OpenShift Dedicated 4

サポート

OpenShift Dedicated サポート

Last Updated: 2024-10-17

OpenShift Dedicated 4 サポート

OpenShift Dedicated サポート

法律上の通知

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

Red Hat は、クラスター、モニタリング、およびトラブルシューティング向けにデータを収集するクラスター管理者ツールを提供します。

目次

第1章 サポートの概要

Red Hat は、クラスター、モニタリング、およびトラブルシューティング向けにデータを収集するクラスター管理者ツールを提供します。

1.1. サポートの利用

サポートの利用: Red Hat カスタマーポータルにアクセスして、ナレッジベースの記事の確認、サポートケースの作成、追加の製品ドキュメントおよびリソースの確認を行ってください。

1.2. リモートヘルスモニタリングの問題

リモートヘルスモニタリングの問題: OpenShift Dedicated はクラスターの Telemetry および設定データを収集し、Telemeter Client および Insights Operator を使用してこのデータを Red Hat に報告します。Red Hat はこのデータを使用して、**オンライン接続されたクラスター** での問題を理解し、解決します。OpenShift Dedicated は、以下を使用してデータを収集し、健全性を監視します。

- **Telemetry**: Telemetry クライアントは、Red Hat に対して、4 分 30 秒ごとにメトリクス値を収集して、アップロードします。Red Hat はこのデータを使用して以下を行います。
  - クラスターの監視。
  - OpenShift Dedicated アップグレードをデプロイメントします。
  - アップグレードエクスペリエンスの向上。
- **Insight Operator**: デフォルトで、OpenShift Dedicated は Insight Operator をインストールして有効にし、2 時間ごとに設定およびコンポーネントの障害ステータスを報告します。Insight Operator は以下に役立ちます。
  - 発生する可能性のあるクラスターの問題を事前に特定しする。
  - Red Hat OpenShift Cluster Manager でソリューションと予防措置を提供する。

Telemetry 情報を確認 できます。

リモートヘルスレポートを有効にしている場合は、Insights を使用して問題を特定 します。必要に応じて、リモートヘルスレポートを無効にできます。

1.3. 問題のトラブルシューティング

クラスター管理者は、次の OpenShift Dedicated コンポーネントの問題を監視し、トラブルシューティングできます。

- ノードの問題: クラスター管理者は、ノードのステータス、リソースの使用状況、および設定を確認して、ノード関連の問題を検証およびトラブルシューティングできます。以下に対してクエリーを実行できます。
  - ノード上の kubelet のステータス。
  - クラスターノードジャーナルログ。
- Operator の問題: クラスター管理者は以下を実行して、Operator の問題を解決できます。
  - Operator サブスクリプションのステータスを確認する。

- Operator Pod の正常性を確認する。
- Operator ログを収集する。

- Pod の問題: クラスター管理者は、Pod のステータスを確認して以下を実行し、Pod 関連の問題のトラブルシューティングを行うことができます。
  - Pod およびコンテナーのログを確認する。
  - root アクセスでデバッグ Pod を起動する。
- ストレージの問題: 障害のあるノードがアタッチしたボリュームをアンマウントできないことが原因で、新しいノードにボリュームをマウントできない場合、マルチアタッチストレージエラーが発生します。クラスター管理者は、以下を実行して、複数アタッチされているストレージの問題を解決できます。
  - RWX ボリュームを使用して、複数割り当てを有効にします。
  - RWO ボリュームの使用時に障害が発生したノードを回復するか、削除します。
- モニタリングの問題: クラスター管理者は、モニタリングに関するトラブルシューティングページの手順を実行してください。ユーザー定義プロジェクトのメトリクスが利用できない場合や、Prometheus が大量のディスク領域を消費している場合は、以下を確認します。
  - ユーザー定義のメトリクスが利用できない理由を調べる。
  - Prometheus が大量のディスク領域を消費している理由を特定する。
- OpenShift CLI (**oc**) の問題: ログレベルを増やすことで OpenShift CLI (**oc**) の問題を調査します。

第2章 クラスターリソースの管理

OpenShift Dedicated でグローバル設定オプションを適用できます。Operator はこれらの設定をクラスター全体に適用します。

2.1. クラスターリソースの操作

OpenShift Dedicated の OpenShift CLI (**oc**) ツールを使用して、クラスターリソースと対話できます。**oc api-resources** コマンドの実行後に表示されるクラスターリソースを編集できます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- Web コンソールにアクセスできるか、**oc** CLI ツールがインストールされている。

手順

1. 適用された設定 Operator を確認するには、以下のコマンドを実行します。

```
$ oc api-resources -o name | grep config.openshift.io
```

2. 設定可能なクラスターリソースを表示するには、以下のコマンドを実行します。

```
$ oc explain <resource_name>.config.openshift.io
```

3. クラスターのカスタムリソース定義 (CRD) オブジェクトの設定を表示するには、以下のコマンドを実行します。

```
$ oc get <resource_name>.config -o yaml
```

4. クラスターリソース設定を編集するには、以下のコマンドを実行します。

```
$ oc edit <resource_name>.config -o yaml
```

第3章 サポート

3.1. サポート

このドキュメントで説明されている手順、または OpenShift Dedicated 全般で問題が発生した場合は、Red Hat カスタマーポータル にアクセスしてください。

カスタマーポータルでは、以下を行うことができます。

- Red Hat 製品に関するアーティクルおよびソリューションを対象とした Red Hat ナレッジベースの検索またはブラウズ。
- Red Hat サポートに対するサポートケースの送信。
- その他の製品ドキュメントへのアクセス。

クラスターの問題を特定するには、OpenShift Cluster Manager で Insights を使用できます。Insights により、問題の詳細と、利用可能な場合は問題の解決方法に関する情報が提供されます。

このドキュメントの改善への提案がある場合、またはエラーを見つけた場合は、最も関連性の高いドキュメントコンポーネントの Jira Issue を送信してください。セクション名や OpenShift Dedicated バージョンなどの具体的な情報を提供してください。

3.2. RED HAT ナレッジベースについて

Red Hat ナレッジベース は、お客様が Red Hat の製品やテクノロジーを最大限に活用できるようにするための豊富なコンテンツを提供します。Red Hat ナレッジベースは、Red Hat 製品のインストール、設定、および使用に関する記事、製品ドキュメント、および動画で構成されています。さらに、既知の問題に対する解決策を検索でき、それぞれに根本原因の簡潔な説明と修復手順が記載されています。

3.3. RED HAT ナレッジベースの検索

OpenShift Dedicated の問題が発生した場合には、初期検索を実行して、Red Hat ナレッジベースにソリューションがすでに存在しているかどうかを確認できます。

前提条件

- Red Hat カスタマーポータルのアカウントがある。

手順

1. Red Hat カスタマーポータル にログインします。
2. **Search** をクリックします。
3. 検索フィールドに、問題に関連する次のようなキーワードと文字列を入力します。
   - OpenShift Dedicated コンポーネント (**etcd** など)
   - 関連する手順 (**installation** など)
   - 明示的な失敗に関連する警告、エラーメッセージ、およびその他の出力
4. **Enter** キーをクリックします。

5. オプション: **OpenShift Dedicated** 製品フィルターを選択します。
6. オプション: **Documentation** コンテンツタイプフィルターを選択します。

3.4. サポートケースの送信

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。
- Red Hat OpenShift Cluster Manager にアクセスできる。

手順

1. Red Hat カスタマーポータルの Customer Support ページ にログインします。
2. **Get support** をクリックします。
3. **Customer Support** ページの **Cases** タブで、以下を行います。
   a. オプション: 必要に応じて、事前に入力されたアカウントと所有者の詳細を変更します。
   b. 問題に該当するカテゴリー (**Bug**、**Defect** など) を選択し、**Continue** をクリックします。
4. 以下の情報を入力します。
   a. **Summary** フィールドには、問題の簡潔で説明的な概要と、確認されている現象および予想される動作の詳細情報を入力します。
   b. **Product** ドロップダウンメニューから **OpenShift Dedicated** を選択します。
5. Red Hat ナレッジベースで推奨されるソリューション一覧を確認してください。この一覧に上げられているソリューションは、報告しようとしている問題に適用される可能性があります。提案されている記事が問題に対応していない場合は、**Continue** をクリックします。
6. 報告している問題に対する一致に基づいて推奨される Red Hat ナレッジベースソリューションの一覧が更新されることを確認してください。ケース作成プロセスでより多くの情報を提供すると、このリストの絞り込みが行われます。提案されている記事が問題に対応していない場合は、**Continue** をクリックします。
7. アカウント情報が予想通りに表示されていることを確認し、そうでない場合は適宜修正します。
8. 自動入力された OpenShift Dedicated クラスター ID が正しいことを確認します。正しくない場合は、クラスター ID を手動で取得します。
   - OpenShift Cluster Manager を使用してクラスター ID を手動で取得するには、以下を行います。
     a. **Cluster List** に移動します。
     b. サポートケースを開く必要があるクラスターの名前をクリックします。
     c. **Overview** タブの **Details** セクションの **Cluster ID** フィールドで値を見つけます。

- OpenShift Dedicated Web コンソールを使用してクラスター ID を手動で取得するには、以下を実行します。
  a. **Home → Overview** に移動します。
  b. **Details** セクションの **Cluster ID** フィールドで値を見つけます。
- または、OpenShift Dedicated Web コンソールから新規のサポートケースを作成し、クラスター ID を自動入力することもできます。
  a. ツールバーから、**(?)Help → Open Support Case** に移動します。
  b. **Cluster ID** 値が自動的に入力されます。
- OpenShift CLI (**oc**) を使用してクラスター ID を取得するには、以下のコマンドを実行します。

```
$ oc get clusterversion -o jsonpath='{.items[].spec.clusterID}{"\n"}'
```

9. プロンプトが表示されたら、以下の質問に回答し、**Continue** をクリックします。
   - What are you experiencing? What are you expecting to happen?
   - Define the value or impact to you or the business.
   - Where are you experiencing this behavior? What environment?
   - When does this behavior occur? Frequency? 繰り返すか。At certain times?
10. 関連する診断データファイルをアップロードし、**Continue** をクリックします。
11. 関連するケース管理の詳細情報を入力し、**Continue** をクリックします。
12. ケースの詳細を確認し、**Submit** をクリックします。

3.5. 関連情報

- クラスターの問題を特定する方法の詳細は、Insights を使用したクラスターの問題の特定 を参照してください。

第4章 接続クラスターを使用したリモートヘルスモニタリング

4.1. リモートヘルスモニタリングについて

OpenShift Dedicated は、クラスターに関する Telemetry および設定データを収集し、Telemeter Client および Insights Operator を使用して Red Hat に報告します。Red Hat に提供されるデータには、このドキュメントで説明されている利点があります。

Telemetry および Insights Operator 経由でデータを Red Hat にレポートするクラスターは **接続クラスター (connected cluster)** と見なされます。

Telemetry は、OpenShift Dedicated Telemeter Client が Red Hat に送信する情報を表す Red Hat 用語です。軽量の属性は、サブスクリプション管理の自動化、クラスターの健全性の監視、サポートの支援、お客様のエクスペリエンスの向上を図るために、接続されたクラスターから Red Hat に送信されます。

Insights Operator は OpenShift Dedicated 設定データを収集し、これを Red Hat に送信します。このデータは、クラスターが直面する可能性のある問題に関する情報を得るために使用されます。これらの洞察は、OpenShift Cluster Manager でクラスター管理者に伝達されます。

これらの 2 つのプロセスの詳細は、このドキュメントを参照してください。

Telemetry および Insights Operator の利点

ユーザーにとって、Telemetry および Insights Operator には次のような利点があります。

- **問題の特定および解決の強化**。エンドユーザーには正常と思われるイベントも、Red Hat は多くのお客様を含む全体的な視点で観察できます。この視点により、一部の問題はより迅速に特定され、エンドユーザーがサポートケースを作成したり、Jira 問題 を作成しなくても解決することが可能です。

- **高度なリリース管理**。OpenShift Dedicated は、更新ストラテジーを選択できる **candidate**、**fast**、および **stable** リリースチャネルを提供します。リリースの **fast** から **stable** に移行できるかどうかは、更新の成功率やアップグレード時に確認されるイベントに依存します。接続されたクラスターが提供する情報により、Red Hat はリリースの品質を **stable** チャネルに引き上げ、**fast** チャネルで見つかった問題により迅速に対応することができます。

- **新機能の明確な優先順位付け**。収集されるデータは、最も使用される OpenShift Dedicated の領域に関する洞察を提供します。この情報により、Red Hat はお客様に最も大きな影響を与える新機能の開発に重点的に取り組むことができます。

- **効率的なサポートエクスペリエンス**。Red Hat カスタマーポータル でサポートチケットを作成する際に、接続されたクラスターのクラスター ID を指定できます。これにより、Red Hat は接続された情報を使用してクラスター固有の効率化されたサポートエクスペリエンスを提供できます。このドキュメントは、強化されたサポートエクスペリエンスの詳細情報を提供しています。

- **予測分析**。OpenShift Cluster Manager でクラスターに表示される洞察は、接続されたクラスターから収集される情報によって有効化されます。Red Hat は、OpenShift Dedicated クラスターがさらされている問題の特定に役立つように、ディープラーニング、機械学習、人工知能の自動化に取り組んでいます。

OpenShift Dedicated では、リモートヘルスレポートが常に有効にされます。オプトアウトすることはできません。

4.1.1. Telemetry について

Telemetry は厳選されたクラスターモニタリングメトリクスのサブセットを Red Hat に送信します。Telemeter Client はメトリクスの値を 4 分 30 秒ごとに取得し、データを Red Hat にアップロードします。これらのメトリクスについては、このドキュメントで説明しています。

このデータストリームは、Red Hat がリアルタイムでクラスターをモニターし、お客様に影響を与える問題に随時対応するために使用されます。Red Hat はこれを使用することで、OpenShift Dedicated アップグレードをお客様にロールアウトして、サービスへの影響を最小限に抑え、アップグレードエクスペリエンスを継続的に改善することもできます。

Red Hat サポートおよびエンジニアリングチームは、サポートケースでレポートされるデータにアクセスする場合と同じ制限が適用された状態で、このデバッグ情報を使用できます。接続クラスターに関するすべての情報は、より使いやすく、直感的に使用できる OpenShift Dedicated を実現するために Red Hat が使用します。。

4.1.1.1. Telemetry で収集される情報

以下の情報は、Telemetry によって収集されます。

4.1.1.1.1. システム情報

- OpenShift Dedicated クラスターのバージョンと、更新バージョンの可用性を判別するために使用されるインストール済み更新の詳細を含むバージョン情報
- クラスターごとに利用可能な更新の数、更新に使用されるチャネルおよびイメージリポジトリー、更新の進捗情報、および更新で発生するエラーの数などの更新情報
- インストール時に生成される一意でランダムな識別子
- クラウドインフラストラクチャーレベルのノード設定、ホスト名、IP アドレス、Kubernetes Pod 名、namespace、およびサービスなど、Red Hat サポートがお客様にとって有用なサポートを提供するのに役立つ設定の詳細
- クラスターにインストールされている OpenShift Dedicated フレームワークコンポーネントおよびそれらの状態およびステータス
- 動作が低下した Operator の "関連オブジェクト" として一覧表示されるすべての namespace のイベント
- 動作が低下したソフトウェアに関する情報
- 証明書の有効性に関する情報
- OpenShift Dedicated がデプロイされているプロバイダープラットフォームの名前とデータセンターの場所

4.1.1.1.2. サイジング情報

- CPU コアの数およびそれぞれに使用される RAM の容量を含む、クラスター、マシンタイプ、およびマシンに関するサイジング情報
- etcd メンバーの数および etcd クラスターに保存されるオブジェクトの数

4.1.1.1.3. 使用情報

- コンポーネント、機能および拡張機能に関する使用率の情報

- テクノロジープレビューおよびサポート対象外の設定に関する使用率の詳細

Telemetry は、ユーザー名やパスワードなどの識別情報を収集しません。Red Hat は、意図的な個人情報の収集は行いません。誤って個人情報を受信したことが明らかになった場合、Red Hat はその情報を削除します。Telemetry データが個人データに該当する場合は、Red Hat プライバシーステートメントで Red Hat のプライバシー方針を確認してください。

4.1.1.2. ユーザーテレメトリー

Red Hat は、ブラウザーから匿名化されたユーザーデータを収集します。この匿名化されたデータには、Telemetry が有効になっているすべてのクラスターのユーザーが使用するページ、機能、リソースタイプが含まれます。

他の考慮事項

- ユーザーイベントは SHA-1 ハッシュとしてグループ化されます。
- ユーザーの IP アドレスは **0.0.0.0** として保存されます。
- ユーザー名と IP アドレスは別々の値として保存されることはありません。

関連情報

- Telemetry が OpenShift Dedicated で Prometheus から収集する属性を一覧表示する方法の詳細は、Telemetry によって収集されるデータの表示 を参照してください。
- Telemetry が Prometheus から収集する属性のリストについては、アップストリームの cluster-monitoring-operator ソースコード を参照してください。

4.1.2. Insights Operator について

Insights Operator は設定およびコンポーネントの障害ステータスを定期的に収集し、デフォルトで 2 時間ごとにそのデータを Red Hat に報告します。この情報により、Red Hat は設定や Telemetry で報告されるデータよりも詳細な障害データを評価できます。

OpenShift Dedicated のユーザーは、Red Hat Hybrid Cloud Console の Insights Advisor サービスで各クラスターのレポートを表示できます。問題が特定されると、Insights は詳細を提供します。利用可能な場合は、問題の解決方法に関する手順が提供されます。

Insights Operator は、ユーザー名、パスワード、または証明書などの識別情報を収集しません。Red Hat Insights のデータ収集とコントロールの詳細は、Red Hat Insights のデータおよびアプリケーションセキュリティー を参照してください。

Red Hat は、接続されたすべてのクラスター情報を使用して、以下を実行します。

- Red Hat Hybrid Cloud Console の Insights Advisor サービスで、潜在的なクラスターの問題を特定し、解決策と予防措置を提供します。
- 製品およびサポートチームに集約された重要な情報を提供することにより、OpenShift Dedicated を改善します。
- OpenShift Dedicated をより直感的なものにします。

4.1.2.1. Insights Operator によって収集される情報

以下の情報は、Insights Operator によって収集されます。

- OpenShift Dedicated バージョンおよび環境に固有の問題を特定するためのクラスターおよびそのコンポーネントに関する一般的な情報
- 誤った設定や設定するパラメーターに固有の問題の判別に使用するクラスターのイメージレジストリー設定などの設定ファイル
- クラスターコンポーネントで発生するエラー
- 実行中の更新の進捗情報、およびコンポーネントのアップグレードのステータス
- OpenShift Dedicated がデプロイされているプラットフォームとクラスターが配置されているリージョンの詳細
- Operator が問題を報告すると、**openshift-*** および **kube-*** プロジェクトのコア OpenShift Dedicated Pod に関する情報が収集されます。これには、状態、リソース、セキュリティーコンテキスト、ボリューム情報などが含まれます。

関連情報

- Insights Operator のソースコードは、レビューおよび提供できます。Insights Operator によって収集される項目のリストについては、Insights Operator のアップストリームプロジェクト を参照してください。

4.1.3. Telemetry および Insights Operator データフローについて

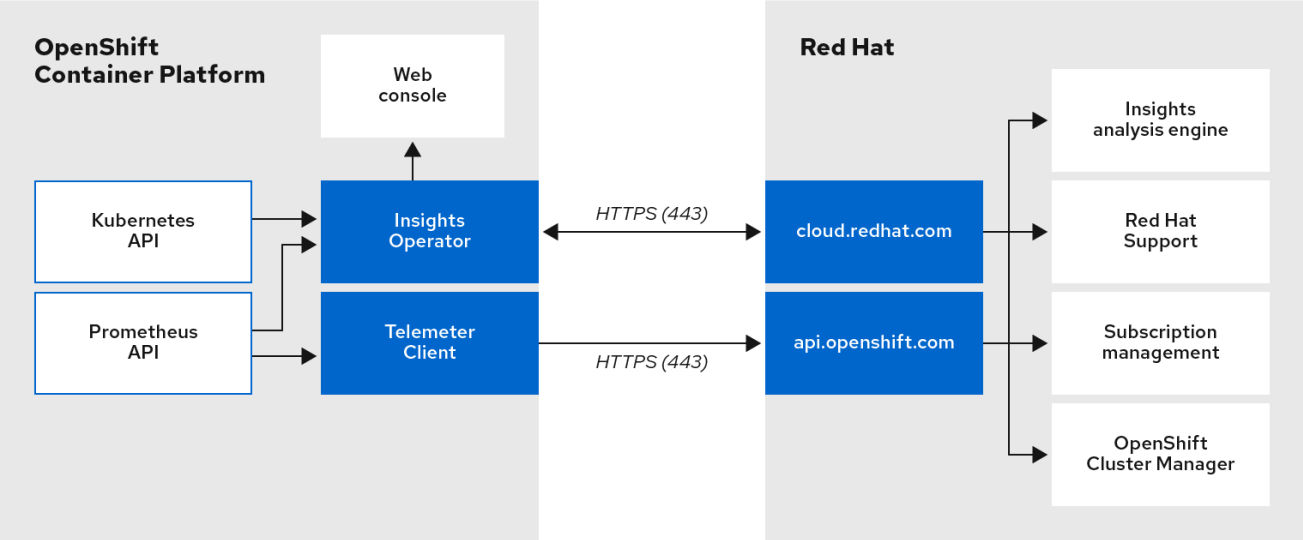
Telemeter Client は、Prometheus API から選択した時系列データを収集します。時系列データは、処理するために 4 分 30 秒ごとに api.openshift.com にアップロードされます。

Insights Operator は、選択したデータを Kubernetes API および Prometheus API からアーカイブに収集します。アーカイブは、処理のために 2 時間ごとに OpenShift Cluster Manager にアップロードされます。Insights Operator は、OpenShift Cluster Manager から最新の Insights 分析もダウンロードします。これは、OpenShift Dedicated Web コンソールの **Overview** ページに含まれる **Insights status** ポップアップを設定するために使用されます。

Red Hat との通信はすべて、Transport Layer Security (TLS) および相互証明書認証を使用して、暗号化されたチャネル上で行われます。すべてのデータは移動中および停止中に暗号化されます。

顧客データを処理するシステムへのアクセスは、マルチファクター認証と厳格な認証制御によって制御されます。アクセスは関係者以外極秘で付与され、必要な操作に制限されます。

Telemetry および Insights Operator データフロー



関連情報

- OpenShift Dedicated モニタリングスタックの詳細は、モニタリングの概要 を参照してください。

4.1.4. リモートヘルスモニタリングデータの使用方法に関する追加情報

リモートヘルスモニタリングを有効にするために収集される情報の詳細は、Information collected by Telemetry および Information collected by the Insights Operator を参照してください。

このドキュメントで前述したとおり、Red Hat は、サポートおよびアップグレードの提供、パフォーマンス/設定の最適化、サービスへの影響の最小化、脅威の特定および修復、トラブルシューティング、オファリングおよびユーザーエクスペリエンスの強化、問題への対応および請求を目的として (該当する場合)、お客様の Red Hat 製品使用データを収集します。

収集における対策

Red Hat は、Telemetry および設定データを保護するために設計された技術的および組織的な対策を採用しています。

共有

Red Hat は、ユーザーエクスペリエンスの向上に向けて、Telemetry および Insights Operator で収集されるデータを内部で共有する場合があります。Red Hat は、以下の目的で Red Hat のビジネスパートナーと、お客様を特定しない集約された形式で Telemetry および設定データを共有する場合があります。つまり、パートナーが市場およびお客様の Red Hat のオファリングの使用についてより良く理解できるように支援することを目的とするか、それらのパートナーと共同でサポートしている製品の統合を効果的に行うことを目的としています。

サードパーティー

Red Hat は、Telemetry および設定データの収集、分析、および保管を支援するために、特定のサードパーティーと連携する場合があります。

4.2. リモートヘルスモニタリングによって収集されるデータの表示

ユーザーコントロール/Telemetry および設定データ収集の有効化および無効化

管理者は、Telemetry および Insights Operator によって収集されるメトリクスを確認できます。

4.2.1. Telemetry によって収集されるデータの表示

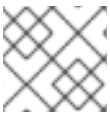
Telemetry でキャプチャーされるクラスターとコンポーネントの時系列データを表示することができます。

前提条件

- OpenShift Container Platform CLI (**oc**) がインストールされている。
- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。

手順

1. クラスターにログインします。
2. 次のコマンドを実行すると、クラスターの Prometheus サービスにクエリーが実行され、Telemetry によってキャプチャーされた時系列データの完全なセットが返されます。



注記

次の例には、AWS 上の OpenShift Dedicated に固有の値がいくつか含まれています。

```
$ curl -G -k -H "Authorization: Bearer $(oc whoami -t)" \
https://$(oc get route prometheus-k8s-federate -n \
openshift-monitoring -o jsonpath="{.spec.host}")/federate \
--data-urlencode 'match[]={__name__=~"cluster:usage:.*"}' \
--data-urlencode 'match[]={__name__="count:up0"}' \
--data-urlencode 'match[]={__name__="count:up1"}' \
--data-urlencode 'match[]={__name__="cluster_version"}' \
--data-urlencode 'match[]={__name__="cluster_version_available_updates"}' \
--data-urlencode 'match[]={__name__="cluster_version_capability"}' \
--data-urlencode 'match[]={__name__="cluster_operator_up"}' \
--data-urlencode 'match[]={__name__="cluster_operator_conditions"}' \
--data-urlencode 'match[]={__name__="cluster_version_payload"}' \
--data-urlencode 'match[]={__name__="cluster_installer"}' \
--data-urlencode 'match[]={__name__="cluster_infrastructure_provider"}' \
--data-urlencode 'match[]={__name__="cluster_feature_set"}' \
--data-urlencode 'match[]={__name__="instance:etcd_object_counts:sum"}' \
--data-urlencode 'match[]={__name__="ALERTS",alertstate="firing"}' \
--data-urlencode 'match[]={__name__="code:apiserver_request_total:rate:sum"}' \
--data-urlencode 'match[]={__name__="cluster:capacity_cpu_cores:sum"}' \
--data-urlencode 'match[]={__name__="cluster:capacity_memory_bytes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="cluster:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="openshift:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="openshift:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="workload:cpu_usage_cores:sum"}' \
--data-urlencode 'match[]={__name__="workload:memory_usage_bytes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:virt_platform_nodes:sum"}' \
--data-urlencode 'match[]={__name__="cluster:node_instance_type_count:sum"}' \
--data-urlencode 'match[]={__name__="cnv:vmi_status_running:count"}' \
--data-urlencode 'match[]={__name__="cluster:vmi_request_cpu_cores:sum"}' \
```

```
--data-urlencode 'match[]={__name__="node_role_os_version_machine:cpu_capacity_cores:sum"}' \
--data-urlencode 'match[]=
{__name__="node_role_os_version_machine:cpu_capacity_sockets:sum"}' \
--data-urlencode 'match[]={__name__="subscription_sync_total"}' \
--data-urlencode 'match[]={__name__="olm_resolution_duration_seconds"}' \
--data-urlencode 'match[]={__name__="csv_succeeded"}' \
--data-urlencode 'match[]={__name__="csv_abnormal"}' \
--data-urlencode 'match[]=
{__name__="cluster:kube_persistentvolumeclaim_resource_requests_storage_bytes:provisioner:sum"}'
\
--data-urlencode 'match[]={__name__="cluster:kubelet_volume_stats_used_bytes:provisioner:sum"}'
\
--data-urlencode 'match[]={__name__="ceph_cluster_total_bytes"}' \
--data-urlencode 'match[]={__name__="ceph_cluster_total_used_raw_bytes"}' \
--data-urlencode 'match[]={__name__="ceph_health_status"}' \
--data-urlencode 'match[]={__name__="odf_system_raw_capacity_total_bytes"}' \
--data-urlencode 'match[]={__name__="odf_system_raw_capacity_used_bytes"}' \
--data-urlencode 'match[]={__name__="odf_system_health_status"}' \
--data-urlencode 'match[]={__name__="job:ceph_osd_metadata:count"}' \
--data-urlencode 'match[]={__name__="job:kube_pv:count"}' \
--data-urlencode 'match[]={__name__="job:odf_system_pvs:count"}' \
--data-urlencode 'match[]={__name__="job:ceph_pools_iops:total"}' \
--data-urlencode 'match[]={__name__="job:ceph_pools_iops_bytes:total"}' \
--data-urlencode 'match[]={__name__="job:ceph_versions_running:count"}' \
--data-urlencode 'match[]={__name__="job:noobaa_total_unhealthy_buckets:sum"}' \
--data-urlencode 'match[]={__name__="job:noobaa_bucket_count:sum"}' \
--data-urlencode 'match[]={__name__="job:noobaa_total_object_count:sum"}' \
--data-urlencode 'match[]={__name__="odf_system_bucket_count", system_type="OCS",
system_vendor="Red Hat"}' \
--data-urlencode 'match[]={__name__="odf_system_objects_total", system_type="OCS",
system_vendor="Red Hat"}' \
--data-urlencode 'match[]={__name__="noobaa_accounts_num"}' \
--data-urlencode 'match[]={__name__="noobaa_total_usage"}' \
--data-urlencode 'match[]={__name__="console_url"}' \
--data-urlencode 'match[]={__name__="cluster:ovnkube_master_egress_routing_via_host:max"}' \
--data-urlencode 'match[]={__name__="cluster:network_attachment_definition_instances:max"}' \
--data-urlencode 'match[]=
{__name__="cluster:network_attachment_definition_enabled_instance_up:max"}' \
--data-urlencode 'match[]={__name__="cluster:ingress_controller_aws_nlb_active:sum"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:min"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:max"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:avg"}' \
--data-urlencode 'match[]={__name__="cluster:route_metrics_controller_routes_per_shard:median"}'
\
--data-urlencode 'match[]={__name__="cluster:openshift_route_info:tls_termination:sum"}' \
--data-urlencode 'match[]={__name__="insightsclient_request_send_total"}' \
--data-urlencode 'match[]={__name__="cam_app_workload_migrations"}' \
--data-urlencode 'match[]=
{__name__="cluster:apiserver_current_inflight_requests:sum:max_over_time:2m"}' \
--data-urlencode 'match[]={__name__="cluster:alertmanager_integrations:max"}' \
--data-urlencode 'match[]={__name__="cluster:telemetry_selected_series:count"}' \
--data-urlencode 'match[]={__name__="openshift:prometheus_tsdb_head_series:sum"}' \
--data-urlencode 'match[]=
{__name__="openshift:prometheus_tsdb_head_samples_appended_total:sum"}' \
--data-urlencode 'match[]={__name__="monitoring:container_memory_working_set_bytes:sum"}' \
--data-urlencode 'match[]={__name__="namespace_job:scrape_series_added:topk3_sum1h"}' \
```

```
--data-urlencode 'match[]=
{__name__="namespace_job:scrape_samples_post_metric_relabeling:topk3"}' \
--data-urlencode 'match[]={__name__="monitoring:haproxy_server_http_responses_total:sum"}' \
--data-urlencode 'match[]={__name__="rhmi_status"}' \
--data-urlencode 'match[]={__name__="status:upgrading:version:rhoam_state:max"}' \
--data-urlencode 'match[]={__name__="state:rhoam_critical_alerts:max"}' \
--data-urlencode 'match[]={__name__="state:rhoam_warning_alerts:max"}' \
--data-urlencode 'match[]={__name__="rhoam_7d_slo_percentile:max"}' \
--data-urlencode 'match[]={__name__="rhoam_7d_slo_remaining_error_budget:max"}' \
--data-urlencode 'match[]={__name__="cluster_legacy_scheduler_policy"}' \
--data-urlencode 'match[]={__name__="cluster_master_schedulable"}' \
--data-urlencode 'match[]={__name__="che_workspace_status"}' \
--data-urlencode 'match[]={__name__="che_workspace_started_total"}' \
--data-urlencode 'match[]={__name__="che_workspace_failure_total"}' \
--data-urlencode 'match[]={__name__="che_workspace_start_time_seconds_sum"}' \
--data-urlencode 'match[]={__name__="che_workspace_start_time_seconds_count"}' \
--data-urlencode 'match[]={__name__="cco_credentials_mode"}' \
--data-urlencode 'match[]={__name__="cluster:kube_persistentvolume_plugin_type_counts:sum"}' \
--data-urlencode 'match[]={__name__="visual_web_terminal_sessions_total"}' \
--data-urlencode 'match[]={__name__="acm_managed_cluster_info"}' \
--data-urlencode 'match[]={__name__="cluster:vsphere_vcenter_info:sum"}' \
--data-urlencode 'match[]={__name__="cluster:vsphere_esxi_version_total:sum"}' \
--data-urlencode 'match[]={__name__="cluster:vsphere_node_hw_version_total:sum"}' \
--data-urlencode 'match[]={__name__="openshift:build_by_strategy:sum"}' \
--data-urlencode 'match[]={__name__="rhods_aggregate_availability"}' \
--data-urlencode 'match[]={__name__="rhods_total_users"}' \
--data-urlencode 'match[]=
{__name__="instance:etcd_disk_wal_fsync_duration_seconds:histogram_quantile",quantile="0.99"}' \
--data-urlencode 'match[]={__name__="instance:etcd_mvcc_db_total_size_in_bytes:sum"}' \
--data-urlencode 'match[]=
{__name__="instance:etcd_network_peer_round_trip_time_seconds:histogram_quantile",quantile="0.99
"}' \
--data-urlencode 'match[]={__name__="instance:etcd_mvcc_db_total_size_in_use_in_bytes:sum"}' \
--data-urlencode 'match[]=
{__name__="instance:etcd_disk_backend_commit_duration_seconds:histogram_quantile",quantile="0.9
9"}' \
--data-urlencode 'match[]={__name__="jaeger_operator_instances_storage_types"}' \
--data-urlencode 'match[]={__name__="jaeger_operator_instances_strategies"}' \
--data-urlencode 'match[]={__name__="jaeger_operator_instances_agent_strategies"}' \
--data-urlencode 'match[]={__name__="appsvcs:cores_by_product:sum"}' \
--data-urlencode 'match[]={__name__="nto_custom_profiles:count"}' \
--data-urlencode 'match[]={__name__="openshift_csi_share_configmap"}' \
--data-urlencode 'match[]={__name__="openshift_csi_share_secret"}' \
--data-urlencode 'match[]={__name__="openshift_csi_share_mount_failures_total"}' \
--data-urlencode 'match[]={__name__="openshift_csi_share_mount_requests_total"}' \
--data-urlencode 'match[]={__name__="cluster:velero_backup_total:max"}' \
--data-urlencode 'match[]={__name__="cluster:velero_restore_total:max"}' \
--data-urlencode 'match[]={__name__="eo_es_storage_info"}' \
--data-urlencode 'match[]={__name__="eo_es_redundancy_policy_info"}' \
--data-urlencode 'match[]={__name__="eo_es_defined_delete_namespaces_total"}' \
--data-urlencode 'match[]={__name__="eo_es_misconfigured_memory_resources_info"}' \
--data-urlencode 'match[]={__name__="cluster:eo_es_data_nodes_total:max"}' \
--data-urlencode 'match[]={__name__="cluster:eo_es_documents_created_total:sum"}' \
--data-urlencode 'match[]={__name__="cluster:eo_es_documents_deleted_total:sum"}' \
--data-urlencode 'match[]={__name__="pod:eo_es_shards_total:max"}' \
--data-urlencode 'match[]={__name__="eo_es_cluster_management_state_info"}' \
```

```
--data-urlencode 'match[]={__name__="imageregistry:imagestreamtags_count:sum"}' \
--data-urlencode 'match[]={__name__="imageregistry:operations_count:sum"}' \
--data-urlencode 'match[]={__name__="log_logging_info"}' \
--data-urlencode 'match[]={__name__="log_collector_error_count_total"}' \
--data-urlencode 'match[]={__name__="log_forwarder_pipeline_info"}' \
--data-urlencode 'match[]={__name__="log_forwarder_input_info"}' \
--data-urlencode 'match[]={__name__="log_forwarder_output_info"}' \
--data-urlencode 'match[]={__name__="cluster:log_collected_bytes_total:sum"}' \
--data-urlencode 'match[]={__name__="cluster:log_logged_bytes_total:sum"}' \
--data-urlencode 'match[]={__name__="cluster:kata_monitor_running_shim_count:sum"}' \
--data-urlencode 'match[]={__name__="platform:hypershift_hostedclusters:max"}' \
--data-urlencode 'match[]={__name__="platform:hypershift_nodepools:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_unhealthy_bucket_claims:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_buckets_claims:max"}' \
--data-urlencode 'match[]=
{__name__="namespace:noobaa_unhealthy_namespace_resources:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_namespace_resources:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_unhealthy_namespace_buckets:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_namespace_buckets:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_accounts:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_usage:max"}' \
--data-urlencode 'match[]={__name__="namespace:noobaa_system_health_status:max"}' \
--data-urlencode 'match[]={__name__="ocs_advanced_feature_usage"}' \
--data-urlencode 'match[]={__name__="os_image_url_override:sum"}' \
--data-urlencode 'match[]={__name__="openshift:openshift_network_operator_ipsec_state:info"}'
```

4.3. INSIGHTS を使用したクラスターの問題の特定

Insights は、Insights Operator の送信データを繰り返し分析します。OpenShift Dedicated のユーザーは、Red Hat Hybrid Cloud Console の Insights Advisor サービスでレポートを表示できます。

4.3.1. OpenShift Dedicated の Red Hat Insights Advisor について

Insights Advisor を使用して、OpenShift Dedicated クラスターの正常性を評価し、監視できます。個々のクラスターとインフラストラクチャー全体のどちらに懸念があるかにかかわらず、サービスの可用性、フォールトトレランス、パフォーマンス、またはセキュリティーに影響を及ぼす可能性のある問題にさらされていることを認識することが重要です。

Insights は、Insights Operator で収集されたクラスターデータを使用して、そのデータを **recommendations** ライブラリーと繰り返し比較します。各推奨事項は、OpenShift Dedicated クラスターを危険にさらす可能性のあるクラスター環境条件です。Insights 分析の結果は、Red Hat Hybrid Cloud Console の Insights Advisor サービスで利用できます。コンソールでは、次のアクションを実行できます。

- 特定の推奨事項の影響を受けるクラスターを確認します。
- 堅牢なフィルタリング機能を使用して、結果をそれらの推奨事項に絞り込みます。
- 個別の推奨事項、それらが示すリスクの詳細、および個別のクラスターに適した解決方法を確認します。
- 結果を他の内容と共有します。

4.3.2. Insights Advisor の推奨事項について

Insights Advisor は、クラスターのサービスの可用性、フォールトトレランス、パフォーマンス、またはセキュリティーに悪影響を与える可能性のあるさまざまなクラスターの状態およびコンポーネント設定に関する情報をバンドルしています。この情報は Insights Advisor で推奨事項と呼ばれ、以下の情報が含まれます。

- **名前:** 推奨事項の簡単な説明
- **追加:** 推奨事項が Insights Advisor アーカイブに公開されている場合
- **カテゴリー:** この問題がサービス可用性、フォールトトレランス、パフォーマンス、またはセキュリティーに悪影響を及ぼす可能性があるかどうか
- **全体のリスク:** 条件がインフラストラクチャーに悪影響を与える **可能性** から導出した値と、それが発生した場合にシステム稼働に及ぼす **影響**
- **クラスター:** 推奨事項が検出されたクラスターのリスト
- **説明:** クラスターへの影響を含む、問題の簡単な概要
- **関連するトピックへのリンク:** Red Hat が提供する、問題に関する詳細情報

4.3.3. クラスターの潜在的な問題の表示

このセクションでは、OpenShift Cluster Manager の **Insights Advisor** に Insights レポートを表示する方法を説明します。

Insights はクラスターを繰り返し分析し、最新の結果を表示することに注意してください。問題を修正した場合や新しい問題が検出された場合などは、これらの結果が変化する可能性があります。

前提条件

- クラスターが OpenShift Cluster Manager に登録されている。
- リモートヘルスレポートが有効になっている (デフォルト)。
- OpenShift Cluster Manager にログインしている。

手順

1. OpenShift Cluster Manager で、**Advisor → Recommendations** に移動します。
結果に応じて、Insights Advisor は次のいずれかを表示します。
   - Insights で問題が特定されなかった場合は、**No matching recommendations found** が表示されます。
   - Insights が検出した問題のリストで、リスク (低、中、重要、および重大) ごとにグループ化されています。
   - Insights がまだクラスターを分析していない場合は、**No clusters yet** が表示されます。分析は、クラスターがインストールされて登録され、インターネットに接続された直後に開始します。
2. 問題が表示された場合は、エントリーの前にある › アイコンをクリックして詳細を確認してください。
問題によっては、Red Hat が提供する関連情報へのリンクがあります。

4.3.4. すべての Insights Advisor の推奨事項を表示

Recommendations ビューはデフォルトで、クラスターで検出された推奨事項のみを表示します。ただし、アドバイザーアーカイブですべての推奨事項を表示できます。

前提条件

- リモートヘルスレポートが有効になっている (デフォルト)。
- クラスターが Red Hat Hybrid Cloud Console に 登録 されています。
- OpenShift Cluster Manager にログインしている。

手順

1. OpenShift Cluster Manager で、**Advisor → Recommendations** に移動します。
2. **Clusters Impacted** フィルターおよび **Status** フィルターの横にある **X** アイコンをクリックします。
これで、クラスターの潜在的な推奨事項をすべて参照できます。

4.3.5. アドバイザーの推奨事項に対するフィルター

Insights アドバイザーサービスは、多数の推奨事項を返すことができます。最も重要な推奨事項に焦点を当てるために、アドバイザーの推奨事項 リストにフィルターを適用して、優先度の低い推奨事項を削除できます。

デフォルトでは、フィルターは 1 つ以上のクラスターに影響を与える有効な推奨事項のみを表示するように設定されています。Insights ライブラリー内のすべての推奨事項または無効化された推奨事項を表示するには、フィルターをカスタマイズできます。

フィルターを適用するには、フィルタータイプを選択し、ドロップダウンリストで使用できるオプションに基づき値を設定します。推奨事項のリストには、複数のフィルターを適用できます。

次のフィルタータイプを設定できます。

- **Name:** 名前で推奨事項を検索します。
- **Total risk:** クラスターに対する悪影響の可能性と重大度を示す値として、**Critical**、**Important**、**Moderate**、**Low** から 1 つ以上選択します。
- **Impact:** クラスター操作の継続性に対する潜在的な影響を示す値を、**Critical**、**High**、**Medium**、**Low** から 1 つ以上選択します。
- **Likelihood:** 推奨事項が実行された場合にクラスターに悪影響を及ぼす可能性を示す値を、**Critical**、**High**、**Medium**、**Low** から 1 つ以上選択します。
- **Category:** 注目するカテゴリーを、**Service Availability**、**Performance**、**Fault Tolerance**、**Security**、**Best Practice** から 1 つ以上選択します。
- **Status:** ラジオボタンをクリックして、有効な推奨事項 (デフォルト)、無効な推奨事項、またはすべての推奨事項を表示します。
- **Clusters impacted:** 現在 1 つ以上のクラスターに影響を与えている推奨事項、影響を与えていない推奨事項、またはすべての推奨事項を表示するようにフィルターを設定します。

- **Risk of change:** 解決策の実装がクラスター操作に及ぼす可能性のあるリスクを示す値を、**High**、**Moderate**、**Low**、**Very low** から 1 つ以上選択します。

4.3.5.1. Insights アドバイザーの推奨事項のフィルタリング

OpenShift Dedicated クラスターマネージャーは、推奨事項リストに表示される推奨事項をフィルターできます。フィルターを適用すると、報告される推奨事項の数を減らし、最も優先度の高い推奨事項に集中できます。

次の手順は、**Category** フィルターの設定方法および削除方法を示していますが、この手順は任意のフィルタータイプおよびそれぞれの値にも適用できます。

前提条件

OpenShift Cluster Manager Hybrid Cloud Console にログインしている。

手順

1. **Red Hat Hybrid Cloud Console→ OpenShift → Advisor recommendations** に移動します。
2. メインのフィルタータイプドロップダウンリストで、**Category** フィルタータイプを選択します。
3. フィルター値のドロップダウンリストを展開し、表示する推奨事項の各カテゴリー横にあるチェックボックスを選択します。不要なカテゴリーのチェックボックスはオフのままにします。
4. オプション: フィルターを追加して、リストをさらに絞り込みます。

選択したカテゴリーの推奨事項のみがリストに表示されます。

検証

- フィルターを適用した後、更新された推奨事項リストを表示できます。適用されたフィルターは、デフォルトのフィルターの隣に追加されます。

4.3.5.2. Insights Advisor の推奨事項からフィルターを削除する

推奨事項のリストには、複数のフィルターを適用できます。準備が完了したフィルターは、個別に削除することも、完全にリセットすることもできます。

フィルターを個別に削除する

- デフォルトのフィルターを含め、各フィルターの横にある **X** アイコンをクリックすると、フィルターを個別に削除できます。

デフォルト以外のフィルターをすべて削除する

- **Reset filters** をクリックすると、適用したフィルターのみが削除され、デフォルトのフィルターはそのまま残ります。

4.3.6. Insights Advisor の推奨事項の無効化

クラスターに影響を与える特定の推奨事項を無効にして、それらがレポートに表示されないようにできます。単一のクラスターまたはすべてのクラスターの推奨を無効にできます。

注記

すべてのクラスターの推奨を無効にすると、今後のクラスターにも適用されます。

前提条件

- リモートヘルスレポートが有効になっている (デフォルト)。
- クラスターが OpenShift Cluster Manager に登録されている。
- OpenShift Cluster Manager にログインしている。

手順

1. OpenShift Cluster Manager で、**Advisor → Recommendations** に移動します。
2. オプション: 必要に応じて、**Clusters Impacted** および **Status** フィルターを使用します。
3. 次のいずれかの方法でアラートを無効にします。
   - アラートを無効にするには、以下を実行します。
     a. アラートの **Options** メニュー  をクリックし、**Disable recommendation** をクリックします。
     b. 理由を入力し、**Save** をクリックします。
   - アラートを無効にする前に、そのアラートの影響を受けるクラスターを表示するには、以下を実行します。
     a. 無効にする推奨事項の名前をクリックします。その推奨事項のページに移動します。
     b. **Affected clusters** セクションで、クラスターのリストを確認します。
     c. **Actions → Disable recommendation** をクリックして、すべてのクラスターのアラートを無効にします。
     d. 理由を入力し、**Save** をクリックします。

4.3.7. 以前に無効にした Insights Advisor の推奨事項を有効にする

すべてのクラスターで推奨事項を無効にすると、Insights Advisor に推奨事項は表示されなくなります。この動作は変更できます。

前提条件

- リモートヘルスレポートが有効になっている (デフォルト)。
- クラスターが OpenShift Cluster Manager に登録されている。
- OpenShift Cluster Manager にログインしている。

手順

1. OpenShift Cluster Manager で、**Advisor → Recommendations** に移動します。

2. 無効になっている推奨事項から、表示する推奨事項をフィルタリングします。
   a. **Status** ドロップダウンメニューから **Status** を選択します。
   b. **Filter by status** ドロップダウンメニューから、**Disabled** を選択します。
   c. オプション: **Clusters impacted** フィルターをクリアします。
3. 有効にする推奨事項を特定します。
4. **Options** メニュー  をクリックし、**Enable recommendation** をクリックします。

4.3.8. Web コンソールでの Insights ステータスの表示

Insights はクラスターを繰り返し分析し、OpenShift Dedicated Web コンソールでクラスターの特定された潜在的な問題のステータスを表示できます。このステータスは、さまざまなカテゴリーの問題の数を示し、詳細については、OpenShift Cluster Manager レポートへのリンクを示します。

前提条件

- クラスターが OpenShift Cluster Manager に 登録されている。
- リモートヘルスレポートが有効になっている (デフォルト)。
- OpenShift Dedicated Web コンソールにログインしている。

手順

1. OpenShift Dedicated Web コンソールで **Home → Overview** に移動します。
2. **Status** カードの **Insights** をクリックします。
   ポップアップウィンドウには、リスクごとにグループ化された潜在的な問題がリスト表示されます。詳細を表示するには、個々のカテゴリーをクリックするか、**View all recommendations in Insights Advisor** を表示します。

4.4. INSIGHTS OPERATOR の使用

Insights Operator は設定およびコンポーネントの障害ステータスを定期的に収集し、デフォルトで 2 時間ごとにそのデータを Red Hat に報告します。この情報により、Red Hat は設定や Telemetry で報告されるデータよりも詳細な障害データを評価できます。OpenShift Dedicated のユーザーは、Red Hat Hybrid Cloud Console の Insights Advisor サービスでレポートを表示できます。

関連情報

- Insights Advisor を使用したクラスターの問題の特定に関する詳細は、Insights を使用したクラスターの問題の特定 を参照してください。

4.4.1. Insights Operator アラートについて

Insights Operator は、Prometheus モニタリングシステムを介して Alertmanager にアラートを宣言します。次のいずれかの方法を使用して、OpenShift Dedicated Web コンソールのアラート UI でこれらのアラートを表示できます。

- **Administrator** パースペクティブで、**Observe** → **Alerting** をクリックします。
- **Developer** パースペクティブで、**Observe** → <project_name> → **Alerts** タブをクリックします。

現在、Insights Operator は、条件が満たされたときに次のアラートを送信します。

表4.1 Insights Operator アラート

アラート	説明
InsightsDisabled	Insights Operator が無効になっています。
SimpleContentAccessNotAvailable	Red Hat Subscription Management で、Simple Content Access が有効になっていません。
InsightsRecommendationActive	Insights に、クラスターに関するアクティブな推奨事項があります。

4.4.2. Deployment Validation Operator のデータの難読化

Deployment Validation Operator (DVO) がインストールされている場合、クラスター管理者は、この Operator からのデータを難読化するように Insight Operator を設定できます。**workload_names** 値を **insights-config ConfigMap** オブジェクトに追加すると、UID ではなくワークロード名が Insights for Openshift に表示され、クラスター管理者が認識しやすくなります。

前提条件

- リモートヘルスレポートが有効になっている (デフォルト)。
- "cluster-admin" ロールで OpenShift Dedicated Web コンソールにログインしている。
- **insights-config ConfigMap** オブジェクトが、**openshift-insights** namespace に存在する。
- クラスターがセルフマネージドであり、Deployment Validation Operator がインストールされている。

手順

1. **Workloads** → **ConfigMaps** に移動し、**Project: openshift-insights** を選択します。
2. **insights-config ConfigMap** オブジェクトをクリックして開きます。
3. **Actions** をクリックし、**Edit ConfigMap** を選択します。
4. **YAML view** のラジオボタンをクリックします。
5. ファイル内で、**workload_names** 値を使用して **obfuscation** 属性を設定します。

```
apiVersion: v1
kind: ConfigMap
# ...
data:
  config.yaml: |
```

```
    dataReporting:
      obfuscation:
        - workload_names
# ...
```

6. **Save** をクリックします。**insights-config** config-map の詳細ページが開きます。
7. **config.yaml** の **obfuscation** 属性の値が **- workload_names** に設定されていることを確認します。

第5章 クラスターに関するデータの収集

次のツールを使用して、OpenShift Dedicated クラスターに関するデバッグ情報を取得できます。

5.1. MUST-GATHER ツールについて

oc adm must-gather CLI コマンドは、以下のような問題のデバッグに必要となる可能性のあるクラスターからの情報を収集します。

- リソース定義
- サービスログ

デフォルトで、**oc adm must-gather** コマンドはデフォルトのプラグインイメージを使用し、**./must-gather.local** に書き込みを行います。

または、以下のセクションで説明されているように、適切な引数を指定してコマンドを実行すると、特定の情報を収集できます。

- 1 つ以上の特定の機能に関連するデータを収集するには、以下のセクションに示すように、イメージと共に **--image** 引数を使用します。
  以下に例を示します。

  ```
  $ oc adm must-gather \
    --image=registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.17.0
  ```

- 監査ログを収集するには、以下のセクションで説明されているように **--** **/usr/bin/gather_audit_logs** 引数を使用します。
  以下に例を示します。

  ```
  $ oc adm must-gather -- /usr/bin/gather_audit_logs
  ```

注記

ファイルのサイズを小さくするために、監査ログはデフォルトの情報セットの一部として収集されません。

oc adm must-gather を実行すると、ランダムな名前を持つ新規 Pod がクラスターの新規プロジェクトに作成されます。データはその Pod 上で収集され、現在の作業ディレクトリー内の **must-gather.local** で始まる新しいディレクトリーに保存されます。

以下に例を示します。

```
NAMESPACE                  NAME              READY   STATUS      RESTARTS      AGE
...
openshift-must-gather-5drcj    must-gather-bklx4    2/2     Running     0          72s
openshift-must-gather-5drcj    must-gather-s8sdh    2/2     Running     0          72s
...
```

任意で、**--run-namespace** オプションを使用して、特定の namespace で **oc adm must-gather** コマンドを実行できます。

以下に例を示します。

```
$ oc adm must-gather --run-namespace <namespace> \
  --image=registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.17.0
```

5.1.1. Red Hat サポート用のクラスターに関するデータの収集

oc adm must-gather CLI コマンドを使用して、クラスターに関するデバッグ情報を収集できます。

前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。

注記

OpenShift Dedicated デプロイメントでは、Customer Cloud Subscription (CCS) モデルを使用していないお客様は、**cluster-admin** 権限が必要なため、**oc adm must-gather** コマンドを使用できません。

- OpenShift CLI (**oc**) がインストールされている。

手順

1. **must-gather** データを保存するディレクトリーに移動します。
2. **oc adm must-gather** コマンドを実行します。

```
$ oc adm must-gather
```

注記

このコマンドは、デフォルトでランダムなコントロールプレーンノードを選択するため、Pod は **NotReady** および **SchedulingDisabled** 状態のコントロールプレーンノードにスケジュールされる場合があります。

a. このコマンドが失敗する場合 (クラスターで Pod をスケジュールできない場合など)、**oc adm inspect** コマンドを使用して、特定リソースに関する情報を収集します。

注記

収集する推奨リソースについては、Red Hat サポートにお問い合わせください。

3. 作業ディレクトリーに作成された **must-gather** ディレクトリーから圧縮ファイルを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar cvaf must-gather.tar.gz must-gather.local.5421342344627712289/ 1
```

1 **must-gather-local.5421342344627712289/** を実際のディレクトリー名に置き換えてください。

4. Red Hat カスタマーポータルの **カスタマーサポート ページ** で、圧縮ファイルをサポートケースに添付します。

5.1.2. must-gather フラグ

以下の表に記載されているフラグは、**oc adm must-gather** コマンドで使用できます。

表5.1 oc adm must-gatherの OpenShift Dedicated フラグ

フラグ	コマンドの例	説明
--all-images	**oc adm must-gather --all-images=false**	**operators.openshift.io/ must-gather -image のアノテーションの付いたクラスター上のすべての Operator のデフォルトイメージを使用して、必須収集データを収集** します。
--dest-dir	**oc adm must-gather --dest-dir='<directory_name>'**	収集したデータを書き込むローカルマシンに特定のディレクトリーを設定します。
--host-network	**oc adm must-gather --host-network=false**	**must-gather** Pod を **hostNetwork: true** として実行します。特定のコマンドおよびイメージがホストレベルのデータを取得する必要がある場合に関連します。
--image	**oc adm must-gather --image=[<plugin_image>]**	実行する **must-gather** プラグインイメージを指定します。指定しない場合、OpenShift Dedicated のデフォルトの **must-gather** イメージが使用されます。
--image-stream	**oc adm must-gather --image-stream=[<image_stream>]**	実行する **must-gather** プラグインイメージが含まれる namespace または name:tag 値を使用して'<image_stream>'を指定します。
--node-name	**oc adm must-gather --node-name='<node>'**	使用する特定のノードを設定します。指定しない場合、デフォルトでランダムなマスターが使用されます。
--node-selector	**oc adm must-gather --node-selector='<node_selector_name>'**	使用する特定のノードセレクターを設定します。クラスターノードの一式のデータを同時にキャプチャーする必要があるコマンドおよびイメージを指定する場合にのみ関連します。
--run-namespace	**oc adm must-gather --run-namespace='<namespace>'**	**must-gather** Pod を実行する既存の特権付き namespace。指定しない場合、一時 namespace が生成されます。

フラグ	コマンドの例	説明
--since	**oc adm must-gather --since=<time>**	指定の期間よりも新しいログのみを返します。デフォルトはすべてのログです。プラグインは推奨されますが、サポートの必要はありません。以降またはそれ **以降は**、1つにしか使用できません。
--since-time	**oc adm must-gather --since-time='<date_and_time>'**	特定の日時の後にログのみを返します。(RFC3339)形式で表されます。デフォルトはすべてのログです。プラグインは推奨されますが、サポートの必要はありません。以降またはそれ **以降は**、1つにしか使用できません。
--source-dir	**oc adm must-gather --source-dir='/<directory_name>/'**	収集したデータをコピーする Pod に特定のディレクトリーを設定します。
--timeout	**oc adm must-gather --timeout='<time>'**	タイムアウト前のデータを収集する時間の長さ（秒、分、または時間（例：3s、5m、または 2h））。指定する時間はゼロより大きくする必要があります。指定しない場合、デフォルトは 10 分です。
--volume-percentage	**oc adm must-gather --volume-percentage=<percent>**	**must-gather** に使用できる Pod の割り当てボリュームの最大パーセンテージを指定します。この制限を超えると、**must-gather** は収集を停止しますが、依然として収集したデータをコピーします。指定しない場合、デフォルトは 30% です。

5.1.3. 特定の機能に関するデータ収集

oc adm must-gather CLI コマンドを **--image** または **--image-stream** 引数と共に使用して、特定に機能に関するデバッグ情報を収集できます。**must-gather** ツールは複数のイメージをサポートするため、単一のコマンドを実行して複数の機能に関するデータを収集できます。

表5.2 サポート対象の must-gather イメージ

イメージ	目的
registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.17.0	OpenShift Virtualization のデータ収集。

イメージ	目的
registry.redhat.io/openshift-serverless-1/svls-must-gather-rhel8	OpenShift Serverless のデータ収集。
registry.redhat.io/openshift-service-mesh/istio-must-gather-rhel8:<installed_version_service_mesh>	Red Hat OpenShift Service Mesh のデータ収集。
registry.redhat.io/rhmtc/openshift-migration-must-gather-rhel8:v<installed_version_migration_toolkit>	Migration Toolkit for Containers のデータ収集。
registry.redhat.io/openshift-logging/cluster-logging-rhel9-operator:v<installed_version_logging>	ロギング用のデータ収集。
registry.redhat.io/openshift4/ose-csi-driver-shared-resource-mustgather-rhel8	OpenShift Shared Resource CSI Driver のデータ収集。
registry.redhat.io/openshift-gitops-1/must-gather-rhel8:v<installed_version_GitOps>	Red Hat OpenShift GitOps のデータ収集。
registry.redhat.io/openshift4/ose-secrets-store-csi-mustgather-rhel8:v<installed_version_secret_store>	Secrets Store CSI Driver Operator のデータ収集。

注記

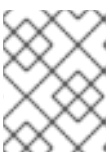
OpenShift Dedicated コンポーネントのイメージの最新バージョンを確認するには、Red Hat カスタマーポータルの OpenShift Operator ライフサイクル Web ページを参照してください。

前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. **must-gather** データを保存するディレクトリーに移動します。
2. **oc adm must-gather** コマンドを 1 つまたは複数の **--image** または **--image-stream** 引数と共に実行します。



注記

- 特定の機能データに加えてデフォルトの **must-gather** データを収集するには、**--image-stream=openshift/must-gather** 引数を追加します。

たとえば、以下のコマンドは、デフォルトのクラスターデータと OpenShift Virtualization に固有の情報の両方を収集します。

```
$ oc adm must-gather \
  --image-stream=openshift/must-gather \ 1
  --image=registry.redhat.io/container-native-virtualization/cnv-must-gather-rhel9:v4.17.0 2
```

1 デフォルトの OpenShift Dedicated **must-gather** イメージ

2 OpenShift Virtualization の must-gather イメージ

must-gather ツールを追加の引数と共に使用し、OpenShift Logging およびクラスター内の Cluster Logging Operator に関連するデータを収集できます。OpenShift Logging の場合、以下のコマンドを実行します。

```
$ oc adm must-gather --image=$(oc -n openshift-logging get deployment.apps/cluster-logging-operator \
  -o jsonpath='{.spec.template.spec.containers[?(@.name == "cluster-logging-operator")].image}')
```

例5.1 OpenShift Logging の must-gather の出力例

```
├── cluster-logging
│   ├── clo
│   │   ├── cluster-logging-operator-74dd5994f-6ttgt
│   │   ├── clusterlogforwarder_cr
│   │   ├── cr
│   │   ├── csv
│   │   ├── deployment
│   │   └── logforwarding_cr
│   ├── collector
│   │   ├── fluentd-2tr64
│   ├── curator
│   │   └── curator-1596028500-zkz4s
│   ├── eo
│   │   ├── csv
│   │   ├── deployment
│   │   └── elasticsearch-operator-7dc7d97b9d-jb4r4
│   ├── es
│   │   ├── cluster-elasticsearch
│   │   │   ├── aliases
│   │   │   ├── health
│   │   │   ├── indices
│   │   │   ├── latest_documents.json
│   │   │   ├── nodes
│   │   │   ├── nodes_stats.json
│   │   │   └── thread_pool
│   │   ├── cr
│   │   ├── elasticsearch-cdm-lp8l38m0-1-794d6dd989-4jxms
│   │   └── logs
│   │       ├── elasticsearch-cdm-lp8l38m0-1-794d6dd989-4jxms
│   ├── install
│   │   ├── co_logs
│   │   ├── install_plan
```

```
│   │   ├── olmo_logs
│   │   └── subscription
│   └── kibana
│       ├── cr
│       └── kibana-9d69668d4-2rkvz
├── cluster-scoped-resources
│   └── core
│       ├── nodes
│       │   ├── ip-10-0-146-180.eu-west-1.compute.internal.yaml
│       └── persistentvolumes
│           ├── pvc-0a8d65d9-54aa-4c44-9ecc-33d9381e41c1.yaml
├── event-filter.html
├── gather-debug.log
└── namespaces
    ├── openshift-logging
    │   ├── apps
    │   │   ├── daemonsets.yaml
    │   │   ├── deployments.yaml
    │   │   ├── replicasets.yaml
    │   │   └── statefulsets.yaml
    │   ├── batch
    │   │   ├── cronjobs.yaml
    │   │   └── jobs.yaml
    │   ├── core
    │   │   ├── configmaps.yaml
    │   │   ├── endpoints.yaml
    │   │   ├── events
    │   │   │   ├── curator-1596021300-wn2ks.162634ebf0055a94.yaml
    │   │   │   ├── curator.162638330681bee2.yaml
    │   │   │   ├── elasticsearch-delete-app-1596020400-gm6nl.1626341a296c16a1.yaml
    │   │   │   ├── elasticsearch-delete-audit-1596020400-9l9n4.1626341a2af81bbd.yaml
    │   │   │   ├── elasticsearch-delete-infra-1596020400-v98tk.1626341a2d821069.yaml
    │   │   │   ├── elasticsearch-rollover-app-1596020400-cc5vc.1626341a3019b238.yaml
    │   │   │   ├── elasticsearch-rollover-audit-1596020400-s8d5s.1626341a31f7b315.yaml
    │   │   │   ├── elasticsearch-rollover-infra-1596020400-7mgv8.1626341a35ea59ed.yaml
    │   │   ├── events.yaml
    │   │   ├── persistentvolumeclaims.yaml
    │   │   ├── pods.yaml
    │   │   ├── replicationcontrollers.yaml
    │   │   ├── secrets.yaml
    │   │   └── services.yaml
    │   ├── openshift-logging.yaml
    │   ├── pods
    │   │   ├── cluster-logging-operator-74dd5994f-6ttgt
    │   │   │   ├── cluster-logging-operator
    │   │   │   │   └── cluster-logging-operator
    │   │   │   │       └── logs
    │   │   │   │           ├── current.log
    │   │   │   │           ├── previous.insecure.log
    │   │   │   │           └── previous.log
    │   │   │   └── cluster-logging-operator-74dd5994f-6ttgt.yaml
    │   │   ├── cluster-logging-operator-registry-6df49d7d4-mxxff
    │   │   │   ├── cluster-logging-operator-registry
    │   │   │   │   └── cluster-logging-operator-registry
    │   │   │   │       └── logs
    │   │   │   │           ├── current.log
```

```
│   │   │   │   │   ├── previous.insecure.log
│   │   │   │   │   └── previous.log
│   │   │   │   ├── cluster-logging-operator-registry-6df49d7d4-mxxff.yaml
│   │   │   │   └── mutate-csv-and-generate-sqlite-db
│   │   │   │       └── mutate-csv-and-generate-sqlite-db
│   │   │   │           └── logs
│   │   │   │               ├── current.log
│   │   │   │               ├── previous.insecure.log
│   │   │   │               └── previous.log
│   │   │   ├── curator-1596028500-zkz4s
│   │   │   ├── elasticsearch-cdm-lp8l38m0-1-794d6dd989-4jxms
│   │   │   ├── elasticsearch-delete-app-1596030300-bpgcx
│   │   │   │   ├── elasticsearch-delete-app-1596030300-bpgcx.yaml
│   │   │   │   └── indexmanagement
│   │   │   │       └── indexmanagement
│   │   │   │           └── logs
│   │   │   │               ├── current.log
│   │   │   │               ├── previous.insecure.log
│   │   │   │               └── previous.log
│   │   │   ├── fluentd-2tr64
│   │   │   │   ├── fluentd
│   │   │   │   │   └── fluentd
│   │   │   │   │       └── logs
│   │   │   │   │           ├── current.log
│   │   │   │   │           ├── previous.insecure.log
│   │   │   │   │           └── previous.log
│   │   │   │   ├── fluentd-2tr64.yaml
│   │   │   │   └── fluentd-init
│   │   │   │       └── fluentd-init
│   │   │   │           └── logs
│   │   │   │               ├── current.log
│   │   │   │               ├── previous.insecure.log
│   │   │   │               └── previous.log
│   │   │   ├── kibana-9d69668d4-2rkvz
│   │   │   │   ├── kibana
│   │   │   │   │   └── kibana
│   │   │   │   │       └── logs
│   │   │   │   │           ├── current.log
│   │   │   │   │           ├── previous.insecure.log
│   │   │   │   │           └── previous.log
│   │   │   │   ├── kibana-9d69668d4-2rkvz.yaml
│   │   │   │   └── kibana-proxy
│   │   │   │       └── kibana-proxy
│   │   │   │           └── logs
│   │   │   │               ├── current.log
│   │   │   │               ├── previous.insecure.log
│   │   │   │               └── previous.log
│   │   └── route.openshift.io
│   │       └── routes.yaml
│   └── openshift-operators-redhat
│       ├── ...
```

3. **oc adm must-gather** コマンドを 1 つまたは複数の **--image** または **--image-stream** 引数と共に実行します。たとえば、以下のコマンドは、デフォルトのクラスターデータと KubeVirt に固有の情報の両方を収集します。

```
$ oc adm must-gather \
 --image-stream=openshift/must-gather \ 1
 --image=quay.io/kubevirt/must-gather 2
```

1. デフォルトの OpenShift Dedicated **must-gather** イメージ
2. KubeVirt の must-gather イメージ

4. 作業ディレクトリーに作成された **must-gather** ディレクトリーから圧縮ファイルを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar cvaf must-gather.tar.gz must-gather.local.5421342344627712289/ 1
```

1. **must-gather-local.5421342344627712289/** を実際のディレクトリー名に置き換えてください。

5. Red Hat カスタマーポータルの **カスタマーサポート** ページ で、圧縮ファイルをサポートケースに添付します。

5.2. 関連情報

- OpenShift Dedicated の更新ライフサイクル

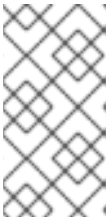
5.2.1. ネットワークログの収集

クラスター内のすべてのノードでネットワークログを収集できます。

手順

1. **-- gather_network_logs** を指定して **oc adm must-gather** コマンドを実行します。

```
$ oc adm must-gather -- gather_network_logs
```



注記

デフォルトでは、**must-gather** ツールはクラスター内のすべてのノードから OVN **nbdb** および **sbdb** データベースを収集します。**--gather_network_logs** オプションを追加して、OVN **nbdb** データベースの OVN-Kubernetes トランザクションを含む追加のログを含めます。

2. 作業ディレクトリーに作成された **must-gather** ディレクトリーから圧縮ファイルを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar cvaf must-gather.tar.gz must-gather.local.472290403699006248 1
```

1. **must-gather-local.472290403699006248** は、実際のディレクトリー名に置き換えます。

3. Red Hat カスタマーポータルの **カスタマーサポート ページ** で、圧縮ファイルをサポートケースに添付します。

5.2.2. must-gather ストレージ制限の変更

oc adm must-gather コマンドを使用してデータを収集する場合、情報のデフォルトの最大ストレージは、コンテナーのストレージ容量の 30% です。30% の制限に達すると、コンテナーが強制終了し、収集プロセスが停止します。すでに収集された情報は、ローカルストレージにダウンロードされます。must-gather コマンドを再度実行するには、ストレージ容量がより大きなコンテナーを使用するか、最大ボリュームの割合を調整する必要があります。

コンテナーがストレージ制限に達すると、次の例のようなエラーメッセージが生成されます。

出力例

```
Disk usage exceeds the volume percentage of 30% for mounted directory. Exiting...
```

前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

- **volume-percentage** フラグを指定して **oc adm must-gather** コマンドを実行します。新しい値として 100 を超える値を指定することはできません。

```
$ oc adm must-gather --volume-percentage <storage_percentage>
```

5.3. クラスター ID の取得

Red Hat サポートに情報を提供する際には、クラスターに固有の識別子を提供していただくと役に立ちます。OpenShift Dedicated Web コンソールを使用してクラスター ID を自動入力できます。Web コンソールまたは OpenShift CLI (**oc**) を使用してクラスター ID を手動で取得することもできます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- Web コンソールまたはインストールされている OpenShift CLI (**oc**) にアクセスできる。

手順

- OpenShift Cluster Manager を使用してクラスター ID を手動で取得するには、以下を行います。
  a. **Cluster List** に移動します。
  b. サポートケースを開く必要があるクラスターの名前をクリックします。
  c. **Overview** タブの **Details** セクションの **Cluster ID** フィールドで値を見つけます。

- Web コンソールを使用してサポートケースを開き、クラスター ID の自動入力を行うには、以下を実行します。
  a. ツールバーから、**(?)Help** に移動し、リストから **Share Feedback** を選択します。
  b. **Tell us about your experience** ウィンドウで **Open a support case** をクリックします。
- Web コンソールを使用してクラスター ID を手動で取得するには、以下を実行します。
  a. **Home → Overview** に移動します。
  b. 値は **Details** セクションの **Cluster ID** フィールドで利用できます。
- OpenShift CLI (**oc**) を使用してクラスター ID を取得するには、以下のコマンドを実行します。

```
$ oc get clusterversion -o jsonpath='{.items[].spec.clusterID}{"\n"}'
```

5.4. クラスターノードジャーナルログのクエリー

個別のクラスターノードの **/var/log** 内で **journald** ユニットログおよびその他のログを収集できます。

前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。

注記

OpenShift Dedicated デプロイメントでは、Customer Cloud Subscription (CCS) モデルを使用していないお客様は、**cluster-admin** 権限が必要なため、**oc adm node-logs** コマンドを使用できません。

- OpenShift CLI (**oc**) がインストールされている。

手順

1. OpenShift Dedicated クラスターノードから **kubelet** の **journald** ユニットログをクエリーします。以下の例では、コントロールプレーンノードのみがクエリーされます。

```
$ oc adm node-logs --role=master -u kubelet 1
```

1 他のユニットログをクエリーするために、**kubelet** を適宜置き換えます。

2. クラスターノードの **/var/log/** の下にある特定のサブディレクトリーからログを収集します。
   a. **/var/log/** サブディレクトリー内に含まれるログの一覧を取得します。以下の例では、すべてのコントロールプレーンノードの **/var/log/openshift-apiserver/** にあるファイルをリスト表示します。

```
$ oc adm node-logs --role=master --path=openshift-apiserver
```

   b. **/var/log/** サブディレクトリー内の特定ログを確認します。以下の例は、すべてのコントロールプレーンノードから **/var/log/openshift-apiserver/audit.log** コンテンツを出力します。

```
$ oc adm node-logs --role=master --path=openshift-apiserver/audit.log
```

5.5. ネットワークトレースメソッド

パケットキャプチャーレコードの形式でネットワークトレースを収集すると、Red Hat がネットワークの問題のトラブルシューティングをサポートできます。

OpenShift Dedicated では、ネットワークトレースの実行方法として 2 種類サポートします。以下の表を確認し、ニーズに合った方法を選択します。

表5.3 サポート対象のネットワークトレース収集の方法

メソッド	利点および機能
ホストのネットワークトレースの収集	1つ以上のノードで同時に指定する期間で、パケットキャプチャーを実行します。パケットキャプチャーファイルは、指定した期間に達すると、ノードからクライアントマシンに転送されます。 特定のアクションが原因でネットワーク通信に問題を発生される理由をトラブルシューティングでいます。パケットキャプチャーを実行し、問題を発生させるアクションを実行してログで問題を診断します。
OpenShift Dedicated ノードまたはコンテナーからのネットワークトレースの収集	1つのノードまたは1つのコンテナーでパケットキャプチャーを実行します。パケットキャプチャーの期間を制御できるように **tcpdump** コマンドを対話的に実行します。 パケットキャプチャーを手動で開始し、ネットワーク通信の問題をトリガーしてから、パケットキャプチャーを手動で停止できます。 この方法では、**cat** コマンドおよびシェルのリダイレクトを使用して、パケットキャプチャーデータをノードまたはコンテナーからクライアントマシンにコピーします。

5.5.1. ホストのネットワークトレースの収集

ネットワーク関連の問題のトラブルシューティングは、ネットワーク通信を追跡して複数のノードで同時にパケットをキャプチャーすることで簡素化されます。

oc adm must-gather コマンドおよび **registry.redhat.io/openshift4/network-tools-rhel8** コンテナーイメージの組み合わせを使用して、ノードからパケットキャプチャーを収集できます。パケットキャプチャーの分析は、ネットワーク通信の問題のトラブルシューティングに役立ちます。

oc adm must-gather コマンドは、特定のノードの Pod で **tcpdump** コマンドの実行に使用されます。**tcpdump** コマンドは、Pod でキャプチャーされたパケットを記録します。**tcpdump** コマンドを終了すると、**oc adm must-gather** コマンドは、Pod からクライアントマシンにキャプチャーされたパケットが含まれるファイルを転送します。

ヒント

以下の手順で使用するコマンド例は、**tcpdump** コマンドを使用してパケットキャプチャーを実行する方法を示しています。ただし、**--image** 引数で指定したコンテナーイメージでコマンドを実行すると、複数のノードから同時にトラブルシューティング情報を収集できます。

前提条件

- OpenShift Dedicated に、**cluster-admin** ロールを持つユーザーとしてログインしている。

注記

OpenShift Dedicated デプロイメントでは、Customer Cloud Subscription (CCS) モデルを使用していないお客様は、**cluster-admin** 権限が必要なため、**oc adm must-gather** コマンドを使用できません。

- OpenShift CLI (**oc**) がインストールされている。

手順

1. 以下のコマンドを実行して、一部のノードでホストネットワークからパケットキャプチャーを実行します。

```
$ oc adm must-gather \
   --dest-dir /tmp/captures \  <.>
   --source-dir '/tmp/tcpdump/' \  <.>
   --image registry.redhat.io/openshift4/network-tools-rhel8:latest \  <.>
   --node-selector 'node-role.kubernetes.io/worker' \  <.>
   --host-network=true \  <.>
   --timeout 30s \  <.>
   -- \
   tcpdump -i any \  <.>
   -w /tmp/tcpdump/%Y-%m-%dT%H:%M:%S.pcap -W 1 -G 300
```

<.> **--dest-dir** 引数では、**oc adm must-gather** の実行時に、クライアントマシンの **/tmp/captures** と相対パスにあるディレクトリーに、キャプチャーしたパケットを保存することを指定します。書き込み可能な任意のディレクトリーを指定できます。<.> **oc adm must-gather** が開始するデバッグ Pod で **tcpdump** が実行される場合に、**--source-dir** 引数は、パケットキャプチャーが Pod の **/tmp/tcpdump** ディレクトリーに一時的に保存されることを指定します。<.> **--image** 引数は、**tcpdump** コマンドを含むコンテナーイメージを指定します。<.> **--node-selector** 引数とサンプル値は、ワーカーノードでパケットキャプチャーを実行するように指定します。別の方法としては、代わりに **--node-name** 引数を指定して、1 つのノードでパケットキャプチャーを実行できます。**--node-selector** と **--node-name** 引数の両方を省略すると、すべてのノードでパケットキャプチャーが実行されます。<.> ノードのネットワークインターフェイスでパケットキャプチャーが実行されるように、**--host-network=true** 引数が必要です。<.> **--timeout** 引数と値は、デバッグ Pod を 30 秒間実行するように指定します。 **--timeout** 引数と期間を指定しない場合、デバッグ Pod は 10 分間実行されます。<.> **tcpdump** コマンドの **-i any** 引数は、すべてのネットワークインターフェイスでパケットをキャプチャーするように指定します。また、ネットワークインターフェイス名を指定することもできます。

2. ネットワークトレースがパケットをキャプチャーしている間に、ネットワーク通信の問題を発生させる、Web アプリケーションにアクセスするなど、特定のアクションを実行します。

3. **oc adm must-gather** で Pod からクライアントマシンに転送したパケットキャプチャーファイルを確認します。

```
tmp/captures
├── event-filter.html
├── ip-10-0-192-217-ec2-internal 1
│   └── registry-redhat-io-openshift4-network-tools-rhel8-sha256-bca...
│       └── 2022-01-13T19:31:31.pcap
├── ip-10-0-201-178-ec2-internal 2
│   └── registry-redhat-io-openshift4-network-tools-rhel8-sha256-bca...
```

```
│       └── 2022-01-13T19:31:30.pcap
├── ip-...
└── timestamp
```

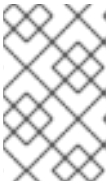
1 2 パケットのキャプチャーは、ホスト名、コンテナー、ファイル名を識別するディレクトリーに保存されます。**--node-selector** 引数を指定しなかった場合には、ホスト名のディレクトリーレベルは存在しません。

5.5.2. OpenShift Dedicated ノードまたはコンテナーからのネットワークトレースの収集

ネットワーク関連の OpenShift Dedicated の潜在的な問題を調査する際に、Red Hat サポートは特定の OpenShift Dedicated クラスターノードまたは特定のコンテナーからネットワークパケットトレースを要求する可能性があります。OpenShift Dedicated でネットワークトレースをキャプチャーする方法として、デバッグ Pod を使用できます。

前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。



注記

OpenShift Dedicated デプロイメントでは、Customer Cloud Subscription (CCS) モデルを使用していないお客様は、**cluster-admin** 権限が必要なため、**oc debug** コマンドを使用できません。

- OpenShift CLI (**oc**) がインストールされている。
- 既存の Red Hat サポートケース ID がある。

手順

1. クラスターノードのリストを取得します。

```
$ oc get nodes
```

2. ターゲットノードのデバッグセッションに入ります。この手順は、**<node_name>-debug** というデバッグ Pod をインスタンス化します。

```
$ oc debug node/my-cluster-node
```

3. **/host** をデバッグシェル内の root ディレクトリーとして設定します。デバッグ Pod は、Pod 内の **/host** にホストの root ファイルシステムをマウントします。root ディレクトリーを **/host** に変更すると、ホストの実行パスに含まれるバイナリーを実行できます。

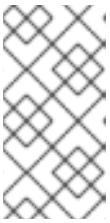
```
# chroot /host
```

4. **chroot** 環境コンソール内から、ノードのインターフェイス名を取得します。

```
# ip ad
```

5. **sosreport** を実行するために必要なバイナリーおよびプラグインが含まれる **toolbox** コンテナーを起動します。

```
# toolbox
```



注記

既存の **toolbox** Pod がすでに実行されている場合、**toolbox** コマンドは以下を出力します: **'toolbox-' already exists.Trying to start…tcpdump** の問題が発生するのを回避するには、**podman rm toolbox-** で実行中の toolbox コンテナーを削除し、新規の toolbox コンテナーを生成します。

6. クラスターノードで **tcpdump** セッションを開始し、出力をキャプチャーファイルにリダイレクトします。この例では、**ens5** をインターフェイス名として使用します。

```
$ tcpdump -nn -s 0 -i ens5 -w /host/var/tmp/my-cluster-node_$(date +%d_%m_%Y-%H_%M_%S-%Z).pcap 1
```

1 toolbox コンテナーはホストの root ディレクトリーを **/host** にマウントするため、**tcpdump** キャプチャーファイルのパスは **chroot** 環境外にあります。

7. ノード上の特定コンテナーに **tcpdump** キャプチャーが必要な場合は、以下の手順に従います。

   a. ターゲットコンテナー ID を確認します。toolbox コンテナーはホストの root ディレクトリーを **/host** にマウントするため、この手順では、**chroot host** コマンドが **crictl** コマンドの前に実行されます。

   ```
   # chroot /host crictl ps
   ```

   b. コンテナーのプロセス ID を確認します。この例では、コンテナー ID は **a7fe32346b120** です。

   ```
   # chroot /host crictl inspect --output yaml a7fe32346b120 | grep 'pid' | awk '{print $2}'
   ```

   c. コンテナーで **tcpdump** セッションを開始し、出力をキャプチャーファイルにリダイレクトします。この例では、**49628** をコンテナーのプロセス ID として使用し、**ens5** をインターフェイス名として使用します。**nsenter** コマンドはターゲットプロセスの namespace に入り、その namespace でコマンドを実行します。この例ではターゲットプロセスがコンテナーのプロセス ID であるため、**tcpdump** コマンドはホストからコンテナーの namespace で実行されます。

   ```
   # nsenter -n -t 49628 -- tcpdump -nn -i ens5 -w /host/var/tmp/my-cluster-node-my-container_$(date +%d_%m_%Y-%H_%M_%S-%Z).pcap 1
   ```

   1 toolbox コンテナーはホストの root ディレクトリーを **/host** にマウントするため、**tcpdump** キャプチャーファイルのパスは **chroot** 環境外にあります。

8. 以下の方法のいずれかを使用して、分析用に **tcpdump** キャプチャーファイルを Red Hat サポートに提供します。

- ファイルを OpenShift Dedicated クラスターから直接既存の Red Hat サポートケースにアップロードします。

  a. toolbox コンテナー内から、**redhat-support-tool** を実行してファイルディレクトリーを既存の Red Hat サポートケースに直接割り当てます。この例では、サポートケース ID **01234567** を使用します。

  ```
  # redhat-support-tool addattachment -c 01234567 /host/var/tmp/my-tcpdump-capture-file.pcap 1
  ```

  1 toolbox コンテナーは、ホストの root ディレクトリーを **/host** にマウントします。**redhat-support-tool** コマンドでアップロードするファイルを指定する場合は、toolbox コンテナーの root ディレクトリー (**/host/** を含む) から絶対パスを参照します。

- 既存の Red Hat サポートケースにファイルをアップロードします。

  a. **oc debug node/<node_name>** コマンドを実行して **sosreport** アーカイブを連結し、出力をファイルにリダイレクトします。このコマンドは、直前の **oc debug** セッションを終了していることを前提としています。

  ```
  $ oc debug node/my-cluster-node -- bash -c 'cat /host/var/tmp/my-tcpdump-capture-file.pcap' > /tmp/my-tcpdump-capture-file.pcap 1
  ```

  1 デバッグコンテナーは、ホストの root ディレクトリーを **/host** にマウントします。連結のためにターゲットファイルを指定する際に、デバッグコンテナーの root ディレクトリー (**/host** を含む) から絶対パスを参照します。

  b. Red Hat カスタマーポータルの Customer Support ページ にある既存のサポートケースに移動します。

  c. **Attach files** を選択し、プロンプトに従ってファイルをアップロードします。

5.5.3. Red Hat サポートへの診断データの提供

OpenShift Dedicated の問題を調査する際に、Red Hat サポートは診断データをサポートケースにアップロードするよう依頼する可能性があります。ファイルは、Red Hat カスタマーポータルからサポートケースにアップロードするか、**redhat-support-tool** コマンドを使用して OpenShift Dedicated クラスターから直接アップロードできます。

前提条件

- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。

  注記

  OpenShift Dedicated デプロイメントでは、Customer Cloud Subscription (CCS) モデルを使用していないお客様は、**cluster-admin** 権限が必要なため、**oc debug** コマンドを使用できません。

- OpenShift CLI (**oc**) がインストールされている。
- 既存の Red Hat サポートケース ID がある。

手順

- Red Hat カスタマーポータルから既存の Red Hat サポートケースに診断データをアップロードします。

  1. **oc debug node/<node_name>** コマンドを使用して OpenShift Dedicated ノードで組み込まれている診断ファイルを連結し、出力をファイルにリダイレクトします。以下の例では、**/host/var/tmp/my-diagnostic-data.tar.gz** をデバッグコンテナーから **/var/tmp/my-diagnostic-data.tar.gz** にコピーします。

     ```
     $ oc debug node/my-cluster-node -- bash -c 'cat /host/var/tmp/my-diagnostic-data.tar.gz' > /var/tmp/my-diagnostic-data.tar.gz 1
     ```

     1 デバッグコンテナーは、ホストの root ディレクトリーを **/host** にマウントします。連結のためにターゲットファイルを指定する際に、デバッグコンテナーの root ディレクトリー (**/host** を含む) から絶対パスを参照します。

  2. Red Hat カスタマーポータルの Customer Support ページ にある既存のサポートケースに移動します。

  3. **Attach files** を選択し、プロンプトに従ってファイルをアップロードします。

- 診断データを OpenShift Dedicated クラスターから直接既存の Red Hat サポートケースにアップロードします。

  1. クラスターノードのリストを取得します。

     ```
     $ oc get nodes
     ```

  2. ターゲットノードのデバッグセッションに入ります。この手順は、**<node_name>-debug** というデバッグ Pod をインスタンス化します。

     ```
     $ oc debug node/my-cluster-node
     ```

  3. **/host** をデバッグシェル内の root ディレクトリーとして設定します。デバッグ Pod は、Pod 内の **/host** にホストの root ファイルシステムをマウントします。root ディレクトリーを **/host** に変更すると、ホストの実行パスに含まれるバイナリーを実行できます。

     ```
     # chroot /host
     ```

  4. **redhat-support-tool** を実行するために必要なバイナリーを含む **toolbox** コンテナーを起動します。

     ```
     # toolbox
     ```

     注記

     既存の **toolbox** Pod がすでに実行されている場合、**toolbox** コマンドは以下を出力します: **'toolbox-' already exists.Trying to start...**問題が発生するのを回避するには、**podman rm toolbox-** で実行中の toolbox コンテナーを削除し、新規の toolbox コンテナーを生成します。

     a. **redhat-support-tool** を実行して、直接デバッグ Pod から既存の Red Hat サポート

a. **redhat-support-tool** を実行して、直接デバッグ Pod から既存の Red Hat サポートケースにファイルを添付します。この例では、サポートケース ID '01234567' とサンプルのファイルパス **/host/var/tmp/my-diagnostic-data.tar.gz** を使用します。

```
# redhat-support-tool addattachment -c 01234567 /host/var/tmp/my-diagnostic-data.tar.gz 1
```

1 toolbox コンテナーは、ホストの root ディレクトリーを **/host** にマウントします。**redhat-support-tool** コマンドでアップロードするファイルを指定する場合は、toolbox コンテナーの root ディレクトリー (**/host/** を含む) から絶対パスを参照します。

5.5.4. toolbox について

toolbox は、Red Hat Enterprise Linux CoreOS (RHCOS) システムでコンテナーを起動するツールです。このツールは、主に **sosreport** や **redhat-support-tool** などのコマンドを実行するために必要なバイナリーおよびプラグインを含むコンテナーを起動するために使用されます。

toolbox コンテナーの主な目的は、診断情報を収集し、これを Red Hat サポートに提供することにあります。ただし、追加の診断ツールが必要な場合は、RPM パッケージを追加するか、標準のサポートツールイメージの代替イメージを実行することができます。

toolbox コンテナーへのパッケージのインストール
デフォルトでは、**toolbox** コマンドを実行すると、**registry.redhat.io/rhel8/support-tools:latest** イメージでコンテナーが起動します。このイメージには、最も頻繁に使用されるサポートツールが含まれます。イメージの一部ではないサポートツールを必要とするノード固有のデータを収集する必要がある場合は、追加のパッケージをインストールできます。

前提条件

- **oc debug node/<node_name>** コマンドでノードにアクセスしている。

手順

1. **/host** をデバッグシェル内の root ディレクトリーとして設定します。デバッグ Pod は、Pod 内の **/host** にホストの root ファイルシステムをマウントします。root ディレクトリーを **/host** に変更すると、ホストの実行パスに含まれるバイナリーを実行できます。

```
# chroot /host
```

2. toolbox コンテナーを起動します。

```
# toolbox
```

3. **wget** などの追加のパッケージをインストールします。

```
# dnf install -y <package_name>
```

toolbox を使用した代替イメージの起動
デフォルトでは、**toolbox** コマンドを実行すると、**registry.redhat.io/rhel8/support-tools:latest** イメージでコンテナーが起動します。**.toolboxrc** ファイルを作成し、実行するイメージを指定して代替イメージを起動できます。

前提条件

- **oc debug node/<node_name>** コマンドでノードにアクセスしている。

手順

1. **/host** をデバッグシェル内の root ディレクトリーとして設定します。デバッグ Pod は、Pod 内の **/host** にホストの root ファイルシステムをマウントします。root ディレクトリーを **/host** に変更すると、ホストの実行パスに含まれるバイナリーを実行できます。

```
# chroot /host
```

2. root ユーザー ID のホームディレクトリーに **.toolboxrc** ファイルを作成します。

```
# vi ~/.toolboxrc
```

```
REGISTRY=quay.io                    (1)
IMAGE=fedora/fedora:33-x86_64       (2)
TOOLBOX_NAME=toolbox-fedora-33      (3)
```

(1) オプション: 代替コンテナーレジストリーを指定します。

(2) 開始する代替イメージを指定します。

(3) オプション: ツールボックスコンテナーの代替名を指定します。

3. 代替イメージを使用して toolbox コンテナーを起動します。

```
# toolbox
```

注記

既存の **toolbox** Pod がすでに実行されている場合、**toolbox** コマンドは以下を出力します: **'toolbox-' already exists.Trying to start…podman rm toolbox-** で実行中の toolbox コンテナーを削除して、**sosreport** プラグインの問題を回避するために、新規の toolbox コンテナーを生成します。

第6章 クラスター仕様の要約

6.1. クラスターバージョンオブジェクトを使用してクラスター仕様を要約する

clusterversion リソースをクエリーし、OpenShift Dedicated クラスター仕様の要約を取得できます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. クラスターバージョン、可用性、アップタイム、および一般的なステータスをクエリーします。

```
$ oc get clusterversion
```

出力例

```
NAME      VERSION   AVAILABLE   PROGRESSING   SINCE   STATUS
version   4.13.8    True        False         8h      Cluster version is 4.13.8
```

2. クラスター仕様の詳細な要約、更新の可用性、および更新履歴を取得します。

```
$ oc describe clusterversion
```

出力例

```
Name:         version
Namespace:
Labels:       <none>
Annotations:  <none>
API Version:  config.openshift.io/v1
Kind:         ClusterVersion
# ...
    Image:    quay.io/openshift-release-dev/ocp-
release@sha256:a956488d295fe5a59c8663a4d9992b9b5d0950f510a7387dbbfb8d20fc5970ce

    URL:      https://access.redhat.com/errata/RHSA-2023:4456
    Version:  4.13.8
  History:
    Completion Time:    2023-08-17T13:20:21Z
    Image:              quay.io/openshift-release-dev/ocp-
release@sha256:a956488d295fe5a59c8663a4d9992b9b5d0950f510a7387dbbfb8d20fc5970ce

    Started Time:       2023-08-17T12:59:45Z
    State:              Completed
```

```
    Verified:          false
    Version:           4.13.8
# ...
```

第7章 トラブルシューティング

7.1. ノードの健全性の確認

7.1.1. ノードのステータス、リソースの使用状況および設定の確認

クラスターノードの健全性ステータス、リソース消費統計、およびノードログを確認します。さらに、個別のノードで **kubelet** ステータスをクエリーします。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

- クラスターのすべてのノードの名前、ステータスおよびロールをリスト表示します。

```
$ oc get nodes
```

- クラスター内の各ノードの CPU およびメモリーの使用状況を要約します。

```
$ oc adm top nodes
```

- 特定のノードの CPU およびメモリーの使用状況を要約します。

```
$ oc adm top node my-node
```

7.2. OPERATOR 関連の問題のトラブルシューティング

Operator は、OpenShift Dedicated アプリケーションをパッケージ化、デプロイ、および管理する方法です。Operator はソフトウェアベンダーのエンジニアリングチームの拡張機能のように動作し、OpenShift Dedicated 環境を監視し、その最新状態に基づいてリアルタイムの意思決定を行います。Operator はアップグレードをシームレスに実行し、障害に自動的に対応するように設計されており、時間の節約のためにソフトウェアのバックアッププロセスを省略するなどのショートカットを実行することはありません。

OpenShift Dedicated 4 には、クラスターが適切に機能するために必要な Operator のデフォルトセットが含まれています。これらのデフォルト Operator は Cluster Version Operator (CVO) によって管理されます。

クラスター管理者は、OpenShift Dedicated Web コンソールまたは CLI を使用して、OperatorHub からアプリケーション Operator をインストールできます。その後、Operator を 1 つまたは複数の namespace にサブスクライブし、クラスター上で開発者が使用できるようにできます。アプリケーション Operator は Operator Lifecycle Manager (OLM) によって管理されます。

Operator に問題が発生した場合には、Operator Subscription のステータスを確認します。クラスター全体で Operator Pod の正常性を確認し、診断用に Operator ログを収集します。

7.2.1. Operator サブスクリプションの状態のタイプ

サブスクリプションは状態に関する以下のタイプを報告します。

表7.1 サブスクリプションの状態のタイプ

状態	説明
CatalogSourcesUnhealthy	解決に使用される一部のまたはすべてのカタログソースは正常ではありません。
InstallPlanMissing	サブスクリプションのインストール計画がありません。
InstallPlanPending	サブスクリプションのインストール計画はインストールの保留中です。
InstallPlanFailed	サブスクリプションのインストール計画が失敗しました。
ResolutionFailed	サブスクリプションの依存関係の解決に失敗しました。

注記

デフォルトの OpenShift Dedicated クラスター Operator は、Cluster Version Operator (CVO) によって管理されます。この Operator には **Subscription** オブジェクトがありません。アプリケーション Operator は、Operator Lifecycle Manager (OLM) によって管理されます。この Operator には **Subscription** オブジェクトがあります。

関連情報

- カタログの正常性要件

7.2.2. CLI を使用した Operator サブスクリプションステータスの表示

CLI を使用して Operator サブスクリプションステータスを表示できます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. Operator サブスクリプションをリスト表示します。

```
$ oc get subs -n <operator_namespace>
```

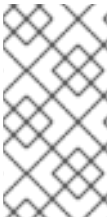
2. **oc describe** コマンドを使用して、**Subscription** リソースを検査します。

```
$ oc describe sub <subscription_name> -n <operator_namespace>
```

3. コマンド出力で、**Conditions** セクションで Operator サブスクリプションの状態タイプのステータスを確認します。以下の例では、利用可能なすべてのカタログソースが正常であるため、**CatalogSourcesUnhealthy** 状態タイプのステータスは **false** になります。

出力例

```
Name:         cluster-logging
Namespace:    openshift-logging
Labels:       operators.coreos.com/cluster-logging.openshift-logging=
Annotations:  <none>
API Version:  operators.coreos.com/v1alpha1
Kind:         Subscription
# ...
Conditions:
  Last Transition Time:  2019-07-29T13:42:57Z
  Message:               all available catalogsources are healthy
  Reason:                AllCatalogSourcesHealthy
  Status:                False
  Type:                  CatalogSourcesUnhealthy
# ...
```



注記

デフォルトの OpenShift Dedicated クラスター Operator は、Cluster Version Operator (CVO) によって管理されます。この Operator には **Subscription** オブジェクトがありません。アプリケーション Operator は、Operator Lifecycle Manager (OLM) によって管理されます。この Operator には **Subscription** オブジェクトがあります。

7.2.3. CLI を使用した Operator カタログソースのステータス表示

Operator カタログソースのステータスは、CLI を使用して確認できます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. namespace のカタログソースをリスト表示します。たとえば、クラスター全体のカタログソースに使用されている **openshift-marketplace** namespace を確認することができます。

```
$ oc get catalogsources -n openshift-marketplace
```

出力例

```
NAME                  DISPLAY               TYPE   PUBLISHER   AGE
certified-operators   Certified Operators   grpc   Red Hat     55m
community-operators   Community Operators   grpc   Red Hat     55m
example-catalog       Example Catalog       grpc   Example Org 2m25s
redhat-marketplace    Red Hat Marketplace   grpc   Red Hat     55m
redhat-operators      Red Hat Operators     grpc   Red Hat     55m
```

2. カタログソースの詳細やステータスを確認するには、**oc describe** コマンドを使用します。

```
$ oc describe catalogsource example-catalog -n openshift-marketplace
```

出力例

```
Name:         example-catalog
Namespace:    openshift-marketplace
Labels:       <none>
Annotations:  operatorframework.io/managed-by: marketplace-operator
              target.workload.openshift.io/management: {"effect": "PreferredDuringScheduling"}
API Version:  operators.coreos.com/v1alpha1
Kind:         CatalogSource
# ...
Status:
  Connection State:
    Address:              example-catalog.openshift-marketplace.svc:50051
    Last Connect:         2021-09-09T17:07:35Z
    Last Observed State:  TRANSIENT_FAILURE
  Registry Service:
    Created At:         2021-09-09T17:05:45Z
    Port:               50051
    Protocol:           grpc
    Service Name:       example-catalog
    Service Namespace:  openshift-marketplace
# ...
```

前述の出力例では、最後に観測された状態が **TRANSIENT_FAILURE** となっています。この状態は、カタログソースの接続確立に問題があることを示しています。

3. カタログソースが作成された namespace の Pod をリストアップします。

```
$ oc get pods -n openshift-marketplace
```

出力例

```
NAME                                  READY   STATUS             RESTARTS   AGE
certified-operators-cv9nn             1/1     Running            0          36m
community-operators-6v8lp             1/1     Running            0          36m
marketplace-operator-86bfc75f9b-jkgbc   1/1     Running            0          42m
example-catalog-bwt8z                 0/1     ImagePullBackOff   0          3m55s
redhat-marketplace-57p8c              1/1     Running            0          36m
redhat-operators-smxx8                1/1     Running            0          36m
```

namespace にカタログソースを作成すると、その namespace にカタログソース用の Pod が作成されます。前述の出力例では、**example-catalog-bwt8z** Pod のステータスが **ImagePullBackOff** になっています。このステータスは、カタログソースのインデックスイメージのプルに問題があることを示しています。

4. **oc describe** コマンドを使用して、より詳細な情報を得るために Pod を検査します。

```
$ oc describe pod example-catalog-bwt8z -n openshift-marketplace
```

出力例

```
Name:         example-catalog-bwt8z
Namespace:    openshift-marketplace
Priority:     0
```

```
Node:         ci-ln-jyryyg2-f76d1-ggdbq-worker-b-vsxjd/10.0.128.2
...
Events:
  Type     Reason          Age                From               Message
  ----     ------          ----               ----               -------
  Normal   Scheduled       48s                default-scheduler  Successfully assigned openshift-marketplace/example-catalog-bwt8z to ci-ln-jyryyf2-f76d1-fgdbq-worker-b-vsxjd
  Normal   AddedInterface  47s                multus             Add eth0 [10.131.0.40/23] from openshift-sdn
  Normal   BackOff         20s (x2 over 46s)  kubelet            Back-off pulling image "quay.io/example-org/example-catalog:v1"
  Warning  Failed          20s (x2 over 46s)  kubelet            Error: ImagePullBackOff
  Normal   Pulling         8s (x3 over 47s)   kubelet            Pulling image "quay.io/example-org/example-catalog:v1"
  Warning  Failed          8s (x3 over 47s)   kubelet            Failed to pull image "quay.io/example-org/example-catalog:v1": rpc error: code = Unknown desc = reading manifest v1 in quay.io/example-org/example-catalog: unauthorized: access to the requested resource is not authorized
  Warning  Failed          8s (x3 over 47s)   kubelet            Error: ErrImagePull
```

前述の出力例では、エラーメッセージは、カタログソースのインデックスイメージが承認問題のために正常にプルできないことを示しています。例えば、インデックスイメージがログイン認証情報を必要とするレジストリーに保存されている場合があります。

関連情報

- gRPC ドキュメント:接続性の状態

7.2.4. Operator Pod ステータスのクエリー

クラスター内の Operator Pod およびそれらのステータスをリスト表示できます。詳細な Operator Pod の要約を収集することもできます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- API サービスが機能している。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. クラスターで実行されている Operator をリスト表示します。出力には、Operator バージョン、可用性、およびアップタイムの情報が含まれます。

```
$ oc get clusteroperators
```

2. Operator の namespace で実行されている Operator Pod をリスト表示し、Pod のステータス、再起動、および経過時間をリスト表示します。

```
$ oc get pod -n <operator_namespace>
```

3. 詳細な Operator Pod の要約を出力します。

```
$ oc describe pod <operator_pod_name> -n <operator_namespace>
```

7.2.5. Operator ログの収集

Operator の問題が発生した場合、Operator Pod ログから詳細な診断情報を収集できます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- API サービスが機能している。
- OpenShift CLI (**oc**) がインストールされている。
- コントロールプレーンまたはコントロールプレーンマシンの完全修飾ドメイン名がある。

手順

1. Operator の namespace で実行されている Operator Pod、Pod のステータス、再起動、および経過時間をリスト表示します。

```
$ oc get pods -n <operator_namespace>
```

2. Operator Pod のログを確認します。

```
$ oc logs pod/<pod_name> -n <operator_namespace>
```

Operator Pod に複数のコンテナーがある場合、前述のコマンドにより各コンテナーの名前が含まれるエラーが生成されます。個別のコンテナーからログをクエリーします。

```
$ oc logs pod/<operator_pod_name> -c <container_name> -n <operator_namespace>
```

3. API が機能しない場合には、代わりに SSH を使用して各コントロールプレーンノードで Operator Pod およびコンテナーログを確認します。**<master-node>.<cluster_name>.<base_domain>** を適切な値に置き換えます。

   a. 各コントロールプレーンノードの Pod をリスト表示します。

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl pods
```

   b. Operator Pod で **Ready** ステータスが表示されない場合は、Pod のステータスを詳細に検査します。**<operator_pod_id>** を直前のコマンドの出力にリスト表示されている Operator Pod の ID に置き換えます。

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl inspectp
<operator_pod_id>
```

   c. Operator Pod に関連するコンテナーをリスト表示します。

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl ps --pod=
<operator_pod_id>
```

d. **Ready** ステータスが Operator コンテナーに表示されない場合は、コンテナーのステータスを詳細に検査します。**<container_id>** を前述のコマンドの出力に一覧表示されているコンテナー ID に置き換えます。

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl inspect
<container_id>
```

e. **Ready** ステータスが表示されない Operator コンテナーのログを確認します。**<container_id>** を前述のコマンドの出力に一覧表示されているコンテナー ID に置き換えます。

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo crictl logs -f
<container_id>
```

注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Dedicated 4 クラスターノードは変更できず、Operator を使用してクラスターの変更を適用します。SSH を使用したクラスターノードへのアクセスは推奨されません。SSH 経由で診断データの収集を試行する前に、**oc adm must gather** およびその他の **oc** コマンドを実行して収集されるデータが十分であるかどうかを確認してください。ただし、OpenShift Dedicated API が使用できない場合、または kubelet がターゲットノード上で適切に機能していない場合は、**oc** 操作が影響を受けます。この場合は、代わりに **ssh core@<node>.<cluster_name>.<base_domain>** を使用してノードにアクセスできます。

7.3. POD の問題の調査

OpenShift Dedicated は、Kubernetes の Pod の概念を活用しています。Pod とは、1 つのホスト上に一緒にデプロイされた 1 つ以上のコンテナーです。Pod は、OpenShift Dedicated 4 で定義、デプロイ、管理できる最小のコンピューティング単位です。

Pod が定義されると、コンテナーが終了するまで、またはコンテナーが削除されるまでノードで実行されるように割り当てられます。ポリシーおよび終了コードに応じて、Pod は終了または保持後に削除され、それらのログがアクセスできるようにします。

Pod の問題が発生した場合には、まず Pod のステータスをチェックします。Pod の明示的な障害が発生した場合には、Pod のエラー状態をチェックして、特定のイメージ、コンテナー、または Pod ネットワークの問題を特定してください。エラー状態に基づく診断データの収集を行います。Pod イベントメッセージおよび Pod およびコンテナーのログ情報を確認します。コマンドライン上で実行中の Pod にアクセスするか、問題のある Pod のデプロイメント設定に基づいて root アクセスでデバッグ Pod を起動して問題を動的に診断します。

7.3.1. Pod のエラー状態について

Pod の障害により、**oc get Pods** の出力の **status** フィールドで確認できる明示的なエラー状態が返されます。Pod のエラー状態は、イメージ、コンテナー、およびコンテナーネットワークに関連する障害に関する状態を示します。

以下の表は、Pod のエラー状態のリストをそれらの説明を記載しています。

表7.2 Pod のエラー状態

Pod のエラー状態	説明
ErrImagePull	一般的なイメージの取得エラー。
ErrImagePullBackOff	イメージの取得に失敗し、取り消されました。
ErrInvalidImageName	指定されたイメージ名は無効です。
ErrImageInspect	イメージの検査に失敗しました。
ErrImageNeverPull	**PullPolicy** は **NeverPullImage** に設定され、ターゲットイメージはホスト上でローカルに見つかりません。
ErrRegistryUnavailable	レジストリーからイメージの取得を試みる際に、HTTP エラーが発生しました。
ErrContainerNotFound	指定されたコンテナーが宣言された Pod 内にないか、kubelet によって管理されていません。
ErrRunInitContainer	コンテナーの初期化に失敗しました。
ErrRunContainer	Pod のコンテナーのいずれも正常に起動しませんでした。
ErrKillContainer	Pod のコンテナーのいずれも正常に強制終了されませんでした。
ErrCrashLoopBackOff	コンテナーが終了しました。kubelet は再起動を試行しません。
ErrVerifyNonRoot	コンテナーまたはイメージが root 権限で実行を試行しました。
ErrCreatePodSandbox	Pod サンドボックスの作成が成功しませんでした。
ErrConfigPodSandbox	Pod サンドボックス設定を取得できませんでした。
ErrKillPodSandbox	Pod サンドボックスは正常に停止しませんでした。
ErrSetupNetwork	ネットワークの初期化に失敗しました。

Pod のエラー状態	説明
ErrTeardownNetwork	ネットワークの終了に失敗しました。

7.3.2. Pod ステータスの確認

Pod のステータスおよびエラー状態をクエリーできます。Pod に関連するデプロイメント設定をクエリーし、ベースイメージの可用性を確認することもできます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。
- **skopeo** がインストールされている。

手順

1. プロジェクトに切り替えます。

```
$ oc project <project_name>
```

2. namespace 内で実行されている Pod、Pod のステータス、エラーの状態、再起動、および経過時間をリスト表示します。

```
$ oc get pods
```

3. namespace がデプロイメント設定で管理されているかどうかを判別します。

```
$ oc status
```

namespace がデプロイメント設定で管理される場合、出力には、デプロイメント設定名とベースイメージの参照が含まれます。

4. 前述のコマンドの出力で参照されているベースイメージを検査します。

```
$ skopeo inspect docker://<image_reference>
```

5. ベースイメージの参照が正しくない場合は、デプロイメント設定の参照を更新します。

```
$ oc edit deployment/my-deployment
```

6. デプロイメント設定が終了時に変更されると、設定が自動的に再デプロイされます。デプロイメントの進行中に Pod ステータスを確認し、問題が解決されているかどうかを判別します。

```
$ oc get pods -w
```

7. Pod の失敗に関連する診断情報については、namespace 内でイベントを確認します。

```
$ oc get events
```

7.3.3. Pod およびコンテナーログの検査

明示的な Pod の失敗に関連する警告およびエラーメッセージの有無について Pod およびコンテナーログを検査できます。ポリシーおよび終了コードによっては、Pod およびコンテナーログは Pod の終了後も利用可能のままになります。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- API サービスが機能している。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. 特定の Pod のログをクエリーします。

```
$ oc logs <pod_name>
```

2. Pod 内の特定コンテナーのログをクエリーします。

```
$ oc logs <pod_name> -c <container_name>
```

前述の **oc logs** コマンドを使用して取得されるログは、Pod またはコンテナー内の標準出力 (stdout) に送信されるメッセージで構成されます。

3. Pod 内の /**var**/**log**/ に含まれるログを検査します。
   a. Pod 内の /**var**/**log** に含まれるファイルおよびサブディレクトリーをリスト表示します。

```
$ oc exec <pod_name>  -- ls -alh /var/log
```

出力例

```
total 124K
drwxr-xr-x. 1 root root   33 Aug 11 11:23 .
drwxr-xr-x. 1 root root   28 Sep  6  2022 ..
-rw-rw----. 1 root utmp    0 Jul 10 10:31 btmp
-rw-r--r--. 1 root root  33K Jul 17 10:07 dnf.librepo.log
-rw-r--r--. 1 root root  69K Jul 17 10:07 dnf.log
-rw-r--r--. 1 root root 8.8K Jul 17 10:07 dnf.rpm.log
-rw-r--r--. 1 root root  480 Jul 17 10:07 hawkey.log
-rw-rw-r--. 1 root utmp    0 Jul 10 10:31 lastlog
drwx------. 2 root root   23 Aug 11 11:14 openshift-apiserver
drwx------. 2 root root    6 Jul 10 10:31 private
drwxr-xr-x. 1 root root   22 Mar  9 08:05 rhsm
-rw-rw-r--. 1 root utmp    0 Jul 10 10:31 wtmp
```

   b. Pod 内の /**var**/**log** に含まれる特定のログファイルをクエリーします。

```
$ oc exec <pod_name> cat /var/log/<path_to_log>
```

出力例

```
2023-07-10T10:29:38+0000 INFO --- logging initialized ---
2023-07-10T10:29:38+0000 DDEBUG timer: config: 13 ms
2023-07-10T10:29:38+0000 DEBUG Loaded plugins: builddep, changelog, config-manager, copr, debug, debuginfo-install, download, generate_completion_cache, groups-manager, needs-restarting, playground, product-id, repoclosure, repodiff, repograph, repomanage, reposync, subscription-manager, uploadprofile
2023-07-10T10:29:38+0000 INFO Updating Subscription Management repositories.
2023-07-10T10:29:38+0000 INFO Unable to read consumer identity
2023-07-10T10:29:38+0000 INFO Subscription Manager is operating in container mode.
2023-07-10T10:29:38+0000 INFO
```

c. 特定のコンテナー内の **/var/log** に含まれるログファイルおよびサブディレクトリーをリスト表示します。

```
$ oc exec <pod_name> -c <container_name> ls /var/log
```

d. 特定のコンテナー内の **/var/log** に含まれる特定のログファイルをクエリーします。

```
$ oc exec <pod_name> -c <container_name> cat /var/log/<path_to_log>
```

7.3.4. 実行中の Pod へのアクセス

Pod 内でシェルを開くか、ポート転送によりネットワークアクセスを取得して、実行中の Pod を動的に確認することができます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- API サービスが機能している。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. アクセスする Pod が含まれるプロジェクトに切り替えます。これは、**oc rsh** コマンドが **-n** namespace オプションを受け入れないために必要です。

```
$ oc project <namespace>
```

2. リモートシェルを Pod で起動します。

```
$ oc rsh <pod_name> 1
```

1 Pod に複数のコンテナーがある場合、**oc rsh** は **-c <container_name>** が指定されていない限り最初のコンテナーにデフォルト設定されます。

3. Pod 内の特定のコンテナーでリモートシェルを起動します。

```
$ oc rsh -c <container_name> pod/<pod_name>
```

4. Pod のポートへのポート転送セッションを作成します。

```
$ oc port-forward <pod_name> <host_port>:<pod_port> 1
```

1 ポート転送セッションをキャンセルするには、**Ctrl+C** を入力します。

7.3.5. root アクセスでのデバッグ Pod の起動

問題のある Pod のデプロイメントまたはデプロイメント設定に基づいて、root アクセスでデバッグ Pod を起動できます。通常、Pod ユーザーは root 以外の権限で実行しますが、問題を調査するために一時的な root 権限で Pod のトラブルシューティングを実行することは役に立ちます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- API サービスが機能している。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. デプロイメントに基づいて、root アクセスでデバッグ Pod を起動します。
   a. プロジェクトのデプロイメント名を取得します。

```
$ oc get deployment -n <project_name>
```

   b. デプロイメントに基づいて、root 権限でデバッグ Pod を起動します。

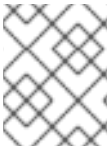
```
$ oc debug deployment/my-deployment --as-root -n <project_name>
```

2. デプロイメント設定に基づいて、root アクセスでデバッグ Pod を起動します。
   a. プロジェクトのデプロイメント設定名を取得します。

```
$ oc get deploymentconfigs -n <project_name>
```

   b. デプロイメント設定に基づいて、root 権限でデバッグ Pod を起動します。

```
$ oc debug deploymentconfig/my-deployment-configuration --as-root -n <project_name>
```



注記

インタラクティブなシェルを実行する代わりに、**-- <command>** を前述の **oc debug** コマンドに追加し、デバッグ Pod 内で個々のコマンドを実行することができます。

7.3.6. Pod およびコンテナーへの/からのファイルのコピー

Pod に/からファイルをコピーして、設定変更をテストしたり、診断情報を収集したりできます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- API サービスが機能している。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. ファイルを Pod にコピーします。

```
$ oc cp <local_path> <pod_name>:/<path> -c <container_name>  1
```

1 **-c** オプションが指定されていない場合、Pod の最初のコンテナーが選択されます。

2. Pod からファイルをコピーします。

```
$ oc cp <pod_name>:/<path>  -c <container_name> <local_path>  1
```

1 **-c** オプションが指定されていない場合、Pod の最初のコンテナーが選択されます。

注記

oc cp が機能するには、**tar** バイナリーがコンテナー内で利用可能である必要があります。

7.4. ストレージの問題のトラブルシューティング

7.4.1. 複数割り当てエラーの解決

ノードが予期せずにクラッシュまたはシャットダウンすると、割り当てられた ReadWriteOnce (RWO) ボリュームがノードからアンマウントされ、その後は別のノードでスケジュールされる Pod で使用可能になることが予想されます。

ただし、障害が発生したノードは割り当てられたボリュームをアンマウントできないため、新規ノードにマウントすることはできません。

複数割り当てのエラーが報告されます。

出力例

```
Unable to attach or mount volumes: unmounted volumes=[sso-mysql-pvol], unattached volumes=
[sso-mysql-pvol default-token-x4rzc]: timed out waiting for the condition
Multi-Attach error for volume "pvc-8837384d-69d7-40b2-b2e6-5df86943eef9" Volume is already used
by pod(s) sso-mysql-1-ns6b4
```

手順

複数割り当ての問題を解決するには、以下のソリューションのいずれかを使用します。

- RWX ボリュームを使用して、複数割り当てを有効にします。
ほとんどのストレージソリューションでは、ReadWriteMany (RWX) ボリュームを使用して、複数割り当てエラーを防ぐことができます。

- RWO ボリュームの使用時に障害が発生したノードを回復するか、削除します。
VMware vSphere などの RWX をサポートしないストレージの場合、RWO ボリュームが代わりに使用される必要があります。ただし、RWO ボリュームは複数のノードにマウントできません。

  複数割り当てのエラーメッセージが RWO ボリュームと共に表示される場合には、シャットダウンまたはクラッシュしたノードで Pod を強制的に削除し、動的永続ボリュームの割り当て時などの重要なワークロードでのデータ損失を回避します。

  ```
  $ oc delete pod <old_pod> --force=true --grace-period=0
  ```

  このコマンドは、シャットダウンまたはクラッシュしたノードで停止したボリュームを 6 分後に削除します。

7.5. モニタリング関連の問題の調査

OpenShift Dedicated には、コアプラットフォームコンポーネントの監視を提供する、事前設定、事前インストールが行われ、自動更新される監視スタックが含まれています。OpenShift Dedicated 4 では、クラスター管理者は任意でユーザー定義プロジェクトのモニタリングを有効にすることができます。

次の問題が発生した場合は、このセクションの手順に従ってください。

- 独自のメトリクスが利用できない。
- Prometheus が大量のディスク容量を消費している。
- Prometheus に対して **KubePersistentVolumeFillingUp** アラートが発生している。

7.5.1. ユーザー定義のプロジェクトメトリクスが使用できない理由の調査

ServiceMonitor リソースを使用すると、ユーザー定義プロジェクトでサービスによって公開されるメトリクスの使用方法を判別できます。**ServiceMonitor** リソースを作成している場合で、メトリクス UI に対応するメトリクスが表示されない場合は、この手順で説明されるステップを実行します。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。
- ユーザー定義のプロジェクトのモニタリングを有効にし、設定している。
- **ServiceMonitor** リソースを作成している。

手順

1. サービスおよび **ServiceMonitor** リソース設定で、**対応するラベルの一致を確認** します。
   a. サービスに定義されたラベルを取得します。以下の例では、**ns1** プロジェクトの **prometheus-example-app** サービスをクエリーします。

```
$ oc -n ns1 get service prometheus-example-app -o yaml
```

出力例

```
  labels:
    app: prometheus-example-app
```

b. **ServiceMonitor** リソース設定の **matchLabels** 定義が、直前の手順のラベルの出力と一致することを確認します。次の例では、**ns1** プロジェクトの **prometheus-example-monitor** サービスモニターをクエリーします。

```
$ oc -n ns1 get servicemonitor prometheus-example-monitor -o yaml
```

出力例

```
apiVersion: v1
kind: ServiceMonitor
metadata:
  name: prometheus-example-monitor
  namespace: ns1
spec:
  endpoints:
  - interval: 30s
    port: web
    scheme: http
  selector:
    matchLabels:
      app: prometheus-example-app
```

注記

プロジェクトの表示権限を持つ開発者として、サービスおよび **ServiceMonitor** リソースラベルを確認できます。

2. **openshift-user-workload-monitoring** プロジェクトの **Prometheus Operator のログを検査**します。

a. **openshift-user-workload-monitoring** プロジェクトの Pod をリスト表示します。

```
$ oc -n openshift-user-workload-monitoring get pods
```

出力例

```
NAME                                  READY   STATUS    RESTARTS   AGE
prometheus-operator-776fcbbd56-2nbfm  2/2     Running   0          132m
prometheus-user-workload-0            5/5     Running   1          132m
prometheus-user-workload-1            5/5     Running   1          132m
thanos-ruler-user-workload-0          3/3     Running   0          132m
thanos-ruler-user-workload-1          3/3     Running   0          132m
```

b. **prometheus-operator** Pod の **prometheus-operator** コンテナーからログを取得します。以下の例では、Pod は **prometheus-operator-776fcbbd56-2nbfm** になります。

```
$ oc -n openshift-user-workload-monitoring logs prometheus-operator-776fcbbd56-
2nbfm -c prometheus-operator
```

サービスモニターに問題がある場合、ログには以下のようなエラーが含まれる可能性があります。

```
level=warn ts=2020-08-10T11:48:20.906739623Z caller=operator.go:1829
component=prometheusoperator msg="skipping servicemonitor" error="it accesses file
system via bearer token file which Prometheus specification prohibits"
servicemonitor=eagle/eagle namespace=openshift-user-workload-monitoring
prometheus=user-workload
```

3. OpenShift Dedicated Web コンソール UI の **Metrics targets** ページで **エンドポイントのターゲットステータスを確認します。**

   a. OpenShift Dedicated Web コンソールにログインし、**Administrator** パースペクティブで **Observe → Targets** に移動します。

   b. リストでメトリクスのエンドポイントを探し、**Status** 列でターゲットのステータスを確認します。

   c. **Status** が **Down** の場合、エンドポイントの URL をクリックすると、そのメトリクスターゲットの **Target Details** ページで詳細情報を見ることができます。

4. **openshift-user-workload-monitoring** プロジェクトで **Prometheus Operator のデバッグレベルのロギングを設定** します。

   a. **openshift-user-workload-monitoring** プロジェクトで **user-workload-monitoring-config ConfigMap** オブジェクトを編集します。

   ```
   $ oc -n openshift-user-workload-monitoring edit configmap user-workload-monitoring-
   config
   ```

   b. **prometheusOperator** の **logLevel: debug** を **data/config.yaml** に追加し、ログレベルを **debug** に設定します。

   ```
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: user-workload-monitoring-config
     namespace: openshift-user-workload-monitoring
   data:
     config.yaml: |
       prometheusOperator:
         logLevel: debug
   # ...
   ```

   c. 変更を適用するためにファイルを保存します。影響を受ける **prometheus-operator** Pod は自動的に再デプロイされます。

   d. **debug** ログレベルが **openshift-user-workload-monitoring** プロジェクトの **prometheus-operator** デプロイメントに適用されていることを確認します。

   ```
   $ oc -n openshift-user-workload-monitoring get deploy prometheus-operator -o yaml |
   grep "log-level"
   ```

出力例

```
- --log-level=debug
```

debug レベルのロギングにより、Prometheus Operator によって行われるすべての呼び出しが表示されます。

e. **prometheus-operator** Pod が実行されていることを確認します。

```
$ oc -n openshift-user-workload-monitoring get pods
```

注記

認識されない Prometheus Operator の **loglevel** 値が config map に含まれる場合、**prometheus-operator** Pod が正常に再起動されない可能性があります。

f. デバッグログを確認し、Prometheus Operator が **ServiceMonitor** リソースを使用しているかどうかを確認します。ログで他の関連するエラーの有無を確認します。

関連情報

- ユーザー定義のワークロードモニタリング設定マップの作成
- サービスモニターまたは Pod モニターの作成方法に関する詳細は、サービスのモニター方法の指定 を参照してください。
- メトリクスターゲットに関する詳細情報の取得 を参照してください。

7.5.2. Prometheus が大量のディスク領域を消費している理由の特定

開発者は、キーと値のペアの形式でメトリクスの属性を定義するためにラベルを作成できます。使用できる可能性のあるキーと値のペアの数は、属性について使用できる可能性のある値の数に対応します。数が無制限の値を持つ属性は、バインドされていない属性と呼ばれます。たとえば、**customer_id** 属性は、使用できる値が無限にあるため、バインドされていない属性になります。

割り当てられるキーと値のペアにはすべて、一意の時系列があります。ラベルに多数のバインドされていない値を使用すると、作成される時系列の数が指数関数的に増加する可能性があります。これは Prometheus のパフォーマンスに影響する可能性があり、多くのディスク領域を消費する可能性があります。

Prometheus が多くのディスクを消費する場合、以下の手段を使用できます。

- どのラベルが最も多くの時系列データを作成しているか詳しく知るには **Prometheus HTTP API を使用して時系列データベース (TSDB) のステータスを確認** します。これを実行するには、クラスター管理者権限が必要です。
- 収集されている **スクレイプサンプルの数を確認** します。
- ユーザー定義メトリクスに割り当てられるバインドされていない属性の数を減らすことで、**作成される一意の時系列の数を減らします**。

注記

使用可能な値の制限されたセットにバインドされる属性を使用すると、可能なキーと値のペアの組み合わせの数が減ります。

- ユーザー定義のプロジェクト全体で **スクレイピングできるサンプルの数に制限を適用** します。これには、クラスター管理者の権限が必要です。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. **Administrator** パースペクティブで、**Observe → Metrics** に移動します。
2. **Expression** フィールドに、Prometheus Query Language (PromQL) クエリーを入力します。次のクエリー例は、ディスク領域の消費量の増加につながる可能性のある高カーディナリティメトリクスを識別するのに役立ちます。
   - 次のクエリーを実行すると、スクレイプサンプルの数が最も多いジョブを 10 個特定できます。

     ```
     topk(10, max by(namespace, job) (topk by(namespace, job) (1,
     scrape_samples_post_metric_relabeling)))
     ```

   - 次のクエリーを実行すると、過去 1 時間に最も多くの時系列データを作成したジョブを 10 個特定して、時系列のチャーンを正確に特定できます。

     ```
     topk(10, sum by(namespace, job) (sum_over_time(scrape_series_added[1h])))
     ```

3. 想定よりもサンプルのスクレイプ数が多いメトリクスに割り当てられたラベルで、値が割り当てられていないものの数を確認します。
   - **メトリクスがユーザー定義のプロジェクトに関連する場合**、ワークロードに割り当てられたメトリクスのキーと値のペアを確認します。これらのライブラリーは、アプリケーションレベルで Prometheus クライアントライブラリーを使用して実装されます。ラベルで参照されるバインドされていない属性の数の制限を試行します。
   - **メトリクスがコア OpenShift Dedicated プロジェクトに関連している場合** は、Red Hat Customer Portal で Red Hat サポートケースを作成します。
4. 以下の手順に従い、**dedicated-admin** としてログインし、Prometheus HTTP API を使用して TSDB ステータスを確認します。
   a. 次のコマンドを実行して、Prometheus API ルート URL を取得します。

      ```
      $ HOST=$(oc -n openshift-monitoring get route prometheus-k8s -ojsonpath=
      {.status.ingress[].host})
      ```

   b. 次のコマンドを実行して認証トークンを抽出します。

      ```
      $ TOKEN=$(oc whoami -t)
      ```

c. 次のコマンドを実行して、Prometheus の TSDB ステータスをクエリーします。

```
$ curl -H "Authorization: Bearer $TOKEN" -k "https://$HOST/api/v1/status/tsdb"
```

出力例

```
"status": "success","data":{"headStats":{"numSeries":507473,
"numLabelPairs":19832,"chunkCount":946298,"minTime":1712253600010,
"maxTime":1712257935346},"seriesCountByMetricName":
[{"name":"etcd_request_duration_seconds_bucket","value":51840},
{"name":"apiserver_request_sli_duration_seconds_bucket","value":47718},
...
```

関連情報

- スクレイプサンプル制限の設定方法と関連するアラートルールの作成方法の詳細は、ユーザー定義プロジェクトのスクレイプサンプル制限の設定 を参照してください。

7.5.3. Prometheus に対する KubePersistentVolumeFillingUp アラートの解決

クラスター管理者は、Prometheus に対してトリガーされている **KubePersistentVolumeFillingUp** アラートを解決できます。

openshift-monitoring プロジェクトの **prometheus-k8s-*** Pod によって要求された永続ボリューム (PV) の合計残り容量が 3% 未満になると、重大アラートが発生します。これにより、Prometheus の動作異常が発生する可能性があります。

注記

KubePersistentVolumeFillingUp アラートは 2 つあります。

- **重大アラート**: マウントされた PV の合計残り容量が 3% 未満になると、**severity="critical"** ラベルの付いたアラートがトリガーされます。
- **警告アラート**: マウントされた PV の合計空き容量が 15% 未満になり、4 日以内にいっぱいになると予想される場合、**severity="warning"** ラベルの付いたアラートがトリガーされます。

この問題に対処するには、Prometheus 時系列データベース (TSDB) のブロックを削除して、PV 用のスペースを増やすことができます。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。

手順

1. 次のコマンドを実行して、すべての TSDB ブロックのサイズを古いものから新しいものの順にリスト表示します。

```
$ oc debug <prometheus_k8s_pod_name> -n openshift-monitoring \ 1
```

```
-c prometheus --image=$(oc get po -n openshift-monitoring <prometheus_k8s_pod_name> \
2
-o jsonpath='{.spec.containers[?(@.name=="prometheus")].image}') \
-- sh -c 'cd /prometheus/;du -hs $(ls -dt */ | grep -Eo "[0-9|A-Z]{26}")'
```

1 2 **<prometheus_k8s_pod_name>** は、**KubePersistentVolumeFillingUp** アラートの説明に記載されている Pod に置き換えます。

出力例

```
308M    01HVKMPKQWZYWS8WVDAYQHNMW6
52M     01HVK64DTDA81799TBR9QDECEZ
102M    01HVK64DS7TRZRWF2756KHST5X
140M    01HVJS59K11FBVAPVY57K88Z11
90M     01HVH2A5Z58SKT810EM6B9AT50
152M    01HV8ZDVQMX41MKCN84S32RRZ1
354M    01HV6Q2N26BK63G4RYTST71FBF
156M    01HV664H9J9Z1FTZD73RD1563E
216M    01HTHXB60A7F239HN7S2TENPNS
104M    01HTHMGRXGS0WXA3WATRXHR36B
```

2. 削除できるブロックとその数を特定し、ブロックを削除します。次のコマンド例は、**prometheus-k8s-0** Pod から最も古い 3 つの Prometheus TSDB ブロックを削除します。

```
$ oc debug prometheus-k8s-0 -n openshift-monitoring \
-c prometheus --image=$(oc get po -n openshift-monitoring prometheus-k8s-0 \
-o jsonpath='{.spec.containers[?(@.name=="prometheus")].image}') \
-- sh -c 'ls -latr /prometheus/ | egrep -o "[0-9|A-Z]{26}" | head -3 | \
while read BLOCK; do rm -r /prometheus/$BLOCK; done'
```

3. 次のコマンドを実行して、マウントされた PV の使用状況を確認し、十分な空き容量があることを確認します。

```
$ oc debug <prometheus_k8s_pod_name> -n openshift-monitoring \ 1
--image=$(oc get po -n openshift-monitoring <prometheus_k8s_pod_name> \ 2
-o jsonpath='{.spec.containers[?(@.name=="prometheus")].image}') -- df -h /prometheus/
```

1 2 **<prometheus_k8s_pod_name>** は、**KubePersistentVolumeFillingUp** アラートの説明に記載されている Pod に置き換えます。

次の出力例は、**prometheus-k8s-0** Pod によって要求されるマウントされた PV に、63% の空き容量が残っていることを示しています。

出力例

```
Starting pod/prometheus-k8s-0-debug-j82w4 ...
Filesystem      Size  Used Avail Use% Mounted on
/dev/nvme0n1p4  40G   15G  40G  37% /prometheus

Removing debug pod ...
```

7.6. OPENSHIFT CLI (OC) 関連の問題の診断

7.6.1. OpenShift CLI (oc) ログレベルについて

OpenShift CLI (**oc**) を使用すると、ターミナルからアプリケーションを作成し、OpenShift Dedicated のプロジェクトを管理できます。

oc コマンド固有の問題が発生した場合は、**oc** のログレベルを引き上げ、コマンドで生成される API 要求、API 応答、および **curl** 要求の詳細を出力します。これにより、特定の **oc** コマンドの基礎となる操作の詳細ビューが得られます。これにより、障害の性質に関する洞察が得られる可能性があります。

oc ログレベルは、1 から 10 まであります。以下の表は、 **oc** ログレベルのリストとそれらの説明を示しています。

表7.3 OpenShift CLI (oc) ログレベル

ログレベル	説明
1 - 5	標準エラー (stderr) への追加のロギングはありません。
6	標準エラー (stderr) に API 要求のログを記録します。
7	標準エラー (stderr) に API 要求およびヘッダーのログを記録します。
8	標準エラー (stderr) に API 要求、ヘッダーおよび本体、ならびに API 応答ヘッダーおよび本体のログを記録します。
9	標準エラー (stderr) に API 要求、ヘッダーおよび本体、API 応答ヘッダーおよび本体、**curl** 要求のログを記録します。
10	標準エラー (stderr) に API 要求、ヘッダーおよび本体、API 応答ヘッダーおよび本体、**curl** 要求のログを詳細に記録します。

7.6.2. OpenShift CLI (oc) ログレベルの指定

コマンドのログレベルを引き上げて、OpenShift CLI (**oc**) の問題を調査できます。

OpenShift Dedicated ユーザーの現在のセッショントークンは、通常、必要に応じてログに記録された **curl** リクエストに含まれます。また、**oc** コマンドの基礎となるプロセスを手順ごとにテストする際に使用するために、現行ユーザーのセッショントークンを手動で取得することもできます。

前提条件

- OpenShift CLI (**oc**) がインストールされている。

手順

- **oc** コマンドの実行時に **oc** ログレベルを指定します。

```
$ oc <command> --loglevel <log_level>
```

ここでは、以下のようになります。

<command>
実行しているコマンドを指定します。

<log_level>
コマンドに適用するログレベルを指定します。

- 現行ユーザーのセッショントークンを取得するには、次のコマンドを実行します。

```
$ oc whoami -t
```

出力例

```
sha256~RCV3Qcn7H-OEfqCGVI0CvnZ6...
```

7.7. RED HAT 管理リソース

7.7.1. 概要

以下は、Service Reliability Engineering Platform (SRE-P)チームで管理または保護されるすべての OpenShift Dedicated リソースを対象としています。クラスターが不安定になる可能性があるため、これらのリソースは変更しないでください。

7.7.2. Hive マネージドリソース

以下のリストは、集中化の設定管理システムである OpenShift Hive によって管理される OpenShift Dedicated リソースを示しています。これらのリソースは、インストール時に作成される OpenShift Container Platform リソースに追加されます。OpenShift Hive は、すべての OpenShift Dedicated クラスターで継続的に一貫性を維持しようとします。OpenShift Dedicated リソースへの変更は、OpenShift Cluster Manager と Hive が同期されるように、OpenShift Cluster Manager を介して行う必要があります。OpenShift Cluster Manager が対象のリソースの変更をサポートしていない場合は、ocm-feedback@redhat.com にお問い合わせください。

例7.1 Hive マネージドリソースのリスト

```
Resources:
  ConfigMap:
  - namespace: openshift-config
    name: rosa-brand-logo
  - namespace: openshift-console
    name: custom-logo
  - namespace: openshift-deployment-validation-operator
    name: deployment-validation-operator-config
  - namespace: openshift-file-integrity
    name: fr-aide-conf
  - namespace: openshift-managed-upgrade-operator
    name: managed-upgrade-operator-config
  - namespace: openshift-monitoring
    name: cluster-monitoring-config
  - namespace: openshift-monitoring
    name: managed-namespaces
  - namespace: openshift-monitoring
```

```
    name: ocp-namespaces
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter-code
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter-code
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter-trusted-ca-bundle
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols-code
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols-trusted-ca-bundle
  - namespace: openshift-security
    name: osd-audit-policy
  - namespace: openshift-validation-webhook
    name: webhook-cert
  - namespace: openshift
    name: motd
  Endpoints:
  - namespace: openshift-deployment-validation-operator
    name: deployment-validation-operator-metrics
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols
  - namespace: openshift-scanning
    name: loggerservice
  - namespace: openshift-security
    name: audit-exporter
  - namespace: openshift-validation-webhook
    name: validation-webhook
  Namespace:
  - name: dedicated-admin
  - name: openshift-addon-operator
  - name: openshift-aqua
  - name: openshift-aws-vpce-operator
  - name: openshift-backplane
  - name: openshift-backplane-cee
  - name: openshift-backplane-csa
  - name: openshift-backplane-cse
  - name: openshift-backplane-csm
  - name: openshift-backplane-managed-scripts
  - name: openshift-backplane-mobb
  - name: openshift-backplane-srep
  - name: openshift-backplane-tam
  - name: openshift-cloud-ingress-operator
  - name: openshift-codeready-workspaces
  - name: openshift-compliance
  - name: openshift-compliance-monkey
  - name: openshift-container-security
  - name: openshift-custom-domains-operator
```

```
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-file-integrity
- name: openshift-logging
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-scanning
- name: openshift-security
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-suricata
- name: openshift-validation-webhook
- name: openshift-velero
- name: openshift-monitoring
- name: openshift
- name: openshift-cluster-version
- name: keycloak
- name: goalert
- name: configure-goalert-operator
ReplicationController:
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-1
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-1
Secret:
- namespace: openshift-authentication
  name: v4-0-config-user-idp-0-file-data
- namespace: openshift-authentication
  name: v4-0-config-user-template-error
- namespace: openshift-authentication
  name: v4-0-config-user-template-login
- namespace: openshift-authentication
  name: v4-0-config-user-template-provider-selection
- namespace: openshift-config
  name: htpasswd-secret
- namespace: openshift-config
  name: osd-oauth-templates-errors
- namespace: openshift-config
  name: osd-oauth-templates-login
- namespace: openshift-config
  name: osd-oauth-templates-providers
- namespace: openshift-config
  name: rosa-oauth-templates-errors
- namespace: openshift-config
  name: rosa-oauth-templates-login
- namespace: openshift-config
  name: rosa-oauth-templates-providers
- namespace: openshift-config
  name: support
```

```
- namespace: openshift-config
  name: tony-devlab-primary-cert-bundle-secret
- namespace: openshift-ingress
  name: tony-devlab-primary-cert-bundle-secret
- namespace: openshift-kube-apiserver
  name: user-serving-cert-000
- namespace: openshift-kube-apiserver
  name: user-serving-cert-001
- namespace: openshift-monitoring
  name: dms-secret
- namespace: openshift-monitoring
  name: observatorium-credentials
- namespace: openshift-monitoring
  name: pd-secret
- namespace: openshift-scanning
  name: clam-secrets
- namespace: openshift-scanning
  name: logger-secrets
- namespace: openshift-security
  name: splunk-auth
ServiceAccount:
- namespace: openshift-backplane-managed-scripts
  name: osd-backplane
- namespace: openshift-backplane-srep
  name: 6804d07fb268b8285b023bcf65392f0e
- namespace: openshift-backplane-srep
  name: osd-delete-ownerrefs-serviceaccounts
- namespace: openshift-backplane
  name: osd-delete-backplane-serviceaccounts
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-machine-api
  name: osd-disable-cpms
- namespace: openshift-marketplace
  name: osd-patch-subscription-source
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-monitoring
  name: osd-cluster-ready
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-network-diagnostics
  name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-rbac-permissions
```

```
    name: rbac-permissions-operator
  - namespace: openshift-splunk-forwarder-operator
    name: splunk-forwarder-operator
  - namespace: openshift-sre-pruning
    name: bz1980755
  - namespace: openshift-scanning
    name: logger-sa
  - namespace: openshift-scanning
    name: scanner-sa
  - namespace: openshift-sre-pruning
    name: sre-pruner-sa
  - namespace: openshift-suricata
    name: ids-test
  - namespace: openshift-suricata
    name: suricata-sa
  - namespace: openshift-validation-webhook
    name: validation-webhook
  - namespace: openshift-velero
    name: managed-velero-operator
  - namespace: openshift-velero
    name: velero
  - namespace: openshift-backplane-srep
    name: UNIQUE_BACKPLANE_SERVICEACCOUNT_ID
Service:
  - namespace: openshift-deployment-validation-operator
    name: deployment-validation-operator-metrics
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols
  - namespace: openshift-scanning
    name: loggerservice
  - namespace: openshift-security
    name: audit-exporter
  - namespace: openshift-validation-webhook
    name: validation-webhook
AddonOperator:
  - name: addon-operator
ValidatingWebhookConfiguration:
  - name: sre-hiveownership-validation
  - name: sre-namespace-validation
  - name: sre-pod-validation
  - name: sre-prometheusrule-validation
  - name: sre-regular-user-validation
  - name: sre-scc-validation
  - name: sre-techpreviewnoupgrade-validation
DaemonSet:
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter
  - namespace: openshift-scanning
    name: logger
  - namespace: openshift-scanning
    name: scanner
  - namespace: openshift-security
```

```
  name: audit-exporter
- namespace: openshift-suricata
  name: suricata
- namespace: openshift-validation-webhook
  name: validation-webhook
DeploymentConfig:
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
ClusterRoleBinding:
- name: aqua-scanner-binding
- name: backplane-cluster-admin
- name: backplane-impersonate-cluster-admin
- name: bz1980755
- name: configure-alertmanager-operator-prom
- name: dedicated-admins-cluster
- name: dedicated-admins-registry-cas-cluster
- name: logger-clusterrolebinding
- name: openshift-backplane-managed-scripts-reader
- name: osd-cluster-admin
- name: osd-cluster-ready
- name: osd-delete-backplane-script-resources
- name: osd-delete-ownerrefs-serviceaccounts
- name: osd-patch-subscription-source
- name: osd-rebalance-infra-nodes
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: splunk-forwarder-operator-clusterrolebinding
- name: sre-pod-network-connectivity-check-pruner
- name: sre-pruner-buildsdeploys-pruning
- name: velero
- name: webhook-validation
ClusterRole:
- name: backplane-cee-readers-cluster
- name: backplane-impersonate-cluster-admin
- name: backplane-readers-cluster
- name: backplane-srep-admins-cluster
- name: backplane-srep-admins-project
- name: bz1980755
- name: dedicated-admins-aggregate-cluster
- name: dedicated-admins-aggregate-project
- name: dedicated-admins-cluster
- name: dedicated-admins-manage-operators
- name: dedicated-admins-project
- name: dedicated-admins-registry-cas-cluster
- name: dedicated-readers
- name: image-scanner
- name: logger-clusterrole
- name: openshift-backplane-managed-scripts-reader
- name: openshift-splunk-forwarder-operator
- name: osd-cluster-ready
- name: osd-custom-domains-dedicated-admin-cluster
- name: osd-delete-backplane-script-resources
- name: osd-delete-backplane-serviceaccounts
- name: osd-delete-ownerrefs-serviceaccounts
```

```
- name: osd-get-namespace
- name: osd-netnamespaces-dedicated-admin-cluster
- name: osd-patch-subscription-source
- name: osd-readers-aggregate
- name: osd-rebalance-infra-nodes
- name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- name: pcap-dedicated-admins
- name: splunk-forwarder-operator
- name: sre-allow-read-machine-info
- name: sre-pruner-buildsdeploys-cr
- name: webhook-validation-cr
RoleBinding:
- namespace: kube-system
  name: cloud-ingress-operator-cluster-config-v1-reader
- namespace: kube-system
  name: managed-velero-operator-cluster-config-v1-reader
- namespace: openshift-aqua
  name: dedicated-admins-openshift-aqua
- namespace: openshift-backplane-managed-scripts
  name: backplane-cee-mustgather
- namespace: openshift-backplane-managed-scripts
  name: backplane-srep-mustgather
- namespace: openshift-backplane-managed-scripts
  name: osd-delete-backplane-script-resources
- namespace: openshift-cloud-ingress-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-codeready-workspaces
  name: dedicated-admins-openshift-codeready-workspaces
- namespace: openshift-config
  name: dedicated-admins-project-request
- namespace: openshift-config
  name: dedicated-admins-registry-cas-project
- namespace: openshift-config
  name: muo-pullsecret-reader
- namespace: openshift-config
  name: oao-openshiftconfig-reader
- namespace: openshift-config
  name: osd-cluster-ready
- namespace: openshift-custom-domains-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-customer-monitoring
  name: dedicated-admins-openshift-customer-monitoring
- namespace: openshift-customer-monitoring
  name: prometheus-k8s-openshift-customer-monitoring
- namespace: openshift-dns
  name: dedicated-admins-openshift-dns
- namespace: openshift-dns
  name: osd-rebalance-infra-nodes-openshift-dns
- namespace: openshift-image-registry
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-ingress
  name: cloud-ingress-operator
- namespace: openshift-kube-apiserver
  name: cloud-ingress-operator
```

```
- namespace: openshift-machine-api
  name: cloud-ingress-operator
- namespace: openshift-logging
  name: admin-dedicated-admins
- namespace: openshift-logging
  name: admin-system:serviceaccounts:dedicated-admin
- namespace: openshift-logging
  name: openshift-logging-dedicated-admins
- namespace: openshift-logging
  name: openshift-logging:serviceaccounts:dedicated-admin
- namespace: openshift-machine-api
  name: osd-cluster-ready
- namespace: openshift-machine-api
  name: sre-ebs-iops-reporter-read-machine-info
- namespace: openshift-machine-api
  name: sre-stuck-ebs-vols-read-machine-info
- namespace: openshift-managed-node-metadata-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-machine-api
  name: osd-disable-cpms
- namespace: openshift-marketplace
  name: dedicated-admins-openshift-marketplace
- namespace: openshift-monitoring
  name: backplane-cee
- namespace: openshift-monitoring
  name: muo-monitoring-reader
- namespace: openshift-monitoring
  name: oao-monitoring-manager
- namespace: openshift-monitoring
  name: osd-cluster-ready
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes-openshift-monitoring
- namespace: openshift-monitoring
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
- namespace: openshift-must-gather-operator
  name: backplane-cee-mustgather
- namespace: openshift-must-gather-operator
  name: backplane-srep-mustgather
- namespace: openshift-must-gather-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-network-diagnostics
  name: sre-pod-network-connectivity-check-pruner
- namespace: openshift-network-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-ocm-agent-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-operators-redhat
  name: admin-dedicated-admins
- namespace: openshift-operators-redhat
  name: admin-system:serviceaccounts:dedicated-admin
```

```
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat-dedicated-admins
- namespace: openshift-operators-redhat
  name: openshift-operators-redhat:serviceaccounts:dedicated-admin
- namespace: openshift-operators
  name: dedicated-admins-openshift-operators
- namespace: openshift-osd-metrics
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-osd-metrics
  name: prometheus-k8s
- namespace: openshift-rbac-permissions
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-rbac-permissions
  name: prometheus-k8s
- namespace: openshift-route-monitor-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-scanning
  name: scanner-rolebinding
- namespace: openshift-security
  name: osd-rebalance-infra-nodes-openshift-security
- namespace: openshift-security
  name: prometheus-k8s
- namespace: openshift-splunk-forwarder-operator
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-suricata
  name: suricata-rolebinding
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-config-create
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-config-edit
- namespace: openshift-user-workload-monitoring
  name: dedicated-admins-uwm-managed-am-secret
- namespace: openshift-user-workload-monitoring
  name: osd-rebalance-infra-nodes-openshift-user-workload-monitoring
- namespace: openshift-velero
  name: osd-rebalance-infra-nodes-openshift-pod-rebalance
- namespace: openshift-velero
  name: prometheus-k8s
Role:
- namespace: kube-system
  name: cluster-config-v1-reader
- namespace: kube-system
  name: cluster-config-v1-reader-cio
- namespace: openshift-aqua
  name: dedicated-admins-openshift-aqua
- namespace: openshift-backplane-managed-scripts
  name: backplane-cee-pcap-collector
- namespace: openshift-backplane-managed-scripts
  name: backplane-srep-pcap-collector
- namespace: openshift-backplane-managed-scripts
  name: osd-delete-backplane-script-resources
- namespace: openshift-codeready-workspaces
  name: dedicated-admins-openshift-codeready-workspaces
- namespace: openshift-config
  name: dedicated-admins-project-request
- namespace: openshift-config
```

```
    name: dedicated-admins-registry-cas-project
  - namespace: openshift-config
    name: muo-pullsecret-reader
  - namespace: openshift-config
    name: oao-openshiftconfig-reader
  - namespace: openshift-config
    name: osd-cluster-ready
  - namespace: openshift-customer-monitoring
    name: dedicated-admins-openshift-customer-monitoring
  - namespace: openshift-customer-monitoring
    name: prometheus-k8s-openshift-customer-monitoring
  - namespace: openshift-dns
    name: dedicated-admins-openshift-dns
  - namespace: openshift-dns
    name: osd-rebalance-infra-nodes-openshift-dns
  - namespace: openshift-ingress-operator
    name: cloud-ingress-operator
  - namespace: openshift-ingress
    name: cloud-ingress-operator
  - namespace: openshift-kube-apiserver
    name: cloud-ingress-operator
  - namespace: openshift-machine-api
    name: cloud-ingress-operator
  - namespace: openshift-logging
    name: dedicated-admins-openshift-logging
  - namespace: openshift-machine-api
    name: osd-cluster-ready
  - namespace: openshift-machine-api
    name: osd-disable-cpms
  - namespace: openshift-marketplace
    name: dedicated-admins-openshift-marketplace
  - namespace: openshift-monitoring
    name: backplane-cee
  - namespace: openshift-monitoring
    name: muo-monitoring-reader
  - namespace: openshift-monitoring
    name: oao-monitoring-manager
  - namespace: openshift-monitoring
    name: osd-cluster-ready
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes-openshift-monitoring
  - namespace: openshift-must-gather-operator
    name: backplane-cee-mustgather
  - namespace: openshift-must-gather-operator
    name: backplane-srep-mustgather
  - namespace: openshift-network-diagnostics
    name: sre-pod-network-connectivity-check-pruner
  - namespace: openshift-operators
    name: dedicated-admins-openshift-operators
  - namespace: openshift-osd-metrics
    name: prometheus-k8s
  - namespace: openshift-rbac-permissions
    name: prometheus-k8s
  - namespace: openshift-scanning
    name: scanner-role
  - namespace: openshift-security
```

```
    name: osd-rebalance-infra-nodes-openshift-security
  - namespace: openshift-security
    name: prometheus-k8s
  - namespace: openshift-suricata
    name: suricata-role
  - namespace: openshift-user-workload-monitoring
    name: dedicated-admins-user-workload-monitoring-create-cm
  - namespace: openshift-user-workload-monitoring
    name: dedicated-admins-user-workload-monitoring-manage-am-secret
  - namespace: openshift-user-workload-monitoring
    name: osd-rebalance-infra-nodes-openshift-user-workload-monitoring
  - namespace: openshift-velero
    name: prometheus-k8s
CronJob:
  - namespace: openshift-backplane-managed-scripts
    name: osd-delete-backplane-script-resources
  - namespace: openshift-backplane-srep
    name: osd-delete-ownerrefs-serviceaccounts
  - namespace: openshift-backplane
    name: osd-delete-backplane-serviceaccounts
  - namespace: openshift-machine-api
    name: osd-disable-cpms
  - namespace: openshift-marketplace
    name: osd-patch-subscription-source
  - namespace: openshift-monitoring
    name: osd-rebalance-infra-nodes
  - namespace: openshift-network-diagnostics
    name: sre-pod-network-connectivity-check-pruner
  - namespace: openshift-sre-pruning
    name: builds-pruner
  - namespace: openshift-sre-pruning
    name: bz1980755
  - namespace: openshift-sre-pruning
    name: deployments-pruner
  - namespace: openshift-suricata
    name: ids-tester
Job:
  - namespace: openshift-monitoring
    name: osd-cluster-ready
CredentialsRequest:
  - namespace: openshift-cloud-ingress-operator
    name: cloud-ingress-operator-credentials-aws
  - namespace: openshift-cloud-ingress-operator
    name: cloud-ingress-operator-credentials-gcp
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter-aws-credentials
  - namespace: openshift-monitoring
    name: sre-stuck-ebs-vols-aws-credentials
  - namespace: openshift-velero
    name: managed-velero-operator-iam-credentials-aws
  - namespace: openshift-velero
    name: managed-velero-operator-iam-credentials-gcp
APIScheme:
  - namespace: openshift-cloud-ingress-operator
    name: rh-api
PublishingStrategy:
```

```
- namespace: openshift-cloud-ingress-operator
  name: publishingstrategy
ScanSettingBinding:
- namespace: openshift-compliance
  name: fedramp-high-ocp
- namespace: openshift-compliance
  name: fedramp-high-rhcos
ScanSetting:
- namespace: openshift-compliance
  name: osd
TailoredProfile:
- namespace: openshift-compliance
  name: rhcos4-high-rosa
OAuth:
- name: cluster
EndpointSlice:
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-metrics-rhtwg
- namespace: openshift-monitoring
  name: sre-dns-latency-exporter-4cw9r
- namespace: openshift-monitoring
  name: sre-ebs-iops-reporter-6tx5g
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols-gmdhs
- namespace: openshift-scanning
  name: loggerservice-zprbq
- namespace: openshift-security
  name: audit-exporter-nqfdk
- namespace: openshift-validation-webhook
  name: validation-webhook-97b8t
FileIntegrity:
- namespace: openshift-file-integrity
  name: osd-fileintegrity
MachineHealthCheck:
- namespace: openshift-machine-api
  name: srep-infra-healthcheck
- namespace: openshift-machine-api
  name: srep-metal-worker-healthcheck
- namespace: openshift-machine-api
  name: srep-worker-healthcheck
MachineSet:
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-infra-us-east-1a
- namespace: openshift-machine-api
  name: sbasabat-mc-qhqkn-worker-us-east-1a
ContainerRuntimeConfig:
- name: custom-crio
KubeletConfig:
- name: custom-kubelet
MachineConfig:
- name: 00-master-chrony
- name: 00-worker-chrony
SubjectPermission:
- namespace: openshift-rbac-permissions
  name: backplane-cee
- namespace: openshift-rbac-permissions
```

```
    name: backplane-csa
  - namespace: openshift-rbac-permissions
    name: backplane-cse
  - namespace: openshift-rbac-permissions
    name: backplane-csm
  - namespace: openshift-rbac-permissions
    name: backplane-mobb
  - namespace: openshift-rbac-permissions
    name: backplane-srep
  - namespace: openshift-rbac-permissions
    name: backplane-tam
  - namespace: openshift-rbac-permissions
    name: dedicated-admin-serviceaccounts
  - namespace: openshift-rbac-permissions
    name: dedicated-admin-serviceaccounts-core-ns
  - namespace: openshift-rbac-permissions
    name: dedicated-admins
  - namespace: openshift-rbac-permissions
    name: dedicated-admins-alert-routing-edit
  - namespace: openshift-rbac-permissions
    name: dedicated-admins-core-ns
  - namespace: openshift-rbac-permissions
    name: dedicated-admins-customer-monitoring
  - namespace: openshift-rbac-permissions
    name: osd-delete-backplane-serviceaccounts
VeleroInstall:
  - namespace: openshift-velero
    name: cluster
PrometheusRule:
  - namespace: openshift-monitoring
    name: rhmi-sre-cluster-admins
  - namespace: openshift-monitoring
    name: rhoam-sre-cluster-admins
  - namespace: openshift-monitoring
    name: sre-alertmanager-silences-active
  - namespace: openshift-monitoring
    name: sre-alerts-stuck-builds
  - namespace: openshift-monitoring
    name: sre-alerts-stuck-volumes
  - namespace: openshift-monitoring
    name: sre-cloud-ingress-operator-offline-alerts
  - namespace: openshift-monitoring
    name: sre-avo-pendingacceptance
  - namespace: openshift-monitoring
    name: sre-configure-alertmanager-operator-offline-alerts
  - namespace: openshift-monitoring
    name: sre-control-plane-resizing-alerts
  - namespace: openshift-monitoring
    name: sre-dns-alerts
  - namespace: openshift-monitoring
    name: sre-ebs-iops-burstbalance
  - namespace: openshift-monitoring
    name: sre-elasticsearch-jobs
  - namespace: openshift-monitoring
    name: sre-elasticsearch-managed-notification-alerts
  - namespace: openshift-monitoring
```

```
    name: sre-excessive-memory
  - namespace: openshift-monitoring
    name: sre-fr-alerts-low-disk-space
  - namespace: openshift-monitoring
    name: sre-haproxy-reload-fail
  - namespace: openshift-monitoring
    name: sre-internal-slo-recording-rules
  - namespace: openshift-monitoring
    name: sre-kubequotaexceeded
  - namespace: openshift-monitoring
    name: sre-leader-election-master-status-alerts
  - namespace: openshift-monitoring
    name: sre-managed-kube-apiserver-missing-on-node
  - namespace: openshift-monitoring
    name: sre-managed-kube-controller-manager-missing-on-node
  - namespace: openshift-monitoring
    name: sre-managed-kube-scheduler-missing-on-node
  - namespace: openshift-monitoring
    name: sre-managed-node-metadata-operator-alerts
  - namespace: openshift-monitoring
    name: sre-managed-notification-alerts
  - namespace: openshift-monitoring
    name: sre-managed-upgrade-operator-alerts
  - namespace: openshift-monitoring
    name: sre-managed-velero-operator-alerts
  - namespace: openshift-monitoring
    name: sre-node-unschedulable
  - namespace: openshift-monitoring
    name: sre-oauth-server
  - namespace: openshift-monitoring
    name: sre-pending-csr-alert
  - namespace: openshift-monitoring
    name: sre-proxy-managed-notification-alerts
  - namespace: openshift-monitoring
    name: sre-pruning
  - namespace: openshift-monitoring
    name: sre-pv
  - namespace: openshift-monitoring
    name: sre-router-health
  - namespace: openshift-monitoring
    name: sre-runaway-sdn-preventing-container-creation
  - namespace: openshift-monitoring
    name: sre-slo-recording-rules
  - namespace: openshift-monitoring
    name: sre-telemeter-client
  - namespace: openshift-monitoring
    name: sre-telemetry-managed-labels-recording-rules
  - namespace: openshift-monitoring
    name: sre-upgrade-send-managed-notification-alerts
  - namespace: openshift-monitoring
    name: sre-uptime-sla
ServiceMonitor:
  - namespace: openshift-monitoring
    name: sre-dns-latency-exporter
  - namespace: openshift-monitoring
    name: sre-ebs-iops-reporter
```

```
- namespace: openshift-monitoring
  name: sre-stuck-ebs-vols
ClusterUrlMonitor:
- namespace: openshift-route-monitor-operator
  name: api
RouteMonitor:
- namespace: openshift-route-monitor-operator
  name: console
NetworkPolicy:
- namespace: openshift-deployment-validation-operator
  name: allow-from-openshift-insights
- namespace: openshift-deployment-validation-operator
  name: allow-from-openshift-olm
ManagedNotification:
- namespace: openshift-ocm-agent-operator
  name: sre-elasticsearch-managed-notifications
- namespace: openshift-ocm-agent-operator
  name: sre-managed-notifications
- namespace: openshift-ocm-agent-operator
  name: sre-proxy-managed-notifications
- namespace: openshift-ocm-agent-operator
  name: sre-upgrade-managed-notifications
OcmAgent:
- namespace: openshift-ocm-agent-operator
  name: ocmagent
- namespace: openshift-security
  name: audit-exporter
Console:
- name: cluster
CatalogSource:
- namespace: openshift-addon-operator
  name: addon-operator-catalog
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator-registry
- namespace: openshift-compliance
  name: compliance-operator-registry
- namespace: openshift-container-security
  name: container-security-operator-registry
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator-registry
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator-catalog
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator-registry
- namespace: openshift-file-integrity
  name: file-integrity-operator-registry
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator-catalog
- namespace: openshift-monitoring
  name: configure-alertmanager-operator-registry
- namespace: openshift-must-gather-operator
  name: must-gather-operator-registry
- namespace: openshift-observability-operator
  name: observability-operator-catalog
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator-registry
```

```
    - namespace: openshift-osd-metrics
      name: osd-metrics-exporter-registry
    - namespace: openshift-rbac-permissions
      name: rbac-permissions-operator-registry
    - namespace: openshift-route-monitor-operator
      name: route-monitor-operator-registry
    - namespace: openshift-splunk-forwarder-operator
      name: splunk-forwarder-operator-catalog
    - namespace: openshift-velero
      name: managed-velero-operator-registry
    OperatorGroup:
    - namespace: openshift-addon-operator
      name: addon-operator-og
    - namespace: openshift-aqua
      name: openshift-aqua
    - namespace: openshift-cloud-ingress-operator
      name: cloud-ingress-operator
    - namespace: openshift-codeready-workspaces
      name: openshift-codeready-workspaces
    - namespace: openshift-compliance
      name: compliance-operator
    - namespace: openshift-container-security
      name: container-security-operator
    - namespace: openshift-custom-domains-operator
      name: custom-domains-operator
    - namespace: openshift-customer-monitoring
      name: openshift-customer-monitoring
    - namespace: openshift-deployment-validation-operator
      name: deployment-validation-operator-og
    - namespace: openshift-managed-node-metadata-operator
      name: managed-node-metadata-operator
    - namespace: openshift-file-integrity
      name: file-integrity-operator
    - namespace: openshift-logging
      name: openshift-logging
    - namespace: openshift-managed-upgrade-operator
      name: managed-upgrade-operator-og
    - namespace: openshift-must-gather-operator
      name: must-gather-operator
    - namespace: openshift-observability-operator
      name: observability-operator-og
    - namespace: openshift-ocm-agent-operator
      name: ocm-agent-operator-og
    - namespace: openshift-osd-metrics
      name: osd-metrics-exporter
    - namespace: openshift-rbac-permissions
      name: rbac-permissions-operator
    - namespace: openshift-route-monitor-operator
      name: route-monitor-operator
    - namespace: openshift-splunk-forwarder-operator
      name: splunk-forwarder-operator-og
    - namespace: openshift-velero
      name: managed-velero-operator
    Subscription:
    - namespace: openshift-addon-operator
      name: addon-operator
```

```
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-compliance
  name: compliance-operator-sub
- namespace: openshift-container-security
  name: container-security-operator-sub
- namespace: openshift-custom-domains-operator
  name: custom-domains-operator
- namespace: openshift-deployment-validation-operator
  name: deployment-validation-operator
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-file-integrity
  name: file-integrity-operator-sub
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-must-gather-operator
  name: must-gather-operator
- namespace: openshift-observability-operator
  name: observability-operator
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-splunk-forwarder-operator
  name: openshift-splunk-forwarder-operator
- namespace: openshift-velero
  name: managed-velero-operator
PackageManifest:
- namespace: openshift-splunk-forwarder-operator
  name: splunk-forwarder-operator
- namespace: openshift-addon-operator
  name: addon-operator
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
- namespace: openshift-cloud-ingress-operator
  name: cloud-ingress-operator
- namespace: openshift-managed-node-metadata-operator
  name: managed-node-metadata-operator
- namespace: openshift-velero
  name: managed-velero-operator
- namespace: openshift-deployment-validation-operator
  name: managed-upgrade-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-container-security
  name: container-security-operator
- namespace: openshift-route-monitor-operator
  name: route-monitor-operator
- namespace: openshift-file-integrity
```

```
  name: file-integrity-operator
- namespace: openshift-custom-domains-operator
  name: managed-node-metadata-operator
- namespace: openshift-route-monitor-operator
  name: custom-domains-operator
- namespace: openshift-managed-upgrade-operator
  name: managed-upgrade-operator
- namespace: openshift-ocm-agent-operator
  name: ocm-agent-operator
- namespace: openshift-observability-operator
  name: observability-operator
- namespace: openshift-monitoring
  name: configure-alertmanager-operator
- namespace: openshift-must-gather-operator
  name: deployment-validation-operator
- namespace: openshift-osd-metrics
  name: osd-metrics-exporter
- namespace: openshift-compliance
  name: compliance-operator
- namespace: openshift-rbac-permissions
  name: rbac-permissions-operator
Status:
- {}
Project:
- name: dedicated-admin
- name: openshift-addon-operator
- name: openshift-aqua
- name: openshift-backplane
- name: openshift-backplane-cee
- name: openshift-backplane-csa
- name: openshift-backplane-cse
- name: openshift-backplane-csm
- name: openshift-backplane-managed-scripts
- name: openshift-backplane-mobb
- name: openshift-backplane-srep
- name: openshift-backplane-tam
- name: openshift-cloud-ingress-operator
- name: openshift-codeready-workspaces
- name: openshift-compliance
- name: openshift-container-security
- name: openshift-custom-domains-operator
- name: openshift-customer-monitoring
- name: openshift-deployment-validation-operator
- name: openshift-managed-node-metadata-operator
- name: openshift-file-integrity
- name: openshift-logging
- name: openshift-managed-upgrade-operator
- name: openshift-must-gather-operator
- name: openshift-observability-operator
- name: openshift-ocm-agent-operator
- name: openshift-operators-redhat
- name: openshift-osd-metrics
- name: openshift-rbac-permissions
- name: openshift-route-monitor-operator
- name: openshift-scanning
- name: openshift-security
```

```
- name: openshift-splunk-forwarder-operator
- name: openshift-sre-pruning
- name: openshift-suricata
- name: openshift-validation-webhook
- name: openshift-velero
ClusterResourceQuota:
- name: loadbalancer-quota
- name: persistent-volume-quota
SecurityContextConstraints:
- name: osd-scanning-scc
- name: osd-suricata-scc
- name: pcap-dedicated-admins
- name: splunkforwarder
SplunkForwarder:
- namespace: openshift-security
  name: splunkforwarder
Group:
- name: cluster-admins
- name: dedicated-admins
User:
- name: backplane-cluster-admin
Backup:
- namespace: openshift-velero
  name: daily-full-backup-20221123112305
- namespace: openshift-velero
  name: daily-full-backup-20221125042537
- namespace: openshift-velero
  name: daily-full-backup-20221126010038
- namespace: openshift-velero
  name: daily-full-backup-20221127010039
- namespace: openshift-velero
  name: daily-full-backup-20221128010040
- namespace: openshift-velero
  name: daily-full-backup-20221129050847
- namespace: openshift-velero
  name: hourly-object-backup-20221128051740
- namespace: openshift-velero
  name: hourly-object-backup-20221128061740
- namespace: openshift-velero
  name: hourly-object-backup-20221128071740
- namespace: openshift-velero
  name: hourly-object-backup-20221128081740
- namespace: openshift-velero
  name: hourly-object-backup-20221128091740
- namespace: openshift-velero
  name: hourly-object-backup-20221129050852
- namespace: openshift-velero
  name: hourly-object-backup-20221129051747
- namespace: openshift-velero
  name: weekly-full-backup-20221116184315
- namespace: openshift-velero
  name: weekly-full-backup-20221121033854
- namespace: openshift-velero
  name: weekly-full-backup-20221128020040
Schedule:
- namespace: openshift-velero
```

```
    name: daily-full-backup
  - namespace: openshift-velero
    name: hourly-object-backup
  - namespace: openshift-velero
    name: weekly-full-backup
```

7.7.3. OpenShift Dedicated コア namespace

OpenShift Dedicated コア namespace は、クラスターのインストール時にデフォルトでインストールされます。

例7.2 コア namespace のリスト

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: ocp-namespaces
  namespace: openshift-monitoring
data:
  managed_namespaces.yaml: |
    Resources:
      Namespace:
      - name: kube-system
      - name: openshift-apiserver
      - name: openshift-apiserver-operator
      - name: openshift-authentication
      - name: openshift-authentication-operator
      - name: openshift-cloud-controller-manager
      - name: openshift-cloud-controller-manager-operator
      - name: openshift-cloud-credential-operator
      - name: openshift-cloud-network-config-controller
      - name: openshift-cluster-api
      - name: openshift-cluster-csi-drivers
      - name: openshift-cluster-machine-approver
      - name: openshift-cluster-node-tuning-operator
      - name: openshift-cluster-samples-operator
      - name: openshift-cluster-storage-operator
      - name: openshift-config
      - name: openshift-config-managed
      - name: openshift-config-operator
      - name: openshift-console
      - name: openshift-console-operator
      - name: openshift-console-user-settings
      - name: openshift-controller-manager
      - name: openshift-controller-manager-operator
      - name: openshift-dns
      - name: openshift-dns-operator
      - name: openshift-etcd
      - name: openshift-etcd-operator
      - name: openshift-host-network
      - name: openshift-image-registry
      - name: openshift-ingress
      - name: openshift-ingress-canary
      - name: openshift-ingress-operator
```

```
    - name: openshift-insights
    - name: openshift-kni-infra
    - name: openshift-kube-apiserver
    - name: openshift-kube-apiserver-operator
    - name: openshift-kube-controller-manager
    - name: openshift-kube-controller-manager-operator
    - name: openshift-kube-scheduler
    - name: openshift-kube-scheduler-operator
    - name: openshift-kube-storage-version-migrator
    - name: openshift-kube-storage-version-migrator-operator
    - name: openshift-machine-api
    - name: openshift-machine-config-operator
    - name: openshift-marketplace
    - name: openshift-monitoring
    - name: openshift-multus
    - name: openshift-network-diagnostics
    - name: openshift-network-operator
    - name: openshift-nutanix-infra
    - name: openshift-oauth-apiserver
    - name: openshift-openstack-infra
    - name: openshift-operator-lifecycle-manager
    - name: openshift-operators
    - name: openshift-ovirt-infra
    - name: openshift-sdn
    - name: openshift-ovn-kubernetes
    - name: openshift-platform-operators
    - name: openshift-route-controller-manager
    - name: openshift-service-ca
    - name: openshift-service-ca-operator
    - name: openshift-user-workload-monitoring
    - name: openshift-vsphere-infra
```

7.7.4. OpenShift Dedicated アドオン namespace

OpenShift Dedicated アドオンは、クラスターのインストール後にインストールできます。これらの追加サービスには、Red Hat OpenShift Dev Spaces、Red Hat OpenShift API Management、および Cluster Logging Operator が含まれます。以下の namespace 内のリソースへの変更は、アップグレード時にアドオンによってオーバーライドされる可能性があります。これにより、アドオン機能でサポートされていない設定が生じる可能性があります。

例7.3 アドオンマネージドの namespace のリスト

```
addon-namespaces:
  ocs-converged-dev: openshift-storage
  managed-api-service-internal: redhat-rhoami-operator
  codeready-workspaces-operator: codeready-workspaces-operator
  managed-odh: redhat-ods-operator
  codeready-workspaces-operator-qe: codeready-workspaces-operator-qe
  integreatly-operator: redhat-rhmi-operator
  nvidia-gpu-addon: redhat-nvidia-gpu-addon
  integreatly-operator-internal: redhat-rhmi-operator
  rhoams: redhat-rhoam-operator
  ocs-converged: openshift-storage
  addon-operator: redhat-addon-operator
```

```
prow-operator: prow
cluster-logging-operator: openshift-logging
advanced-cluster-management: redhat-open-cluster-management
cert-manager-operator: redhat-cert-manager-operator
dba-operator: addon-dba-operator
reference-addon: redhat-reference-addon
ocm-addon-test-operator: redhat-ocm-addon-test-operator
```

7.7.5. OpenShift Dedicated 検証用 Webhook

OpenShift Dedicated 検証 Webhook は、OpenShift SRE チームによって維持される動的受付制御のセットです。これらの HTTP コールバック (Webhook とも呼ばれる) は、さまざまなタイプの要求に対して呼び出され、クラスターの安定性を確保します。以下のリストは、登録された操作および制御されるリソースが含まれるルールが含まれる各種 Webhook を説明しています。これらの検証用 Webhook を回避しようとすると、クラスターの安定性およびサポート性に影響が出る可能性があります。

例7.4 検証用 Webhook のリスト

```
[
  {
    "webhookName": "clusterlogging-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          "logging.openshift.io"
        ],
        "apiVersions": [
          "v1"
        ],
        "resources": [
          "clusterloggings"
        ],
        "scope": "Namespaced"
      }
    ],
    "documentString": "Managed OpenShift Customers may set log retention outside the allowed range of 0-7 days"
  },
  {
    "webhookName": "clusterrolebindings-validation",
    "rules": [
      {
        "operations": [
          "DELETE"
        ],
        "apiGroups": [
          "rbac.authorization.k8s.io"
        ],
        "apiVersions": [
          "v1"
```

```
        ],
        "resources": [
          "clusterrolebindings"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift Customers may not delete the cluster role bindings
under the managed namespaces: (^openshift-.*|kube-system)"
  },
  {
    "webhookName": "customresourcedefinitions-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          "apiextensions.k8s.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "customresourcedefinitions"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift Customers may not change
CustomResourceDefinitions managed by Red Hat."
  },
  {
    "webhookName": "hiveownership-validation",
    "rules": [
      {
        "operations": [
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          "quota.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "clusterresourcequotas"
        ],
        "scope": "Cluster"
      }
    ],
    "webhookObjectSelector": {
      "matchLabels": {
```

```
        "hive.openshift.io/managed": "true"
      }
    },
    "documentString": "Managed OpenShift customers may not edit certain managed resources. A managed resource has a \"hive.openshift.io/managed\": \"true\" label."
  },
  {
    "webhookName": "imagecontentpolicies-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          "config.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "imagedigestmirrorsets",
          "imagetagmirrorsets"
        ],
        "scope": "Cluster"
      },
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          "operator.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "imagecontentsourcepolicies"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift customers may not create ImageContentSourcePolicy, ImageDigestMirrorSet, or ImageTagMirrorSet resources that configure mirrors that would conflict with system registries (e.g. quay.io, registry.redhat.io, registry.access.redhat.com, etc). For more details, see https://docs.openshift.com/"
  },
  {
    "webhookName": "ingress-config-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
```

```
        ],
        "apiGroups": [
          "config.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "ingresses"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift customers may not modify ingress config resources
because it can can degrade cluster operators and can interfere with OpenShift SRE monitoring."
  },
  {
    "webhookName": "ingresscontroller-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          "operator.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "ingresscontroller",
          "ingresscontrollers"
        ],
        "scope": "Namespaced"
      }
    ],
    "documentString": "Managed OpenShift Customer may create IngressControllers without
necessary taints. This can cause those workloads to be provisioned on infra or master nodes."
  },
  {
    "webhookName": "namespace-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          ""
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
```

```
          "namespaces"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift Customers may not modify namespaces specified in the [openshift-monitoring/managed-namespaces openshift-monitoring/ocp-namespaces] ConfigMaps because customer workloads should be placed in customer-created namespaces. Customers may not create namespaces identified by this regular expression (^com$|^io$|^in$) because it could interfere with critical DNS resolution. Additionally, customers may not set or change the values of these Namespace labels [managed.openshift.io/storage-pv-quota-exempt managed.openshift.io/service-lb-quota-exempt]."
  },
  {
    "webhookName": "networkpolicies-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          "networking.k8s.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "networkpolicies"
        ],
        "scope": "Namespaced"
      }
    ],
    "documentString": "Managed OpenShift Customers may not create NetworkPolicies in namespaces managed by Red Hat."
  },
  {
    "webhookName": "node-validation-osd",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          ""
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "nodes",
          "nodes/*"
        ],
```

```
      "scope": "*"
    }
   ],
   "documentString": "Managed OpenShift customers may not alter Node objects."
  },
  {
   "webhookName": "pod-validation",
   "rules": [
    {
     "operations": [
      "*"
     ],
     "apiGroups": [
      "v1"
     ],
     "apiVersions": [
      "*"
     ],
     "resources": [
      "pods"
     ],
     "scope": "Namespaced"
    }
   ],
   "documentString": "Managed OpenShift Customers may use tolerations on Pods that could
cause those Pods to be scheduled on infra or master nodes."
  },
  {
   "webhookName": "prometheusrule-validation",
   "rules": [
    {
     "operations": [
      "CREATE",
      "UPDATE",
      "DELETE"
     ],
     "apiGroups": [
      "monitoring.coreos.com"
     ],
     "apiVersions": [
      "*"
     ],
     "resources": [
      "prometheusrules"
     ],
     "scope": "Namespaced"
    }
   ],
   "documentString": "Managed OpenShift Customers may not create PrometheusRule in
namespaces managed by Red Hat."
  },
  {
   "webhookName": "regular-user-validation",
   "rules": [
    {
     "operations": [
```

```
        "*"
      ],
      "apiGroups": [
        "cloudcredential.openshift.io",
        "machine.openshift.io",
        "admissionregistration.k8s.io",
        "addons.managed.openshift.io",
        "cloudingress.managed.openshift.io",
        "managed.openshift.io",
        "ocmagent.managed.openshift.io",
        "splunkforwarder.managed.openshift.io",
        "upgrade.managed.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "*/*"
      ],
      "scope": "*"
    },
    {
      "operations": [
        "*"
      ],
      "apiGroups": [
        "autoscaling.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "clusterautoscalers",
        "machineautoscalers"
      ],
      "scope": "*"
    },
    {
      "operations": [
        "*"
      ],
      "apiGroups": [
        "config.openshift.io"
      ],
      "apiVersions": [
        "*"
      ],
      "resources": [
        "clusterversions",
        "clusterversions/status",
        "schedulers",
        "apiservers",
        "proxies"
      ],
      "scope": "*"
    },
```

```
{
  "operations": [
    "CREATE",
    "UPDATE",
    "DELETE"
  ],
  "apiGroups": [
    ""
  ],
  "apiVersions": [
    "*"
  ],
  "resources": [
    "configmaps"
  ],
  "scope": "*"
},
{
  "operations": [
    "*"
  ],
  "apiGroups": [
    "machineconfiguration.openshift.io"
  ],
  "apiVersions": [
    "*"
  ],
  "resources": [
    "machineconfigs",
    "machineconfigpools"
  ],
  "scope": "*"
},
{
  "operations": [
    "*"
  ],
  "apiGroups": [
    "operator.openshift.io"
  ],
  "apiVersions": [
    "*"
  ],
  "resources": [
    "kubeapiservers",
    "openshiftapiservers"
  ],
  "scope": "*"
},
{
  "operations": [
    "*"
  ],
  "apiGroups": [
    "managed.openshift.io"
  ],
```

```
        "apiVersions": [
          "*"
        ],
        "resources": [
          "subjectpermissions",
          "subjectpermissions/*"
        ],
        "scope": "*"
      },
      {
        "operations": [
          "*"
        ],
        "apiGroups": [
          "network.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "netnamespaces",
          "netnamespaces/*"
        ],
        "scope": "*"
      }
    ],
    "documentString": "Managed OpenShift customers may not manage any objects in the
following APIGroups [autoscaling.openshift.io network.openshift.io machine.openshift.io
admissionregistration.k8s.io addons.managed.openshift.io cloudingress.managed.openshift.io
splunkforwarder.managed.openshift.io upgrade.managed.openshift.io managed.openshift.io
ocmagent.managed.openshift.io config.openshift.io machineconfiguration.openshift.io
operator.openshift.io cloudcredential.openshift.io], nor may Managed OpenShift customers alter
the APIServer, KubeAPIServer, OpenShiftAPIServer, ClusterVersion, Proxy or SubjectPermission
objects."
  },
  {
    "webhookName": "scc-validation",
    "rules": [
      {
        "operations": [
          "UPDATE",
          "DELETE"
        ],
        "apiGroups": [
          "security.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "securitycontextconstraints"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift Customers may not modify the following default SCCs:
```

```
[anyuid hostaccess hostmount-anyuid hostnetwork hostnetwork-v2 node-exporter nonroot
nonroot-v2 privileged restricted restricted-v2]"
  },
  {
    "webhookName": "sdn-migration-validation",
    "rules": [
      {
        "operations": [
          "UPDATE"
        ],
        "apiGroups": [
          "config.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "networks"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift customers may not modify the network config type
because it can can degrade cluster operators and can interfere with OpenShift SRE monitoring."
  },
  {
    "webhookName": "service-mutation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          ""
        ],
        "apiVersions": [
          "v1"
        ],
        "resources": [
          "services"
        ],
        "scope": "Namespaced"
      }
    ],
    "documentString": "LoadBalancer-type services on Managed OpenShift clusters must contain
an additional annotation for managed policy compliance."
  },
  {
    "webhookName": "serviceaccount-validation",
    "rules": [
      {
        "operations": [
          "DELETE"
        ],
        "apiGroups": [
```

```
          ""
        ],
        "apiVersions": [
          "v1"
        ],
        "resources": [
          "serviceaccounts"
        ],
        "scope": "Namespaced"
      }
    ],
    "documentString": "Managed OpenShift Customers may not delete the service accounts under the managed namespaces。"
  },
  {
    "webhookName": "techpreviewnoupgrade-validation",
    "rules": [
      {
        "operations": [
          "CREATE",
          "UPDATE"
        ],
        "apiGroups": [
          "config.openshift.io"
        ],
        "apiVersions": [
          "*"
        ],
        "resources": [
          "featuregates"
        ],
        "scope": "Cluster"
      }
    ],
    "documentString": "Managed OpenShift Customers may not use TechPreviewNoUpgrade FeatureGate that could prevent any future ability to do a y-stream upgrade to their clusters."
  }
]
```