Red Hat OpenShift Data Foundation 4.16

4.16 リリースノート

機能および拡張機能、既知の問題、その他の重要なリリース情報に関するリリースノート

Last Updated: 2024-09-10

Red Hat OpenShift Data Foundation 4.16 4.16 リリースノート

機能および拡張機能、既知の問題、その他の重要なリリース情報に関するリリースノート

法律上の通知

概要

Red Hat OpenShift Data Foundation 4.16 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をまとめています。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

第1章 概要

Red Hat OpenShift Data Foundation は、コンテナー環境向けに最適化されたソフトウェア定義のストレージです。このソフトウェアは、OpenShift Container Platform の Operator として実行されるため、コンテナーの永続ストレージ管理を高度に統合し、簡素化できます。

Red Hat OpenShift Data Foundation 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 Data Foundation は FIPS 用に設計されています。RHEL または FIPS モードでブートされた RHEL CoreOS で実行する場合、OpenShift Container Platform コアコンポーネントは、x86_64、ppc64le、および s390X アーキテクチャー上でのみ、FIPS 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。RHEL 暗号化ライブラリーの個別バージョンに関して検証用に提出された最新の NIST ステータスは、Compliance Activities and Government Standards を参照してください。

Red Hat OpenShift Data Foundation 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. このリリースについて

Red Hat OpenShift Data Foundation 4.16 (RHSA-2024:4591) が利用可能になりました。以下では、OpenShift Data Foundation 4.16 に関連する新たな拡張機能、新機能、および既知の問題を説明します。

Red Hat OpenShift Data Foundation 4.16 は、Red Hat OpenShift Container Platform バージョン 4.16 でサポートされます。詳細は、Red Hat OpenShift Data Foundation Supportability and Interoperability Checker を参照してください。

Red Hat OpenShift Data Foundation のライフサイクル情報は、Red Hat OpenShift Container Platform ライフサイクルポリシー で、階層化された製品 (および依存関係のある製品) ライフサイクルのセクション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 Data Foundation 4.16 で導入された新機能を説明します。

2.1. 障害復旧ソリューション

2.1.1. 障害復旧で検出されたアプリケーションのユーザーインターフェイスサポート

RHACM を使用してデプロイされていない検出されたアプリケーション (検出されたアプリケーション) の場合、OpenShift Data Foundation 障害復旧ソリューションは、RHACM を使用して管理されるフェイルオーバーおよびフェイルバック操作の新しいユーザーエクスペリエンスによって保護を拡張します。

詳細は、検出されたアプリケーションの Metro-DR 保護 および 検出されたアプリケーションの Regional-DR 保護 を参照してください。

2.1.2. ラベルによる Kube リソース保護を必要とするアプリケーション向けの障害復旧ソリューション

OpenShift Data Foundation 障害復旧ソリューションは、命令型モデルを使用して開発またはデプロイされたアプリケーションをサポートします。検出されたアプリケーションのクラスターリソースは、OpenShift APIs for Data Protection (OADP) を使用してセカンダリークラスターで保護および復元されます。

検出されたアプリケーションを登録する方法については、Metro-DR 用の検出されたアプリケーションの登録 および Regional-DR 用の検出されたアプリケーションの登録 を参照してください。

2.1.3. 検出されたアプリケーション DR サポートを namespace が複数あるアプリケーションに拡張

OpenShift Data Foundation Disaster Recovery ソリューションによる保護は、複数の namespace にまたがる検出対象アプリケーションにまで拡張されました。

2.1.4. Regional-DR 向け OpenShift 仮想化ワークロード

OpenShift Data Foundation を使用すると、OpenShift Virtualization ワークロードに対して Regional disaster recovery (Regional-DR) ソリューションを簡単に設定できます。

詳細は、ナレッジベースの記事 Use OpenShift Data Foundation Disaster Recovery to Protect Virtual Machines を参照してください。

2.1.5. ストレッチクラスターでの OpenShift 仮想化

OpenShift Data Foundation を使用した OpenShift Virtualization テクノロジーに基づくワークロードのストレッチクラスターによる障害復旧を簡単に設定できるようになりました。

詳細は、OpenShift Container Platform ガイドの OpenShift Virtualization を参照してください。

2.1.6. Regional-DR の代替クラスターへの復旧

Regional-DR のプライマリークラスターまたはセカンダリークラスターに障害が発生した場合、クラスターを修復するか、既存のクラスターの回復を待つか、クラスターが修復不可能な場合はクラスター全体を置き換えることができます。OpenShift Data Foundation は、障害が発生したプライマリーまたは

セカンダリークラスターを新しいクラスターに置き換え、新しいクラスターへのフェイルオーバー (再配置) を可能にする機能を提供します。

詳細は、代替クラスターへの復元 を参照してください。

2.1.7. ACM サブスクリプションアプリケーションタイプの監視サポートの有効化

Red Hat Advanced Cluster Management (RHACM) コンソールの障害復旧ダッシュボードは、ApplicationSet タイプのアプリケーションに加えて、サブスクリプションタイプのアプリケーションの監視データを表示するように拡張されました。

以下のようなデータを監視できます。

- ボリュームレプリケーションの遅延
- レプリケーションの問題の有無にかかわらず、保護されているサブスクリプションタイプのアプリケーションの数
- レプリケーションが正常または異常な永続ボリュームの数
- アプリケーション単位のデータは以下のようになります。
  - Recovery Point Objective (RPO)
  - 最後の同期時間
  - 現在の DR アクティビティーステータス (Relocating、Failing over、Deployed、Relocated、Failed Over)
- 正常なレプリケーションと異常なレプリケーションを含む、アプリケーションごとの永続ボリューム数

2.1.8. 共同サイトおよび中立サイトの Regional-DR デプロイメントに対するハブ復旧サポート

OpenShift Data Foundation の Regional disaster recovery ソリューションは、Red Hat Advanced Cluster Management を使用して、中立サイトのデプロイメントと、共存するマネージドクラスターのハブ復旧をサポートするようになりました。ハブリカバリーセットアップを設定するには、パッシブハブとして機能する 4 番目のクラスターが必要です。パッシブハブクラスターは、次のいずれかの方法で設定できます。

- プライマリーマネージドクラスター (Site-1) は、アクティブな RHACM ハブクラスターと共存でき、パッシブハブクラスターは、セカンダリーマネージドクラスター (Site-2) とともに配置します。
- アクティブな RHACM ハブクラスターは、サイト 1 のプライマリーマネージドクラスターまたはサイト 2 のセカンダリークラスターのいずれかの障害の影響を受けない中立サイト (サイト 3) に配置できます。このような状況では、パッシブハブクラスターを使用する場合は、Site-2 のセカンダリークラスターと一緒に配置できます。

詳細は、Red Hat Advanced Cluster Management を使用したハブのリカバリーの Regional-DR の章 を参照してください。

2.2. 毎週のクラスター全体の暗号鍵のローテーション

一般的なセキュリティープラクティスでは、定期的な暗号鍵のローテーションが求められます。OpenShift Data Foundation は、Kubernetes シークレット (KMS 以外) に保存されている暗号鍵を毎週自動的にローテーションします。

詳細は、クラスター全体の暗号化 を参照してください。

2.3. カスタムの TAINT のサポート

カスタムの taint は、ストレージクラスター CR を使用して、CR の配置セクションの下に toleration を直接追加することで設定できます。これにより、カスタムの taint を追加するプロセスが簡素化されます。

詳細は、ナレッジベースの記事 How to add toleration for the "non-ocs" taints to the OpenShift Data Foundation pods? を参照してください。

2.4. READWRITEONCEPOD アクセスモードによる SELINUX マウント機能のサポート

OpenShift Data Foundation は、ReadWriteOncePod アクセスモードで SELinux マウント機能をサポートするようになりました。この機能を使用することで、特にボリュームに多数のファイルがあり、CephFS などのリモートファイルシステム上にある場合に、ボリューム内のファイルとフォルダーの SELinux ラベル変更にかかる時間を短縮できます。

2.5. READWRITEONCEPOD アクセスモードのサポート

OpenShift Data Foundation は、クラスター全体で 1 つの Pod のみが永続ボリューム要求 (PVC) を読み取ったり、書き込んだりできるようにするための ReadWriteOncePod (RWOP) アクセスモードを提供します。

2.6. OSD バックフィル中のクライアント IO またはリカバリー IO の高速化

メンテナンスウィンドウ中にクライアント IO またはリカバリー IO を優先するように設定できます。クライアント IO よりもリカバリー IO を優先すると、OSD リカバリー時間が大幅に短縮されます。

リカバリープロファイルの設定の詳細は、OSD バックフィル中のクライアント IO またはリカバリー IO の高速化の有効化 を参照してください。

2.7. POD 用の汎用一時ストレージのサポート

OpenShift Data Foundation は、汎用の一時ボリュームをサポートします。このサポートにより、ユーザーは Pod 仕様で汎用の一時ボリュームを指定し、PVC のライフサイクルを Pod に結び付けることができます。

2.8. クロスストレージクラスクローン

OpenShift Data Foundation は、クローン作成中にレプリカ 3 を含むストレージクラスからレプリカ 2 またはレプリカ 1 に移動する機能を提供します。これにより、ストレージの占有スペースを削減できます。

詳細は、クローンの作成 を参照してください。

2.9. オーバープロビジョニングレベルのポリシー制御

オーバープロビジョニング制御メカニズムにより、特定のアプリケーション namespace に基づいて、ストレージクラスターから消費される永続ボリューム要求 (PVC) の量に対するクォータを定義できます。

このオーバープロビジョニング制御メカニズムを有効にすると、ストレージクラスターから消費される PVC のオーバープロビジョニングが防止されます。

詳細は、Overprovision level policy control を参照してください。

第3章 機能拡張

このセクションでは、Red Hat OpenShift Data foundation 4.16 で導入された主な拡張機能を説明します。

3.1. バケットポリシーの新しい要素

OpenShift Data Foundation に、バケットポリシー要素 **NotPrincipal**、**NotAction**、**NotResource** が追加されました。これらの要素の詳細は、IAM JSON policy elements reference を参照してください。

3.2. MULTICLOUD OBJECT GATEWAY OPERATOR への新しい AWS リージョンの追加

デフォルトのバッキングストアを作成するために、Multicloud Object Gateway (MCG) Operator のサポート対象リージョンに新しい AWS リージョン **ca-west-1** が追加されました。

3.3. OPENSHIFT DATA FOUNDATION MULTICLOUD OBJECT GATEWAY BACKINGSTORE のリソース割り当ての増加

OpenShift Data Foundation MCG BackingStore にさらに多くのリソースを割り当てられるように、PV プールの CPU とメモリーのデフォルトリソースがそれぞれ 999m と 1Gi に増えました。

3.4. MULTICLOUD OBJECT GATEWAY による HTTPS のみで動作するルートの作成

HTTP を無効にして HTTPS のみを使用する必要があるデプロイメントの場合、ストレージクラスター CR **spec.multiCloudGateway.denyHTTP** に **DenyHTTP** を設定するオプションが追加されます。これにより、Multicloud Object Gateway によって作成されたルートは HTTPS のみを使用するようになります。

3.5. DR 保護ワークロードの保護条件の追加および監視用のメトリクスとアラートの追加

ManagedCluster からの DR 保護ワークロードに関するさまざまな条件をまとめることで、DR 保護ワークロードへの保護条件が追加され、それに基づいてメトリクスとアラートが生成されます。

それぞれの PVC の内容が同期されたタイミングをもってのみ、ハブで DR 保護されたワークロードの健全性が反映されます。これは、RegionalDR のユースケースにのみ適用され、MetroDR のユースケースには適用されません。**ManagedCluster** では、ワークロード DR 保護の健全性がいくつかの条件に拡張されます。そのため、これらの条件全体でワークロード DR の健全性を監視することは簡単ではありません。このように保護条件とアラートを追加することで、ワークロードの DR 保護監視が向上されます。

3.6. NAMESPACESTORE ファイルシステムでの複数のアップロードのリスト表示のサポート

次のコマンドを使用して、NamespaceStore ファイルシステムでまだアップロード中のファイルや不完全なマルチパートアップロードをリスト表示できるようになりました。

```
$ s3api list--multipart-uploads --bucket <bucket_name>
```

3.7. CEPH の FULL、 NEARFULL、 BACKFILLFULL 属性のしきい値を変更するオプション

クラスターの要件に応じて、**odf-cli** CLI コマンドを使用して、**full**、**nearfull**、および **backfillfull** しきい値を更新できます。

以下に例を示します。

odf set full <val>

odf set nearful <val>

odf set backfillfull <val>

注記

値は 0.0 - 1.0 の範囲でなければならず、値が 1.0 に極めて近くならないようにする必要があります。

第4章 テクノロジープレビュー

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 Data Foundation 4.16 で導入されたテクノロジープレビュー機能を説明します。

重要

テクノロジープレビュー機能は、実稼働環境での Red Hat サービスレベルアグリーメント (SLA) ではサポートされておらず、機能的に完全ではない可能性があるため、Red Hat では実稼働環境での使用を推奨していません。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、お客様は機能性をテストし、開発プロセス中にフィードバックをお寄せいただくことができます。

テクノロジープレビュー機能は、カスタマーポータルの テクノロジー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。

4.1. クラスター全体/PV 暗号化のための AZURE KEY VAULT オプション

OpenShift Data Foundation は、Microsoft Azure プラットフォーム上のクラスター全体で PV を暗号化するために Azure Key Vault をサポートしています。これにより、サードパーティーツールの代わりに Azure のローカルネイティブソリューションを使用できるようになります。

詳細は、OpenShift Data Foundation クラスターの作成 を参照してください。

4.2. MULTICLOUD OBJECT GATEWAY バケットのバケットロギングとログベースのレプリケーション最適化

Multicloud Object Gateway (MCG) と Amazon Web Services (AWS) 間、または MCG と MCG 間の大量データのレプリケーションをサポートします。バケットロギングを使用した AWS S3 のログベースレプリケーションのサポートが MCG バケットに拡張され、最適化されました。ログベースのレプリケーション最適化では、オブジェクト接頭辞フィルタリングもサポートされます。

詳細は、Multicloud Object Gateway のバケットログ記録の有効化 を参照してください。

4.3. IPV6 のマルチネットワークプラグイン (MULTUS) のサポート

Multus ネットワークは、IPv4 または IPv6 のいずれかを使用するように設定できます。OpenShift Data Foundation は、ピュア IPv4 またはピュア IPv6 の Multus ネットワークをサポートします。ネットワークは混在モードにできません。Mutlus の詳細は、マルチネットワークプラグイン (Multus) のサポート を参照してください。

第5章 開発者向けプレビュー

このセクションでは、Red Hat OpenShift Data Foundation 4.16 で導入された開発者プレビュー機能を説明します。

重要

開発者プレビュー機能は、開発者プレビューのサポート制限の対象となります。開発者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。開発者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。開発者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。

5.1. OPENSHIFT DATA FOUNDATION 外部モードでのトポロジー認識とレプリカ 1 のサポート

OpenShift Data Foundation は、ストレージクラスを使用して replica-1 からのストレージのプロビジョニングをサポートします。ストレージクラスは、別のゾーンにある replica-1 Ceph プールからストレージをプロビジョニングするために作成されます。こうすることで、アプリケーションで、複数のインスタンスを実行して、サービスインスタンスごとに、それぞれ異なるゾーンに配置されるように新しいクレームを作成する場合に役立ちます。これらのアプリケーションには独自の冗長インスタンスがあるため、データ層での冗長性は必要ありません。詳細は、ナレッジベースの記事 OpenShift Data Foundation external mode support for RBD/block Replica-1 pools and topology awareness を参照してください。

5.2. バックアップができるようにマルチボリュームの一貫性を確保 - CEPHFS

アプリケーションのサポートを強化し、OpenShift Virtualization をサポートするために、バックアップソリューションにクラッシュ整合性のあるマルチボリューム整合性グループが提供されます。これは、複数のボリュームにデプロイされるアプリケーションに有用です。

5.3. CEPHFS のレプリカ 2 を備えたストレージクラス

OpenShift Data Foundation は、レプリカを 2 つ使用して新しい CephFS ベースのストレージクラスを作成する方法を提供します。これにより、CephFs のみが使用されている場合に、ストレージ効率が向上します。また、これにより、RBD または CephFS がバランスよく使用されていない場合の解決策となります。詳細は、ナレッジベースの記事 Using replica 2 for CephFS を参照してください。

5.4. RGW の自動スケーリング

OpenShift Data Foundation は、自動スケーリングを有効にして、S3 負荷に応じて RADOS Gateway (RGW) の保守性とパフォーマンスを自動的に調整する機能を提供します。詳細は、ナレッジベースの記事 Autoscaling for RGW in OpenShift Data Foundation via HPA using KEDA を参照してください。

5.5. 両方のディスクが同じゾーンにある CEPH REPLICA-2 プール

OSD ディスク障害が発生した場合にアプリケーションを保護するできるように、1 つのゾーンに両方のディスクが配置された replica-2 を作成できます。

詳細は、ナレッジベースの記事 RBD Replica-2 with both disks in same zone を参照してください。

5.6. 内部モードでの RGW イレージャーコーディング

CLI を使用した RGW の消去コーディングのデプロイメントがサポートされ、ストレージ効率を向上することでコスト削減を実現します。

詳細は、ナレッジベースの記事 Support for RGW Erasure Coding in Internal Mode 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 Data Foundation 4.16 で導入された重要なバグ修正を説明します。

6.1. 障害復旧

アプリケーションのフェイルオーバーが FailingOver の状態でハングする

以前は、提供されていた S3 ストアに必要とされるリソースが正常に保護されなかったため、アプリケーションが正しく DR 保護されませんでした。そのため、このようなアプリケーションをフェイルオーバーすると、FailingOver 状態になります。

この修正により、メトリクスと関連のアラートがアプリケーション DR 保護の健全性機能に追加され、DR の保護機能がアプリケーションに適用された後に、保護に関する問題が発生した場合に修正を促すアラートが表示されます。その結果、正常に保護されたアプリケーションがフェイルオーバーされます。

(BZ#2248723)

ハブの回復後、FailedOver 状態にあったアプリケーションは一貫して FailingOver を報告する

以前は、回復したハブクラスター上の Ramen ハブ Operator は、ハブとそのピアのマネージドクラスターの両方がなくなったにも関わらずダウンしなかったマネージドクラスターを、今後のフェイルオーバーアクションに対して **Ready** の状態であると、このようなステータスがこれらのクラスターから報告されているか確認せずに、報告しました。

この修正により、Ramen ハブ Operator は、アクションを開始する前に、ターゲットクラスターがフェイルオーバー操作の準備ができているかどうかを確認します。その結果、開始されたフェイルオーバーはすべて成功します。または、フェイルオーバーターゲットクラスターに古いリソースがまだ存在する場合、Operator は古いリソースがクリーンアップされるまでフェイルオーバーを停止します。

(BZ#2270259)

6.2. MULTICLOUD OBJECT GATEWAY

Multicloud Object Gateway (MCG) DB PVC 消費量が 400 GB を超える

以前は、アクティビティーログが DB に保存されていたため、Multicloud Object Gateway (MCG) データベース (DB) では、必要のないときに DB サイズが増加していました。

この修正により、オブジェクトアクティビティーログは通常のデバッグログに変換されます。その結果、NooBaa DB では DB サイズの増加が表示されなくなりました。

(BZ#2141422)

ログベースのレプリケーションが OBC からレプリケーションポリシーを削除した後でも機能する

以前は、空の文字列が提示された場合にレプリケーションポリシーの評価でエラーが発生したため、Object Bucket Claim (OBC) からログベースのレプリケーションポリシーを削除できませんでした。

この修正により、レプリケーションポリシーの評価方法が変更され、OBC からレプリケーションポリシーを削除できるようになりました。

(BZ#2266805)

Multicloud Object Gateway (MCG) コンポーネントのセキュリティーコンテキストの修正

以前は、OpenShift によって設定されたデフォルトを回避するために、Multicloud Object Gateway (MCG) Pod のデフォルトのセキュリティーコンテキスト制約 (SCC) が更新されると、セキュリティースキャンプロセスが失敗しました。

この修正により、SCC がデフォルトのオーバーライドに更新されても、MCG の動作は変更されず、セキュリティースキャンが成功します。

(BZ#2273670)

NooBaa Operator のログが AWS のシークレットを公開する

以前は、NooBaa Operator のログは AWS シークレットをプレーンテキストとして公開していたため、ログを参照できるすべての人がバケットにアクセスできるという潜在的なリスクがありました。

この修正により、noobaa-Operator ログは AWS シークレットを公開しなくなりました。

(BZ#2277186)

AWS S3 リストに時間がかかる

以前は、1 つのデータベースクエリーではなく 2 つのデータベースクエリーが使用されていたため、AWS S3 ではオブジェクトのリスト表示に長い時間がかかっていました。

この修正により、クエリーが 1 つに再設定され、データベースへの呼び出しとオブジェクトリスト操作の完了にかかる時間が削減されます。

(BZ#2277990)

OpenShift Data Foundation にアップグレードすると、スタンドアロンの MCG バッキングストアが拒否される

以前は、永続ボリューム (PV) プールを使用しようとすると、オブジェクトのメタデータを保存するために **xattr** が使用されていました。にかかわらず、PV 上のファイルシステムは **xattr** をサポートしていないため、そのメタデータの更新は失敗します。

この修正により、ファイルシステムが **xattr** をサポートしておらず、メタデータがファイルに保存されている場合にフェイルバックが行われるようになりました。

(BZ#2278389)

Multicloud Object Gateway データベースの永続ボリューム要求 (PVC) の消費が継続的に増加する

以前は、Object Bucket Claim (OBC) を削除すると、そのオブジェクトがすべて削除され、データベースから解放されるまでに時間がかかっていました。これは、MCG のデータベースクリーナーの作業が限られていたために、データベースからのエントリーの削除が遅くなり、削除が制限されたためです。

この修正により、MCG の DB クリーナー設定の更新が可能になります。DB Cleaner は、MCG データベースから、以前の削除済みエントリーを削除するプロセスです。公開されていた設定は、実行の頻度と削除されるエントリーの経過時間です。

(BZ#2279742)

Multicloud Object Gateway バケットライフサイクルポリシーではすべてのオブジェクトが削除されない

以前は、期限切れのオブジェクトの削除までかなり時間がかかっていました。

この修正により、期限切れのオブジェクトを削除するためのバッチサイズと 1 日あたりの実行回数が増加します。

(BZ#2279964) (BZ#2283753)

HEAD リクエストが API から 404 の代わりに接頭辞パスの HTTP 200 コードを返す

以前は、Multicloud Object Gateway の NamespaceStore Filesystem バケット上のディレクトリーであるオブジェクトを読み取ったり、ヘッダーを作成したりしようとし、末尾の / 文字が欠落していると、リクエストは接頭辞パスに対して 404 ではなく HTTP 200 コードを返していました。

この修正により、オブジェクトがディレクトリーであるにもかかわらず、キーに末尾の / がない場合に **ENOENT** が返されます。

(BZ#2280664)

Multicloud Object Gateway Backingstore In Phase: "Connecting" with "Invalid URL"のエラー

以前は、Operator が調整ループでシステム情報を取得できなかったため、調整が正常に完了しませんでした。これは、アドレスが IPv6 の場合に解析が失敗する原因となった URL 解析のバグが原因でした。

この修正により、IPv6 アドレスの場合は URL ホストとして処理されるようになりました。その結果、Operator はシステムの調整を正常に完了します。

(BZ#2284652)

6.3. CEPH CONTAINER STORAGE INTERFACE (CSI) ドライバー

PVC のクローン作成が "RBD image not found" というエラーで失敗する

以前は、CephCSI ドライバーのバグが原因で、ドライバーがゴミ箱の中の RBD イメージを間違って識別したため、スナップショットの親が存在しない場合にボリュームのスナップショットの復元に失敗しました。

この修正により、CephCSI ドライバーのバグが修正され、ゴミ箱内のイメージが適切に識別されるようになり、その結果、スナップショットの親が存在しない場合でもボリュームスナップショットが正常に復元されるようになりました。

(BZ#2264900)

FUSE マウントが使用されていない場合でも、fuserecovery.go からの警告ログが不正確になる

以前は、カーネルマウンターが選択されている場合でも、**fuserecovery.go** などの Fuse 回復機能からの警告ログが記録され、誤解を招いていました。

この修正により、Fuse マウントが選択された場合にのみ Fuse 回復関数が試行または呼び出され、その結果、カーネルマウントが選択された場合には **fuesreovery.go** からのログは記録されなくなります。

(BZ#2266237)

6.4. OCS OPERATOR

RGW エンドポイントに到達できない場合、StorageClasses が作成されない

以前は、ストレージクラスが RADOS ゲートウェイ (RGW) ストレージクラスの作成に依存しており、RGW エンドポイントに到達できない場合に RADOS Block Device (RBD) および CephFS ストレージクラスが作成されませんでした。

この修正により、ストレージクラスの作成が独立し、結果としてストレージクラスは RGW ストレージクラスの作成に依存しなくなります。

(BZ#2213757)

6.5. OPENSHIFT DATA FOUNDATION コンソール

ステータスカードがスタンドアロン MCG デプロイメントのステータスを反映するようになる

以前は、Multicloud Object Gateway (MCG) スタンドアロンモードでは、OpenShift クラスターの概要ダッシュボードに、健全性のステータスが表示されず、ストレージに不明なアイコンが表示されていました。

この修正により、クラスターがスタンドアロンモードでデプロイされたときに MCG ヘルスメトリクスがプッシュされ、その結果、ストレージの健全性がクラスターの概要ダッシュボードに表示されるようになります。

(BZ#2256563)

StorageSystem の作成ウィザードがプロジェクトドロップダウンと重なる

以前は、**Create StorageSystem** ページの上部にある未使用の **Project** ドロップダウンが混乱を招き、どのシナリオでも使用されませんでした。

この修正により、**Project** ドロップダウンが削除され、結果としてページのヘッダーに StorageSystem creation namespace が生成されます。

(BZ#2271593)

容量と使用率カードにはカスタムストレージクラスが含まれない

以前は、要求された容量と使用率カードには、ストレージシステム作成の一環として OCS Operator によって作成されたデフォルトのストレージクラスのデータのみが表示されていました。カードには、後で作成されたカスタムストレージクラスは含まれません。これは、複数のストレージクラスターをサポートするために Prometheus がリファクタリングされたためです。

この修正により、クエリーが更新され、カードにはデフォルトとカスタムで作成されたストレージクラスの両方のレポート容量が表示されるようになりました。

(BZ#2284090)

6.6. ROOK

名前が重複した状態でストレージクラスデバイスセットがデプロイされると、Rook-Ceph Operator デプロイメントが失敗する

以前は、名前が重複した状態で StorageClassDeviceSets が StorageCluster CR に追加されると、OSD が失敗し、Rook は OSD 設定について混乱していました。

この修正により、CR 内に重複したデバイスセット名が見つかった場合、Rook はそれが修正されるまで OSD の調整を拒否します。Rook Operator ログに、OSD の調整に失敗したというエラーが表示されます。

(BZ#2259209)

Rook-ceph-mon Pod は 3300 ポートと 6789 ポートの両方をリッスンする

以前は、クラスターが MSGRv2 を使用してデプロイされると、mon pod はポート 6789 で MSGR1 トラフィックを不必要にリッスンしていました。

この修正により、mon デーモンは、v1 ポート 6789 でのリッスンを抑制し、v2 ポート 3300 のみを排他的にリッスンするフラグ付きで起動し、攻撃対象領域が縮小されます。

(BZ#2262134)

従来の LVM ベースの OSD がクラッシュループ状態にある

以前は、OpenShift Data Foundation 4.14 以降では、OSD のサイズを変更する init コンテナーでレガシー OSD がクラッシュしていました。これは、OpenShift Container Storage 4.3 で作成され、それ以降のバージョンにアップグレードされたレガシー OSD が失敗した可能性があるためです。

この修正により、クラッシュする resize init コンテナーが OSD Pod 仕様から削除されました。そのため、レガシー OSD は起動しますが、レガシー OSD をすぐに置き換えることを推奨します。

(BZ#2273398) (BZ#2274757)

6.7. CEPH の監視

クォータアラートが重複している

以前は、Object Bucket Claim (OBC) のクォータ制限に達すると、冗長なアラートが発生していました。これは、OBC クォータが 100% に達したときに、**ObcQuotaObjectsAlert** (OBC オブジェクトクォータが制限の 80% を超えたとき) と **ObcQuotaObjectsExhausedAlert** (クォータが 100% に達したとき) の両方のアラートが発動されたためです。

この修正により、アラートのクエリーが変更され、問題を示すアラートが一度に 1 つだけトリガーされるようになりました。その結果、クォータが 80% を超えると **ObcQuotaObjectsAlert** がトリガーされ、クォータが 100% になると **ObcQuotaObjectsExhausedAlert** がトリガーされます。

(BZ#2257949X)

プールクォータルールの PrometheusRule 評価が失敗する

以前は、マルチクラスター設定で **pool-quota** ルールにより **PrometheusRuleFailures** アラートが発行されたため、Ceph プールクォータアラートは表示されませんでした。**pool-quota** セクションのクエリーでは、マルチクラスター設定でアラートが発行されたクラスターを区別できませんでした。

この修正により、**pool-quota** 内のすべてのクエリーに **managedBy** ラベルが追加され、各クラスターから一意の結果が生成されるようになりました。その結果、**PrometheusRuleFailures** アラートは表示されなくなり、**pool-quota** 内のすべてのアラートが期待どおりに機能します。

(BZ#2262943)

一部のアラートの runbook に間違ったヘルプテキストが表示される

以前は、一部のアラートの runbook マークダウンファイルに間違ったテキストが含まれていたため、一部のアラートの runbook に間違ったヘルプテキストが表示されていました。

この修正により、runbook マークダウンファイル内のテキストが修正され、アラートに正しいヘルプテキストが表示されるようになります。

(BZ#2265492)

インストールまたはアップグレード後の PrometheusRuleFailures アラート

以前は、Ceph クォーラム関連のアラートが Prometheus 障害アラートとして認識されず、クエリーがあいまいな結果を生成した場合に通常出される **PrometheusRuleFailures** が発生していました。マルチクラスターのシナリオでは、**quorum-alert** がどのクラスターから発行されたかを識別できなかったため、クォーラムアラートルールのクエリーは区別できない結果を返していました。

この修正により、クォーラムルール内の各クエリーに一意の **managedBy** ラベルが追加され、クエリー結果に、結果を受信したクラスター名に関するデータが含まれるようになりました。その結果、Prometheus の障害は発生せず、クラスターは Ceph mon quorum 関連のアラートをすべてトリガーできるようになります。

(BZ#2266316)

2 つの ServiceMonitor、rook-ceph-exporter と rook-ceph-mgr のデフォルトの間隔期間が短い

以前は、サービスモニター、**rook-ceph-exporter**、および **rook-ceph-mgr** に提供される Prometheus scrapePVC の間隔がわずか 5 秒であったため、Prometheus によって収集されたエクスポーターデータによりシステムに負荷がかかっていました。

この修正により、Prometheus のスクレイピングのバランスをとるために間隔が 30 秒に増加され、システム負荷が軽減されます。

(BZ#2269354)

アップグレード中に LVM でバックアップされたレガシー OSD がある場合に警告が表示される

以前は、レガシー OSD を備えた OpenShift Data Foundation をバージョン 4.12 から 4.14 にアップグレードすると、すべての OSD がクラッシュループに陥ってダウンすることが確認されました。これにより、データが利用できなくなり、サービスが中断される可能性があります。

この修正により、ローカルボリュームマネージャー (LVM) に基づくレガシー OSD を検出し、アップグレードプロセス中にそのような OSD が存在する場合に警告するチェックが含まれるようになりました。その結果、アップグレード中にレガシー OSD に関する警告が表示され、適切なアクションを実行できるようになります。

(BZ#2279928)

第7章 既知の問題

このセクションでは、Red Hat OpenShift Data Foundation 4.16 の既知の問題を説明します。

7.1. 障害復旧

- **マネージドクラスターのアプリケーション namespace の作成**
  アプリケーション namespace は、Disaster Recovery(DR) 関連の事前デプロイアクションのために RHACM マネージドクラスターに存在する必要があるため、アプリケーションが ACM ハブクラスターにデプロイされるときに事前に作成されます。ただし、アプリケーションがハブクラスターで削除され、対応する namespace がマネージドクラスターで削除された場合、それらはマネージドクラスターに再表示されます。

  回避策: **openshift-dr** は、ACM ハブのマネージドクラスター namespace に namespace **manifestwork** リソースを維持します。これらのリソースは、アプリケーションの削除後に削除する必要があります。たとえば、クラスター管理者として、ハブクラスターで以下のコマンドを実行します。

  ```
  $ oc delete manifestwork -n <managedCluster namespace> <drPlacementControl name>-<namespace>-ns-mw
  ```

  (BZ#2059669)

- **クラスターがストレッチモードの場合、ceph df が無効な MAX AVAIL 値を報告する**
  Red Hat Ceph Storage クラスターのクラッシュルールに複数の "take" ステップがある場合、**ceph df** レポートは、マップの使用可能な最大サイズを間違って表示します。この問題は、今後のリリースで修正される予定です。

  (BZ#2100920)

- **両方の DRPC が、同じ namespace で作成されたすべての永続ボリューム要求を保護する**
  複数の障害復旧 (DR) で保護されたワークロードをホストする namespace は、指定されていないハブクラスター上の同じ namespace 内の各 DRPlacementControl リソースの namespace にある永続ボリュームクレーム (PVC) をすべて保護し、その **spec.pvcSelector** フィールドを使用してワークロードに基づいて PVC を分離します。

  これにより、複数のワークロードにわたって DRPlacementControl **spec.pvcSelector** に一致する PVC が生成されます。あるいは、すべてのワークロードでセレクターが欠落している場合、レプリケーション管理が各 PVC を複数回管理し、個々の DRPlacementControl アクションに基づいてデータの破損または無効な操作を引き起こす可能性があります。

  回避策: ワークロードに属する PVC に一意のラベルを付け、選択したラベルを DRPlacementControl **spec.pvcSelector** として使用して、どの DRPlacementControl が namespace 内の PVC のどのサブセットを保護および管理するかを明確にします。ユーザーインターフェイスを使用して DRPlacementControl の **spec.pvcSelector** フィールドを指定することはできません。したがって、そのようなアプリケーションの DRPlacementControl を削除し、コマンドラインを使用して作成する必要があります。

  結果: PVC は複数の DRPlacementControl リソースによって管理されなくなり、操作およびデータの不整合は発生しません。

  (BZ#2128860)

- **MongoDB Pod は、cephrbd ボリュームのデータを読み取る許可エラーのため、CrashLoopBackoff になっています**

異なるマネージドクラスターにまたがる OpenShift プロジェクトには、異なるセキュリティーコンテキスト制約 (SCC) があり、特に指定された UID 範囲と **FSGroups** が異なります。これにより、特定のワークロード Pod とコンテナーが、ログ内のファイルシステムアクセスエラーが原因で、これらのプロジェクト内でフェイルオーバーの操作または再配置操作を開始できなくなります。

回避策: ワークロードプロジェクトが同じプロジェクトレベルの SCC ラベルを持つすべてのマネージドクラスターで作成されていることを確認し、フェイルオーバーまたは再配置時に同じファイルシステムコンテキストを使用できるようにします。Pod は、ファイルシステム関連のアクセスエラーで DR 後のアクションに失敗しなくなりました。

(BZ#2081855)

- **障害復旧のワークロードが削除されたままになる**
クラスターからワークロードを削除すると、対応する Pod が **FailedKillPod** などのイベントで終了しない場合があります。これによ
り、**PVC**、**VolumeReplication**、**VolumeReplicationGroup** などの DR リソースに依存するガベージコレクションで遅延または障害が発生する可能性があります。また、古いリソースがまだガベージコレクションされていないため、クラスターへの同じワークロードの今後のデプロイもできなくなります。

  回避策: Pod が現在実行中で、終了状態でスタックしているワーカーノードを再起動します。これにより、Pod が正常に終了し、その後、関連する DR API リソースもガベージコレクションされます。

  (BZ#2159791)

- **Regional DR CephFS ベースのアプリケーションのフェイルオーバーで、サブスクリプションに関する警告が表示される**
アプリケーションがフェイルオーバーまたは再配置されると、ハブサブスクリプションに "Some resources failed to deployUse View status YAML link to view the details." というエラーが表示されます。これは、バッキングストレージプロビジョナーとして CephFS を使用し、Red Hat Advanced Cluster Management for Kubernetes (RHACM) サブスクリプションでデプロイし、DR で保護されたアプリケーションの永続ボリューム要求 (PVC) がそれぞれの DR コントローラーにより所有されているためです。

  回避策: サブスクリプションステータスのエラーを修正する回避策はありません。ただし、デプロイに失敗したサブスクリプションリソースをチェックして、それらが PVC であることを確認できます。これにより、他のリソースに問題が発生しないようにします。サブスクリプション内のデプロイに失敗した唯一のリソースが DR で保護されているリソースである場合、エラーは無視できます。

  (BZ-2264445)

- **PeerReady フラグを無効にすると、アクションをフェイルオーバーに変更できなくなります**
DR コントローラーは、必要に応じて完全な調整を実行します。クラスターにアクセスできなくなると、DR コントローラーは健全性チェックを実行します。ワークロードがすでに再配置されている場合、この健全性チェックによりワークロードに関連付けられた **PeerReady** フラグが無効になり、クラスターがオフラインであるため健全性チェックは完了しません。その結果、無効にされた **PeerReady** フラグは、アクションを Failover に変更できなくなります。

  回避策: コマンドラインインターフェイスを使用して、**PeerReady** フラグが無効になっているにもかかわらず、DR アクションをフェイルオーバーに変更します。

  (BZ-2264765)

- **ストレッチクラスター内の 2 つのデータセンター間の接続が失われると、Ceph にアクセスできなくなり、IO が一時停止します。**
2 つのデータセンターが相互の接続を失っても Arbiter ノードに接続されたままの場合は、モニター間で無限の選出が発生するという選出ロジックに不具合があります。その結果、モニターはリーダーを選出できず、Ceph クラスターが使用できなくなります。また、接続が切断されている間は IO が一時停止されます。

  回避策: モニターがクォーラムを超えているデータセンターの 1 つでモニターをシャットダウンし (**ceph -s** コマンドを実行すると確認可)、残りのモニターの接続スコアをリセットします。

  その結果、モニターがクォーラムを形成できるようになり、Ceph が再び使用可能になり、IOs resume が再開します。

  (Partner BZ#2265992)

- **交換前のクラスターからの古い Ceph プール ID を使用すると、RBD アプリケーションの再配置に失敗する**
新しいピアクラスターが作成される前に作成されたアプリケーションの場合、ピアクラスターが置き換えられると CSI configmap 内の CephBlockPoolID のマッピングを更新できないため、RBD PVC をマウントできません。

  回避策: 交換されていないピアクラスター上の cephBlockPoolID のマッピングを使用して **rook-ceph-csi-mapping-config** configmap を更新します。これにより、アプリケーション用の RBD PVC をマウントできるようになります。

  (BZ#2267731)

- **使用できない管理対象クラスター上のプライマリーワークロードのハブ回復後、lastGroupSyncTime に関する情報が失われる**
以前に管理対象クラスターにフェイルオーバーされたアプリケーションは **lastGroupSyncTime** を報告しないため、**VolumeSynchronizationDelay** のアラートがトリガーされます。これは、DRPolicy の一部である ACM ハブと管理対象クラスターが使用できない場合、バックアップから新しい ACM ハブクラスターが再構築されるためです。

  回避策: ワークロードのフェイルオーバー先のマネージドクラスターが使用できない場合でも、残っているマネージドクラスターにフェイルオーバーできます。

  (BZ#2275320)

- **MCO Operator が veleroNamespaceSecretKeyRef と CACertificates フィールドを調整する**
OpenShift Data Foundation Operator がアップグレードされると、Ramen 設定の **s3StoreProfiles** の下の **CACertificates** フィールドと **veleroNamespaceSecretKeyRef** フィールドが失われます。

  回避策: Ramen 設定に **CACertificates** フィールドと **veleroNamespaceSecretKeyRef** フィールドのカスタム値がある場合は、アップグレードの実行後にそれらのカスタム値を設定します。

  (BZ#2277941)

- **アップグレード後の token-exchange-agent Pod が不安定である**
以前のデプロイメントリソースが適切にクリーンアップされていないため、マネージドクラスター上の **token-exchange-agent** Pod が不安定になります。これにより、アプリケーションのフェイルオーバーアクションが失敗する可能性があります。

  回避策: ナレッジベースの記事 "token-exchange-agent" pod on managed cluster is unstable after upgrade to ODF 4.16.0 を参照してください。

結果: 回避策に従うと、"token-exchange-agent" pod が安定し、フェイルオーバーアクションが期待どおりに機能します。

(BZ#2293611)

- **再配置時に MAC 割り当てに失敗したため、virtualmachines.kubevirt.io リソースの復元に失敗する**
仮想マシンを優先クラスターに再配置すると、MAC アドレスが使用できないために再配置を完了できない場合があります。これは、仮想マシンがフェイルオーバークラスターにフェイルオーバーされたときに、優先されるクラスター上で完全に消去されていない場合に発生します。

  ワークロードを再配置する前に、ワークロードが優先されるクラスターから完全に削除されていることを確認します。

  (BZ#2295404)

- **ハブの復旧後にフェイルオーバーするとサブスクリプションアプリケーション Pod が起動しない**
ハブの回復後、プライマリーマネージドクラスターからセカンダリーマネージドクラスターにフェイルオーバーすると、サブスクリプションアプリケーション Pod が起動しません。マネージドクラスターの **AppSub** サブスクリプションリソースで RBAC エラーが発生します。これは、バックアップと復元のシナリオにおけるタイミングの問題が原因です。各管理対象クラスターで application-manager Pod が再起動されると、ハブサブスクリプションとチャネルリソースは新しいハブで再作成されません。その結果、子の **AppSub** サブスクリプションリソースはエラーで調整されます。

  回避策:

  次のコマンドを使用して、**appsub** の名前を取得します。

  ```
  % oc get appsub -n <namespace of sub app>
  ```

  次のコマンドを使用して、ハブの AppSub に任意の値を指定して新しいラベルを追加します。

  ```
  % oc edit appsub -n <appsub-namespace> <appsub>-subscription-1
  ```

  不明な証明書の問題を示す子の appsub エラーが引き続き存在する場合は、ワークロードがフェイルオーバーされるマネージドクラスターでアプリケーションマネージャー Pod を再起動します。

  ```
  % oc delete pods -n open-cluster-management-agent-addon application-manager-<>-<>
  ```

  (BZ#2295782)

7.2. MULTICLOUD OBJECT GATEWAY

- **Multicloud Object Gateway インスタンスが初期化を完了できない**
Pod のコード実行と OpenShift が証明局 (CA) バンドルを Pod に読み込むタイミングが競合するため、Pod はクラウドストレージサービスと通信できません。そのたま、デフォルトのバッキングストアを作成できません。

  回避策: Multicloud Object Gateway (MCG) Operator Pod を再起動します。

```
$ oc delete pod noobaa-operator-<ID>
```

この回避策により、バッキングストアが調整され、機能するようになります。

(BZ#2271580)

- **OpenShift Data Foundation 4.16 にアップグレードすると、noobaa-db Pod が CrashLoopBackOff 状態になる**
常に PostgresSQL バージョン 15 で起動する Multicloud Object Gateway で PostgreSQL のアップグレードが失敗すると、OpenShift Data Foundation 4.15 から OpenShift Data Foundation 4.16 へのアップグレードは失敗します。PostgreSQL のアップグレードに失敗した場合、**NooBaa-db-pg-0** Pod は起動に失敗します。

  回避策: ナレッジベースの記事 Recover NooBaa's PostgreSQL upgrade failure in OpenShift Data Foundation 4.16 を参照してください。

  (BZ#2298152)

7.3. CEPH

- **CephFS でのストレッチクラスターのパフォーマンスが低下する**
マルチサイトの Data Foundation クラスターにメタデータサーバー (MDS) を任意に配置するため、小さなメタデータ操作が多数あるワークロードでは、パフォーマンスが低下する可能性があります。

  (BZ#1982116)

- **非常に多くのファイルによる SELinux の再ラベル付けの問題**
Red Hat OpenShift Container Platform でボリュームを Pod にアタッチすると、Pod が起動しないか、起動に過度に時間がかかることがあります。この動作は一般的なもので、Kubelet による SELinux の再ラベル付けの処理方法に関係しています。この問題は、ファイル数が非常に多いファイルシステムベースのボリュームで発生します。OpenShift Data Foundation では、非常に多くのファイルがある CephFS ベースのボリュームを使用すると、この問題が発生します。この問題の回避にはさまざまな方法があります。ビジネスニーズに応じて、ナレッジベースソリューション https://access.redhat.com/solutions/6221251 から回避策の 1 つを選択できます。

  (Jira#3327)

- **Ceph がワークロードのデプロイ後にアクティブなマネージャーを報告しません**
ワークロードのデプロイメント後に、Ceph マネージャーは MON への接続を失うか、liveness プローブに応答できなくなります。

  これが原因で、OpenShift Data Foundation クラスターのステータスが "no active mgr" と報告し、また、Ceph マネージャーを使用してリクエスト処理を行う複数の操作が失敗します。たとえば、ボリュームのプロビジョニング、CephFS スナップショットの作成などです。

  OpenShift Data Foundation クラスターのステータスを確認するには、コマンド **oc get cephcluster -n openshift-storage** を使用します。クラスターにこの問題がある場合、ステータス出力の **status.ceph.details.MGR_DOWN** フィールドに "no active mgr" というメッセージが表示されます。

  回避策: 次のコマンドを使用して Ceph マネージャー Pod を再起動します。

```
# oc scale deployment -n openshift-storage rook-ceph-mgr-a --replicas=0
```

```
# oc scale deployment -n openshift-storage rook-ceph-mgr-a --replicas=1
```

これらのコマンドを実行すると、OpenShift Data Foundation クラスターのステータスは正常なクラスターを報告し、**MGR_DOWN** に関する警告やエラーは表示されません。

(BZ#2244873)

7.4. CSI ドライバー

- **スナップショットの自動フラット化が機能しない**
一般的な親 RBD PVC が 1 つあり、ボリュームスナップショット、復元、およびスナップショットが 450 回以上連続して実行する場合は、ボリュームスナップショットまたは共通の親 RBD PVC のクローンを取得することはできません。

  この問題を回避するには、順番にボリュームスナップショット、復元、および削除を行う代わりに、PVC を使用して PVC のクローンを作成することで、この問題を完全に回避できます。

  この問題が発生した場合は、カスタマーサポートに連絡して、最終復元 PVC の手動フラット化を実行し、共通の親 PVC のボリュームスナップショットまたはクローンを再度取得してください。

  (BZ#2232163)

7.5. OPENSHIFT DATA FOUNDATION コンソール

- **複数のワークロードが単一の namespace にデプロイされている場合に DRPC の作成を最適化する**
複数のアプリケーションが同じ配置を参照している場合、いずれかのアプリケーションに対して DR を有効にすると、その配置を参照するすべてのアプリケーションに対して DR が有効になります。

  DRPC の作成後にアプリケーションが作成された場合、DRPC の PVC ラベルセレクターは新しいアプリケーションのラベルと一致しない可能性があります。

  回避策: このような場合は、DR を無効にし、適切なラベルセレクターを使用して再度有効にすることを推奨します。

  (BZ#2294704)

- **DR 監視ダッシュボード上のアプリセットベースのアプリケーションで最後に同期されたスナップショットが見つからない**
ApplicationSet タイプのアプリケーションでは、監視ダッシュボードに最後のボリュームスナップショットの同期時刻が表示されません。

  回避策: ACM パースペクティブの **Applications** ナビゲーションに移動し、リストから目的のアプリケーションをフィルターします。次に、**Data policy** 列 (ポップオーバー) から "Sync status" を確認します。

  (BZ#2295324)

7.6. OCS OPERATOR

- **グラフ内の ceph_mds_mem_rss メトリクスの単位が正しくない**
OpenShift ユーザーインターフェイス (UI) で **ceph_mds_mem_rss** メトリクスを検索すると、

Ceph がキロバイト (KB) 単位で **ceph_mds_mem_rss** メトリクスを返すため、グラフの Y 軸はメガバイト (MB) 単位で表示されます。これにより、**MDSCacheUsageHigh** アラートの結果を比較する際に混乱が発生する可能性があります。

回避策: OpenShift UI でこのメトリクスを検索するときに **ceph_mds_mem_rss * 1000** を使用すると、グラフの Y 軸が GB 単位で表示されます。これにより、**MDSCacheUsageHigh** アラートに表示される結果を簡単に比較できます。

(BZ#2261881)

- **MDS メモリーを増やすと、Pod が CLBO 状態のときに CPU 値が消去される**
  MDS Pod がクラッシュループバックオフ (CLBO) 状態にあるときにメタデータサーバー (MDS) メモリーが増加すると、MDS Pod の CPU リクエストまたは制限が削除されます。その結果、MDS に設定された CPU 要求または制限が変更されます。

  回避策: **oc patch** コマンドを実行して CPU 制限を調整します。

  以下に例を示します。

  ```
  $ oc patch -n openshift-storage storagecluster ocs-storagecluster \
      --type merge \
      --patch '{"spec": {"resources": {"mds": {"limits": {"cpu": "3"},
      "requests": {"cpu": "3"}}}}}'
  ```

  (BZ#2265563)

7.7. IBM Z プラットフォームが利用できない

IBM Z プラットフォームは、OpenShift Data Foundation 4.16 リリースでは使用できません。IBM Z は、今後のリリースで完全な機能を装備して提供される予定です。

(BZ#2279527)