修正されました。(OCPBUGS-60979)

1.9.14.3. 更新

OpenShift Container Platform 4.19 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-2025:14823 - OpenShift Container Platform 4.19.10 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 9 月 2 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.10 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-2025:14823 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-2025:14817 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 4.19.10 --pullspecs
```

1.9.15.1. 機能拡張

- オンクラスターイメージモードで使用される **MachineOSConfig** オブジェクトの名前は、カスタムレイヤー化イメージをデプロイするマシン設定プールと同じである必要があります。この変更により、各マシン設定プールで複数の **MachineOSConfig** オブジェクトが使用されなくなります。(OCPBUGS-60414)

1.9.15.2. バグ修正

- この更新前は、管理クラスターに多数のイメージリポジトリーが設定されている場合、Hosted Control Plane (HCP) はペイロードリポジトリーを順番にクエリーしなかったため、最初のミラーが利用できない場合に非接続環境でホステッドクラスターのデプロイメントが失敗していました。次の利用可能なイメージを検索する代わりに、システムでエラーが発生しました。このリリースでは、HCP ペイロードは、利用可能なイメージが見つかるまでミラーのリスト全体をイテレート処理し、デプロイメントが期待どおりに成功できるようになります。(OCPBUGS-57141)

- この更新前は、プライマリーインターフェイスに多数の IP アドレスが設定されているリリース 4.19 でゼロタッチプロビジョニング (ZTP) を使用してシングルノードの OpenShift をデプロイすると、**apiserver** Pod が etcd に接続できませんでした。その結果、etcd 証明書には設定されたすべての IP アドレスが含まれておらず、Transport Layer Security (TLS) 認証エラーが発生しました。このリリースでは、**apiserver** Pod がこれらの設定で etcd に正常に接続できるようになり、多くのプライマリーインターフェイス IP アドレスを持つシングルノードの OpenShift デプロイメントを正しく初期化できるようになりました。(OCPBUGS-59285)

- この更新前は、IBM Cloud はシングルノードの OpenShift インストールの検証チェックに含まれていなかったため、IBM Cloud にシングルノードの OpenShift をインストールしようとすると検証エラーが発生していました。このリリースでは、IBM Cloud はシングルノードの OpenShift インストールをサポートするようになり、IBM Cloud 上のエンドユーザーのインストールエクスペリエンスが向上します。(OCPBUGS-59607)

- この更新前は、**Delete** ワークフローで誤って **workflow mode: diskToMirror** / **delete** と表示され、正しいワークフローモードに関してユーザーが混乱する原因となっていました。このリリースでは、削除操作中に **workflow mode: delete** が表示されます。(OCPBUGS-59761)

- この更新前は、異なるコンテナーイメージ間で重複したイメージを共有すると、**oc-mirror** 内の

Helm チャートのミラーイメージの合計数が誤って計算されていました。その結果、一部の Helm イメージがミラーリングされませんでした。このリリースでは、**oc-mirror** 内のミラーリングされた Helm イメージの誤ったカウントが修正され、ミラーリングされたイメージのカウントの精度が向上しました。(OCPBUGS-60086)

- この更新前は、**HorizontalPodAutoscaler** が **istiod-openshift-gateway** を一時的に 2 つのレプリカにスケーリングし、テストが 1 つのレプリカのみを想定していたため継続的インテグレーション (CI) が失敗していました。このリリースでは、**HorizontalPodAutoscaler** のスケーリングが調整され、**istiod-openshift-gateway** の単一レプリカをサポートするようになりました。(OCPBUGS-60204)

- この更新前は、4.15 より前のバージョンへのアップグレード、または 4.15 の新規インストールにより、テクノロジープレビューであるにもかかわらず、**MachineConfigNode** カスタムリソース定義 (CRD) がデプロイされていました。その結果、不要な CRD が原因でクラスターのアップグレードに失敗しました。このリリースでは、テクノロジープレビューの **MachineConfigNode** CRD がデフォルトのクラスターから削除され、シームレスなアップグレードが確保されました。(OCPBUGS-60265)

- 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ルプログラム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-60402)

- この更新前は、Amazon Web Services (AWS) **machinesets** の **userDataSecret** 名が null になる可能性があり、その結果、マシンがプロビジョニング状態のままになる可能性がありました。このリリースでは、空でない **userDataSecret** 名が必須となり、予期しないマシンの動作が防止されます。(OCPBUGS-60427)

- この更新前は、証明書の有効期限が署名者の有効期限を超えることができないという制限がありました。これにより、**localhost-recovery.kubeconfig** に影響が及びました。node-system-admin-client 証明書が、意図した 2 年間ではなく 1 年間の有効期間で誤って生成されたため、**localhost-recovery.kubeconfig** の有効期限が早期に切れてしまいました。このリリースでは、署名者証明書の有効期間が 3 年に延長され、node-system-admin-client 証明書の有効期間が 2 年になりました。(OCPBUGS-60495)

- この更新前は、バージョン 4.13 以前で作成された AWS 上の OpenShift Container Platform クラスターは、バージョン 4.19 に更新できませんでした。バージョン 4.14 以降で作成されたクラスターには、デフォルトで AWS **cloud-conf** ConfigMap が含まれており、この ConfigMap は OpenShift Container Platform 4.19 以降では必須となっています。このリリースでは、Cloud Controller Manager Operator が更新され、デフォルトの **cloud-conf** ConfigMap がクラスターに存在しない場合に作成されるようになりました。この変更により、バージョン 4.13 以前で作成されたクラスターをバージョン 4.19 に更新できるようになります。(OCPBUGS-60950)

1.9.15.3. 更新

OpenShift Container Platform 4.19 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-2025:13848 - OpenShift Container Platform 4.19.9 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 8 月 19 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.9 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-2025:13848 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-2025:13827 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 4.19.9 --pullspecs
```

1.9.16.1. 機能拡張

- この更新により、Hosted Control Plane に NUMA Resources Operator をインストールして、NUMA 対応のスケジューリングサポートを有効にできるようになります。詳細は、Hosted Control Plane の NUMAResourcesOperator カスタムリソースの作成 を参照してください。この機能拡張は、テクノロジープレビュー機能として利用できます。

1.9.16.2. バグ修正

- この更新前は、4.1 および 4.2 のブートイメージが OpenShift Container Platform 4.19 で動作せず、クラスターの機能低下を引き起こしていました。このリリースにより、Extensible Firmware Interface (EFI) およびファームウェアコンポーネントに対して静的な Grand Unified Bootloader (GRUB) 設定がインストールされ、ノードのスケーリング中にクラスターが正常に動作します。(OCPBUGS-52485)

- この更新前は、Google Cloud machine API は順次リコンシリエーション処理によってブロックされていました。その結果、ユーザーは GCP 統合中に、ノードのスケーリングが遅くなるという問題がユーザー側で発生しました。このリリースでは、多くのリコンシリエーションプロセスの並列実行が可能になり、GCP Machine API のパフォーマンスが向上しました。その結果、GCP ノードのスケーリングパフォーマンスが向上します。(OCPBUGS-59386)

- この更新前は、ユーザーは、Vertical Pod Autoscaler (VPA) のアップストリームの問題があるバージョンを使用して、OpenShift Container Platform VPA カスタムレコメンダーを設定していました。その結果、この問題により VPA の更新が不安定になりました。このリリースでは、カスタム VPA チェックポイントガベージコレクターは追跡されていないチェックポイントを削除せず、OpenShift Container Platform の不安定さを防止します。その結果、OpenShift Container Platform VPA の更新は安定し、Pod の定期的な再スケジューリングは発生しなくなります。(OCPBUGS-59638)

- この更新前は、VMware vSphere インフラストラクチャーでの OpenShift Container Platform 4.16 マニフェストの適用中に、machine config デーモンは Domain Name System (DNS) ルックアップに失敗していました。その結果、OpenShift Container Platform 4.16 のアップグレード中にユーザーの DNS ルックアップが失敗し、アップグレードが無期限に停止しました。このリリースでは、アップグレード中に CoreDNS Pod が再起動することによる失敗を回避するために、バックオフを使用したリモートオペレーティングシステム更新の再試行が実装されています。(OCPBUGS-59899)

- この更新前は、調整試行の制限が増加したためにクラスターのアップグレードに失敗していました。この障害により、Prometheus Pod が使用できなくなり、サービスの低下が発生しました。このリリースでは、Operator は失敗を報告する前に追加の調整試行を許可します。その結果、クラスターのアップグレードテストの安定性が向上し、障害率が低減し、アップグレードの信頼性が向上します。(OCPBUGS-59932)

- この更新前は、OpenShift Container Platform Precision Time Protocol (PTP) Pod のサイド

カーが終了後に予期せず再起動し、**exit code 7** エラーでクロッククラスの終了が失敗していました。その結果、メトリクスは利用できなくなりました。このリリースでは、サイドカーの再起動によって OpenShift Container Platform PTP Pod でクロッククラスの終了エラーが発生しなくなり、再起動中に停止しなくなりました。(OCPBUGS-59970)

- この更新前は、ユーザーが OpenShift Container Platform 4.19 にアップグレードすると、Machine Config Operator (MCO) が Transport Layer Security (TLS) 証明書をローテーションしていました。これにより、スケールアッププロセス中にノードがクラスターに参加できないという問題が発生しました。このリリースでは、MCO は、必要なサブジェクト代替名 (SAN) IP アドレスを決定し、それをローテーションされた TLS 証明書に追加するカスタム ARO リソースを提供します。その結果、スケールアッププロセス中にノードがクラスターに参加できるようになります。(OCPBUGS-59978)

- この更新前は、**ResourceEventStream** コード形式の補間エラーにより、ユーザーがイベントストリームに接続した際に、誤った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、イベントストリーム内のエラーメッセージの補間形式が正しくなりました。その結果、ユーザーがイベントストリームに接続した際に、正確なエラーメッセージが表示されます。(OCPBUGS-60039)

- この更新前は、通信マトリックスプロジェクトのプライマリーノードポートがバインドされておらず、プライマリーノードで通信フローが欠落し、サービスが利用できなくなっていました。このリリースでは、コントローラーマネージャーのポートが閉じられており、**localhost** からのみ利用可能になります。その結果、サービスは正しいポートにバインドされます。(OCPBUGS-60132)

- この更新前は、複数のアーチアノテーションラベルが原因で **MachineSet** カスタムリソースの更新に失敗していました。その結果、マシンの更新は失敗しました。このリリースでは、**{{capacity.cluster-autoscaler.kubernetes.io/labels}}** アノテーションで複数のラベルを許可することで更新の問題が修正され、アーキテクチャー値が適切に解析されるようになりました。その結果、Machine Config Operator は更新中に失敗しなくなります。(OCPBUGS-60224)

- この更新前は、**LeaderWorkerSet** Operator の説明が古いままでした。その結果、ユーザーには誤った説明が表示されていました。このリリースでは、**LeaderWorkerSet** Operator の説明が更新され、概念の説明が正確に表示されるようになりました。(OCPBUGS-60225)

- この更新前は、**cloud-event-proxy** サイドカープロセスが終了し、Pod が回復しても通知 API が **clockClass=0** 状態のままになっていました。その結果、サイドカープロセスが終了した後も通知 API は非アクティブのままになりました。このリリースでは、**cloud-event-proxy** プロセスのリカバリーによって通知 API の **clockClass=0** 状態が発生しなくなりました。これで、通知 API は、**cloud-event-proxy** が回復したときに **clockClass** 変数を正しく更新するようになりました。(OCPBUGS-60261)

- この更新前は、OVN-K ホステッドクラスター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、機密データが公開されていました。その結果、ユーザーデータが公開されていました。このリリースでは、匿名化機能が更新され、新しいネットワークデータタイプを検出して難読化し、セキュアな通信が確保されるようになりました。(OCPBUGS-60295)

1.9.16.3. 更新

OpenShift Container Platform 4.19 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-2025:12341 - OpenShift Container Platform 4.19.7 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 8 月 5 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.7 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-2025:12341 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-2025:12342 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 4.19.7 --pullspecs
```

1.9.17.1. 機能拡張

- KubeVirt Container Storage Interface (CSI) ドライバーがボリューム拡張をサポートするようになりました。ユーザーは、テナントクラスター内の永続ボリュームのサイズを動的に増やすことができます。この機能によりストレージ管理が簡素化され、より柔軟でスケーラブルなインフラストラクチャーが実現します。(OCPBUGS-58239)

1.9.17.2. バグ修正

- この更新前は、複数のプラグインが同じ **CreateProjectModal** 拡張ポイントを使用していたため、コンソールモーダルでプラグインの競合が発生していました。その結果、プラグイン拡張機能は 1 つだけ使用され、リストの順序を変更できませんでした。このリリースでは、プラグインストアの更新により、コンソール Operator の設定で定義されているのと同じ順序で拡張機能が解決されます。その結果、Operator の設定を更新する権限を持つユーザーは誰でも、プラグインの優先順位を設定できるようになります。(OCPBUGS-56280)

- この更新前は、**Overview** ページの **AlertmanagerReceiversNotConfigured** アラートで **Configure** をクリックすると、ランタイムエラーが発生していました。このリリースでは、ナビゲーション処理が改善され、**Configure** をクリックしても、ランタイムエラーが発生しなくなりました。(OCPBUGS-57105)

- この更新前は、**/metrics/usage** エンドポイントが更新され、認証とクロスサイトリクエストフォージェリー (CSRF) に対する保護が追加されました。その結果、リクエスト Cookie に必要な CSRF トークンが含まれていないため、このエンドポイントへのリクエストが失敗し、"forbidden" エラーメッセージが表示されるようになりました。このリリースでは、CSRF トークンが **/metrics/usage** のリクエスト Cookie に追加され、"forbidden" エラーメッセージが解決されました。(OCPBUGS-58331)

- この更新前は、クライアントシークレットを指定していない Open ID クラスターを持つ **HostedCluster** リソースの OpenID Connect (OIDC) プロバイダーを設定すると、デフォルトのシークレット名が自動的に生成されていました。その結果、OIDC パブリッククライアントはクライアントシークレットを使用できないため、これらのクライアントを設定できませんでした。このリリースでは、クライアントシークレットが提供されない場合、デフォルトのシークレット名は生成されません。その結果、OIDC パブリッククライアントを設定できるようになります。(OCPBUGS-58683)

- この更新前は、Bare Metal Host (BMH) が **Provisioned** または **ExternallyProvisioned** としてマークされている場合、システムはまずそのプロビジョニング解除または電源オフを試み、BMH にアタッチされている **DataImage** も削除を妨げていました。この問題はホストの削除を妨げたり、遅延させたりするため、運用上の非効率性を引き起こしていました。このリリースでは、BMH のステータスが **detached annotation** で削除が要求された場合、BMH は deleting 状態に移行し、直接削除できるようになります。(OCPBUGS-59133)

- 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-59488)

- この更新前は、OpenShift Container Platform 4.18 へのクラスターのアップグレードにより、古いネットワークアドレス変換 (NAT) 処理が原因で、Egress IP の割り当てに一貫性がありませんでした。この問題は、Egress ノードの OVN-Kubernetes コントローラーがダウンしているときに Egress IP Pod を削除した場合にのみ発生しました。その結果、論理ルーターポリシーと Egress IP の使用が重複し、トラフィックフローの不一致と停止が発生しました。このリリースにより、Egress IP 割り当てがクリーンアップされ、OpenShift Container Platform 4.18 クラスターでの一貫性のある信頼性の高い Egress IP 割り当てが行われるようになりました。(OCPBUGS-59530)

- この更新前は、コンソールにログインしたときに十分な特権がなかった場合、**get started** メッセージがページ上で過剰なスペースを占有していました。この問題により、**no resources found** などの重要なステータスメッセージが完全に表示されなくなりました。その結果、メッセージの短縮バージョンが表示されました。このリリースでは、**get started** メッセージのサイズが変更され、ページの無効化プロパティーが削除されて、画面スペースの使用量が削減されたことで、スクロールが可能になりました。この修正により、ユーザーはすべてのページで完全なステータスと情報を表示できるようになります。すべてのページで完全なステータスと情報を表示できるようになりました。その結果、**get started** コンテンツはスクロールすることで完全にアクセス可能となり、新しいユーザーガイダンスと重要なシステムメッセージが確実に表示されます。(OCPBUGS-59639)

- 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-59779)

- 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-59799)

1.9.17.3. 更新

OpenShift Container Platform 4.19 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-2025:11673 - OpenShift Container Platform 4.19.6 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 7 月 29 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.6 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-2025:11673 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-2025:11674 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 4.19.6 --pullspecs
```

1.9.18.1. 機能拡張

- KubeVirt Container Storage Interface (CSI) ドライバーがボリューム拡張をサポートするようになりました。ユーザーは、テナントクラスター内の永続ボリュームのサイズを動的に増やすことができます。この機能によりストレージ管理が簡素化され、より柔軟でスケーラブルなインフラストラクチャーが実現します。(OCPBUGS-58239)

1.9.18.2. バグ修正

- この更新前は、**/metrics/usage** エンドポイントが更新され、認証とクロスサイトリクエストフォージェリー (CSRF) に対する保護が追加されました。その結果、リクエスト Cookie に必要な CSRF トークンが含まれていないため、このエンドポイントへのリクエストが失敗し、"forbidden" エラーメッセージが表示されるようになりました。このリリースでは、CSRF トークンが **/metrics/usage** のリクエスト Cookie に追加され、"forbidden" エラーメッセージが解決されました。(OCPBUGS-58331)

- この更新前は、**console.flag/model** 拡張ポイントが機能せず、関連付けられたモデルが提供されたときにフラグが適切に設定されていませんでした。このリリースでは、**console.flag/model** が期待どおりに動作し、関連付けられたモデルが提供されたときにフラグが適切に設定されます。(OCPBUGS-59513)

1.9.18.3. 更新

OpenShift Container Platform 4.19 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-2025:11363 - OpenShift Container Platform 4.19.5 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 7 月 22 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.5 が利用可能になりました。更新に含まれるバグ修正のリストは、RHSA-2025:11363 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-2025:11364 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 4.19.5 --pullspecs
```

1.9.19.1. バグ修正

- 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-59258)

- この更新前は、`OVNkubernetes` の状態更新が一貫していなかったため、断続的な Egress インターネットプロトコル (IP) 処理によってパケットがドロップされていました。このパケットドロップはネットワークトラフィックフローに影響を与えていました。このリリースでは、`OVNkubernetes` Pod が割り当てられた Egress IP を一貫して使用します。その結果、パッケージのドロップが減り、ネットワークトラフィックの流れが改善します。(OCPBUGS-59234)

- この更新前は、Amazon Web Services (AWS) クラウドプロバイダーが、AWS ロードバランサーのデフォルトの ping ターゲットを **HTTP:10256/healthz** に設定していませんでした。AWS 上で実行される LoadBalancer サービスの場合、AWS で作成される Load Balancer オブジェクトの ping ターゲットは **TCP:32518** でした。その結果、クラスター全体のサービスのヘルスプローブが機能せず、アップグレード中にサービスが停止していました。このリリースでは、クラウド設定の **ClusterServiceLoadBalancerHealthProbeMode** プロパティーが **Shared** に設定され、設定が AWS クラウドプロバイダーに渡されるようになりました。その結果、AWS ロードバランサーに **HTTP:10256/healthzwhich** という正しいヘルスチェック ping ターゲットが設定されます。(OCPBUGS-59101)

- この更新前は、**MachineConfigOperator** (MCO) が、RPM Package Manager (RPM) 版がリポジトリーで利用可能になるのを待つ間、テストを有効にするために **podman-etcd** エージェントをインストールしていました。このリリースでは、RPM 版が利用可能になったため、MCO によってインストールされたエージェントが削除されます。(OCPBUGS-58894)

- 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-58341)

- 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、コントローラーが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、サービスアカウントにリンクされている **ImagePullSecrets** がビルドで使用されます。(OCPBUGS-57951)

- 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、ベースボード管理コントローラー (BMC) URL 追加時の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-56765)

- この更新前は、**oc-mirror v2** の **imageSetConfiguration** パラメーターで **blockedImages** 値を定義するときに、ミラーリングからイメージを除外するための広範なイメージ参照リストを指定する必要がありました。実行間でイメージダイジェストが変わるため、この要件によりイメージをミラーリングから除外できないことがありました。このリリースでは、**blockedImages** 値に正規表現を使用できるようになり、ミラーリングからイメージを除外することが容易になりました。(OCPBUGS-56728)

- 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。そのため、OpenShift Container Platform 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-52592)

1.9.19.2. 更新

OpenShift Container Platform 4.19 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-2025:10771 - OpenShift Container Platform 4.19.4 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 7 月 15 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.4 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-2025:10771 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-2025:10772 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 4.19.4 --pullspecs
```

1.9.20.1. バグ修正

- 以前は、Gateway API 機能が有効になっていると、1 つの Pod レプリカと関連する **PodDisruptionBudget** が設定された Istio コントロールプレーンがインストールされていました。**PodDisruptionBudget** 設定により、唯一の Pod レプリカの削除が阻止され、クラスターのアップグレードがブロックされていました。このリリースでは、**PodDisruptionBudget** 設定を使用して Istio コントロールプレーンを設定することが Ingress Operator によって防止されるため、クラスターのアップグレードが可能になりました。(OCPBUGS-58394)

- 以前は、フォームビューを使用して **Edit HorizontalPodAutoscaler** をクリックすると、ランタイムエラーが発生していました。このリリースでは、**Edit HorizontalPodAutoscaler** フォームビューが期待どおりにレンダリングされるようになりました。(OCPBUGS-58377)

- 以前は、**console.tab/horizontalNav** の **href** 値でスラッシュが許可されていました。バージョン 4.15 以降は、リグレッションにより、**href** 値でスラッシュを使用すると正しく機能しませんでした。このリリースでは、**console.tab/horizontalNav** の **href** 値のスラッシュが以前のように期待どおりに機能します。(OCPBUGS-58375)

- 以前は、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-58335)

- 以前は、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-58316)

- 以前は、oc-mirror プラグイン 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たため、コンテナーレジストリーが **too many requests** というエラーにより一部のリクエストを拒否していました。このリリースでは、いくつかの関連パラメーターのデフォルト値が調整され、コンテナーレジストリーに送信されるリクエストの数が少なくなりました。(OCPBUGS-58279)

- 以前は、証明書のローテーション後、API サーバーへの不正アクセスが原因で kubelet サーバー証明書が更新されませんでした。その結果、クラスターが健全でない状態で起動していました。このリリースでは、証明書のローテーション後に kubelet サーバー証明書が更新されるため、健全なクラスター状態が維持されます。(OCPBUGS-58116)

- 以前は、オンプレミスの installer-provisioned infrastructure 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-57781)

- 以前は、**--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** コマンドに正しく関連付けられました。その結果、**--dry-run=server** オプションの使用時に、イメージオブジェクトの誤った削除が防止され、**istag** オブジェクトがそのまま残るようになりました。(OCPBUGS-57206)

- 以前は、古いバージョンの 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、そのグループをマシンセットに指定できませんでした。このリリースでは、OpenShift Container Platform がこの設定と互換性のある新しいバージョンの Azure API を使用します。(OCPBUGS-56163)

1.9.20.2. 更新

OpenShift Container Platform 4.19 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. RHBA-2025:10290 - OpenShift Container Platform 4.19.3 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 7 月 8 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.3 が利用可能になりました。更新に含まれるバグ修正のリストは、RHBA-2025:10290 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-2025:10291 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 4.19.3 --pullspecs
```

1.9.21.1. バグ修正

- 以前は、**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表示されます。(OCPBUGS-58077)

- 以前は、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-57781)

- 以前は、**oc-mirror v2** の **imageSetConfiguration** パラメーターで **blockedImages** 値を定義するときに、ミラーリングからイメージを除外するための広範なイメージ参照リストを指定する必要がありました。実行間でイメージダイジェストが変わるため、この要件によりイメージをミラーリングから除外できないことがありました。このリリースでは、**blockedImages** 値に正規表現を使用できるようになり、ミラーリングからイメージを除外することが容易になりました。(OCPBUGS-56728)

- 以前は、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生成されていました。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 のノードが大きなパケットを含む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-55997)

- 以前は、OpenShift Container Platform 4.19 を実行中のクラスターが、VMWare vSAN ファイルからエクスポートされたネットワークファイルシステム (NFS) ボリュームをマウントできるようにするには、vSAN ファイルを 8.0 P05 以降に更新する必要がありました。このリリースでは、VMWare vSAN ファイルボリュームをマウントするために、既存の vSAN ファイルサービスのバージョンをアップグレードする必要はありません。(OCPBUGS-55978)

1.9.21.2. 更新

OpenShift Container Platform 4.19 クラスターをこの最新リリースに更新するには、CLI を使用したクラスターの更新 を参照してください。

1.9.22. RHSA-2025:9750 - OpenShift Container Platform 4.19.2 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 7 月 1 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.2 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHSA-2025:9750 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-2025:9751 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 4.19.2 --pullspecs
```

1.9.22.1. バグ修正

- 以前は、インストールプログラムが、インストール設定の最初のコンピュートマシンプールエントリーのみをチェックして、Machine Config Operator (MCO) ブートイメージ管理機能を無

効にするかどうかを判断していました。複数のコンピュートプールが指定されている場合 (Amazon Web Services (AWS) エッジノードが唯一のサポート対象環境)、別のコンピュートマシンプールにカスタムの Amazon Machine Image (AMI) があると、インストールプログラムが MCO ブートイメージ管理を無効にせず、カスタム AMI が MCO によって上書きされていました。このリリースでは、インストールプログラムがすべてのコンピュートマシンプールのエントリーをチェックするようになり、カスタムイメージが見つかった場合は MCO ブートイメージ管理が無効になります。(OCPBUGS-58060)

- 以前は、ユーザーが Amazon Web Services (AWS) または Google Cloud のカスタムブートイメージを指定した場合、Machine Config Operator (MCO) がインストール中にそのイメージをデフォルトのブートイメージで上書きしていました。このリリースでは、MCO 設定用のマニフェスト生成機能が追加され、カスタムイメージが指定された場合にインストール中にデフォルトのブートイメージが無効化されるようになりました。(OCPBUGS-57796)

- 以前は、**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://.** を使用しようとすると、**content filepath is tainted** 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、**oc-mirror** プラグインが '.' ディレクトリー参照を適切に検証します。(OCPBUGS-57786)

- 以前は、**oc-mirror v2** コマンド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。そのため、設定で指定されたよりも多くの Operator が追加されたり、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カタログレジストリーに接続しようとしたりするなどのエラーが発生しました。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-57784)

- 以前は、**Create Project** モーダルが開いたとき、または Networking ページのモーダルがトリガーされたときに、Red Hat OpenShift Lightspeed の UI が消えていました。これは、モーダルが **useModal** フックを使用して、モーダルが互いに上書きしてしまうことが原因でした。このリリースでは、モーダルが互いに上書きしなくなり、複数の UI 要素を同時に表示できるようになりました。(OCPBUGS-57755)

- 以前は、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、liveness プローブがカスタマイズされました。IBM Cloud では、Hypershift 上の不適切なプローブ設定による中断を回避しつつ、より正確なヘルスチェックを行うために、**/livez?exclude=etcd&exclude=log** が使用されます。一方、他のプラットフォームでは、引き続き **/version** が使用されます。(OCPBUGS-57485)

- 以前は、AWS の認証情報が見つからない状態でサーベイが AWS のリージョンを取得しようとすると、インストーラーが失敗し、ユーザーが **install-config** ファイルを作成できませんでした。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ラーが失敗しなくなり、ユーザーがサーベイの途中で認証情報を入力できるようになりました。(OCPBUGS-57394)

- 以前は、Web コンソールで永続ボリューム要求 (PVC) のクローンを作成すると、ストレージサイズの単位 **B** がサポートされていないためにエラーが発生していました。そのため、ストレージサイズの単位が正しく解析されず、Red Hat OpenShift コンソールの PVC のクローンを作成するときにエラーが発生していました。このリリースでは、ストレージサイズの単位 **B** のサポートが Red Hat OpenShift コンソールの PVC から削除されました。(OCPBUGS-57391)

- 以前は、**olm.maxOpenShiftVersion** が **4.19** に設定された Operator をインストールするために、Operator Lifecycle Manager (OLM) v1 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 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、olm.maxOpenShiftVersion:4.19**

が設定された Operator がインストールされている場合に、OpenShift Container Platform へのアップグレードが防止されるようになりました。(OCPBUGS-56852)

- 以前は、権限が不足しているために、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。これにより、共有 Ingress サービスを使用している環境で、Ingress 仮想 IP アドレス (VIP) が誤って割り当てら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たため、ヘルスチェックが正しく機能するようになりました。(OCPBUGS-56623)

1.9.22.2. 更新

OpenShift Container Platform 4.19 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-2025:9278 - OpenShift Container Platform 4.19.1 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 6 月 24 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.1 が利用可能になりました。この更新に含まれるバグ修正のリストは、RHSA-2025:9278 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-2025:9279 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 4.19.1 --pullspecs
```

1.9.23.1. バグ修正

- 以前は、Assisted Installer のインストール後用に vCenter クラウド認証情報を追加すると、クラウドプロバイダー設定の無効な ConfigMap オブジェクトが原因でバグがトリガーされていました。その結果、missing vcenterplaceholder エラーが表示されました。このリリースにより、ConfigMap データが正しくなり、エラーが表示されなくなりました。(OCPBUGS-57384)

- 以前は、クラスターの API 呼び出し中のネットワークの問題により、Operator Lifecycle Manager (OLM) Classic でタイムアウトが生じました。その結果、Operator のインストールはタイムアウトの問題が原因で失敗することがよくありました。このリリースでは、カタログキャッシュの更新間隔が更新され、タイムアウトの問題が解決されました。その結果、Operator のインストールがタイムアウトする可能性が低減されます。(OCPBUGS-57352)

- 以前は、Operator Lifecycle Manager (OLM) Classic での Operator グループの調整は、集計ルールセレクターの順序が変更されるため、不要な ClusterRole の更新をトリガーしていました。その結果、不要な API サーバーの書き込みが発生していました。このリリースでは、バグ修正により、アグリゲーションルールで ClusterRoleSelectors 配列の確定的な順序が確保され、不要な API サーバーの書き込みが削減されて、クラスターの安定性が向上しました。(OCPBUGS-57279)

- 以前は、assisted-service のインストール設定で AdditionalTrustBundlePolicy 設定を無視したため、Federal Information Processing Standard (FIPS) およびその他のインストール設定のオーバーライドが発生していました。このリリースでは、インストール設定には AdditionalTrustBundlePolicy フィールドが含まれ、これを設定して FIPS およびその他のインストール設定のオーバーライドが意図された通りに機能するようになりました。(OCPBUGS-57208)

- 以前は、/metrics エンドポイントの認証プロセスにはトークンレビューチェックがなく、不正な要求が発生していました。その結果、OpenShift Container Platform コンソールで TargetDown アラートが発生しやすくなっていました。このリリースにより、承認されていないリクエストのトークンレビューは、要求コンテキストで提供されるユーザートークンで実行されます。その結果、OpenShift Container Platform コンソールへの認可されていない要求は TargetDown アラートを発生させません。(OCPBUGS-57180)

- 以前は、画面サイズの縮小時に Started 列が非表示になりました。その結果、ソート機能がないため、VirtualizedTable コンポーネントは機能せず、テーブルの並べ替え機能が PipelineRun リストページで影響を受けました。このリリースでは、画面サイズが小さい場合にテーブルコンポーネントにソート機能がなくても、正しく処理されるようになりました。(OCPBUGS-57110)

- 以前は、テーマにマストヘッドロゴを設定しても、テーマの他の部分にデフォルト設定を使用した場合、ユーザーインターフェイスに表示されるロゴに一貫性がありませんでした。このリリースでは、マストヘッドロゴにライトテーマとダークテーマの両方のデフォルトオプションが表示され、インターフェイスの整合性が向上しました。(OCPBUGS-57054)

- 以前は、Network Load Balancer (NLB) のセキュリティーグループ設定が無効であるため、クラスターのインストールが失敗していました。この失敗により、ブートストラップ用の

両方のプライマリーサブネットからのトラフィックが妨げられていました。このリリースにより、セキュリティーグループはブートストラップ用の両方のプライマリーサブネットからのトラフィックを許可し、追加のプライマリーサブネットにセキュリティーグループの制限があるため、クラスターのインストールが失敗しなくなりました。(OCPBUGS-57039)

- 以前は、プロジェクトアクセスのないユーザーは、不適切な API グループアクセスが原因で、Roles ページに不完全なロールリストを表示していました。このリリースにより、プロジェクトアクセスのないユーザーには、Roles ページの不完全なロールリストが表示されなくなりました。(OCPBUGS-56987)

- 以前は、node-image create コマンドはディレクトリーパーミッションを変更し、操作中にユーザーディレクトリーが元のパーミッションを失うことがありました。このリリースにより、node-image create コマンドは、rsync ツールを使用してファイルのコピープロセス中にファイルパーミッションを保存し、ユーザーディレクトリーが操作中に元のパーミッションを維持できるようになりました。(OCPBUGS-56905)

- 以前は、ImageSetConfiguration ファイル内で delete というキーワードを含むイメージ名が許可されていましたが、これはサポートされていない仕様です。その結果、ユーザによるイメージのミラーリング中にエラーが発生していました。このリリースにより、ImageSetConfiguration ファイルで delete で終わるイメージ名のエラーが削除されました。その結果、ユーザーは delete で終わる名前を持つイメージを正常にミラーリングできるようになりました。(OCPBUGS-56798)

- 以前は、Observe Alerting フィールドのユーザーインターフェイスに、情報アラートの誤ったアラート重大度アイコンが表示されていました。このリリースでは、アラートの重大度アイコンが Observe Alerting フィールドで一致します。その結果、アラートアイコンは一貫して一致し、ユーザーが混乱する可能性を軽減します。(OCPBUGS-56470)

- 以前は、oc-mirror コマンドで不正アクセス設定ファイルを使用すると、イメージセットの同期時に Unauthorized エラーが表示されていました。このリリースにより、認証にカスタム認証ファイルを使用するように Docker 設定が更新されました。Unauthorized エラーが発生することなく、イメージセットを正常に同期できます。(OCPBUGS-55701)

1.9.23.2. 更新

OpenShift Container Platform 4.19 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-2024:11038 - OpenShift Container Platform 4.19.0 イメージのリリース、バグ修正、およびセキュリティー更新アドバイザリー

発行日: 2025 年 6 月 17 日

セキュリティー更新を含む OpenShift Container Platform リリース 4.19.0 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-2024:11038 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-2025:2851 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。

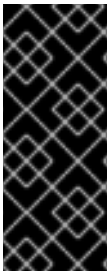
```
$ oc adm release info 4.19.0 --pullspecs
```

1.9.24.1. 更新

OpenShift Container Platform 4.19 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 4.19 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

External Secrets Operator for Red Hat OpenShift

F

File Integrity Operator

H

Hosted Control Plane

K

Kube Descheduler Operator

Red Hat build of Kueue

L

Leader Worker Set Operator

ロギング

M

Migration Toolkit for Containers (MTC)

N

Network Observability Operator

Network-bound Disk Encryption (NBDE) Tang Server Operator

O

OpenShift API for Data Protection (OADP)

Red Hat OpenShift Dev Spaces

Red Hat OpenShift Distributed Tracing Platform

Red Hat OpenShift GitOps

Red Hat OpenShift Local (アップストリームの CRC ドキュメント)

Red Hat OpenShift Pipelines

OpenShift sandboxed containers

Red Hat OpenShift Serverless

Red Hat OpenShift Service Mesh 2.x

Red Hat OpenShift Service Mesh 3.x

Red Hat OpenShift support for Windows Containers

Red Hat OpenShift Virtualization

Red Hat build of OpenTelemetry

P

Red Hat OpenShift 用パワーモニタリング

R

Run Once Duration Override Operator

S

Secondary Scheduler Operator for Red Hat OpenShift

Security Profiles Operator

Z

Zero Trust Workload Identity Manager