Red Hat OpenShift Container Storage 4.8

4.8 リリースノート

機能および拡張機能についてのリリースノート、既知の問題その他重要なリリース情報

Last Updated: 2021-12-09

Red Hat OpenShift Container Storage 4.8 4.8 リリースノート

機能および拡張機能についてのリリースノート、既知の問題その他重要なリリース情報

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

法律上の通知

概要

以下の Red Hat OpenShift Container Storage 4.8 リリースノートでは、新機能および拡張機能のすべて、主な技術上の変更点、および一般公開バージョンの既知の問題についてまとめています。

目次

第1章 はじめに

Red Hat OpenShift Container Storage は、コンテナー環境向けに最適化されたソフトウェアで定義されるストレージです。これは OpenShift Container Platform の Operator として実行され、コンテナーの統合され、単純化された永続ストレージの管理を可能にします。

Red Hat OpenShift Container Storage は最新の Red Hat OpenShift Container Platform に統合され、プラットフォームサービス、アプリケーションの移植性、および永続性の課題に対応します。これは、Red Hat Ceph Storage、Rook.io Operator、および NooBaa の Multicloud Object Gateway テクノロジーを含む新たなテクノロジースタックに構築された、次世代クラウドネイティブアプリケーション向けの高度にスケーラブルなバックエンドを提供します。

Red Hat OpenShift Container Storage は、数多くの方法でアプリケーションのライフサイクル全体におけるユーザーエクスペリエンスを単純化し、強化する、信頼できるエンタープライズクラスのアプリケーション開発環境を提供します。

- データベースのブロックストレージを提供します。
- 継続的な統合、メッセージングおよびデータ集約のための共有ファイルストレージ。
- クラウドファースト開発、アーカイブ、バックアップ、およびメディアストレージ用のオブジェクトストレージ。
- アプリケーションとデータの飛躍的なスケーリングが可能です。
- 永続データボリュームの割り当てと割り当て解除を加速的に実行します。
- 複数のデータセンターまたはアベイラビリティーゾーンにクラスターを拡張します。
- 包括的なアプリケーションコンテナーレジストリーを確立します。
- データアナリティクス、人工知能、機械学習、ディープラーニング、および IoT (モノのインターネット) などの次世代の OpenShift ワークロードをサポートします。
- アプリケーションコンテナーだけでなく、データサービスボリュームおよびコンテナー、さらに追加の OpenShift Container Platform ノード、Elastic Block Store (EBS) ボリュームおよびその他のインフラストラクチャーサービスを動的にプロビジョニングします。

1.1. 本リリースについて

Red Hat OpenShift Container Storage 4.8 (RHBA-2021:3002 および RHBA-2021:3003) をご利用いただけるようになりました。以下では、OpenShift Container Storage 4.8 に関連する新たな拡張機能、新機能、および既知の問題について説明します。

Red Hat OpenShift Container Storage 4.8 は、Red Hat OpenShift Container Platform バージョン 4.8 でサポートされます。詳細は、『Red Hat OpenShift Container Storage のサポート容易性および相互運用性ガイド』を参照してください。

OpenShift Container Storage 4.8 のリリースで、バージョン 4.5 のライフサイクルは終了します。詳細は、「Red Hat OpenShift Container Platform ライフサイクルポリシー」を参照してください。

第2章 新機能

このセクションでは、Red Hat OpenShift Container Storage 4.8 で導入された新機能について説明します。

コンパクトなデプロイメント一般公開サポート

OpenShift Container Storage は、3 ノードの OpenShift のコンパクトなベアメタルクラスターにインストールできるようになりました。ここでは、すべてのワークロードが 3 つの強力なマスターノードで実行されます。ワーカーノードまたはストレージノードは含まれません。

コンパクトなベアメタルクラスターで OpenShift Container Platform を設定するには、3 ノードクラスターの設定について、またエッジデプロインメントの 3 ノードアーキテクチャーの提供について参照してください。

オブジェクトバケットのキャッシュポリシー

Red Hat OpenShift Container Storage の Multicloud Object Gateway では、キャッシュバケットを作成できるようになりました。キャッシュバケットは、ハブのターゲットとキャッシュターゲットが指定された namespace バケットです。詳細は、オブジェクトバケットのキャッシュポリシーについて参照してください。

ストレージクラスの一般公開サポートによる永続ボリュームの暗号化

デバイスの暗号化キーを保存するために外部の鍵管理システム (KMS) を使用して、ストレージクラスの暗号化で永続ボリューム (ブロックのみ) を暗号化できます。永続ボリュームの暗号化は RBD 永続ボリュームでのみ利用できます。ストレージクラスの暗号化は OpenShift Container Storage 4.7 以降でサポートされます。詳細は、永続ボリュームの暗号化を使用したストレージクラスの作成方法について参照してください。

永続ボリュームの暗号化はスナップショットおよびクローンもサポートします。

VMware プラットフォームのプロビジョニングされたストレージの使用

VMware がホストする OpenShift Container Platform のシンプロビジョニングされたストレージに加えて、パフォーマンスとセキュリティーが向上します。OpenShift Container Storage でシックプロビジョニングのストレージを使用するように柔軟性が必要な場合、OpenShift Container Platform で zeroedthick または eagerzeroedthick 形式でストレージクラスを作成する必要があります。OpenShift Container Storage クラスターサービスの作成時に、デフォルトのシンストレージクラスに加えて作成されるストレージクラスを選択するオプションを取得できます。

詳細は、「OpenShift Container Storage Cluster Service の作成 」を参照してください。

新しいプール管理ユーザーインターフェース

新しい管理機能には、シンプルで、ストレージクラスの作成や、自動的にアタッチされたプールの作成や、既存のプールの特性を更新したい場合 (圧縮、レプリカなど) を簡単に使用できます。この機能は、既存のストレージクラス設定の代わりではありません。詳細は、**『ストレージリソースの管理および割り当て』**ガイドの「ブロックプール」の章を参照してください。

IBM Power Systems および IBM Z インフラストラクチャーでのエアギャップ (オフライン環境) のサポート

OpenShift Container Storage 4.8 のデプロイメントがエアギャップされた環境で、インターネット接続のない環境で実行できるようになりました。

IBM Power Systems および IBM Z インフラストラクチャーでの Multicloud Object Gateway

IBM Power Systems および IBM Z インフラストラクチャー上の Red Hat OpenShift Container Storage

4.8 では、オブジェクトワークロードにマルチクラウドおよびハイブリッド機能を提供する Noobaa のマルチクラウドオブジェクトサービスのサポートが追加されました。デフォルトで、Multicloud Object Gateway はクラウドネイティブまたは RGW のデフォルトのバッキングストアを使用します。

IBM Power Systems の暗号化されたストレージデータ

管理者は、デプロイメントプロセスの一部として OpenShift Container Storage 4.8 クラスターのすべてのデータを暗号化することを選択できるようになりました。詳細は、「データ暗号化オプション」を参照してください。

IBM Z インフラストラクチャーでの DASD のサポート

DASD が IBM Z インフラストラクチャーのストレージノードでサポートされるようになりました。

第3章 機能拡張

ここでは、Red Hat OpenShift Container Storage 4.8 で導入された主な拡張機能について説明します。

1つ以上の OSD 要求を処理する時間が長い場合にユーザーに通知を改善するために新規アラートを追加

このアラートは、OpenShift Container Storage の管理者に低速な操作について通知することが重要です。これは、極端の負荷、低速なストレージデバイス、またはソフトウェアのバグを示します。ユーザーは、Ceph のステータスを確認して低速さの有無を確認することができます。

ClusterObjectStoreState アラートメッセージは、RADOS Object Gatewa y(RGW) が利用できない場合に生成されます。

以前のバージョンでは、RADOS Object Gateway (RGW) が利用できないか、または正常ではない場合、**ClusterObjectStoreState** アラートメッセージは生成されませんでした。OpenShift Container Storage Operator に実装される修正では、RADOS Object Gateway (RGW) が利用できない場合に、または正常ではない場合に ClusterObjectStoreState アラートが表示されるようになりました。

プールで圧縮を有効または無効にする機能

OpenShift Container Storage 4.8 以降では、ユーザーインターフェースを使用して、プールで圧縮を有効または無効にすることができます。

OpenShift Container Platform ユーザーインターフェースを使用して namespace バケットを作成する機能を追加

namespace バケットは、OpenShift Container Platform ユーザーインターフェースを使用して追加できます。namespace バケットは、クラウドまたは S3 と互換性のあるストレージ (オンプレミス) の既存オブジェクトバケットの集計ビューを提供します。ユーザーインターフェースを使用して namespace バケットを追加する方法の詳細は、「OpenShift Container Platform ユーザーインターフェースを使用した namespace バケットの追加」を参照してください。

初回のデプロイメント時に利用可能なすべてのデバイスの使用およびローカルストレージデバイスのスケールアップ

割り当てられたモードのデプロイメントですべてのローカルストレージデバイスが、ローカルで利用可能なストレージデバイスをすべて使用するようになりました。同様に、容量を追加してスケールアップする際に、利用可能なストレージデバイスをすべて追加できます。

ノードドレイン（解放）以外の理由により OSD が停止している場合に、障害ドメインに no-out フラグを追加しないようにします。

ディスク障害により OSD がダウンすると、障害ドメインに **no-out** フラグが追加されます。これにより、OSD が標準の ceph mon_osd_down_out_interval を使用してマークアウトされないようにします。今回の更新により、ノードのドレイン以外の理由で OSD がダウンすると、pgs が正常でなくなると、他の障害ドメインでブロックする PodDisruptionBudget が作成され、さらにノードがドレインされないようにするようになります。この場合、**noout** フラグはノードに設定されません。OSD がダウンしているものの、すべての pgs が **active+clean** の場合、クラスターは完全に正常なものとして処理されます。デフォルトの PodDisruptionBudget (maxUnavailable=1 を使用) は再び追加され、ブロックするものが削除されます。

第4章 テクノロジープレビュー

テクノロジープレビュー機能は、カスタマーポータルの「テクノロジプレビュー機能のサポート範囲」で詳細に説明されているように制限されたサポート範囲で提供されます。

このセクションでは、テクノロジープレビューのサポート制限に基づいて、Red Hat OpenShift Container Storage 4.8 で導入されたテクノロジープレビュー機能について説明します。

Arbiter を使用した障害復旧

今回のリリースにより、Red Hat OpenShift Container Storage は、ストレージクラスターの作成時に、3 番目のゾーンを arbiter の場所とした上で、単一クラスターを 2 つのゾーンに展開できるように Metro-DR ストレッドクラスター (arbiter) 機能を提供するようになりました。

詳細は、『デプロイメントプランニング』ガイドの障害復旧について参照してください。

マルチネットワークプラグイン (Multus) のサポート

ネットワークの分離によるセキュリティーとパフォーマンスを向上させるためにマルチコンテナーネットワークプラグイン (multus) を使用する機能をサポートします。この機能は、ベアメタルおよび VMWare デプロイメントでのみテストされています。multus の詳細は、「Multi network plug-in (Multus) support」を参照してください。

注記

プラグイン Pod を削除すると、ノードの再起動が実行されるまでデータにアクセスできません。これは既知の問題です。詳細は、プラグイン Pod が削除されると、ノードの再起動が行われるまでデータはアクセス不可能になります。 を参照してください。

第5章 DEVELOPER プレビュー

このセクションでは、Red Hat OpenShift Container Storage 4.7 で導入された Developer プレビュー機能について説明します。

Developer プレビュー機能は、Developer プレビューのサポート制限の対象となります。Developer プレビューのリリースは、実稼働環境で実行することは意図されていません。Developer プレビュー機能と共にデプロイしたクラスターは開発用クラスターとして考慮され、Red Hat カスタマーポータルのケース管理システムではサポートされません。Developer プレビュー機能に関してサポートが必要な場合には、ocs-devpreview@redhat.com メーリングリストに連絡してください。Red Hat Development Team のメンバーが稼働状況とスケジュールに応じて可能な限り迅速に対応します。

ホストグループごとのデータ分離

ワークロードは特定の分離された IO パスを使用し、特定のストレージノードに分散して、部分的なクラスターに障害が発生した場合や、テナントを分離させる場合にの影響を制限できます。

詳細は、ナレッジベースのアーティクルを参照してください。

地域による障害復旧

Red Hat OpenShift Container Storage は、 2 つの kubernetes クラスターを提供する 2 つの Openshift Container Storage クラスター全体でのストレージボリュームのマルチクラスターの非同期レプリケーションを提供します。ステートレスアプリケーションを含むステートフルなアプリケーションには、ピアクラスターに同じものをデプロイする前に準備が必要です。

オブジェクトストレージデバイスの重みおよび Pod のアフィニティー設定

OpenShift Container Storage 以外のデバイスでパーティション化されたディスクを効率的に使用して、ワークロードをブロックしずに容量の使用率を最大化できるようになりました。オペレーティングシステム用の専用パーティションを持つパーティション化デバイスなど、ホストマシン上のすべてのソリッドステートドライブ (SSD) にオブジェクトストレージデバイス (OSD) を割り当てることができます。同じ物理デバイスを共有するので、効率を向上させるために、OSD の負荷を軽減することができます。負荷を減らすために、OSD の重みおよび Pod のアフィニティーパラメーターを Storage Cluster CR に設定できます。

詳細は、ナレッジベースのアーティクルを参照してください。

OpenShift Container Storage コンポーネントのデプロイメントでの柔軟性

コンポーネントデプロイメントの柔軟性により、デプロイメント中に、コンポーネントのマルチクラウドオブジェクトゲートウェイ、RGW、および CephFS を無効にできるようになりました。OpenShift Container Storage の作成後にこれらのコンポーネントを有効または無効にすることもできます。この柔軟性により、Amazon S3 を使用する際にリソースコストを削減できます。

詳細は、ナレッジベースのアーティクルを参照してください。

第6章 バグ修正

このセクションでは、Red Hat OpenShift Container Storage 4.8 で導入された主なバグ修正について説明します。

Arbiter と柔軟なスケーリングを同時に有効にすることはできません。

Arbiter と柔軟なスケーリングの両方が有効にされると、ログやエラー **arbiter and flexibleScaling both can't be enabled** のメッセージが存在する場合でも、ストレージクラスターは **READY** 状態のままと表示されませんでした。これは、ストレージクラスター CR の正しくない仕様が原因で発生します。今回の更新により、ストレージクラスターは正しいエラーメッセージを出して「ERROR」の状態になりました。

(BZ#1946595)

バケットは、ライブラリーでクリーンアップが必要な場合に常に削除されます。

以前のバージョンでは、OBC の作成に失敗しました。lib-bucket-provisioner は再試行前にクリーンアップ目的で削除要求をプロビジョナーに送信していました。NooBaa プロビジョナーはオブジェクトバケットの回収ポリシーを確認しますが、場合によっては基礎となるバケットは削除されませんでした。今回の更新により、クリーンアップのシナリオにおいて、基礎となるバケットが回収ポリシーに関係なく削除されるようになりました。

(BZ#1947796)

アタッチされた各 OSD の設定の収集

以前のバージョンでは、各 OSD の詳細な設定を特定する方法はありませんでした。今回の更新により、**must-gather** は OSD のすべての設定を収集し、デバッグをさらに改善するようになりました。

(BZ#1962755)

gRPC メトリクスがデフォルトで無効になりました

以前のバージョンでは、**cephcsi** Pod はデバッグ目的でリモートプロシージャーコール (gRPC) メトリクスを公開していました。**cephcsi** ノードプラグイン Pod は、**cephcsi** ノードプラグイン Pod が実行されているノードで、CephFS のホストポート 9091 と RBD 用のホストポート 9090 を使用していました。そのため、**cephcsi** Pod は起動しませんでした。今回の更新により、gRPC メトリクスはデフォルトで無効になり、**cephcsi** Pod はノードプラグイン Pod が実行されているノードでポート 9091 および 9090 を使用しなくなりました。

(BZ#1923819)

MDS レポートがサイズの大きいキャッシュを報告する

以前のバージョンでは、Rook はアップグレード時に mds_cache_memory_limit を適用していませんでした。つまり、そのオプションが適用されていない OpenShift Container Storage 4.2 クラスターは正しい値 (通常は Pod のメモリー制限のサイズの半分) で更新されませんでした。そのため、standby-replay の MDS は、サイズの大きいキャッシュを報告する可能性があります。

(BZ#1944148)

新たに復元された PVC がノードにマウント可能に

以前のバージョンでは、Ceph-CSI ドライバーのバグにより、Red Hat Enterprise Linux バージョンの 8.2 よりも少ないノードで、削除された親スナップショットで新たに復元された PVC をマウントする際に (深いフラット化機能がない)、誤った「RBD image not found」エラーが発生しました。この問題は、Red Hat Enterprise Linux のバージョンが 8.2 未満のノードにマウントする前に、新たに復元された PVC をフラット化することで修正されました (ディープフラット化機能がない場合)。

(BZ#1956232)

信頼性のある mon クォーラム

以前のバージョンでは、mon フェイルオーバー中に Operator が再起動されると、Operator は新しい mon を誤って削除する可能性があります。したがって、Operator が新しい mon を削除した場合、mon のクォーラムはリスクとして必要になります。今回の更新により、Operator は mon フェイルオーバーが進行中の状態を復元し、Operator の再起動後に mon フェイルオーバーを適切に完了するようになりました。ノードのドレインおよび mon フェイルオーバーのシナリオで mon クォーラムがより信頼できるようになりました。

(BZ#1955831)

第7章 既知の問題

このセクションでは、Red Hat OpenShift Container Storage 4.8 の既知の問題について説明します。

Arbiter ノードに OpenShift Container Storage ノードラベルでラベル付けできない

Arbiter ノードは、OpenShift Container Storage ノードラベル **cluster.ocs.openshift.io/openshift-storage** でラベル付けされた場合に、有効な Arbiter 以外のノードとみなされます。これは、Arbiter 以外のリソースの配置が確定されないことを意味します。この問題を回避するには、Arbiter リソースのみが Arbiter ノードに配置されるように Arbiter ノードに OpenShift Container Storage ノードラベルを付けないようにします。

(BZ#1947110)

Ceph のステータスは、ディスクの交換後の HEALTH_WARN です。

ディスクの交換後に、すべての OSD Pod が稼働している場合でも、**1 daemons have recently crashed** 警告が見られます。この警告により、Ceph のステータスが変更されます。Ceph のステータスは、HEALTH_WARN ではなく HEALTH_OK である必要があります。この問題を回避するには、rsh を ceph-tools Pod に実行し警告を非表示にすると、Ceph の正常性は HEALTH_OK に戻ります。

(BZ#1896810)

CephCluster リソースでのモニタリング仕様がリセットされる

ocs-operator が再起動するか、またはアップグレード時には常に監視仕様は空になります。これは機能への影響はありませんが、モニタリングエンドポイントの詳細が必要な場合は、空にします。

この問題を解決するには、4.7 から 4.8 にアップグレードした後に **rook-ceph-external-cluster-details** シークレットを更新し、すべてのエンドポイントの詳細 (active および standby MGRs など) が「MonitoringEndpoint」データキーに更新されます。これは、新規でアップグレードされたクラスターとアップグレードされたクラスターにあるエンドポイントの数が異なるため、今後発生する問題を回避するのに役立ちます。

(BZ#1984735)

noobaa-db-pg-0 の問題

noobaa-db-pg-0 Pod は、ホストしているノードがダウンしても他のノードに移行しません。NooBaa は、ノードがダウンすると noobaa-db-pg-0 Pod の移行がブロックされるために機能しません。

(BZ#1783961)

プラグイン Pod が削除されると、ノードの再起動が行われるまでデータはアクセス不可能になります。

この問題は、**csi-cephfsplugin** Pod が再起動すると、マウントの **netns** が破棄されるため、**csi-cephfsplugin** はすべてのマウントされたボリュームをロックします。この問題は、multus を有効にしてクラスターでのみ見られます。

この問題は、削除後に **csi-cephfsplugin** が再起動したノードを再起動する際に解決されます。

(BZ#1979561)

暗号化パスフレーズは、スナップショットからボリュームを復元するためのソース KMS に保存されます。

親と復元された PVC の異なるバックエンドパスを持つ StorageClass が異なる場合、復元された PVC は **Bound** 状態に行われ、スナップショットから KMS 設定のバックエンドパスに暗号化パスフレーズ

が作成されます。暗号化パスフレーズの確認は 2 番目の StorageClass パスにリンクされた設定を使用するので、復元された PVC は Pod に割り当てられないようにすることができます。この場合、暗号化パスフレーズはバックエンドパスに見つかりません。

この問題を防ぐために、PVC はスナップショットを作成し、それらを復元する際に常に同じ KMS 設定を使用する必要があります。

(BZ#1975730)

キーは、kv-v2 シークレットエンジンを使用する場合に、暗号化された PVC を削除した後に Vault に一覧表示されます。

HashiCorp Vault は、保存されたキーの削除先である key-value store v2 の機能を追加しました。これにより、削除されたキーのメタデータが別のステップで削除されない場合にコンテンツを回復できます。Hashicorp Vault のシークレットに key-value v2 ストレージを使用する場合に、ボリュームを削除すると、KMS から暗号化パスフレーズのメタデータは削除されません。後で暗号化パスフレーズを復元することが可能です。これらの部分的に削除されたキーは、KMS によって自動的にクリーンアップされません。

この問題を解決するには、削除されたキーのメタデータを手動で削除します。メタデータで **deletion_time** が設定されているキーはすべて、キー/値のストレージ v1 が使用され、v2 で利用可能になる際に削除されていると想定されます。

(BZ#1979244)

親 PVC よりもサイズが大きい Restore Snapshot/Clone 操作により無限ループが生じる

Ceph CSI は、親 PVC よりもサイズが大きい場合にスナップショットの復元やクローンの作成をサポートしません。そのため、サイズが多い Restore Snapshot/Clone 操作により、無限ループが生じます。この問題を回避するには、保留中の PVC を削除します。より大きい PVC を取得するには、仕様しちえる操作に基づいて以下のいずれかを完了する必要があります。スナップショットを使用する場合、既存のスナップショットを復元し、親 PVC と同じサイズのボリュームを作成し、これを Pod に割り当て、PVC を必要なサイズに拡張します。詳細は、「Volume snapshots」を参照してください。Clone を使用する場合、親 PVC のクローンを作成し、親 PVC と同じサイズのボリュームを作成し、これを Pod に割り当て、PVC を必要なサイズに拡張します。詳細は、「ボリュームのクローン作成」を参照してください。

(BZ#1870334)

PVC はスナップショットから復元するか、シックプロビジョニングされた PVC からクローンがプロビジョニングされていません。

シックプロビジョニングされた PVC のスナップショットが **thic provisioning** のストレージクラスを使用して復元されると、復元されたボリュームはプロビジョニングされません。復元される PVC は、シックプロビジョニングなしで **Bound** 状態に達します。この問題は、RHCS-5.x が使用される場合にのみ修正できます。以前の Ceph バージョンは、ゼロ入力データブロックのコピーをサポートしません (シックプロビジョニング時に使用)。

現在、RHCS-4.x ベースのデプロイメントで問題を解決するには、プロビジョニングされているボリュームの PVC-cloning および snapshot-restor に上限としてマークを付けることです。新規に作成されたボリュームは、シンプロビジョニングされます。

(BZ#1959793)

プロビジョニングが進行中に保留中の PVC および RBD プロビジョナーリーダー Pod を削除すると、古いイメージと OMAP メタデータが残されます。

RBD PVC がプロビジョニングされている場合、Persistent Volume Claim (永続ボリューム要求、PVC) は **Pending** 状態になります。RBD プロビジョナーリーダーおよび PVC 自体が削除されても、RBD イメージと OMAP メタデータは削除されません。

この問題に対処するには、プロビジョニングが進行中に PVC を削除しないでください。

(BZ#1962956)

ストレージクラスターの使用が 85% に達するか、PVC を削除した後にも、プロビジョニングは停止しませんでした。

RBD シック PVC がプロビジョニングされている間にストレージクラスターの使用状況が 85% に達すると、プロビジョニングは保留中の PVC を削除して自動的に停止しません。また、保留中の PVC を削除しても RBD イメージは削除されません。

要求されたサイズが利用可能なストレージを超えても、プロビジョニングを開始しないのが最良のアプローチではありません。

(BZ#1965016)

kv-v2 が使用されると、Vault の OSD のキーはアンインストール時に削除されません

キー暗号化キー**データ**は、Vault K/V Secret エンジンがバージョン 2 の場合に、クラスターの削除時に Vault からソフト削除されます。つまり、任意のバージョンのキーを取得できるため、削除が元に戻されます。メタデータは引き続き表示されるので、鍵を復元できます。これによって不整合が生じても、vault コマンドに「destroy」引数を指定して手動でキーを削除できます。

(BZ#1975323)

CephBlockPool の削除がスタックし、新規プールの作成をブロックします。

Multus が有効なクラスターでは、Rook Operator にはネットワークアノテーションがないため、OSD ネットワークにアクセスできません。つまり、プールのクリーンアップ中に「rbd」タイプコマンドを実行すると、OSD と通信できないためコマンドがハングします。回避策として、toolbox を使用して **CephBlockPool** を手動で削除します。

(BZ#1983756)

デバイス置き換えのアクションは、暗号化された OpenShift Container Storage クラスター用のユーザーインターフェースから実行できません。

暗号化された OpenShift Container Storage クラスターでは、検出の結果 CR は Ceph OSD (Object Storage Daemon) がサポートするデバイスを検出します。これは、Ceph アラートで報告されるデバイスとは異なります。アラートをクリックすると、ユーザーには「Disk not found」というメッセージが表示されます。不一致があるため、コンソール UI は OpenShift Container Storage ユーザー用にディスク置き換えオプションを有効にすることはできません。この問題を回避するには、『デバイスの置き換え』ガイドにあるように、障害のあるデバイスの置き換えに CLI 手順を使用します。

(BZ#1906002)

volumeMode をブロックとして持つ PVC の false 通知

Kubernetes の変更により、OpenShift Container Platform の Prometheus アラートでリグレッションが発生します。この変更は以下に影響があります。

Alert: KubePersistentVolumeFillingUp.

PVC: volumeMode: Block の PVC

namespace の一致する正規表現: "(openshift-.|kube-.|default|logging)"

Metric: **kubelet_volume_stats_available_bytes**

その結果、アラートの kubelet_volume_stats_available_bytes は PVC の作成時から利用可能なサイズを 0 として報告します。また、正規表現 "(openshift-.|kube-.|default|logging)" に一致する namespace の volumeMode: Block のすべての PVC 似対して false アラートが実行されます。これは、内部および内部接続モードにデプロイされた OpenShift Container Storage の OSD デバイスセット用に作成されたすべての PVC と Amazon Web Services、VMware、ベアメタルなどの異なるインフラストラクチャーに影響を与えます。これは、お客様のワークロード PVC にも影響します。

現在、OpenShift Container Platform 4.8.z の今後のマイナーリリースで修正されるまで、この問題に対する回避策はありません。そのため、OpenShift Container Storage によるストレージ容量に関するアラートに厳密に迅速に対応し、緊急性のあるアラートに対処します。

(BZ#1984817)

ストレージクラスターの再インストール中に cephobjectstore の ceph オブジェクトが作成されると、Arbiter ストレージクラスターのインストール後に重大なアラート通知が送信されます。

CephCluster および 1 つ以上の **CephObjectStores** を含むストレージクラスターでは、**CephCluster** リソースがすべて **CephObjectStore** リソースを完全に削除する前に削除しても、Rook Operator はメモリー内の CephObjectStore(s)に関する接続の詳細を保持できます。同じ **CephCluster** および CephObjectStore(s)が再作成されると、CephObjectStore(s)は「Failed」の状態になる可能性があります。

この問題を回避するには、CephCluster を削除する前に CephObjectStore(s) を完全に削除します。

- CephObjectStore(s)が削除されるのを待機しない場合は、Rook Operator を再起動して (Operator Pod を削除して)、アンインストール後に実行しても問題がなくなります。
- この問題が発生している場合、Rook Operator を再起動すると、Operator の古い **CephObjectStore** 接続の詳細をクリアし、Rook Operator を再起動してこれを解決します。

(BZ#1974344)