OpenShift Dedicated 4

サポート

OpenShift Dedicated 4 のサポート

Last Updated: 2021-10-17

OpenShift Dedicated 4 サポート

OpenShift Dedicated 4 のサポート

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

法律上の通知

概要

本書では、OpenShfit Dedicated のサポートを取得する方法について詳しく説明します。

目次

第1章 サポート **3**
1.1. サポート 3
1.2. RED HAT ナレッジベースについて 3
1.3. RED HAT ナレッジベースの検索 3
1.4. サポートケースの送信 4
1.5. 関連情報 5

第2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 **6**
2.1. リモートヘルスモニタリングについて 6
2.1.1. Telemetry について 6
2.1.1.1. Telemetry で収集される情報 7
2.1.2. Insights Operator について 8
2.1.2.1. Insights Operator によって収集される情報 8
2.1.3. Telemetry および Insights Operator データフローについて 9
2.1.4. 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 9
2.2. 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 10
2.2.1. Telemetry によって収集されるデータの表示 10
2.2.2. Insights Operator によって収集されるデータの表示 11
2.3. リモートヘルスレポートのオプトアウト 11
2.4. INSIGHTS を使用したクラスターの問題の特定 11
2.4.1. クラスターの潜在的な問題の表示 11
2.4.2. Web コンソールでの Insights ステータスの表示 12

第3章 クラスターに関するデータの収集 **13**
3.1. MUST-GATHER ツールについて 13
3.2. RED HAT サポート用のクラスターについてのデータの収集 13
3.3. 特定の機能に関するデータ収集 14
3.4. クラスター ID の取得 18
3.5. SOSREPORT について 19
3.6. OPENSHIFT CONTAINER PLATFORM クラスターノードの SOSREPORT アーカイブの生成 19
3.7. ブートストラップノードのジャーナルログのクエリー 21
3.8. クラスターノードジャーナルログのクエリー 22
3.9. OPENSHIFT CONTAINER PLATFORM 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 23
3.10. RED HAT サポートへの診断データの提供 26
3.11. TOOLBOX について 28
toolbox コンテナーへのパッケージのインストール 28
toolbox を使用した代替イメージの起動 29

第4章 クラスター仕様の要約 **30**
4.1. CLUSTERVERSIONによるクラスター仕様の要約 30

第1章 サポート

1.1. サポート

本書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についての 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 (OCM) 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。

本書の改善が提案される場合や、エラーが見つかった場合は、**Documentation** コンポーネントの **OpenShift Container Platform** 製品に対して、Bugzilla レポート 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。

1.2. 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、簡潔な根本的な原因についての説明や修正手順を説明した既知の問題のソリューションを検索できます。

1.3. 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. 主な Red Hat カスタマーポータルの検索フィールドには、問題に関連する入力キーワードおよび文字列を入力します。これらには、以下が含まれます。
   - 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
3. **Search** をクリックします。
4. **OpenShift Dedicated** 製品フィルターを選択します。

5. **ナレッジベース** のコンテンツタイプフィルターを選択します。

1.4. サポートケースの送信

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。
- Red Hat カスタマーポータルのアカウントがある。
- Red Hat の標準またはプレミアムサブスクリプションがある。

手順

1. Red Hat カスタマーポータル にログインし、**SUPPORT CASES → Open a case** を選択します。
2. 問題 (**Defect / Bug** など)、製品 (**OpenShift Dedicated**)、および製品バージョン (すでに自動入力されていない場合は **4**) に該当するカテゴリーを選択します。
3. 報告されている問題に対する一致に基づいて提案される Red Hat ナレッジベースソリューションの一覧を確認してください。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。
4. 問題について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についての詳細情報を入力します。
5. 報告されている問題に対する一致に基づいて提案される Red Hat ナレッジベースソリューションの更新された一覧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、この一覧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。
6. 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。
7. 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 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。
     i. **Home → Dashboards → Overview** に移動します。
     ii. **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。
     i. ツールバーから、**(?) Help → Open Support Case** に移動します。
     ii. **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"}'
```

8. プロンプトが表示されたら、以下の質問に入力し、**Continue** をクリックします。
   - 動作はどこで発生しているか?どの環境を使用しているか?
   - 動作はいつ発生するか?頻度は?繰り返し発生するか?特定のタイミングで発生するか?
   - 時間枠およびビジネスへの影響について提供できるどのような情報があるか?
9. 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。まず **oc adm must-gather** コマンドを使用して収集されるデータと、そのコマンドによって収集されない問題に固有のデータを含めることが推奨されます。
10. 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。
11. ケースの詳細をプレビューし、**Submit** をクリックします。

1.5. 関連情報

- クラスターの問題を特定する方法の詳細は、「Using Insights to identify issues with your cluster」を参照してください。

第2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

2.1. 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は、本書で説明されている利点を提供します。

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 によって Red Hat に送信される情報を説明するために Red Hat が使用する用語です。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。データは、クラスターがさらされる可能性のある問題に関する洞察を生み出すために使用されます。これらの洞察は、cloud.redhat.com/openshift のクラスター管理者に通信されます。

これらの 2 つのプロセスについての詳細は、本書を参照してください。

Telemetry および Insights Operator の利点

Telemetry および Insights Operator はエンドユーザーに以下の利点を提供します。

- **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 が複数のお客様の幅広い視点から観察します。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、Bugzilla 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。

- **ターゲットが絞られた新機能の優先付け**。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。

- **効率された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することができます。本書には、強化されたサポートエクスペリエンスについての詳細情報を提供しています。

- **予測分析**。cloud.redhat.com/openshift に表示されるクラスターについての洞察は、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にされます。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、人工知能の自動化の適用に取り組んでいます。

2.1.1. 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 はメトリクス値を 4 分 30 秒ごとにフェッチし、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、本書で説明しています。

このデータのストリームは、Red Hat によって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。これにより、Red Hat は、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。

このデバッグ情報は、サポートケースでレポートされるデータへのアクセスと同じ制限が適用された状態で Red Hat サポートおよびエンジニアリングチームが利用できます。接続クラスターのすべての情報は、OpenShift Dedicated をより使用しやすく、より直感的に使用できるようにするために Red Hat によって使用されます。

2.1.1.1. 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。

- インストール時に生成される一意でランダムな識別子
- 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
- 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
- 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、およびマシンについてのサイジング情報
- 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
- 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
- コンポーネント、機能および拡張機能に関する使用状況の情報
- 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状況の詳細
- 動作が低下したソフトウェアに関する情報
- **NotReady** とマークされているノードについての情報
- 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
- 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。これには、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、およびサービスが含まれます。
- 証明書の有効性についての情報

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、個人情報を収集することを意図していません。Red Hat は、個人情報が誤って受信したことを検知した場合に、該当情報を削除します。Telemetry データが個人データを構成する場合において、Red Hat のプライバシー方

針については、「Red Hat Privacy Statement」を参照してください。

2.1.2. 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深層度の高いデータを評価できます。

OpenShift Dedicated のユーザーは、OpenShift Cluster Manager (OCM) 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 Data & Application Security」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。

- OpenShift Cluster Manager (OCM) で、潜在的なクラスターの問題をプロアクティブに特定し、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。

関連情報

- Insights Operator はデフォルトでインストールされ、有効にされます。リモートヘルスレポートをオプトアウトする必要がある場合は、「Opting out of remote health reporting」を参照してください。

2.1.2.1. 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ついての一般的な情報
- 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
- Amazon Web Services などの OpenShift Dedicated がデプロイされるプラットフォームや、クラスターが置かれるリージョンについての詳細情報
- 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 のソースコードは確認したり、提供したりできます。Insights Operator によって収集される項目の一覧については、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。

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

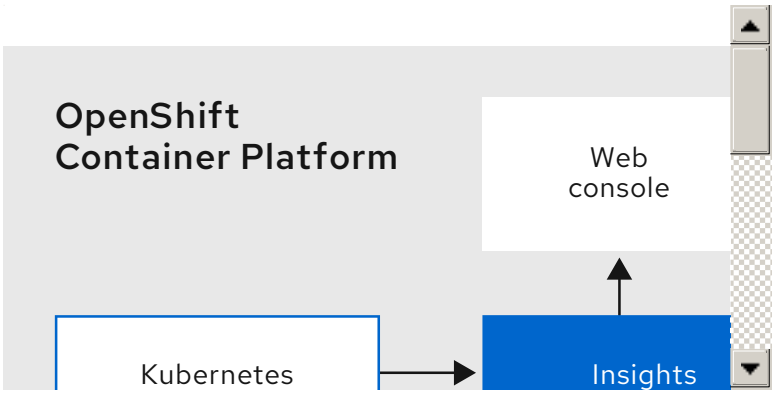
Telemeter Client は、Prometheus API から選択した時系列データを収集します。時系列データは、処理するために 4 分 30 秒ごとに api.openshift.com にアップロードされます。

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、処理するために 2 時間ごとに cloud.redhat.com にアップロードされます。さらに Insights Operator は、cloud.redhat.com から最新の Insights 分析を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



2.1.4. 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。

本書の前のセクションで説明したように、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課金の目的で (該当する場合)、Red Hat 製品のお客様の使用についての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目的で定められた技術および組織上の対策を講じます。

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

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、または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。

サードパーティーのサービスプロバイダー

Red Hat は、Telemetry および設定データの収集と保管を支援する特定のサービスプロバイダーと連携する場合があります。

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

「Opting out of remote health reporting 」の手順に従って、OpenShift Dedicated Telemetry および Insights Operator を無効にすることができます。

2.2. 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

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。

2.2.1. 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 CLI (**oc**) のインストール。
- **cluster-admin** ロールまたは **cluster-monitoring-view** ロールのいずれかを持つユーザーとしてクラスターにログインする必要があります。

手順

1. OpenShift Dedicated クラスターで実行される Prometheus サービスの URL を見つけます。

```
$ oc get route prometheus-k8s -n openshift-monitoring -o jsonpath="{.spec.host}"
```

2. URL に移動します。
3. このクエリーを **Expression** 入力ボックスに入力し、**Execute** を押します。

```
{__name__=~"cluster:usage:.*|count:up0|count:up1|cluster_version|cluster_version_available_updates|cluster_operator_up|cluster_operator_conditions|cluster_version_payload|cluster_installer|cluster_infrastructure_provider|cluster_feature_set|instance:etcd_object_counts:sum|ALERTS|code:apiserver_request_total:rate:sum|cluster:capacity_cpu_cores:sum|cluster:capacity_memory_bytes:sum|cluster:cpu_usage_cores:sum|cluster:memory_usage_bytes:sum|openshift:cpu_usage_cores:sum|openshift:memory_usage_bytes:sum|workload:cpu_usage_cores:sum|workload:memory_usage_bytes:sum|cluster:virt_platform_nodes:sum|cluster:node_instance_type_count:sum|cnv:vmi_status_running:count|node_role_os_version_machine:cpu_capacity_cores:sum
node_role_os_version_machine:cpu_capacity_sockets:sum|subscription_sync_total|csv_succeeded|csv_abnormal|ceph_cluster_total_bytes|ceph_cluster_total_used_raw_bytes|ceph_health_status|job:ceph_osd_metadata:count|job:kube_pv:count|job:ceph_pools_iops:total|job:ceph_pools_iops_bytes:total|job:ceph_versions_running:count|job:noobaa_total_unhealthy_buckets:sum|job:noobaa_bucket_count:sum|job:noobaa_total_object_count:sum|noobaa_accounts_num|noobaa_total_usage|console_url|cluster:network_attachment_definition_instances:max|cluster:netwo
```

```
rk_attachment_definition_enabled_instance_up:max|insightsclient_request_send_total|cam_app
_workload_migrations|cluster:apiserver_current_inflight_requests:sum:max_over_time:2m|clust
er:telemetry_selected_series:count",alertstate=~"firing|"}
```

このクエリーは、Telemetry が実行中の OpenShift Dedicated クラスターの Prometheus サービスに対して行う要求をレプリケートし、Telemetry によってキャプチャーされる時系列の完全なセットを返します。

2.2.2. Insights Operator によって収集されるデータの表示

Insights Operator で収集されるデータを確認することができます。

前提条件

- **cluster-admin** ロールを持つユーザーとしてのクラスターへのアクセスがあること。

手順

1. Insights Operator の現在実行中の Pod の名前を検索します。

```
$ INSIGHTS_OPERATOR_POD=$(oc get pods --namespace=openshift-insights -o custom-
columns=:metadata.name --no-headers  --field-selector=status.phase=Running)
```

2. Insights Operator で収集される最近のデータアーカイブをコピーします。

```
$ oc cp openshift-insights/$INSIGHTS_OPERATOR_POD:/var/lib/insights-operator ./insights-
data
```

最近の Insights Operator アーカイブが **insights-data** ディレクトリーで利用可能になります。

2.3. リモートヘルスレポートのオプトアウト

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。

2.4. 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、OpenShift Cluster Manager (OCM) の各クラスターの **Insights** タブにレポートを表示できます。

2.4.1. 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 (OCM) で 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に、これらの結果は変更する可能性があります。

前提条件

- クラスターが OpenShift Cluster Manager (OCM) 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 (OCM) にログインしている。

手順

1. 左側のペインで **Clusters** メニューをクリックします。
2. クラスターの名前をクリックして、クラスターの詳細を表示します。
3. クラスターの **Insights** タブを開きます。
   その結果に応じて、タブには以下のいずれかが表示されます。
   - **Your cluster passed all health checks** Insights がいずれの問題も特定しなかった場合。
   - Insights が検出さる問題の一覧。これらの問題には、リスクに基づいて優先度 (低「low」、中「moderate」、重要「importanto」および重大「critical」）が付けられます。
   - **No health checks to display** Insights がクラスターを分析していない場合。この分析は、クラスターがインストールされ、インターネットに接続された直後に開始します。
4. 問題がタブに表示される場合、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。
   この問題によっては、詳細情報に Red Hat ナレッジベースアーティクルへのリンクが含まれることがあります。問題の解決方法の詳細については、**How to remediate this issue** をクリックしてください。

2.4.2. 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することができます。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 (OCM) 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 (OCM) 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、優先順にグループ化された潜在的な問題が一覧表示されます。個別のカテゴリーまたは **View all in OpenShift Dedicated** をクリックして、詳細を表示します。

第3章 クラスターに関するデータの収集

サポートケースを作成する際、ご使用のクラスターについてのデバッグ情報を Red Hat サポートに提供していただくと Red Hat のサポートに役立ちます。

以下を提供することが推奨されます。

- **oc adm must-gather** コマンドを使用して収集されるデータ
- 一意のクラスター ID

3.1. 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
- 監査ログ
- サービスログ

--image 引数を指定してコマンドを実行する際にイメージを指定できます。イメージを指定する際、ツールはその機能または製品に関連するデータを収集します。

oc adm must-gather を実行すると、新しい Pod がクラスターに作成されます。データは Pod で収集され、**must-gather.local** で始まる新規ディレクトリーに保存されます。このディレクトリーは、現行の作業ディレクトリーに作成されます。

3.2. RED HAT サポート用のクラスターについてのデータの収集

oc adm must-gather CLI コマンドを使用して、クラスターについてのデバッグ情報を収集できます。

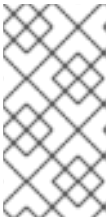
前提条件

- **cluster-admin** ロールを持つユーザーとしてのクラスターへのアクセスがあること。
- 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ついての情報を収集します。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。

注記

クラスターがネットワークが制限された環境を使用している場合、追加の手順を実行する必要があります。ミラーレジストリーに信頼される CA がある場合、まず信頼される CA をクラスターに追加する必要があります。ネットワークが制限された環境のすべてのクラスターについて、**oc adm must-gather** コマンドを使用する前に、デフォルトの **must-gather** イメージをイメージストリームとしてインポートする必要があります。

```
$ oc import-image is/must-gather -n openshift
```

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. 圧縮ファイルを Red Hat カスタマーポータル で作成したサポートケースに添付します。

3.3. 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、特定に機能についての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ついてのデータを収集できます。

表3.1 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-rhel8:v2.6.0	OpenShift Virtualization のデータ収集。
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-rhel7	Red Hat OpenShift Service Mesh のデータ収集。
registry.redhat.io/rhcam-1-2/openshift-migration-must-gather-rhel8	移行関連情報のデータ収集。
registry.redhat.io/ocs4/ocs-must-gather-rhel8:v4.7	Red Hat OpenShift Container Storage のデータ収集。
registry.redhat.io/openshift4/ose-cluster-logging-operator	OpenShift Logging のデータ収集。

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。

前提条件

- **cluster-admin** ロールを持つユーザーとしてのクラスターへのアクセスがあること。
- 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。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-rhel8:v2.6.0 2
```

1 デフォルトの OpenShift Container Platform **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。

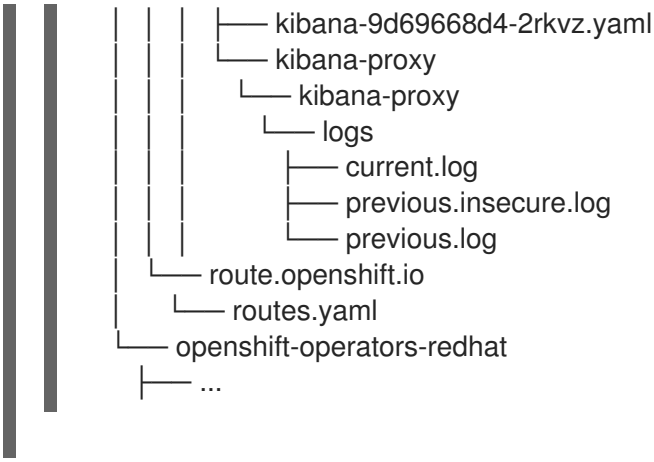
```
$ oc adm must-gather --image=$(oc -n openshift-logging get deployment.apps/cluster-logging-operator \
 -o jsonpath='{.spec.template.spec.containers[?(@.name == "cluster-logging-operator")].image}')
```

例3.1 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
```



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. 圧縮ファイルを Red Hat カスタマーポータル で作成したサポートケースに添付します。

3.4. 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 Container Platform 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

- **cluster-admin** ロールを持つユーザーとしてのクラスターへのアクセスがあること。
- Web コンソールまたはインストールされている OpenShift CLI (**oc**) へのアクセスがあること。

手順

- 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 → Open Support Case** に移動します。
  b. **Cluster ID** 値が自動的に入力されます。
- 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 → Dashboards → 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"}'
```

3.5. SOSREPORT について

sosreport は、設定の詳細、システム情報、および診断データを Red Hat Enterprise Linux (RHEL) および Red Hat Enterprise Linux CoreOS (RHCOS) システムから収集するツールです。**sosreport** は、ノードに関連する診断情報を収集するための標準化した方法を提供します。この情報は、問題の診断のために Red Hat サポートに提供できます。

サポートによっては、Red Hat サポートは特定の OpenShift Container Platform ノードの **sosreport** アーカイブを収集するよう依頼する場合があります。たとえば、**oc adm must-gather** の出力に含まれないシステムログまたは他のノード固有のデータを確認する必要がある場合があります。

3.6. OPENSHIFT CONTAINER PLATFORM クラスターノードの SOSREPORT アーカイブの生成

OpenShift Container Platform 4 クラスターノードの **sosreport** を生成する方法として、デバッグ Pod を使用することが推奨されます。

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。
- ホストへの SSH アクセスがあること。
- OpenShift CLI (**oc**) がインストールされている。
- Red Hat の標準またはプレミアムサブスクリプションがある。
- Red Hat カスタマーポータルのアカウントがある。
- 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一覧を取得します。

```
$ 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
```

注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Container Platform 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ず、ノードは **accessed** のテイントのマークが付けられます。ただし、OpenShift Container Platform API が利用できない場合や、kubelet がターゲットノードで適切に機能しない場合、**oc** 操作がその影響を受けます。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。

4. **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…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。

5. **sosreport** アーカイブを収集します。

   a. **sosreport** コマンドを実行して、**crio.all** および **crio.logs** CRI-O コンテナーエンジン **sosreport** プラグインを有効にします。

```
# sosreport -k crio.all=on -k crio.logs=on (1)
```

   (1) **-K** により、デフォルト以外の **sosreport** プラグインパラメーターを定義できます。

   b. プロンプトが表示されたら **Enter** を押して続行します。

   c. Red Hat サポートケース ID を指定します。**sosreport** は ID をアーカイブのファイル名に追加します。

   d. **sosreport** 出力は、アーカイブの場所とチェックサムを提供します。以下の出力参照例は、ケース ID **01234567** を参照します。

```
Your sosreport has been generated and saved in:
  /host/var/tmp/sosreport-my-cluster-node-01234567-2020-05-28-eyjknxt.tar.xz (1)

The checksum is: 382ffc167510fd71b4f12a4f40b97a4e
```

   (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、**sosreport** アーカイブのファイルパスは **chroot** 環境外にあります。

6. 以下の方法のいずれかを使用して、解析のために **sosreport** アーカイブを Red Hat サポートに提供します。

   - ファイルを OpenShift Container Platform 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** を実行してアーカイブを既存の 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-sosreport.tar.xz
```
(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/sosreport-my-cluster-node-01234567-2020-05-28-eyjknxt.tar.xz' > /tmp/sosreport-my-cluster-node-01234567-2020-05-28-eyjknxt.tar.xz
```
(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。

注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Container Platform 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。**scp** を使用してクラスターノードから **sosreport** アーカイブを転送することは推奨されず、ノードには **accessed** のテイントのマークが付けられます。ただし、OpenShift Container Platform API が利用できない場合や、kubelet がターゲットノードで適切に機能しない場合、**oc** 操作がその影響を受けます。この状態では、**scp core@<node>.<cluster_name>.<base_domain>:<file_path> <local_path>** を実行して、ノードから **sosreport** アーカイブをコピーすることができます。

b. https://access.redhat.com/support/cases/ 内の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。

3.7. ブートストラップノードのジャーナルログのクエリー

ブートストラップ関連の問題が発生した場合、ブートストラップノードから **bootkube.service** の**journald** ユニットログおよびコンテナーログを収集できます。

前提条件

- ブートストラップノードへの SSH アクセスがある。

- ブートストラップノードの完全修飾ドメイン名がある。

手順

1. OpenShift Container Platform のインストール時にブートストラップノードから **bootkube.service** の**journald** ユニットログをクエリーします。**<bootstrap_fqdn>** をブートストラップノードの完全修飾ドメイン名に置き換えます。

```
$ ssh core<bootstrap_fqdn> journalctl -b -f -u bootkube.service
```

注記

ブートストラップノードで **bootkube.service** のログは etcd の **connection refused** エラーを出力し、ブートストラップサーバーがマスターノードの etcd に接続できないことを示します。etcd が各マスターノードで起動し、ノードがクラスターに参加した後には、エラーは発生しなくなるはずです。

2. ブートストラップノードで **podman** を使用してブートストラップノードのコンテナーからログを収集します。**<bootstrap_fqdn>** をブートストラップノードの完全修飾ドメイン名に置き換えます。

```
$ ssh core@<bootstrap_fqdn> 'for pod in $(sudo podman ps -a -q); do sudo podman logs
$pod; done'
```

3.8. 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。
- 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。
- ホストへの SSH アクセスがあること。

手順

1. OpenShift Container Platform 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、マスター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、すべてのマスターノードの **/var/log/openshift-apiserver/** にあるファイルを一覧表示します。

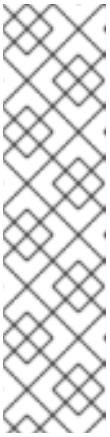
```
$ oc adm node-logs --role=master --path=openshift-apiserver
```

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、すべてのマスターノードから **/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
```

c. API が機能しない場合は、代わりに SSH を使用して各ノードのログを確認します。以下の例は、**/var/log/openshift-apiserver/audit.log** をベースとしています。

```
$ ssh core@<master-node>.<cluster_name>.<base_domain> sudo tail -f
/var/log/openshift-apiserver/audit.log
```



注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Container Platform 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ず、ノードは **accessed** のテイントのマークが付けられます。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 Container Platform API が利用できない場合や、kubelet がターゲットノードで適切に機能しない場合、**oc** 操作がその影響を受けます。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。

3.9. OPENSHIFT CONTAINER PLATFORM 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 Container Platform 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 Container Platform 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 Container Platform 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。
- OpenShift CLI (**oc**) がインストールされている。
- Red Hat の標準またはプレミアムサブスクリプションがある。
- Red Hat カスタマーポータルのアカウントがある。
- 既存の Red Hat サポートケース ID がある。
- ホストへの SSH アクセスがあること。

手順

1. クラスターノードの一覧を取得します。

```
$ 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
```

注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Container Platform 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ず、ノードは **accessed** のテイントのマークが付けられます。ただし、OpenShift Container Platform API が利用できない場合や、kubelet がターゲットノードで適切に機能しない場合、**oc** 操作がその影響を受けます。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。

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

```
# 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** をインターフェー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** をインターフェー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.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 Container Platform 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。

注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Container Platform 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。**scp** を使用してクラスターノードから **tcpdump** キャプチャーファイルを転送することは推奨されず、ノードには **accessed** のテイントのマークが付けられます。ただし、OpenShift Container Platform API が利用できない場合や、kubelet がターゲットノードで適切に機能しない場合、**oc** 操作がその影響を受けます。この状態では、**scp core@<node>.<cluster_name>.<base_domain>:<file_path> <local_path>** を実行して、ノードから **tcpdump** キャプチャーファイルをコピーすることができます。

b. https://access.redhat.com/support/cases/ 内の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。

3.10. RED HAT サポートへの診断データの提供

OpenShift Container Platform 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、または **redhat-support-tool** コマンドを使用して OpenShift Container Platform 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。
- ホストへの SSH アクセスがあること。
- OpenShift CLI (**oc**) がインストールされている。
- Red Hat の標準またはプレミアムサブスクリプションがある。
- Red Hat カスタマーポータルのアカウントがある。
- 既存の Red Hat サポートケース ID がある。

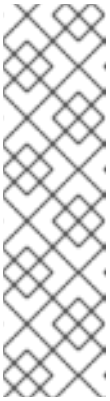
手順

- 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 Container Platform 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。



注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Container Platform 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。**scp** を使用してクラスターノードからファイルを転送することは推奨されず、ノードには **accessed** のテイントのマークが付けられます。ただし、OpenShift Container Platform API が利用できない場合や、kubelet がターゲットノードで適切に機能しない場合、**oc** 操作がその影響を受けます。この状態では、**scp core@<node>.<cluster_name>.<base_domain>:<file_path> <local_path>** を実行してノードから診断ファイルをコピーすることができます。

2. https://access.redhat.com/support/cases/ 内の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。

- OpenShift Container Platform クラスターから直接診断データを既存の 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一覧を取得します。

```
$ 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
```

注記

Red Hat Enterprise Linux CoreOS (RHCOS) を実行する OpenShift Container Platform 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ず、ノードは **accessed** のテイントのマークが付けられます。ただし、OpenShift Container Platform API が利用できない場合や、kubelet がターゲットノードで適切に機能しない場合、**oc** 操作がその影響を受けます。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。

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。

3.11. 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、または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4章 クラスター仕様の要約

4.1. CLUSTERVERSIONによるクラスター仕様の要約

clusterversion リソースをクエリーすることにより、OpenShift Container Platform クラスター仕様の要約を取得できます。

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。
- 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
```

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
```