OpenShift Dedicated 4

OpenShift Dedicated の紹介

OpenShift 専用アーキテクチャーの概要

Last Updated: 2022-11-22

OpenShift Dedicated 4 OpenShift Dedicated の紹介

OpenShift 専用アーキテクチャーの概要

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、OpenShift Dedicated のプラットフォームおよびアプリケーションのアーキテクチャーの概要を解説します。

目次

第1章 OPENSHIFT DEDICATED について

OpenShift Dedicated は Kubernetes を基盤とする完全な OpenShift Container Platform クラスターで、高可用性のために設定された、単一のお客様専用のクラウドサービスとして提供されます。

1.1. OPENSHIFT DEDICATED の概要

OpenShift Dedicated は Red Hat によって管理され、Amazon Web Services (AWS) または Google Cloud Platform (GCP) でホストされます。各 OpenShift Dedicated クラスターには、完全に管理される コントロールプレーン (Control および Infrastructure ノード)、アプリケーションノード、Red Hat Site Reliability Engineer (SRE) によるインストールおよび管理、プレミアム Red Hat サポート、およびクラスターサービス (ロギング、メトリクス、監視、通知ポータル、クラスターポータル) が含まれます。

OpenShift Dedicated は、以下を含むエンタープライズ対応の拡張機能を Kubernetes に提供します。

- OpenShift Dedicated クラスターは AWS または GCP 環境にデプロイされ、アプリケーション管理のハイブリッドアプローチの一部として使用できます。
- Red Hat の統合されたテクノロジー。OpenShift Dedicated の主なコンポーネントは、Red Hat Enterprise Linux と関連する Red Hat の技術に由来します。OpenShift Dedicated は、Red Hat の高品質エンタープライズソフトウェアの集中的なテストや認定の取り組みによる数多くの利点を活用しています。
- オープンソースの開発モデル。開発はオープンソースで行われ、ソースコードはソフトウェアのパブリックリポジトリーから入手可能です。このオープンな共同作業が迅速な技術と開発を促進します。

OpenShift Container Platform でコンテナー化された Kubernetes アプリケーションをビルドおよびデプロイする際に作成できるアセットのオプションを確認するには、OpenShift Container Platform ドキュメントの Understanding OpenShift Container Platform development を参照してください。

1.1.1. カスタムオペレーティングシステム

OpenShift Dedicated はコンテナー指向の新しいオペレーティングシステムであり、CoreOS と Red Hat Atomic Host オペレーティングシステムの最良の機能の一部を組み合わせた Red Hat Enterprise Linux CoreOS (RHCOS) を採用しています。RHCOS は、OpenShift Dedicated のコンテナー化されたアプリケーションを実行する目的で設計されており、新規ツールと連携して迅速なインストール、Operator ベースの管理、および単純化されたアップグレードを実現します。

RHCOS には以下が含まれます。

- Ignition。OpenShift Dedicated が使用するマシンを最初に起動し、設定するための初回起動時のシステム設定です。
- CRI-O、Kubernetes ネイティブコンテナーランタイム実装。これはオペレーティングシステムに密接に統合し、Kubernetes の効率的で最適化されたエクスペリエンスを提供します。CRI-O は、コンテナーを実行、停止および再起動を実行するための機能を提供します。
- Kubelet、Kubernetes のプライマリーノードエージェント。 これは、コンテナーを起動し、これを監視します。

1.1.2. その他の主な機能

Operator は、OpenShift Dedicated コードベースの基本単位であるだけでなく、アプリケーションとア

プリケーションで使用されるソフトウェアコンポーネントをデプロイするための便利な手段です。Operator をプラットフォームの基盤として使用することで、OpenShift Dedicated ではオペレーティングシステムおよびコントロールプレーンアプリケーションの手動によるアップグレードが不要になります。Cluster Version Operator や Machine Config Operator などの OpenShift Dedicated の Operator が、それらの重要なコンポーネントのクラスター全体での管理を単純化します。

Operator Lifecycle Manager (OLM) および OperatorHub は、Operator を保管し、アプリケーションの開発やデプロイを行う人々に Operator を提供する機能を提供します。

Red Hat Quay Container Registry は、ほとんどのコンテナーイメージと Operator を OpenShift Dedicated クラスターに提供する Quay.io コンテナーレジストリーです。Quay.io は、何百万ものイメージやタグを保存する Red Hat Quay の公開レジストリー版です。

OpenShift Dedicated での Kubernetes のその他の拡張には、SDN (Software Defined Networking)、認証、ログ集計、監視、およびルーティングの強化された機能が含まれます。OpenShift Dedicated は、包括的な Web コンソールとカスタム OpenShift CLI (**oc**) インタフェースも提供します。

1.1.3. OpenShift Dedicated のインターネットアクセスおよび Telemetry アクセス

OpenShift Dedicated では、クラスターのインストールおよびアップグレードにインターネットへのアクセスが必要です。

テレメトリーサービスを通じて、情報は OpenShift Dedicated クラスターから Red Hat に送信され、サブスクリプション管理の自動化を可能にし、クラスターの状態を監視し、サポートを支援し、カスタマーエクスペリエンスを向上させます。

テレメトリーサービスは自動的に実行し、クラスターは Red Hat OpenShift Cluster Manager に登録されます。OpenShift Dedicated では、リモートヘルスレポートは常に有効になっており、オプトアウトすることはできません。Red Hat Site Reliability Engineering (SRE) チームは、OpenShift Dedicated クラスターを効果的にサポートするための情報を必要としています。

関連情報

- OpenShift Dedicated クラスターのテレメトーリとリモートヘルスモニタリングの詳細については、リモートヘルスモニタリングについて を参照してください。

第2章 アーキテクチャーの概念

OpenShift Dedicated アーキテクチャーで使用される基本的なコンテナー概念について説明します。

2.1. KUBERNETES について

Kubernetes は、コンテナー化されたアプリケーションのデプロイ、スケーリング、管理を自動化するための、オープンソースのコンテナーオーケストレーションエンジンです。Kubernetes の一般的概念は非常にシンプルです。

- 1 つまたは複数のワーカーノードを使用することからスタートし、コンテナーのワークロードを実行します。
- 1 つまたは複数のコントロールノードからワークロードのデプロイを管理します。
- Pod と呼ばれるデプロイメント単位にコンテナーをラップします。Pod を使うことでコンテナーに追加のメタデータが付与され、複数のコンテナーを単一のデプロイメントエンティティーにグループ化する機能が提供されます。
- 特殊な種類のアセットを作成します。たとえば、サービスは一連の Pod とそのアクセス方法を定義するポリシーによって表されます。このポリシーにより、コンテナーはサービス用の特定の IP アドレスを持っていない場合でも、必要とするサービスに接続することができます。レプリケーションコントローラーは、一度に実行するのに必要な Pod Replicas の数を示すもう一つの特殊なアセットです。この機能を使うと、現在の需要に対応できるようにアプリケーションを自動的にスケーリングすることができます。

Kubernetes の詳細は、Kubernetes ドキュメント を参照してください。

2.2. コンテナー化されたアプリケーションの利点

アプリケーションは、アプリケーションのすべての依存関係が含まれるオペレーティングシステムにインストールすることが予想されていました。ただし、コンテナーは、コンピュートサーバーでリソース分離プロセスとして実行できる単一ユニットにアプリケーションコード、設定、および依存関係をパッケージ化する標準的な方法を提供します。OpenShift Dedicated の Kubernetes でアプリケーションを実行するには、まずコンテナーレジストリーに保存するコンテナーイメージを作成してアプリケーションをコンテナー化する必要があります。

2.2.1. オペレーティングシステムの利点

コンテナーは、小型の、専用の Linux オペレーティングシステムをカーネルなしで使用します。ファイルシステム、ネットワーク、cgroups、プロセステーブル、namespace は、ホストの Linux システムから分離されていますが、コンテナーは、必要に応じてホストとシームレスに統合できます。Linux を基盤とすることで、コンテナーでは、迅速なイノベーションを可能にするオープンソース開発モデルに備わっているあらゆる利点を活用することができます。

各コンテナーは専用のオペレーティングシステムを使用するため、競合するソフトウェアの依存関係を必要とする複数のアプリケーションを、同じホストにデプロイできます。各コンテナーは、それぞれの依存するソフトウェアを持ち運び、ネットワークやファイルシステムなどの独自のインターフェイスを管理します。 したがってアプリケーションはそれらのアセットについて競い合う必要はありません。

2.2.2. デプロイメントの利点

アプリケーションのメジャーリリース間でローリングアップグレードを行うと、ダウンタイムなしにアプリケーションを継続的に改善し、かつ現行リリースとの互換性を維持することができます。

さらに、アプリケーションの新バージョンを、旧バージョンと並行してデプロイおよびテストすることもできます。アプリケーションの旧バージョンに加えて、新バージョンをデプロイできます。コンテナーがテストにパスしたら、新規コンテナーを追加でデプロイし、古いコンテナーを削除できます。

アプリケーションのソフトウェアの依存関係すべてはコンテナー内で解決されるので、データセンターの各ホストには汎用のオペレーティングシステムを使用できます。各アプリケーションホスト向けに特定のオペレーティングシステムを設定する必要はありません。データセンターでさらに多くの容量が必要な場合は、別の汎用ホストシステムをデプロイできます。

2.3. OPENSHIFT DEDICATED と OPENSHIFT CONTAINER PLATFORM の違い

OpenShift Dedicated は OpenShift Container Platform と同じコードベースを使用しますが、パフォーマンス、スケーラビリティー、およびセキュリティーに対して最適化されるように意見をもとにした方法でインストールされます。OpenShift Dedicated は完全なマネージドサービスです。そのため、OpenShift Container Platform で手動で設定した OpenShift Dedicated コンポーネントおよび設定の多くは、デフォルトで設定されています。

独自のインフラストラクチャーで OpenShift Dedicated と OpenShift Container Platform の標準インストールとの以下の違いを確認します。

OpenShift Container Platform	OpenShift Dedicated
お客様が OpenShift Container Platform をインストールし、設定します。	OpenShift Dedicated は、ユーザーフレンドリーな Web ページを使用し、パフォーマンス、スケーラビリティー、およびセキュリティーに最適化された標準的な方法でインストールされます。
お客様がコンピューティングリソースを選択できます。	OpenShift Dedicated は、Red Hat 所有またはお客様提供のパブリッククラウド (Amazon Web Services または Google Cloud Platform) でホストおよび管理されます。
お客様はインフラストラクチャーに対して上位レベルの管理権限を持ちます。	お客様には組み込みの管理者グループがありますが、お客様がクラウドアカウントを提供した場合にトップレベルの管理権限を利用できます。
お客様は OpenShift Container Platform で利用可能なすべてのサポート対象機能と設定設定を使用できます。	一部の OpenShift Container Platform 機能と設定は、OpenShift Dedicated で利用または変更できない場合があります。
control ロールを取得するマシンに API サーバーおよび etcd などのコントロールプレーンコンポーネントを設定します。コントロールプレーンコンポーネントを変更することはできますが、コントロールプレーンデータのバックアップや復元、およびコントロールプレーンデータの高可用性の確保はお客様が行う必要があることにご注意ください。	Red Hat はコントロールプレーンをセットアップし、コントロールプレーンコンポーネントを管理します。コントロールプレーンは高可用性を維持します。

OpenShift Container Platform	OpenShift Dedicated
お客様は、コントロールプレーンおよびワーカーノードの基礎となるインフラストラクチャーを更新する必要があります。OpenShift Web コンソールを使用して、OpenShift Container Platform のバージョンを更新できます。	Red Hat は、更新が利用可能になると自動的にお客様に通知します。Red Hat OpenShift Cluster Manager のアップグレードは、手動または自動でスケジュールできます。
サポートは、Red Hat サブスクリプションまたはクラウドプロバイダーの規約に基づいて提供されます。	99.95% のアップタイムを保持する SLA で、Red Hat による設計、運営、およびサポートが 週 7 日、1 日 24 時間 対象になります。

第3章 ポリシーおよびサービス定義

3.1. OPENSHIFT DEDICATED サービス定義

3.1.1. アカウント管理

3.1.1.1. 課金

各 OpenShift Dedicated クラスターには、最低年間ベースクラスター購入が必要であり、各クラスターで使用できる課金オプションは、Standard および Customer Cloud Subscription (CCS) の 2 つです。

標準の OpenShift Dedicated クラスターは、Red Hat が所有する各クラウドインフラストラクチャーアカウントにデプロイされます。Red Hat はこのアカウントを担当し、クラウドインフラストラクチャーの費用は、Red Hat が直接支払います。お客様は、Red Hat サブスクリプションの費用のみを支払うことになります。

CCS モデルでは、お客様はクラウドインフラストラクチャープロバイダーにクラウドコストを直接支払うことになりますが、クラウドインフラストラクチャーアカウントはお客様の組織の一部であり、Red Hat に付与される特定のアクセスです。このモデルでは、お客様は Red Hat に CCS サブスクリプションを支払い、クラウドプロバイダーにクラウド費用を支払うことになります。予備インスタンス (RI) コンピュートインスタンスを事前購入または提供して、クラウドインフラストラクチャーのコストを削減するのは、お客様の責任です。

以下を含む追加のリソースを OpenShift Dedicated クラスター用に購入できます。

- 追加のノード (マシンプールの使用により異なるタイプおよびサイズになります)
- ミドルウェア (JBoss EAP、JBoss Fuse など): 特定のミドルウェアコンポーネントに基づく追加の価格
- 追加のストレージが 500 GB の増分 (標準のみ、100 GB を含む)
- 追加の 12 TiB ネットワーク I/O (標準のみ、12 TB が含まれる)
- サービスのロードバランサーは 4 のバンドルで利用できます。HTTP/SNI 以外のトラフィックまたは非標準ポートを有効にします (標準のみ)。

3.1.1.2. クラスターのセルフサービス

必要なサブスクリプションを購入している場合は、OpenShift Cluster Manager Hybrid Cloud Console からクラスターを作成、スケーリング、および削除できます。

Red Hat OpenShift Cluster Manager で利用可能なアクションは、クラスター内から直接実行することはできません。これは、すべてのアクションが自動的に元に戻されるなど、悪影響を与える可能性があるためです。

3.1.1.3. クラウドプロバイダー

OpenShift Dedicated は、以下のクラウドプロバイダーで OpenShift Container Platform クラスターを管理サービスとして提供します。

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

3.1.1.4. インスタンスタイプ

単一アベイラビリティーゾーンのクラスターでは、単一のアベイラビリティーゾーンにデプロイされた Customer Cloud Subscription (CCS) クラスター用に最低でも 2 つのワーカーノードが必要です。標準クラスターには、最低でも 4 つのワーカーノードが必要です。これらの 4 つのワーカーノードはベースサブスクリプションに含まれます。

複数のアベイラビリティーゾーンのクラスターでは、Customer Cloud Subscription (CCS) クラスター用に少なくとも 3 つのワーカーノードが必要です。3 つの各アベイラビリティーゾーンに 1 つずつデプロイされます。標準クラスターに 9 つ以上のワーカーノードが必要です。これらの 9 個以上のワーカーノードはベースサブスクリプションに含まれます。適切なノードの分散を維持するために、追加のノードを 3 の倍数に購入する必要があります。

ワーカーノードは、すべて単一の OpenShift Dedicated クラスター内で同じタイプおよびサイズである必要があります。

注記

デフォルトのマシンプールノードタイプおよびサイズは、クラスターの作成後に変更できません。

コントロールプレーンとインフラストラクチャーノードも Red Hat から提供されます。etcd および API 関連のワークロードを処理する 3 つ以上のコントロールプレーンノードが使用されます。メトリクス、ルーティング、Web コンソール、および他のワークロードを処理するインフラストラクチャーノードが少なくとも 2 つあります。コントロールプレーンノードとインフラストラクチャーノードでワークロードを実行しないでください。実行する予定のワークロードはすべて、ワーカーノードにデプロイする必要があります。ワーカーノードにデプロイする必要がある Red Hat ワークロードの詳細については、以下の Red Hat Operator サポートセクションを参照してください。

注記

約 1 vCPU コアおよび 1 GiB のメモリーが各ワーカーノードで予約され、割り当て可能なリソースから削除されます。これは、基礎となるプラットフォームに必要なプロセス を実行する必要があります。これには、udev、kubelet、コンテナーランタイムなどのシステムデーモンや、カーネル予約のアカウントが含まれます。監査ログの集計、メトリクスコレクション、DNS、イメージレジストリー、SDN などの OpenShift Container Platform コアシステムは、追加の割り当て可能なリソースを使用し、クラスターの安定性および保守性を確保できる可能性があります。消費される追加リソースは、使用方法によって異なる場合があります。

重要

OpenShift Dedicated バージョン 4.8.35、4.9.26、4.10.6 の時点で、OpenShift Dedicated のデフォルトの Pod ごとの PID 制限は **4096** です。この PID 制限を有効にする場合は、OpenShift Dedicated クラスターをこれらのバージョン以降にアップグレードする必要があります。以前のバージョンの OpenShift Dedicated クラスターは、デフォルトの PID 制限である **1024** を使用します。

OpenShift Dedicated クラスターでは、Pod ごとの PID 制限を設定することはできません。

関連情報

- Red Hat Operator のサポート

3.1.1.5. Customer Cloud Subscription クラスターの AWS インスタンスタイプ

OpenShift Dedicated は以下のワーカーノードのインスタンスタイプおよび AWS のサイズを提供します。

例3.1 一般的用途

- m5.metal (96† vCPU, 384 GiB)
- m5.xlarge (4 vCPU, 16 GiB)
- m5.2xlarge (8 vCPU, 32 GiB)
- m5.4xlarge (16 vCPU, 64 GiB)
- m5.8xlarge (32 vCPU, 128 GiB)
- m5.12xlarge (48 vCPU, 192 GiB)
- m5.16xlarge (64 vCPU, 256 GiB)
- m5.24xlarge (96 vCPU, 384 GiB)
- m5a.xlarge (4 vCPU, 16 GiB)
- m5a.2xlarge (8 vCPU, 32 GiB)
- m5a.4xlarge (16 vCPU, 64 GiB)
- m5a.8xlarge (32 vCPU, 128 GiB)
- m5a.12xlarge (48 vCPU, 192 GiB)
- m5a.16xlarge (64 vCPU, 256 GiB)
- m5a.24xlarge (96 vCPU, 384 GiB)
- m5ad.xlarge (4 vCPU, 16 GiB)
- m5ad.2xlarge (8 vCPU, 32 GiB)
- m5ad.4xlarge (16 vCPU, 64 GiB)
- m5ad.8xlarge (32 vCPU, 128 GiB)
- m5ad.12xlarge (48 vCPU, 192 GiB)
- m5ad.16xlarge (64 vCPU, 256 GiB)
- m5ad.24xlarge (96 vCPU, 384 GiB)
- m5d.metal (96† vCPU, 384 GiB)
- m5d.xlarge (4 vCPU、16 GiB)
- m5d.2xlarge (8 vCPU、32 GiB)
- m5d.4xlarge (16 vCPU、64 GiB)

- m5d.8xlarge (32 vCPU, 128 GiB)
- m5d.12xlarge (48 vCPU, 192 GiB)
- m5d.16xlarge (64 vCPU、256 GiB)
- m5d.24xlarge (96 vCPU、384 GiB)
- m5n.metal (96 vCPU, 384 GiB)
- m5n.xlarge (4 vCPU、16 GiB)
- m5n.2xlarge (8 vCPU、32 GiB)
- m5n.4xlarge (16 vCPU、64 GiB)
- m5n.8xlarge (32 vCPU、128 GiB)
- m5n.12xlarge (48 vCPU、192 GiB)
- m5n.16xlarge (64 vCPU、256 GiB)
- m5n.24xlarge (96 vCPU、384 GiB)
- m5dn.metal (96 vCPU、384 GiB)
- m5dn.xlarge (4 vCPU、16 GiB)
- m5dn.2xlarge (8 vCPU、32 GiB)
- m5dn.4xlarge (16 vCPU、64 GiB)
- m5dn.8xlarge (32 vCPU、128 GiB)
- m5dn.12xlarge (48 vCPU、192 GiB)
- m5dn.16xlarge (64 vCPU、256 GiB)
- m5dn.24xlarge (96 vCPU、384 GiB)
- m5zn.metal (48 vCPU、192 GiB)
- m5zn.xlarge (4 vCPU、16 GiB)
- m5zn.2xlarge (8 vCPU、32 GiB)
- m5zn.3xlarge (12 vCPU、48 GiB)
- m5zn.6xlarge (24 vCPU、96 GiB)
- m5zn.12xlarge (48 vCPU、192 GiB)
- m6i.metal (128 vCPU、512 GiB)
- m6i.xlarge (4 vCPU、16 GiB)
- m6i.2xlarge (8 vCPU、32 GiB)

- m6i.4xlarge (16 vCPU、64 GiB)
- m6i.8xlarge (32 vCPU、128 GiB)
- m6i.12xlarge (48 vCPU、192 GiB)
- m6i.16xlarge (64 vCPU、256 GiB)
- m6i.24xlarge (96 vCPU、384 GiB)
- m6i.32xlarge (128 vCPU、512 GiB)

† これらのインスタンスタイプは、48 個の物理コアで 96 個の論理プロセッサーを提供します。これらは、2 つの物理 Intel ソケットを備えた単一サーバー上で実行されます。

例3.2 バースト可能な汎用目的

- t3.xlarge (4 vCPU、16 GiB)
- t3.2xlarge (8 vCPU、32 GiB)
- t3a.xlarge (4 vCPU、16 GiB)
- t3a.2xlarge (8 vCPU、32 GiB)

例3.3 メモリー最適化

- r4.xlarge (4 vCPU、30.5 GiB)
- r4.2xlarge (8 vCPU、61 GiB)
- r4.4xlarge (16 vCPU、122 GiB)
- r4.8xlarge (32 vCPU、244 GiB)
- r4.16xlarge (64 vCPU、488 GiB)
- r5.metal (96† vCPU, 768 GiB)
- r5.xlarge (4 vCPU, 32 GiB)
- r5.2xlarge (8 vCPU, 64 GiB)
- r5.4xlarge (16 vCPU, 128 GiB)
- r5.8xlarge (32 vCPU, 256 GiB)
- r5.12xlarge (48 vCPU, 384 GiB)
- r5.16xlarge (64 vCPU, 512 GiB)
- r5.24xlarge (96 vCPU, 768 GiB)
- r5a.xlarge (4 vCPU、32 GiB)

- r5a.2xlarge (8 vCPU、64 GiB)
- r5a.4xlarge (16 vCPU、128 GiB)
- r5a.8xlarge (32 vCPU、256 GiB)
- r5a.12xlarge (48 vCPU、384 GiB)
- r5a.16xlarge (64 vCPU、512 GiB)
- r5a.24xlarge (96 vCPU、768 GiB)
- r5ad.xlarge (4 vCPU、32 GiB)
- r5ad.2xlarge (8 vCPU、64 GiB)
- r5ad.4xlarge (16 vCPU、128 GiB)
- r5ad.8xlarge (32 vCPU、256 GiB)
- r5ad.12xlarge(48 vCPU、384 GiB)
- r5ad.16xlarge (64 vCPU、512 GiB)
- r5ad.24xlarge (96 vCPU、768 GiB)
- r5d.metal (96† vCPU, 768 GiB)
- r5d.xlarge (4 vCPU、32 GiB)
- r5d.2xlarge (8 vCPU、64 GiB)
- r5d.4xlarge (16 vCPU、128 GiB)
- r5d.8xlarge (32 vCPU、256 GiB)
- r5d.12xlarge (48 vCPU、384 GiB)
- r5d.16xlarge (64 vCPU、512 GiB)
- r5d.24xlarge (96 vCPU、768 GiB)
- r5n.metal (96 vCPU, 768 GiB)
- r5n.xlarge (4 vCPU、32 GiB)
- r5n.2xlarge (8 vCPU、64 GiB)
- r5n.4xlarge (16 vCPU、128 GiB)
- r5n.8xlarge (32 vCPU、256 GiB)
- r5n.12xlarge (48 vCPU、384 GiB)
- r5n.16xlarge (64 vCPU、512 GiB)
- r5n.24xlarge (96 vCPU、768 GiB)

- r5dn.metal (96 vCPU、768 GiB)
- r5dn.xlarge (4 vCPU、32 GiB)
- r5dn.2xlarge (8 vCPU、64 GiB)
- r5dn.4xlarge (16 vCPU、128 GiB)
- r5dn.8xlarge (32 vCPU、256 GiB)
- r5dn.12xlarge(48 vCPU, 384 GiB)
- r5dn.16xlarge (64 vCPU、512 GiB)
- r5dn.24xlarge (96 vCPU、768 GiB)
- r6i.metal (128 vCPU、1,024 GiB)
- r6i.xlarge (4 vCPU, 32 GiB)
- r6i.2xlarge (8 vCPU, 64 GiB)
- r6i.4xlarge (16 vCPU, 128 GiB)
- r6i.8xlarge (32 vCPU, 256 GiB)
- r6i.12xlarge (48 vCPU, 384 GiB)
- r6i.16xlarge (64 vCPU, 512 GiB)
- r6i.24xlarge (96 vCPU, 768 GiB)
- r6i.32xlarge (128 vCPU, 1,024 GiB)
- x1.16xlarge (64 vCPU, 976GiB)
- x1.32xlarge (128 vCPU, 1952GiB)
- x1e.xlarge (4 vCPU, 122GiB)
- x1e.2xlarge (8 vCPU, 244GiB)
- x1e.4xlarge (16 vCPU, 488GiB)
- x1e.8xlarge (32 vCPU, 976GiB)
- x1e.16xlarge (64 vCPU, 1,952GiB)
- x1e.32xlarge (128 vCPU, 3,904GiB)
- x2idn.16xlarge (64 vCPU, 1024GiB)
- x2idn.24xlarge (96 vCPU, 1536GiB)
- x2idn.32xlarge (128 vCPU, 2048GiB)
- x2iedn.xlarge (4 vCPU, 128GiB)

- x2iedn.2xlarge (8 vCPU, 256GiB)
- x2iedn.4xlarge (16 vCPU, 512GiB)
- x2iedn.8xlarge (32 vCPU, 1024GiB)
- x2iedn.16xlarge (64 vCPU, 2048GiB)
- x2iedn.24xlarge (96 vCPU, 3072GiB)
- x2iedn.32xlarge (128 vCPU, 4096GiB)
- x2iezn.2xlarge (8 vCPU, 256 GiB)
- x2iezn.4xlarge (16vCPU, 512 GiB)
- x2iezn.6xlarge (24vCPU, 768 GiB)
- x2iezn.8xlarge (32vCPU, 1,024GiB)
- x2iezn.12xlarge (48vCPU, 1,536GiB)
- x2idn.metal (128vCPU, 2,048GiB)
- x2iedn.metal (128vCPU, 4,096GiB)
- x2iezn.metal (48 vCPU、1,536 GiB)
- z1d.metal (48 vCPU, 384 GiB)
- z1d.xlarge (4 vCPU, 32 GiB)
- z1d.2xlarge (8 vCPU、64 GiB)
- z1d.3xlarge (12 vCPU、96 GiB)
- z1d.6xlarge (24 vCPU, 192 GiB)
- z1d.12xlarge (48 vCPU、384 GiB)

† これらのインスタンスタイプは、48 個の物理コアで 96 個の論理プロセッサーを提供します。これらは、2 つの物理 Intel ソケットを備えた単一サーバー上で実行されます。

これらのインスタンスタイプは、24 個の物理コアで 48 個の論理プロセッサーを提供します。

例3.4 コンピュート最適化

- c5.metal (96 vCPU、192 GiB)
- c5.xlarge (4 vCPU, 8 GiB)
- c5.2xlarge (8 vCPU、16 GiB)
- c5.4xlarge (16 vCPU、32 GiB)
- c5.9xlarge (36 vCPU、72 GiB)

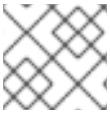
- c5.12xlarge (48 vCPU、96 GiB)
- c5.18xlarge (72 vCPU、144 GiB)
- c5.24xlarge (96 vCPU、192 GiB)
- c5d.metal (96 vCPU、192 GiB)
- c5d.xlarge (4 vCPU、8 GiB)
- c5d.2xlarge (8 vCPU、16 GiB)
- c5d.4xlarge (16 vCPU、32 GiB)
- c5d.9xlarge (36 vCPU、72 GiB)
- c5d.12xlarge (48 vCPU、96 GiB)
- c5d.18xlarge(72 vCPU, 144 GiB)
- c5d.24xlarge (96 vCPU、192 GiB)
- c5a.xlarge (4 vCPU、8 GiB)
- c5a.2xlarge (8 vCPU、16 GiB)
- c5a.4xlarge (16 vCPU、32 GiB)
- c5a.8xlarge (32 vCPU、64 GiB)
- c5a.12xlarge (48 vCPU、96 GiB)
- c5a.16xlarge (64 vCPU、128 GiB)
- c5a.24xlarge (96 vCPU、192 GiB)
- c5ad.xlarge (4 vCPU、8 GiB)
- c5ad.2xlarge (8 vCPU、16 GiB)
- c5ad.4xlarge (16 vCPU、32 GiB)
- c5ad.8xlarge (32 vCPU、64 GiB)
- c5ad.12xlarge (48 vCPU、96 GiB)
- c5ad.16xlarge (64 vCPU、128 GiB)
- c5ad.24xlarge (96 vCPU、192 GiB)
- c5n.metal (72 vCPU、192 GiB)
- c5n.xlarge (4 vCPU、10.5 GiB)
- c5n.2xlarge (8 vCPU、21 GiB)
- c5n.4xlarge (16 vCPU、42 GiB)

- c5n.9xlarge (36 vCPU、96 GiB)
- c5n.18xlarge (72 vCPU、192 GiB)
- c6i.metal (128 vCPU、256 GiB)
- c6i.xlarge (4 vCPU、8 GiB)
- c6i.2xlarge (8 vCPU、16 GiB)
- c6i.4xlarge (16 vCPU、32 GiB)
- c6i.8xlarge (32 vCPU、64 GiB)
- c6i.12xlarge (48 vCPU、96 GiB)
- c6i.16xlarge (64 vCPU、128 GiB)
- c6i.24xlarge (96 vCPU、192 GiB)
- c6i.32xlarge (128 vCPU、256 GiB)

例3.5 ストレージの最適化

- i3.metal (72† vCPU, 512 GiB)
- i3.xlarge (4 vCPU, 30.5 GiB)
- i3.2xlarge (8 vCPU, 61 GiB)
- i3.4xlarge (16 vCPU, 122 GiB)
- i3.8xlarge (32 vCPU, 244 GiB)
- i3.16xlarge (64 vCPU, 488 GiB)
- i3en.metal (96 vCPU、768 GiB)
- i3en.xlarge (4 vCPU, 32 GiB)
- i3en.2xlarge (8 vCPU, 64 GiB)
- i3en.3xlarge (12 vCPU, 96 GiB)
- i3en.6xlarge (24 vCPU, 192 GiB)
- i3en.12xlarge (48 vCPU, 384 GiB)
- i3en.24xlarge (96 vCPU, 768 GiB)

† このインスタンスタイプは、36 個の物理コアで 72 個の論理プロセッサーを提供します。



注記

仮想インスタンスタイプは、.metal インスタンスタイプよりも速く初期化されます。

関連情報

- AWS インスタンスタイプ

3.1.1.6. 標準クラスターの AWS インスタンスタイプ

OpenShift Dedicated は以下のワーカーノードのタイプおよび AWS のサイズを提供します。

例3.6 一般的用途

- m5.xlarge (4 vCPU, 16 GiB)
- m5.2xlarge (8 vCPU, 32 GiB)
- m5.4xlarge (16 vCPU, 64 GiB)

例3.7 メモリー最適化

- r5.xlarge (4 vCPU, 32 GiB)
- r5.2xlarge (8 vCPU, 64 GiB)
- r5.4xlarge (16 vCPU, 128 GiB)

例3.8 コンピュート最適化

- c5.2xlarge (8 vCPU、16 GiB)
- c5.4xlarge (16 vCPU、32 GiB)

3.1.1.7. Google Cloud コンピュートタイプ

OpenShift Dedicated は、他のクラウドインスタンスタイプと同じ共通の CPU およびメモリーの容量を持つために選択される Google Cloud の以下のワーカーノードタイプおよびサイズを提供します。

例3.9 一般的用途

- custom-4-16384 (4 vCPU、16 GiB)
- custom-8-32768 (8 vCPU、32 GiB)
- custom-16-65536 (16 vCPU、64 GiB)

例3.10 メモリー最適化

- custom-4-32768-ext (4 vCPU、32 GiB)
- custom-8-65536-ext (8 vCPU、64 GiB)
- custom-16-131072-ext (16 vCPU、128 GiB)

例3.11 コンピュート最適化

- custom-8-16384 (8 vCPU、16 GiB)
- custom-16-32768 (16 vCPU、32 GiB)

3.1.1.8. リージョンおよびアベイラビリティーゾーン

以下の AWS リージョンは OpenShift Container Platform 4 でサポートされ、OpenShift Dedicated についてサポートされます。

- af-south-1 (Cape Town, AWS オプトインが必要)
- ap-east-1 (Hong Kong, AWS オプトインが必要)
- ap-northeast-1 (Tokyo)
- ap-northeast-2 (Seoul)
- ap-northeast-3 (Osaka)
- ap-south-1 (Mumbai)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-southeast-3 (Jakarta, AWS オプトインが必要)
- ca-central-1 (Central Canada)
- eu-central-1 (Frankfurt)
- eu-north-1 (Stockholm)
- eu-south-1 (Milan, AWS オプトインが必要)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)
- me-south-1 (Bahrain, AWS オプトインが必要)
- sa-east-1 (São Paulo)
- us-east-1 (N. Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)

以下の Google Cloud リージョンは現在サポートされています。

- asia-east1, Changhua County, Taiwan
- asia-east2, Hong Kong
- asia-northeast1, Tokyo, Japan
- asia-northeast2, Osaka, Japan
- asia-northeast3, Seoul, Korea
- asia-south1, Mumbai, India
- asia-southeast1, Jurong West, Singapore
- asia-southeast2, Jakarta, Indonesia
- europe-north1, Hamina, Finland
- europe-west1, St. Ghislain, Belgium
- europe-west2, London, England, UK
- europe-west3, Frankfurt, Germany
- europe-west4, Eemshaven, Netherlands
- europe-west6, Zürich, Switzerland
- northamerica-northeast1, Montréal, Québec, Canada
- southamerica-east1, Osasco (São Paulo), Brazil
- us-central1, Council Bluffs, Iowa, USA
- us-east1, Moncks Corner, South Carolina, USA
- us-east4, Ashburn, Northern Virginia, USA
- us-west1, The Dalles, Oregon, USA
- us-west2, Los Angeles, California, USA
- us-west3, Salt Lake City, Utah, USA
- us-west4, Las Vegas, Nevada, USA

Multi-AZ クラスターは、3 つ以上のアベイラビリティーゾーンを持つリージョンにのみデプロイできます (AWS および Google Cloud を参照してください)。

新規 OpenShift Dedicated クラスターは、単一のリージョンの専用 Virtual Private Cloud (VPC) 内にインストールされます。また、単一アベイラビリティーゾーン (Single-AZ) または複数のアベイラビリティーゾーン (Multi-AZ) にデプロイするオプションを選択できます。これにより、クラスターレベルのネットワークおよびリソースの分離が行われ、VPN 接続や VPC ピアリングなどのクラウドプロバイダーの VPC 設定が有効になります。永続ボリュームはクラウドブロックストレージによってサポートされ、それらがプロビジョニングされるアベイラビリティーゾーンに固有のものです。永続ボリュームは、Pod がスケジュール対象外にされないように、関連付けられた Pod リソースが特定のアベイラビリティーゾーンに割り当てられるまでボリュームにバインドされません。アベイラビリティーゾーン固有のリソースは、同じアベイラビリティーゾーン内のリソースでのみ利用できます。

警告

リージョンおよび単一またはマルチアベイラビリティーゾーンの選択肢は、クラスターがデプロイされた後には変更できません。

3.1.1.9. サービスレベルアグリーメント (SLA)

サービスの SLA は、Red Hat Enterprise Agreement Appendix 4 (Online Subscription Services) の Appendix 4 で定義されています。

3.1.1.10. 限定的なサポートのステータス

クラスターが **限定サポート** ステータスに移行すると、Red Hat はクラスターをプロアクティブに監視しなくなり、SLA は適用されなくなり、SLA に対して要求されたクレジットは拒否されます。製品サポートがなくなったという意味ではありません。場合によっては、違反要因を修正すると、クラスターが完全にサポートされた状態に戻ることがあります。ただし、それ以外の場合は、クラスターを削除して再作成する必要があります。

クラスターは、次のシナリオなど、さまざまな理由で限定サポートステータスに移行する場合があります。

サポート終了日までにクラスターをサポートされるバージョンにアップグレードしない場合

Red Hat は、サポート終了日以降のバージョンについて、ランタイムまたは SLA を保証しません。継続的なサポートを受けるには、サポートが終了する前に、クラスターを、サポートされているバージョンにアップグレードしてください。有効期限が切れる前にクラスターをアップグレードしない場合、クラスターは、サポートされているバージョンにアップグレードされるまで、限定サポートステータスに移行します。

Red Hat は、サポートされていないバージョンからサポートされているバージョンにアップグレードするための商業的に合理的なサポートを提供します。ただし、サポートされるアップグレードパスが利用できなくなった場合は、新規クラスターを作成し、ワークロードを移行することが必要になることがあります。

ネイティブの OpenShift Dedicated コンポーネント、または Red Hat によってインストールおよび管理されているその他のコンポーネントを削除または交換した場合

クラスター管理者パーミッションを使用した場合、Red Hat は、インフラストラクチャーサービス、サービスの可用性、またはデータ損失に影響を与えるアクションを含む、ユーザーまたは認可されたユーザーのアクションに対して責任を負いません。Red Hat がそのようなアクションを検出した場合、クラスターは限定サポートステータスに移行する可能性があります。Red Hat はステータスの変更を通知します。アクションを元に戻すか、サポートケースを作成して、クラスターの削除と再作成が必要になる可能性のある修復手順を検討する必要があります。

クラスターが限定サポートステータスに移行する可能性のある特定のアクションについて質問がある場合、またはさらに支援が必要な場合は、サポートチケットを作成します。

3.1.1.11. サポート

OpenShift Dedicated には Red Hat Premium サポートが含まれており、これは Red Hat カスタマーポータル を使用してアクセスできます。

OpenShift Dedicated のサポートに含まれるものについての 詳細は、製品サポートの対象範囲 を参照してください。

サポートの応答時間については、OpenShift Dedicated の SLA を参照してください。

3.1.2. ロギング

OpenShift Dedicated は、Amazon CloudWatch への任意の統合ログ転送を提供します。

3.1.2.1. クラスター監査ロギング

クラスター監査ログは、インテグレーションが有効になっている場合に Amazon CloudWatch 経由で利用できます。インテグレーションが有効でない場合は、サポートケースを作成して監査ログをリクエストできます。監査ログのリクエストでは、日時の範囲が 21 日を超えないように指定する必要があります。監査ログをリクエストする際には、監査ログのサイズが 1 日あたり数 GB になることに注意してください。

3.1.2.2. アプリケーションロギング

STDOUT に送信されるアプリケーションログは Fluentd によって収集され、クラスターロギングスタック経由で Amazon CloudWatch に転送されます (インストールされている場合)。

3.1.3. モニタリング

3.1.3.1. クラスターメトリクス

OpenShift Dedicated クラスターには、CPU、メモリー、ネットワークベースのメトリクスを含むクラスターモニタリングの統合された Prometheus/Grafana スタックが同梱されます。これは Web コンソールからアクセスでき、Grafana ダッシュボードを使用してクラスターレベルのステータスおよび容量/使用状況を表示することもできます。また、これらのメトリクスは OpenShift Dedicated ユーザーによって提供される CPU またはメモリーメトリクスをベースとする Horizontal Pod Autoscaling を許可します。

3.1.3.2. クラスターステータスの通知

Red Hat は、Red Hat OpenShift Cluster Manager で利用可能なクラスターダッシュボードと、クラスターの初回デプロイで使用した連絡先のメールアドレスに送信されるメール通知を使用して、OpenShift Dedicated クラスターの正常性およびステータスについて通信します。

3.1.4. ネットワーク

3.1.4.1. アプリケーションのカスタムドメイン

ルートにカスタムホスト名を使用するには、正規名 (CNAME) レコードを作成して DNS プロバイダーを更新する必要があります。CNAME レコードは、OpenShift の正規ルーターのホスト名をカスタムドメインにマッピングする必要があります。OpenShift の正規ルーターのホスト名は、ルートの作成後に **Route Details** ページに表示されます。または、ワイルドカード CNAME レコードを 1 度作成して、指定のホスト名のすべてのサブドメインをクラスターのルーターにルーティングできます。

3.1.4.2. クラスターサービスのカスタムドメイン

カスタムドメインおよびサブドメインは、プラットフォームサービスルート (API、Web コンソールルート、またはデフォルトのアプリケーションルート) では使用できません。

3.1.4.3. ドメイン検証証明書

OpenShift Dedicated には、クラスターの内部サービスと外部サービスの両方に必要な TLS セキュリティー証明書が含まれます。外部ルートの場合、2 つの別個の TLS ワイルドカード証明書があり、各クラスターに提供され、これが各クラスターにインストールされます。1 つは Web コンソールとルートのデフォルトホスト名用、もう 1 つは API エンドポイント用です。**Let's Encrypt** は証明書に使用される認証局です。たとえば、内部 API エンドポイント などのクラスター内のルートでは、クラスターの組み込み認証局によって署名された TLS 証明書を使用し、TLS 証明書を信頼するためにすべての Pod で CA バンドルが利用可能である必要があります。

3.1.4.4. ビルド用のカスタム認証局

OpenShift Dedicated は、イメージレジストリーからイメージをプルする際にビルドによって信頼されるカスタム認証局の使用をサポートします。

3.1.4.5. ロードバランサー

OpenShift Dedicated は、最大 5 つの異なるロードバランサーを使用します。

- クラスターの内部にあり、内部クラスター通信のトラフィックのバランスを取るために使用される内部コントロールプレーンのロードバランサー。
- OpenShift Container Platform および Kubernetes API へのアクセスに使用される外部コントロールプレーンのロードバランサー。このロードバランサーは、Red Hat OpenShift Cluster Manager で無効にできます。このロードバランサーが無効になると、Red Hat は API DNS を内部コントロールロードバランサーを参照するように再設定します。
- Red Hat によるクラスター管理用に予約される Red Hat の外部コントロールプレーンのロードバランサー。アクセスは厳密に制御され、許可リストの bastion ホストからの通信のみが可能です。
- デフォルトのアプリケーションロードバランサーであるデフォルトの router/ingress ロードバランサー (URL の **apps** で表される)。デフォルトのロードバランサーを OpenShift Cluster Manager で設定して、インターネット上で一般にアクセス可能にしたり、既存のプライベート接続でプライベートにのみアクセス可能にしたりできます。ロギング UI、メトリクス API、レジストリーなどのクラスターサービスを含む、クラスターのすべてのアプリケーションルートは、このデフォルトのルーターロードバランサーで公開されます。
- オプション: セカンダリーアプリケーションロードバランサーであるセカンダリールーター/ingress ロードバランサー (URL の **apps2** で表される)。セカンダリーロードバランサーを OpenShift Cluster Manager で設定して、インターネット上で一般にアクセス可能にしたり、既存のプライベート接続でプライベートにのみアクセス可能にしたりできます。Label match がこのルーターロードバランサーに設定されている場合は、このラベルに一致するアプリケーションルートのみがこのルーターロードバランサーで公開されます。そうでない場合は、すべてのアプリケーションルートもこのルーターのロードバランサーで公開されます。
- オプション: OpenShift Dedicated で実行しているサービスにマップできるサービスのロードバランサー。HTTP/SNI 以外のトラフィックや標準以外のポートの使用などの高度な ingress 機能を有効にします。これらは、標準クラスター用に 4 のグループで購入したり、Customer Cloud Subscription (CCS) クラスターで課金せずにプロビジョニングできます。ただし、各 AWS アカウントには、各クラスター内で使用できる Classic Load Balancer の数を制限する クォータがあります。

3.1.4.6. ネットワーク使用量

標準の OpenShift Dedicated クラスターの場合、ネットワーク使用量は、インバウンド、VPC ピアリ

ング、VPN、および AZ トラフィック間のデータ転送に基づいて測定されます。標準の OpenShift Dedicated ベースクラスターで、ネットワーク I/O の 12 TB が提供されます。追加のネットワーク I/O は、12 TB の増分で購入できます。CCS OpenShift Dedicated クラスターの場合、ネットワークの使用量は監視されず、クラウドプロバイダーによって直接請求されます。

3.1.4.7. クラスター ingress

プロジェクト管理者は、IP 許可リストによる ingress コントロールなど、さまざまな目的でルートアノテーションを追加できます。

Ingress ポリシーは、**ovs-networkpolicy** プラグインを使用する **NetworkPolicy** オブジェクトを使用して変更することもできます。これにより、同じクラスターの Pod 間や同じ namespace にある Pod 間など、Ingress ネットワークポリシーを Pod レベルで完全に制御できます。

すべてのクラスター Ingress トラフィックは定義されたロードバランサーを通過します。すべてのノードへの直接のアクセスは、クラウド設定によりブロックされます。

3.1.4.8. クラスター egress

EgressNetworkPolicy オブジェクトでの Pod egress トラフィックの制御は、OpenShift Dedicated での送信トラフィックを防ぐか、またはこれを制限するために使用できます。

コントロールプレーンおよびインフラストラクチャーノードからのパブリック送信トラフィックは、クラスターイメージのセキュリティーおよびクラスターのモニタリングを維持するために必要です。これには、**0.0.0.0/0** ルートがインターネットゲートウェイにのみ属している必要があります。プライベート接続でこの範囲をルーティングすることはできません。

OpenShift Dedicated クラスターは NAT ゲートウェイを使用して、クラスターから出るパブリック送信トラフィックのパブリック静的 IP を表示します。クラスターがデプロイされる各サブネットは、個別の NAT ゲートウェイを受信します。複数のアベイラビリティーゾーンで AWS にデプロイされるクラスターの場合は、最大 3 つの固有の静的 IP アドレスがクラスターの egress トラフィック用に存在できます。アベイラビリティーゾーントポロジーに関係なく、Google Cloud にデプロイされたクラスターの場合は、ワーカーノードの egress トラフィックに 1 つの静的 IP アドレスがあります。クラスター内に留まるトラフィックや、パブリックインターネットに送信されないトラフィックは NAT ゲートウェイを通過せず、トラフィックの発信元のノードに属するソース IP アドレスを持ちます。ノードの IP アドレスは動的であるため、お客様はプライベートリソースへのアクセス時に個々の IP アドレスを許可しないようにする必要があります。

お客様は、クラスターで Pod を実行し、外部サービスをクエリーすることで、パブリックの静的 IP アドレスを判別できます。以下に例を示します。

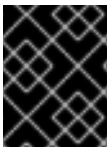
```
$ oc run ip-lookup --image=busybox -i -t --restart=Never --rm -- /bin/sh -c "/bin/nslookup -type=a
myip.opendns.com resolver1.opendns.com | grep -E 'Address: [0-9.]+'"
```

3.1.4.9. クラウドネットワーク設定

OpenShift Dedicated では、複数のクラウドプロバイダー管理テクノロジーを介したプライベートネットワーク接続の設定を可能にします。

- VPN 接続
- AWS VPC ピアリング
- AWS Transit Gateway

- AWS Direct Connect
- Google Cloud VPC Network ピアリング
- Google Cloud Classic VPN
- Google Cloud HA VPN



重要

Red Hat SRE はプライベートネットワーク接続を監視しません。これらの接続の監視は、お客様の責任で行われます。

3.1.4.10. DNS 転送

プライベートクラウドネットワーク設定を持つ OpenShift Dedicated クラスターの場合、お客様は、明示的に提供されたドメインを照会する必要がある、そのプライベート接続で使用可能な内部 DNS サーバーを指定できます。

3.1.5. ストレージ

3.1.5.1. 暗号化された保存時の OS/ノードストレージ

コントロールプレーンノードは、encrypted-at-rest-EBS ストレージを使用します。

3.1.5.2. 暗号化された保存時の PV

永続ボリューム (PV) に使用される EBS ボリュームは、デフォルトで保存時に暗号化されます。

3.1.5.3. ブロックストレージ (RWO)

永続ボリューム (PV) は、ReadWriteOnce (RWO) アクセスモードを使用する AWS EBS および Google Cloud の永続ディスクブロックストレージによってサポートされます。標準の OpenShift Dedicated ベースクラスターでは、100 GB のブロックストレージは、アプリケーション要求に基づいて動的にプロビジョニングされ、再利用されます。追加の永続ストレージは 500 GB の増分で購入できます。

PV は一度に 1 つのノードにのみ割り当てられ、それらがプロビジョニングされるアベイラビリティーゾーンに固有のものですが、アベイラビリティーゾーンの任意のノードに割り当てることができます。

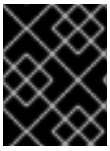
各クラウドプロバイダーには、1 つのノードに割り当てることのできる PV の数について独自の制限があります。詳細は、AWS インスタンスタイプの制限 または Google Cloud Platform カスタムマシンタイプ を参照してください。

3.1.5.4. 共有ストレージ (RWX)

AWS CSI ドライバーは、AWS での OpenShift Dedicated の RWX サポートを提供するために使用できます。コミュニティー Operator は、設定を簡素化するために提供されます。詳細は、AWS EFS Setup for OpenShift Dedicated and Red Hat OpenShift Service on AWS を参照してください。

3.1.6. プラットフォーム

3.1.6.1. クラスターバックアップポリシー



重要

お客様がアプリケーションとアプリケーションデータのバックアップ計画を立てることが重要です。

アプリケーションおよびアプリケーションデータのバックアップは、OpenShift Dedicated サービスの一部ではありません。各 OpenShift Dedicated クラスターのすべての Kubernetes オブジェクトは、クラスターが回復不能になる場合に備えて迅速なリカバリーを可能にするためにバックアップされます。

バックアップは、クラスターと同じアカウントのセキュアなオブジェクトストレージ (Multi-AZ) バケットに保存されます。Red Hat Enterprise Linux CoreOS は OpenShift Container Platform クラスターによって完全に管理され、ステートフルなデータはノードのルートボリュームに保存されないため、ノードのルートボリュームはバックアップされません。

以下の表は、バックアップの頻度を示しています。

コンポーネント	スナップショットの頻度	保持期間	注記
完全なオブジェクトストアのバックアップ	日次 (0100 UTC)	7 日	これは、すべての Kubernetes オブジェクトの完全バックアップです。このバックアップスケジュールでは、永続ボリューム (PV) がバックアップされていません。
完全なオブジェクトストアのバックアップ	週次 (月曜日: 0200 UTC)	30 日	これは、すべての Kubernetes オブジェクトの完全バックアップです。このバックアップスケジュールでは、PV はバックアップされません。
完全なオブジェクトストアのバックアップ	毎時 (1 時間ごとに 17 分を経過した時点)	24 時間	これは、すべての Kubernetes オブジェクトの完全バックアップです。このバックアップスケジュールでは、PV はバックアップされません。

3.1.6.2. 自動スケーリング

現時点で、ノードの自動スケーリングは OpenShift Dedicated では使用できません。

3.1.6.3. デーモンセット

お客様は OpenShift Dedicated で DaemonSet を作成し、実行できます。DeamonSet をワーカーノードでのみの実行に制限するには、以下の nodeSelector を使用します。

```
...
spec:
```

```
  nodeSelector:
    role: worker
...
```

3.1.6.4. 複数のアベイラビリティーゾーン

複数アベイラビリティーゾーンのクラスターでは、コントロールノードは複数のアベイラビリティーゾーンに分散され、各アベイラビリティーゾーンに 3 つ以上のワーカーノードが必要です。

3.1.6.5. ノードラベル

カスタムノードラベルはノードの作成時に Red Hat によって作成され、現時点では OpenShift Dedicated クラスターで変更することはできません。

3.1.6.6. OpenShift バージョン

OpenShift Dedicated はサービスとして実行し、最新の OpenShift Container Platform バージョンで最新の状態に維持されます。

3.1.6.7. アップグレード

アップグレードポリシーおよび手順についての詳細は、OpenShift Dedicated のライフサイクル を参照してください。

3.1.6.8. Windows コンテナー

Windows コンテナーは、現時点で OpenShift Dedicated では利用できません。

3.1.6.9. コンテナーエンジン

OpenShift Dedicated は OpenShift 4 で実行し、唯一の利用可能なコンテナーエンジンとして CRI-O を使用します。

3.1.6.10. オペレーティングシステム

OpenShift Dedicated は OpenShift 4 で実行し、すべてのコントロールプレーンおよびワーカーノードのオペレーティングシステムとして Red Hat Enterprise Linux CoreOS を使用します。

3.1.6.11. Red Hat Operator のサポート

通常、Red Hat ワークロードは、Operator Hub を通じて利用できる Red Hat 提供の Operator を指します。Red Hat ワークロードは Red Hat SRE チームによって管理されないため、ワーカーノードにデプロイする必要があります。これらの Operator は、追加の Red Hat サブスクリプションが必要になる場合があり、追加のクラウドインフラストラクチャーコストが発生する場合があります。これらの Red Hat 提供の Operator の例は次のとおりです。

- Red Hat Quay
- Red Hat Advanced Cluster Management
- Red Hat Advanced Cluster Security
- Red Hat OpenShift Service Mesh

- OpenShift Serverless
- Red Hat OpenShift Logging
- Red Hat OpenShift Pipelines

3.1.6.12. Kubernetes Operator のサポート

OperatorHub marketplace に一覧表示されるすべての Operator はインストールに利用できるはずです。Red Hat Operator を含む OperatorHub からインストールされる Operator は、OpenShift Dedicated サービスの一部として管理されている SRE ではありません。特定の Operator のサポート可能性についての詳細は、Red Hat カスタマーポータル を参照してください。

3.1.7. セキュリティー

このセクションでは、OpenShift Dedicated セキュリティーのサービス定義について説明します。

3.1.7.1. 認証プロバイダー

クラスターの認証は、 Red Hat OpenShift Cluster Manager クラスター作成プロセスの一部として設定されます。OpenShift はアイデンティティープロバイダーではないため、クラスターへのアクセスすべてが統合ソリューションの一部としてお客様によって管理される必要があります。同時にプロビジョニングされる複数のアイデンティティープロバイダーのプロビジョニングがサポートされています。以下のアイデンティティープロバイダーがサポートされます。

- GitHub または GitHub Enterprise OAuth
- GitLab OAuth
- Google OAuth
- LDAP
- OpenID Connect

3.1.7.2. 特権付きコンテナー

特権付きコンテナーは、デフォルトで OpenShift Dedicated では使用できません。**anyuid** および **nonroot** 以外の Security Context Constraints は **dedicated-admins** グループのメンバーに利用でき、多くのユースケースに対応する必要があります。特権付きコンテナーは **cluster-admin** ユーザーのみが利用できます。

3.1.7.3. お客様管理者ユーザー

OpenShift Dedicated は、通常のユーザーのほかに、**dedicated-admin** という OpenShift Dedicated 固有のグループへのアクセスを提供します。**dedicated-admin** グループのメンバーであるクラスターのすべてのユーザー:

- クラスターのお客様が作成したすべてのプロジェクトへの管理者アクセスがある。
- クラスターのリソースクォータおよび制限を管理できる。
- **NetworkPolicy** オブジェクトを追加し、管理できる。

- スケジューラー情報を含む、クラスター内の特定のノードおよび PV に関する情報を表示できる。
- クラスターの予約された **dedicated-admin** プロジェクトにアクセスできる。これにより、昇格した権限を持つサービスアカウントの作成が可能になり、クラスターのプロジェクトのデフォルトの制限およびクォータを更新する機能も提供されます。

3.1.7.4. クラスター管理ロール

Customer Cloud Subscriptions (CCS) のある OpenShift Dedicated の管理者として、**cluster-admin** ロールにアクセスできます。**cluster-admin** ロールを持つアカウントにログインしている場合、ユーザーはクラスターを制御し、設定するためのほとんど無制限のアクセスを持っています。クラスターの不安定化を防ぐため、または OpenShift Cluster Manager で管理されており、クラスター内の変更が上書きされるために、Webhook でブロックされる設定がいくつかあります。

3.1.7.5. プロジェクトのセルフサービス

デフォルトでは、すべてのユーザーにはプロジェクトの作成、更新、および削除を行うことができます。これは、**dedicated-admin** グループのメンバーが認証されたユーザーから self-provisioner ロールを削除すると制限されます。

```
$ oc adm policy remove-cluster-role-from-group self-provisioner system:authenticated:oauth
```

以下を適用すると、制限を元に戻すことができます。

```
$ oc adm policy add-cluster-role-to-group self-provisioner system:authenticated:oauth
```

3.1.7.6. 規制コンプライアンス

OpenShift Dedicated は、セキュリティーおよび管理に関する一般的な業界のベストプラクティスに従います。認定の概要を以下の表に示します。

表3.1 OpenShift Dedicated のセキュリティーおよびコントロール認定

認定	AWS 専用の OpenShift	GCP 専用の OpenShift
ISO 27001	はい	はい
PCI DSS	はい	はい
SOC 2 タイプ 2	はい	はい

3.1.7.7. ネットワークセキュリティー

OpenShift Dedicated on AWS では、AWS は AWS Shield と呼ばれる標準の DDoS 保護をすべてのロードバランサーで提供します。これにより、OpenShift Dedicated に使用されるすべてのパブリック向けロードバランサーで最も一般的に使用されるレベル 3 および 4 攻撃に対し、95% の保護が提供されます。応答を受信するために haproxy ルーターに送信される HTTP 要求に 10 秒のタイムアウトが追加されるか、追加の保護を提供するために接続が閉じられます。

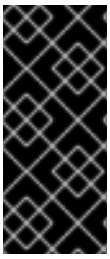
3.1.7.8. etcd 暗号化

OpenShift Dedicated では、コントロールプレーンストレージはデフォルトで保存時に暗号化されます。これには、etcd ボリュームの暗号化が含まれます。このストレージレベルの暗号化は、クラウドプロバイダーのストレージ層を介して提供されます。

etcd 暗号化を有効にして、キーではなく etcd のキーの値を暗号化することもできます。etcd 暗号化を有効にすると、以下の Kubernetes API サーバーおよび OpenShift API サーバーリソースが暗号化されます。

- シークレット
- 設定マップ
- ルート
- OAuth アクセストークン
- OAuth 認証トークン

etcd 暗号化機能はデフォルトで有効にされず、これはクラスターのインストール時にのみ有効にできます。etcd 暗号化が有効にされている場合でも、コントロールプレーンノードにアクセスできるユーザーまたは **cluster-admin** 権限を持つユーザーは、etcd キーの値にアクセスできます。



重要

etcd のキー値の etcd 暗号化を有効にすると、約 20% のパフォーマンスのオーバーヘッドが発生します。このオーバーヘッドは、etcd ボリュームを暗号化するデフォルトのコントロールプレーンのストレージ暗号化に加えて、この 2 つ目の暗号化レイヤーの導入により生じます。Red Hat は、お客様のユースケースで特に etcd 暗号化が必要な場合にのみ有効にすることを推奨します。

3.2. 責任分担マトリクス

OpenShift Dedicated マネージドサービスにおける Red Hat、クラウドプロバイダー、およびお客様の責任についての理解。

3.2.1. OpenShift Dedicated における責任の概要

Red Hat は OpenShift Dedicated サービスを管理しますが、お客様は特定の側面に関して責任を負います。OpenShift Dedicated サービスは、リモートでアクセスされ、パブリッククラウドリソースでホストされ、Red Hat またはお客様が所有するクラウドサービスプロバイダーアカウントで作成され、Red Hat が所有する基礎となるプラットフォームおよびデータセキュリティーがあります。

重要

cluster-admin ロールがクラスターで有効にされている場合は、Red Hat Enterprise Agreement Appendix 4 (Online Subscription Services) の責任および除外事項について参照してください。

リソース	インシデントおよびオペレーション管理	変更管理	アイデンティティーおよびアクセス管理	セキュリティーおよび規制コンプライアンス	障害復旧
お客様データ	お客様	お客様	お客様	お客様	お客様
お客様のアプリケーション	お客様	お客様	お客様	お客様	お客様
開発者サービス	お客様	お客様	お客様	お客様	お客様
プラットフォームモニタリング	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
ロギング	Red Hat	共有	共有	共有	Red Hat
アプリケーションのネットワーク	共有	共有	共有	Red Hat	Red Hat
クラスターネットワーク	Red Hat	共有	共有	Red Hat	Red Hat
仮想ネットワーク	共有	共有	共有	共有	共有
コントロールプレーンおよびインフラストラクチャーノード	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
ワーカーノード	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
クラスターのバージョン	Red Hat	共有	Red Hat	Red Hat	Red Hat
容量の管理	Red Hat	共有	Red Hat	Red Hat	Red Hat
仮想ストレージ	Red Hat およびクラウドプロバイダー	Red Hat およびクラウドプロバイダー	Red Hat およびクラウドプロバイダー	Red Hat およびクラウドプロバイダー	Red Hat およびクラウドプロバイダー
物理インフラストラクチャーおよびセキュリティー	クラウドプロバイダー	クラウドプロバイダー	クラウドプロバイダー	クラウドプロバイダー	クラウドプロバイダー

3.2.2. 共有される責任のマトリクス

お客様および Red Hat は、OpenShift Dedicated クラスターのモニタリングおよびメンテナーンスについての責任を共有します。このドキュメントは、領域およびタスクごとの責任の説明を示しています。

3.2.2.1. インシデントおよびオペレーション管理

お客様は、お客様のアプリケーションデータおよびお客様がクラスターネットワークまたは仮想ネットワークに設定した可能性のあるカスタムネットワークに関するインシデントおよびオペレーションの管理を行います。

リソース	Red Hat の責任	お客様の責任
アプリケーションのネットワーク	クラウドロードバランサーおよびネイティブ OpenShift ルーターサービスを監視し、アラートに応答します。	• サービ出力ドバランサーのエンドポイントの正常性の監視 • アプリケーションルート、およびその背後のエンドポイントの正常性を監視します。 • Red Hat に停電を報告します。
仮想ネットワーク	クラウドロードバランサー、サブネット、およびデフォルトのプラットフォームネットワークに必要なパブリッククラウドコンポーネントを監視し、アラートに応答します。	潜在的な問題やセキュリティーの脅威について、VPC から VPC 接続、VPN 接続、または直接接続を介して任意で設定されているネットワークトラフィックを監視します。

3.2.2.2. 変更管理

Red Hat は、お客様が制御するクラスターインフラストラクチャーおよびサービスへの変更を有効にし、コントロールプレーンノード、インフラストラクチャーノードおよびサービス、ならびにワーカーノードのバージョンを維持します。お客様は、インフラストラクチャーの変更要求を開始し、クラスターでの任意のサービスおよびネットワーク設定のインストールおよび維持、およびお客様データおよびお客様のアプリケーションに対するすべての変更を行います。

リソース	Red Hat の責任	お客様の責任

リソース	Red Hat の責任	お客様の責任
ロギング	● プラットフォーム監査ログを一元的に集計し、監視します。 ● ロギング Operator を提供して維持し、お客様がデフォルトのアプリケーションロギングのロギングスタックをデプロイできるようにします。 ● 顧客の要求時に監査ログを指定します。	● オプションのデフォルトのアプリケーションロギング Operator をクラスターにインストールします。 ● サイドカーコンテナーのロギングやサードパーティーのロギングアプリケーションなど、任意のアプリロギングソリューションをインストール、設定、および保守します。 ● ロギングスタックまたはクラスターの安定性に影響がある場合に、お客様のアプリケーションによって生成されるアプリケーションログのサイズおよび頻度を調整します。 ● 特定のインシデントを調査するためにサポートケースを使用してプラットフォーム監査ログを要求します。
アプリケーションのネットワーク	● パブリッククラウドロードバランサーを設定します。プライベートロードバランサーを設定し、必要に応じて追加のロードバランサーを 1 つまで設定する機能を提供します。 ● ネイティブ OpenShift ルーターサービスを設定します。ルーターをプライベートとして設定し、1 つのルーターシャードを追加する機能を提供します。 ● デフォルトの内部 Pod トラフィック用に OpenShift SDN コンポーネントをインストールし、設定し、維持します。 ● お客様が **NetworkPolicy** および **EgressNetworkPolicy** (ファイアウォール) オブジェクトを管理できる機能を提供します。	● **NetworkPolicy** オブジェクトを使用して、プロジェクトおよび Pod ネットワーク、Pod ingress、および Pod egress のデフォルト以外の Pod ネットワークのパーミッションを設定します。 ● Red Hat OpenShift Cluster Manager を使用して、デフォルトのアプリケーションルートのプライベートロードバランサーを要求します。 ● OpenShift Cluster Manager を使用して、追加の 1 つのパブリックまたはプライベートルーターシャードおよび対応するロードバランサーを設定します。 ● 特定サービスの追加のサービス出力ドバランサーを要求し、設定します。 ● 必要な DNS 転送ルールを設定します。

リソース	Red Hat の責任	お客様の責任
クラスターネットワーク	● パブリックまたはプライベートサービスのエンドポイントや仮想ネットワークコンポーネントとの必要な統合などのクラスター管理コンポーネントを設定します。 ● ワーカー、インフラストラクチャー、およびコントロールプレーンノード間の内部クラスター通信に必要な内部ネットワークコンポーネントを設定します。	● クラスターのプロビジョニング時に OpenShift Cluster Manager で必要な場合は、マシン CIDR、サービス CIDR、および Pod CIDR の任意のデフォルト以外の IP アドレス範囲を指定します。 ● クラスターの作成時または OpenShift Cluster Manager でクラスターの作成後に、API サービスエンドポイントをパブリックまたはプライベートにするように要求します。
仮想ネットワーク	● クラスターのプロビジョニングに必要な仮想ネットワークコンポーネント (仮想プライベートクラウド、サブネット、ロードバランサー、インターネットゲートウェイ、NAT ゲートウェイなど) をセットアップし、設定します。 ● お客様が OpenShift Cluster Manager で必要に応じて、オンプレミスリソース、VPC 間の接続、および直接接続を管理できる機能を提供します。 ● サービ出力ドバランサーと共に使用できるように、お客様がパブリッククラウドロードバランサーを作成およびデプロイできるようにします。	● VPC 間の接続、VPN 接続、直接接続などの任意のパブリッククラウドネットワークコンポーネントを設定し、維持します。 ● 特定サービスの追加のサービ出力ドバランサーを要求し、設定します。

リソース	Red Hat の責任	お客様の責任
クラスターのバージョン	● アップグレードのスケジューリングプロセスを有効にします。 ● アップグレードの進捗を監視し、発生した問題をすべて修正します。 ● マイナーおよびメンテナーンスアップグレードのための変更ログおよびリリースノートを公開します。	● メンテナンスバージョンのアップグレードを即時、後日、または自動で行うようにスケジュールします。 ● マイナーバージョンのアップグレードを確認し、スケジュールします。 ● クラスターのバージョンがサポート範囲のマイナーバージョンであることを確認します。 ● 互換性を確保するために、マイナーバージョンおよびメンテナーンスバージョンでお客様のアプリケーションをテストします。
容量の管理	● コントロールプレーン (コントロールプレーンノードとインフラストラクチャーノード) の使用率を監視します。 ● QoS (Quality of Service) を維持するために、コントロールプレーンノードのスケーリングまたはサイズ変更を行います。 ● ネットワーク、ストレージ、コンピュート容量など、カスタマーリソースの使用状況を監視します。自動スケーリング機能が有効にされていない場合は、クラスターリソースに必要な変更についてお客様に警告します (例: スケーリングする新規コンピュートノード、追加のストレージなど)。	● 提供される OpenShift Cluster Manager コントロールを使用して、必要に応じて追加のワーカーノードを追加または削除します。 ● クラスターリソース要件に関する Red Hat の通知に対応します。

3.2.2.3. アイデンティティーおよびアクセス管理

Identity and Access Management マトリックスには、クラスター、アプリケーション、およびインフラストラクチャーリソースへの承認されたアクセスを管理する責任が含まれます。これには、アクセス制御メカニズム、認証、および認可を提供し、リソースへのアクセスを管理するタスクが含まれます。

リソース	Red Hat の責任	お客様の責任

リソース	Red Hat の責任	お客様の責任
ロギング	• プラットフォーム監査ログについて、業界標準に基づく段階的な内部アクセスプロセスを順守します。 • ネイティブな OpenShift RBAC 機能を提供します。	• プロジェクトへのアクセス、およびプロジェクトのアプリケーションログへのアクセスを制御するように OpenShift RBAC を設定します。 • サードパーティーまたはカスタムのアプリケーションロギングソリューションについては、お客様がアクセス管理を行います。
アプリケーションのネットワーク	ネイティブ OpenShift RBAC および **dedicated-admin** 機能を提供します。	• OpenShift dedicated-admins および RBAC を、必要に応じてルート設定へのアクセスを制御するように設定します。 • Red Hat 組織が OpenShift Cluster Manager へのアクセス権限を付与する組織管理者を管理します。OpenShift Cluster Manager は、ルーターオプションを設定し、サービ出力ドバランサークォータを提供するために使用されます。
クラスターネットワーク	• OpenShift Cluster Manager を使用してお客様のアクセス制御を提供します。 • ネイティブ OpenShift RBAC および **dedicated-admin** 機能を提供します。	• Red Hat アカウントの Red Hat 組織のメンバーシップを管理します。 • Red Hat 組織が OpenShift Cluster Manager へのアクセス権限を付与する組織管理者を管理します。 • OpenShift dedicated-admins および RBAC を、必要に応じてルート設定へのアクセスを制御するように設定します。
仮想ネットワーク	OpenShift Cluster Manager を使用してお客様のアクセス制御を提供します。	OpenShift Cluster Manager を使用してパブリッククラウドコンポーネントへの任意のユーザーアクセスを管理します。

3.2.2.4. セキュリティーおよび規制コンプライアンス

以下は、コンプライアンスに関連する責任および管理について示しています。

リソース	Red Hat の責任	お客様の責任
ロギング	セキュリティーイベントについて分析するために、クラスターの監査ログを Red Hat SIEM に送信します。フォレンジック分析をサポートするために、定義された期間の監査ログを保持します。	セキュリティーイベントのアプリケーションログを分析します。デフォルトのロギングスタックで指定されるよりも長い保持期間が必要な場合に、ロギングサイドカーコンテナーまたはサードパーティーのロギングアプリケーション経由でアプリケーションログを外部エンドポイントに送信します。
仮想ネットワーク	● 潜在的な問題やセキュリティーの脅威について、仮想ネットワークのコンポーネントを監視します。 ● 追加のパブリッククラウドプロバイダーツールを活用して、追加の監視および保護を行います。	● 潜在的な問題やセキュリティーの脅威について、任意で設定された仮想ネットワークのコンポーネントを監視します。 ● 必要に応じて、必要なファイアウォールルールまたはデータセンターの保護を設定します。

3.2.2.5. 障害復旧

障害復旧には、データおよび設定のバックアップ、障害復旧環境へのデータおよび設定の複製、および障害イベント発生時のフェイルオーバーが含まれます。

リソース	Red Hat の責任	お客様の責任
仮想ネットワーク	プラットフォームが機能するために必要な、影響を受けた仮想ネットワークコンポーネントを復元するか、再作成します。	● パブリッククラウドプロバイダーが推奨されるように、障害に対する保護のために、可能な場合は複数のトンネルで仮想ネットワーク接続を設定します。 ● 複数のクラスターでグローバルロードバランサーを使用する場合は、フェイルオーバー DNS および負荷分散を維持します。

3.2.3. データおよびアプリケーションに関するお客様の責任

お客様は、OpenShift Dedicated にデプロイするアプリケーション、ワークロード、およびデータに責任を負います。ただし、Red Hat は、お客様がプラットフォームでデータおよびアプリケーションを管理するのに役立つ各種ツールを提供します。

リソース	Red Hat の責任	お客様の責任
お客様データ	● データ暗号化のプラットフォームレベルの標準を維持します。 ● シークレットなどのアプリケーションデータの管理に役立つ OpenShift コンポーネントを提供します。 ● サードパーティーのデータサービス (AWS RDS や Google Cloud SQL など) との統合を有効にして、クラスターやクラウドプロバイダー外にあるデータを保存し、管理します。	プラットフォームに保存されるすべてのお客様データと、お客様のアプリケーションがこのデータを使用し、公開する方法について責任を持ちます。

リソース	Red Hat の責任	お客様の責任
お客様のアプリケーション	● お客様が OpenShift および Kubernetes API にアクセスし、コンテナー化されたアプリケーションをデプロイし、管理できるように、OpenShift コンポーネントと共にクラスターをプロビジョニングします。 ● イメージプルシークレットでクラスターを作成し、お客様のデプロイメントで Red Hat Container Catalog レジストリーからイメージをプルできるようにします。 ● お客様が Operator を設定してコミュニティー、サードパーティー、および Red Hat サービスをクラスターに追加するために使用できる OpenShift API へのアクセスを提供します。 ● ストレージクラスとプラグインを提供し、お客様のアプリケーションで使用できるように永続ボリュームをサポートします。 ● お客様がクラスター上にアプリケーションコンテナーイメージを安全に保存し、アプリケーションをデプロイおよび管理できるようにコンテナーイメージレジストリーを提供します。	● お客様およびサードパーティーのアプリケーション、データ、およびそれらの完全なライフサイクルに関する責任を持ちます。 ● Operator または外部イメージを使用して Red Hat、コミュニティー、サードパーティー、お客様独自のサービス、またはその他のサービスをクラスターに追加する場合、お客様はこれらのサービスについてと、問題をトラブルシューティングするために適切なプロバイダー (Red Hat を含む) と連携します。 ● 提供されるツールおよび機能を使用して設定およびデプロイし、最新の状態に維持し、リソース要求および制限を設定し、アプリケーションを実行するのに十分なリソースを持つようにクラスターのサイズを設定し、パーミッションを設定し、他のサービスと統合し、お客様がデプロイするイメージストリームまたはテンプレートを管理し、外部に提供し、保存し、バックアップし、データを復元し、データを保存、バックアップし、復元し、さらに可用性と回復性の高いワークロードを管理します。 ● メトリクスを収集し、アラートを作成するためにソフトウェアをインストールし、操作することを含め、OpenShift Dedicated で実行されるアプリケーションのモニタリングについての責任を持ちます。

3.3. OPENSHIFT DEDICATED のプロセスおよびセキュリティーについて

3.3.1. インシデントおよびオペレーション管理

以下では、OpenShift Dedicated マネージドサービスにおける Red Hat の責任について詳しく説明します。

3.3.1.1. プラットフォームモニタリング

Red Hat Site Reliability Engineer (SRE) は、すべての OpenShift Dedicated クラスターコンポーネン

ト、SRE サービス、および基礎となるクラウドプロバイダーアカウントに関する一元管理されたモニタリングおよびアラートシステムを維持します。プラットフォーム監査ログは、集中 SIEM (Security Information and Event Monitoring) システムに安全に転送されます。この場合は、SRE チームに対して設定されたアラートがトリガーされる可能性があり、手動によるレビューの対象となります。監査ログは SIEM に 1 年間保持されます。指定されたクラスターの監査ログは、クラスターの削除時に削除されません。

3.3.1.2. インシデント管理

インシデントは、1 つ以上の Red Hat サービスの低下や停止をもたらすイベントです。インシデントは、お客様または Customer Experience and Engagement (CEE) メンバーによって、一元化されたモニタリングおよびアラートシステムにより直接、または SRE チームのメンバーから直接作成されます。

サービスおよびお客様への影響に応じて、インシデントは 重大度 に基づいて分類されます。

新しいインシデントが Red Hat によってどのように管理されるかの一般的なワークフロー:

1. SRE の最初の応答は新たなインシデントに警告され、最初の調査が開始されます。
2. 初回の調査後、インシデントには復旧作業を調整するインシデントのリードが割り当てられます。
3. インシデントのリードは、関連する通知やサポートケースの更新など、復旧に関するすべての通信および調整を管理します。
4. インシデントの復旧が行われます。
5. インシデントが文書化され、根本原因分析はインシデントの 5 営業日以内に行われます。
6. 根本原因分析 (RCA) のドラフトドキュメントは、インシデント発生の 7 営業日以内にお客様に共有されます。

3.3.1.3. 通知

プラットフォーム通知は、メールを使用して設定されます。お客様通知も、対応する Red Hat アカウントチームに送信され、該当する場合は Red Hat Technical Account Manager に送信されます。

以下のアクティビティーは通知をトリガーできます。

- プラットフォームのインシデント
- パフォーマンスの低下
- クラスター容量に関する警告
- 重大な脆弱性および解決
- アップグレードのスケジュール

3.3.1.4. バックアップおよび復元

すべての OpenShift Dedicated クラスターは、クラウドプロバイダーのスナップショットを使用してバックアップされます。特に、これには永続ボリュームに格納されているお客様のデータは含まれません。すべてのスナップショットは適切なクラウドプロバイダースナップショット API を使用して取得され、クラスターと同じアカウントでセキュアなオブジェクトストレージバケット (AWS の S3、および Google Cloud の GCS) にアップロードされます。

コンポーネント	スナップショットの頻度	保持期間	注記
完全なオブジェクトストアのバックアップ、すべてのクラスターの永続ボリューム (PV)	毎日	7 日	これは、etcd などのすべての Kubernetes オブジェクトとクラスター内のすべての PV の完全バックアップです。
	週次	30 日	
完全なオブジェクトストアのバックアップ	毎時	24 時間	これは、etcd などのすべての Kubernetes オブジェクトの完全バックアップです。このバックアップスケジュールでは、PV はバックアップされません。
ノードのルートボリューム	なし	該当なし	ノードは短期的なものと見なされます。ノードのルートボリュームには、何も保存できません。

- Red Hat は、RTO (Recovery Point Objective) または RTO (Recovery Time Objective) にコミットしません。
- お客様はデータのバックアップを定期的に行う必要があります。
- お客様は、Kubernetes のベストプラクティスに従ったワークロードでマルチ AZ クラスターをデプロイして、リージョン内の高可用性を確保する必要があります。
- クラウドリージョン全体が利用できない場合、お客様は新しいクラスターを異なるリージョンにインストールし、バックアップデータを使用してアプリケーションを復元する必要があります。

3.3.1.5. クラスター容量

クラスター容量の評価および管理に関する責任は、Red Hat とお客様との間で共有されます。Red Hat SRE は、クラスター上のすべてのコントロールプレーンおよびインフラストラクチャーノードの容量に関する責任を負います。

Red Hat SRE はアップグレード時に、またクラスターのアラートへの対応としてクラスター容量の評価も行います。クラスターアップグレードの容量に与える影響は、アップグレードのテストプロセスの一部として評価され、容量がクラスターへの新たな追加内容の影響を受けないようにします。クラスターのアップグレード時にワーカーノードが追加され、クラスターの容量全体がアップグレードプロセス時に維持されるようにします。

SRE のスタッフによる容量評価は、クラスターからのアラートへの対応も行われます。また、使用状況のしきい値が一定期間を超えると、SRE スタッフによる容量の評価も行われます。このようなアラートにより、通知がお客様に出される可能性があります。

3.3.2. 変更管理

このセクションでは、クラスターおよび設定変更、パッチ、およびリリースの管理方法に関するポリシーについて説明します。

3.3.2.1. お客様が開始する変更

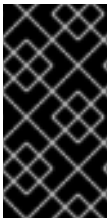
クラスターデプロイメント、ワーカーノードのスケーリング、またはクラスターの削除などのセルフサービス機能を使用して変更を開始できます。

変更履歴は、OpenShift Cluster Manager の **概要タブ** の **クラスター履歴** セクションにキャプチャーされ、表示できます。変更履歴には、以下の変更のログが含まれますが、これに限定されません。

- アイデンティティープロバイダーの追加または削除
- **dedicated-admins** グループへの/からのユーザーの追加または削除
- クラスターコンピュートノードのスケーリング
- クラスターロードバランサーのスケーリング
- クラスター永続ストレージのスケーリング
- クラスターのアップグレード

以下のコンポーネントの OpenShift Cluster Manager での変更を回避することで、メンテナーンスの除外を実装できます。

- クラスターの削除
- ID プロバイダーの追加、変更、または削除
- 昇格されたグループからのユーザーの追加、変更、または削除
- アドオンのインストールまたは削除
- クラスターネットワーク設定の変更
- マシンプールの追加、変更、または削除
- ユーザーワークロードの監視の有効化または無効化
- アップグレードの開始



重要

メンテナンスの除外を適用するには、マシンプールの自動スケーリングまたは自動アップグレードポリシーが無効になっていることを確認してください。メンテナンスの除外が解除されたら、必要に応じてマシンプールの自動スケーリングまたは自動アップグレードポリシーを有効にします。

3.3.2.2. Red Hat が開始する変更

Red Hat サイトリライアビリティエンジニアリング (SRE) は、GitOps ワークフローと完全に自動化された CI/CD パイプラインを使用して、OpenShift Dedicated のインフラストラクチャー、コード、および設定を管理します。このプロセスにより、Red Hat は、お客様に悪影響を与えることなく、継続的にサービスの改善を安全に導入できます。

提案されるすべての変更により、チェック時にすぐに一連の自動検証が実行されます。変更は、自動統合テストが実行されるステージング環境にデプロイされます。最後に、変更は実稼働環境にデプロイされます。各ステップは完全に自動化されます。

認可された SRE レビュー担当者は、各ステップに進む前にこれを承認する必要があります。変更を提案した個人がレビュー担当者になることはできません。すべての変更および承認は、GitOps ワークフローの一部として完全に監査可能です。

一部の変更は、機能フラグを使用して指定されたクラスターまたはお客様に対する新機能の可用性を制御することで、段階的にリリースされます。

3.3.2.3. パッチ管理

OpenShift Container Platform ソフトウェアおよび基礎となるイミュータブルな Red Hat Enterprise Linux CoreOS (RHCOS) オペレーティングシステムイメージには、通常の z-stream アップグレードのバグおよび脆弱性のパッチが適用されます。OpenShift Container Platform ドキュメントの RHCOS アーキテクチャー を参照してください。

3.3.2.4. リリース管理

Red Hat はクラスターを自動的にアップグレードしません。OpenShift Cluster Manager Web コンソールを使用して、クラスターの更新を定期的に (定期的なアップグレード) または 1 回だけ (個別にアップグレード) 行うようにスケジュールできます。クラスターが重大な影響を与える CVE の影響を受ける場合にのみ、Red Hat はクラスターを新しい z-stream バージョンに強制的にアップグレードする可能性があります。お客様は OpenShift Cluster Manager Web コンソールで、すべてのクラスターアップグレードイベントの履歴を確認できます。リリースの詳細は、ライフサイクルポリシー を参照してください。

3.3.3. アイデンティティーおよびアクセス管理

Red Hat Site Reliability Engineering (SRE) チームによるアクセスのほとんどは、自動化された設定管理によりクラスター Operator を使用して行われます。

3.3.3.1. サブプロセッサー

利用可能なサブプロセスの一覧は、Red Hat カスタマーポータルの Red Hat Subprocessor List を参照してください。

3.3.3.2. SRE のすべての OpenShift Dedicated クラスターへのアクセス

SRE は、プロキシーを介して OpenShift Dedicated クラスターにアクセスします。プロキシーは、SRE がログインするときに、OpenShift Dedicated クラスター内のサービスアカウントをミントします。OpenShift Dedicated クラスター用に ID プロバイダーが設定されていないため、SRE はローカル Web コンソールコンテナーを実行してプロキシーにアクセスします。SRE は、クラスター Web コンソールに直接アクセスしません。SRE は、監査可能性を確保するために、個々のユーザーとして認証する必要があります。すべての認証試行は、セキュリティー情報およびイベント管理 (SIEM) システムに記録されます。

3.3.3.3. OpenShift Dedicated の特権アクセスの制御

Red Hat SRE は、OpenShift Dedicated およびパブリッククラウドプロバイダーのコンポーネントにアクセスする場合の最小限の権限の原則に従います。手動による SRE アクセスには、基本的に以下の 4 つのカテゴリーがあります。

- 通常の 2 要素認証を使用するが、権限の昇格のない Red Hat カスタマーポータル経由での SRE の管理者アクセス。
- 通常の 2 要素認証があり、権限の昇格のない Red Hat の企業 SSO を使用した SRE の管理者アクセス。

- OpenShift の昇格。これは Red Hat SSO を使用した手動による昇格です。これは完全に監査されており、SRE が行うすべての操作には管理者の承認が必要です。
- クラウドプロバイダーコンソールまたは CLI アクセスの手動昇格である、クラウドプロバイダーのアクセスまたは昇格。アクセスは 60 分間に制限され、完全に監査されます。

これらのアクセスタイプのそれぞれには、コンポーネントへの異なるレベルのアクセスがあります。

コンポーネント	通常の SRE 管理者アクセス (Red Hat カスタマーポータル)	通常の SRE 管理者アクセス (Red Hat SSO)	OpenShift の昇格	クラウドプロバイダーのアクセス
OpenShift Cluster Manager	R/W	アクセスなし	アクセスなし	アクセスなし
OpenShift Web コンソール	アクセスなし	R/W	R/W	アクセスなし
ノードのオペレーティングシステム	アクセスなし	昇格した OS およびネットワークのパーミッションの一覧。	昇格した OS およびネットワークのパーミッションの一覧。	アクセスなし
AWS コンソール	アクセスなし	アクセスはありませんが、これはクラウドプロバイダーのアクセスを要求するために使用されるアカウントです。	アクセスなし	SRE アイデンティティーを使用したすべてのクラウドプロバイダーのパーミッション。

3.3.3.4. SRE のクラウドインフラストラクチャーアカウントへのアクセス

Red Hat の担当者は、通常の OpenShift Dedicated 操作ではクラウドインフラストラクチャーアカウントにアクセスしません。緊急のトラブルシューティングの目的で、Red Hat SRE にはクラウドインフラストラクチャーアカウントにアクセスするための明確に定義された監査可能な手順があります。

AWS では、SRE は AWS Security Token Service (STS) を使用して **BYOCAdminAccess** ユーザーの有効期限の短い AWS アクセストークンを生成します。STS トークンへのアクセスは監査ログに記録され、個別のユーザーまでトレースできます。**BYOCAdminAccess** には **AdministratorAccess** IAM ポリシーが割り当てられます。

Google Cloud では、SRE は Red Hat SAML アイデンティティープロバイダー (IDP) に対して認証された後にリソースにアクセスします。IDP は、生存期間のあるトークンを承認します。トークンの発行は、企業の Red Hat IT により監査可能で、個別のユーザーにリンクされます。

3.3.3.5. Red Hat サポートのアクセス

通常、Red Hat CEE チームメンバーは、クラスターの一部に対する読み取り専用アクセスを持ちます。特に、CEE にはコアおよび製品の namespace への制限されたアクセスがありますが、お客様の namespace にはアクセスできません。

ロール	コア namespace	階層化した製品 namespace	お客様の namespace	クラウドインフラストラクチャーアカウント*
OpenShift SRE	読み取り: All 書き込み: Very 限定的 [1]	読み取り: All 書き込み: None	読み取り: None[2] 書き込み: None	読み取り: All [3] 書き込み: All [3]
CEE	読み取り: All 書き込み: None	読み取り: All 書き込み: None	読み取り: None[2] 書き込み: None	読み取り: None 書き込み: None
お客様管理者	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: All 書き込み: All	読み取り: Limited[4] 書き込み: Limited[4]
お客様ユーザー	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: Limited[5] 書き込み: Limited[5]	読み取り: None 書き込み: None
上記以外	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: None 書き込み: None

Cloud Infrastructure Account は基礎となる AWS または Google Cloud アカウントを参照します。

1. デプロイメントの失敗、クラスターのアップグレード、および適切でないワーカーノードの置き換えなどの一般的なユースケースに対応することに限定されます。
2. Red Hat は、デフォルトではお客様のデータにアクセスできません。
3. SRE のクラウドインフラストラクチャーアカウントへのアクセスは、文書化されたインシデントの発生時の例外的なトラブルシューティングのための break-glass 手順です。
4. 顧客管理者は、Cloud Infrastructure Access を通じてクラウドインフラストラクチャーアカウントコンソールへのアクセスが限定されます。
5. 顧客管理者によって RBAC で許可される内容や、ユーザーが作成した namespace に限定されます。

3.3.3.6. お客様のアクセス

お客様のアクセスは、お客様によって作成される namespace および顧客管理者ロールによって RBAC を使用して付与されるパーミッションに限定されます。基礎となるインフラストラクチャーまたは製品

namespace へのアクセスは通常、**cluster-admin** アクセスなしでは許可されません。お客様のアクセスおよび認証の詳細は、本書の認証に関するセクションを参照してください。

3.3.3.7. アクセスの承認およびレビュー

新規の SRE ユーザーアクセスには、管理者の承認が必要です。分離された SRE アカウントまたは転送された SRE アカウントは、自動化されたプロセスで認可されたユーザーとして削除されます。さらに、SRE は、許可されたユーザー一覧の管理のサインオフを含む定期的なアクセスレビューを実行します。

3.3.4. セキュリティーおよび規制コンプライアンス

セキュリティーおよび規制コンプライアンスには、セキュリティー管理の実装やコンプライアンス認定などのタスクが含まれます。

3.3.4.1. データの分類

Red Hat は、データの機密性を判断し、収集、使用、送信、保存、処理中にそのデータの機密性および整合性に対する固有のリスクを強調表示するために、データ分類標準を定義し、フォローします。お客様が所有するデータは、最高レベルの機密性と処理要件に分類されます。

3.3.4.2. データ管理

OpenShift Dedicated は、AWS Key Management Service (KMS) や Google Cloud KMS などのクラウドプロバイダーサービスを使用して、永続データの暗号化キーを安全に管理します。これらのキーは、すべてのコントロールプレーン、インフラストラクチャー、およびワーカーノードのルートボリュームを暗号化するのに使用されます。お客様は、インストール時にルートボリュームを暗号化するための独自の KMS キーを指定できます。永続ボリューム (PV) も、キー管理に KMS を使用します。お客様は、KMS キーの Amazon リソース名 (ARN) または ID を参照する新しい **StorageClass** を作成することにより、PV を暗号化するための独自の KMS キーを指定できます。

お客様が OpenShift Dedicated クラスターを削除すると、コントロールプレーンのデータボリュームや、永続ボリューム (PV) などのお客様のアプリケーションデータボリュームを含め、すべてのクラスターのデータが永久に削除されます。

3.3.4.3. 脆弱性管理

Red Hat は業界標準ツールを使用して OpenShift Dedicated の定期的な脆弱性スキャンを実行します。特定された脆弱性は、重大度に基づくタイムラインに応じて修復で追跡されます。コンプライアンス認定監査の過程で、脆弱性スキャンと修復のアクティビティーが文書化され、サードパーティーの評価者による検証が行われます。

3.3.4.4. ネットワークセキュリティー

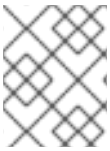
3.3.4.4.1. ファイアウォールおよび DDoS 保護

各 OpenShift Dedicated クラスターは、ファイアウォールルール (AWS Security Groups または Google Cloud Compute Engine ファイアウォールルール) を使用して、クラウドインフラストラクチャーレベルでセキュアなネットワーク設定で保護されます。AWS の OpenShift Dedicated のお客様は、AWS Shield Standard による DDoS 攻撃に対する保護されます。

3.3.4.4.2. プライベートクラスターおよびネットワーク接続

必要に応じて、OpenShift Dedicated クラスターエンドポイント (Web コンソール、API、およびアプリケーションルーター) をプライベートに設定し、クラスターのコントロールプレーンまたはアプリケーションがインターネットからアクセスできないようにできます。

AWS の場合、お客様は AWS VPC のピアリング、AWS VPN、または AWS Direct Connect を使用して OpenShift Dedicated クラスターへのプライベートネットワーク接続を設定できます。



注記

現時点では、プライベートクラスターは Google Cloud の OpenShift Dedicated クラスターではサポートされません。

3.3.4.4.3. クラスターのネットワークアクセス制御

粒度の細かいネットワークアクセス制御ルールは、お客様が、**NetworkPolicy** オブジェクトおよび OpenShift SDN を使用してプロジェクトごとに設定できます。

3.3.4.5. ペネトレーションテスト

Red Hat は、OpenShift Dedicated に対して定期的なペネトレーションテストを実行します。テストは、業界標準ツールおよびベストプラクティスを使用して独立した内部チームによって実行されます。

検出される問題は、重大度に基づいて優先されます。オープンソースプロジェクトに属する問題については、解決のためにコミュニティーと共有されます。

3.3.4.6. コンプライアンス

OpenShift Dedicated は、セキュリティーおよび管理に関する一般的な業界のベストプラクティスに従います。認定の概要を以下の表に示します。

表3.2 OpenShift Dedicated のセキュリティーおよびコントロール認定

認定	AWS 専用の OpenShift	GCP 専用の OpenShift
ISO 27001	はい	はい
PCI DSS	はい	はい
SOC 2 タイプ 2	はい	はい

関連情報

- SRE の常駐に関する詳細は、Red Hat Subprocessor List を参照してください。

3.3.5. 障害復旧

OpenShift Dedicated は、Pod、ワーカーノード、インフラストラクチャーノード、コントロールプレーンノード、およびアベイラビリティーゾーンレベルで発生する障害について障害復旧を行います。

すべての障害復旧では、必要な可用性レベルを確保するために、可用性の高いアプリケーション、ストレージ、およびクラスターアーキテクチャー (例: 単一ゾーンデプロイメント対マルチゾーンデプロイメント) をデプロイする上でベストプラクティスを使用する必要があります。

1 つの単一ゾーンクラスターは、アベイラビリティーゾーンやリージョンが停止した場合に、災害回避や復旧を行うことはできません。お客様によってメンテナーンスされるフェイルオーバーが設定される複数の単一ゾーンクラスターは、ゾーンまたはリージョンレベルで停止に対応できます。

1 つのマルチゾーンクラスターは、リージョンが完全に停止した場合に障害を防止したり、リカバリーを行ったりしません。お客様によってメンテナーンスされるフェイルオーバーが設定される複数のマルチゾーンクラスターは、リージョンレベルで停止に対応できます。

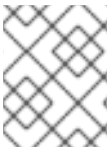
3.4. OPENSHIFT DEDICATED の可用性について

可用性と障害回避は、どのアプリケーションプラットフォームでも非常に重要な要素です。OpenShift Dedicated は複数のレベルで障害に対する保護を提供しますが、お客様がデプロイするアプリケーションは高可用性を確保するために適切に設定される必要があります。さらに、複数のアベイラビリティーゾーンにクラスターをデプロイしたり、フェイルオーバーメカニズムで複数のクラスターを維持したりするなど、その他のオプションが生じる可能性のあるクラウドプロバイダーの停止に対応するため、いくつかのオプションを利用できます。

3.4.1. 潜在的な障害点

OpenShift Container Platform は、ダウンタイムに対してワークロードを保護するために多くの機能とオプションを提供しますが、アプリケーションはこれらの機能を利用できるように適切に設計される必要があります。

OpenShift Dedicated は、Red Hat Site Reliability Engineer (SRE) サポートと、マルチゾーンクラスターをデプロイするオプションを追加することで、Kubernetes の数多くの一般的な問題からさらに保護しますが、コンテナーまたはインフラストラクチャーが引き続き失敗できる数多くの方法を利用できます。潜在的な障害点を理解することで、リスクを理解し、アプリケーションとクラスターの両方が特定のレベルで必要に応じて回復性を持つように設計できます。



注記

停止状態は、インフラストラクチャーおよびクラスターコンポーネントの複数の異なるレベルで生じる可能性があります。

3.4.1.1. コンテナーまたは Pod の障害

設計上、Pod は短期間存在することが意図されています。アプリケーション Pod の複数のインスタンスが個別の Pod またはコンテナーの問題から保護されるように、サービスを適切にスケーリングします。ノードスケジューラーは、回復性をさらに強化するために、これらのワークロードが異なるワーカーノードに分散されるようにすることもできます。

Pod の障害に対応する場合は、ストレージがアプリケーションに割り当てられる方法も理解することが重要になります。単一 Pod に割り当てられる単一の永続ボリュームは、Pod のスケーリングを完全に活用できませんが、複製されるデータベース、データベースサービス、または共有ストレージは使用できます。

アップグレードなど、計画メンテナーンス中にアプリケーションが中断されるのを防ぐには、Pod の停止状態の予算を定義することが重要です。これらは Kubernetes API の一部で、他のオブジェクトタイプと同様に OpenShift CLI (**oc**) で管理できます。この設定により、メンテナーンスのためのノードのドレイン (解放) などの操作時に Pod への安全面の各種の制約を指定できます。

3.4.1.2. ワーカーノードの障害

ワーカーノードは、アプリケーション Pod が含まれる仮想マシンです。デフォルトで、OpenShift Dedicated クラスターには単一アベイラビリティーゾーンクラスター用のワーカーノードが 4 つ以上含

まれます。ワーカーノードに障害が発生した場合、Pod は、既存ノードに関する問題が解決するか、ノードが置き換えられるまで、十分な容量がある限り、機能しているワーカーノードに移行します。ワーカーノードを追加することは、単一ノードの停止に対する保護を強化し、ノードに障害が発生した場合に再スケジュールされた Pod の適切なクラスター容量を確保します。

注記

ノードの障害に対応する場合、ストレージへの影響を把握することも重要になります。

3.4.1.3. クラスターの障害

OpenShift Dedicated クラスターには、選択したクラスタータイプに応じて、単一ゾーンまたはマルチゾーンのいずれかで、高可用性を確保するために事前設定された 3 つ以上のコントロールプレーンノードと 3 つのインフラストラクチャーノードがあります。つまり、コントロールプレーンノードとインフラストラクチャーノードはワーカーノードの回復性と同じ耐障害性を持ち、Red Hat によって完全に管理される利点を活用できます。

コントロールプレーンノードが完全に停止する場合、OpenShift API は機能せず、既存のワーカーノード Pod は影響を受けません。ただし、Pod またはノードが同時に停止している場合、コントロールプレーンノードは新規 Pod またはノードを追加またはスケジュールする前に復元する必要があります。

インフラストラクチャーノードで実行しているすべてのサービスは、高可用性を持ち、インフラストラクチャーノード間に分散されるように Red Hat によって設定されます。インフラストラクチャーが完全に停止すると、これらのノードが回復するまで、これらのサービスは利用できなくなります。

3.4.1.4. ゾーンの障害

パブリッククラウドプロバイダーからのゾーン障害は、ワーカーノード、ブロックまたは共有ストレージ、および単一のアベイラビリティーゾーンに固有のロードバランサーなどのすべての仮想コンポーネントに影響を与えます。ゾーンの障害から保護するために、OpenShift Dedicated は、マルチアベイラビリティーゾーンクラスターと呼ばれる 3 つのアベイラビリティーゾーンに分散されるクラスターのオプションを提供します。既存のステートレスワークロードは、十分な容量がある限り、停止時に影響を受けないゾーンに再分散されます。

3.4.1.5. ストレージの障害

ステートフルなアプリケーションをデプロイしている場合、ストレージは重要なコンポーネントであり、高可用性を検討する際に考慮に入れる必要があります。単一ブロックストレージ PV は、Pod レベルでも停止状態になった状態では実行できません。ストレージの可用性を維持する最適な方法として、複製されたストレージソリューション、停止による影響を受けない共有ストレージ、またはクラスターから独立したデータベースサービスを使用できます。

3.5. OPENSHIFT DEDICATED の更新ライフサイクル

3.5.1. 概要

Red Hat は、お客様およびパートナー各社がプラットフォームで実行するアプリケーションの計画、デプロイ、サポートを効果的に行えるように、OpenShift Dedicated の製品ライフサイクルを公開しています。Red Hat は、可能な限りの透明性を実現するためにこのライフサイクルを公開していますが、問題が発生した場合はこれらのポリシーに例外を設ける場合もあります。

OpenShift Dedicated は Red Hat OpenShift のマネージドインスタンスであり、独立したリリーススケジュールを維持します。マネージドオファリングの詳細は、OpenShift Dedicated のサービス定義を参照してください。特定バージョンのセキュリティーアドバイザリーおよびバグ修正アドバイザリーは、

Red Hat OpenShift Container Platform のライフサイクルポリシーに基づいて利用可能となり、OpenShift Dedicated のメンテナーンススケジュールに基づいて提供されます。

関連情報

- OpenShift Dedicated サービス定義

3.5.2. 定義

表3.3 バージョン参照

バージョンの形式	メジャー	マイナー	パッチ	major.minor.patch
	x	y	z	x.y.z
例	4	5	21	4.5.21

メジャーリリースまたは X リリース

メジャーリリース または **X リリース** (X.y.z) としてのみ言及されます。

例

- "メジャーリリース 5" → 5.y.z
- "メジャーリリース 4" → 4.y.z
- "メジャーリリース 3" → 3.y.z

マイナーリリースまたは Y リリース

マイナーリリース または **Y リリース** (x.Y.z) としてのみ言及されます。

例

- "マイナーリリース 4" → 4.4.z
- "マイナーリリース 5" → 4.5.z
- "マイナーリリース 6" → 4.6.z

パッチリリースまたは Z リリース

パッチリリース または **Z リリース** (x.y.Z) としてのみ言及されます。

例

- "マイナーリリース 5 のパッチリリース 14" → 4.5.14
- "マイナーリリース 5 のパッチリリース 25" → 4.5.25
- "マイナーリリース 6 のパッチリリース 26" → 4.6.26

3.5.3. メジャーバージョン (X.y.z)

OpenShift Dedicated のメジャーバージョン (例: バージョン 4 など) は、後続のメジャーバージョンのリリースまたは製品の終了後 1 年間サポートされます。

例

- OpenShift Dedicated バージョン 5 が 1 月 1 日に利用可能になる場合、バージョン 4 は 12 月 31 日までの 12 カ月間、マネージドクラスターで継続して稼働させることができます。その後、クラスターはバージョン 5 にアップグレードまたは移行する必要があります。

3.5.4. マイナーバージョン (x.Y.z)

OpenShift Container Platform 4.8 のマイナーバージョン以降、Red Hat は、該当のマイナーバージョンの一般提供後 14 カ月間、すべてのマイナーバージョンをサポートします。パッチバージョンは、14 か月のサポート期間の影響を受けません。

14 カ月間の終了 60 日、30 日、および 15 日前に、お客様は通知を受けます。クラスターは 14 カ月間が終了する前にサポート対象のマイナーバージョンにアップグレードする必要があります。アップグレードしないと、クラスターは限定的なサポートのステータスになります。

例

1. 現時点で、お客様のクラスターは 4.8.14 で実行しているとします。4.8 マイナーバージョンは、2021 年 7 月 27 日に一般提供されました。
2. 2022 年 7 月 29 日、8 月 28 日、および 9 月 12 日に、クラスターがまだサポート対象のマイナーバージョンにアップグレードされていない場合、2022 年 9 月 27 日にクラスターが「制限付きサポート」ステータスになることがお客様に通知されます。
3. クラスターは、2022 年 9 月 27 日までに 4.9 以降にアップグレードする必要があります。
4. アップグレードが実行されていない場合、クラスターには限定的なサポートのステータスのフラグが設定されます。

3.5.5. パッチバージョン (x.y.Z)

マイナーバージョンがサポートされる期間中、とくに指定がない限り、Red Hat はすべての OpenShift Container Platform パッチバージョンをサポートします。

プラットフォームのセキュリティーおよび安定性の理由から、あるパッチリリースが非推奨になる可能性があります。この場合は、そのリリースのインストールができなくなり、そのリリースからの強制的なアップグレードが必要となります。

例

1. 4.7.6 に重要な CVE が含まれることが確認されるとします。
2. CVE の影響を受けるすべてのリリースは、サポートされるパッチリリースの一覧から削除されます。さらに、4.7.6 を実行するクラスターについては、自動アップグレードのスケジュールが 48 時間以内に行われます。

3.5.6. 限定的なサポートのステータス

クラスターが **限定サポート** ステータスに移行すると、Red Hat はクラスターをプロアクティブに監視

しなくなり、SLA は適用されなくなり、SLA に対して要求されたクレジットは拒否されます。製品サポートがなくなったという意味ではありません。場合によっては、違反要因を修正すると、クラスターが完全にサポートされた状態に戻ることがあります。ただし、それ以外の場合は、クラスターを削除して再作成する必要があります。

クラスターは、次のシナリオなど、さまざまな理由で限定サポートステータスに移行する場合があります。

サポート終了日までにクラスターをサポートされるバージョンにアップグレードしない場合

Red Hat は、サポート終了日以降のバージョンについて、ランタイムまたは SLA を保証しません。継続的なサポートを受けるには、サポートが終了する前に、クラスターを、サポートされているバージョンにアップグレードしてください。有効期限が切れる前にクラスターをアップグレードしない場合、クラスターは、サポートされているバージョンにアップグレードされるまで、限定サポートステータスに移行します。

Red Hat は、サポートされていないバージョンからサポートされているバージョンにアップグレードするための商業的に合理的なサポートを提供します。ただし、サポートされるアップグレードパスが利用できなくなった場合は、新規クラスターを作成し、ワークロードを移行することが必要になることがあります。

ネイティブの OpenShift Dedicated コンポーネント、または Red Hat によってインストールおよび管理されているその他のコンポーネントを削除または交換した場合

クラスター管理者パーミッションを使用した場合、Red Hat は、インフラストラクチャーサービス、サービスの可用性、またはデータ損失に影響を与えるアクションを含む、ユーザーまたは認可されたユーザーのアクションに対して責任を負いません。Red Hat がそのようなアクションを検出した場合、クラスターは限定サポートステータスに移行する可能性があります。Red Hat はステータスの変更を通知します。アクションを元に戻すか、サポートケースを作成して、クラスターの削除と再作成が必要になる可能性のある修復手順を検討する必要があります。

クラスターが限定サポートステータスに移行する可能性のある特定のアクションについて質問がある場合、またはさらに支援が必要な場合は、サポートチケットを作成します。

3.5.7. サポート対象バージョンの例外ポリシー

Red Hat は、事前通知なしに新規または既存のバージョンを追加または削除したり、実稼働環境に影響を与える重要なバグまたはセキュリティーの問題があることが確認された今後のマイナーリリースバージョンを遅延させる権利を留保します。

3.5.8. インストールポリシー

Red Hat は、最新のサポートリリースのインストールを推奨していますが、OpenShift Dedicated は前述のポリシーに記載されているサポート対象のリリースのインストールをサポートします。

3.5.9. 必須アップグレード

Critical (重大) または Important (重要) の CVE、または Red Hat が特定するその他のバグが、クラスターのセキュリティーまたは安定性に大幅に影響を与える場合、お客様は 2 営業日 以内にサポート対象の次のパッチリリースにアップグレードする必要があります。

極端な場合、また Red Hat による CVE の環境に対する重大度の評価に基づき、次のサポート対象のパッチリリースへのアップグレードが通知後 2 営業日 以内に実行されていない場合に、セキュリティー違反または不安定な状態が発生する可能性を軽減するために、クラスターは最新のパッチリリースに自動的に更新されます。

3.5.10. ライフサイクルの日付

バージョン	一般公開	ライフサイクルの終了日
4.11	2022 年 8 月 10 日	2023 年 10 月 10 日
4.10	2022 年 3 月 10 日	2023 年 5 月 10 日
4.9	2021 年 10 月 18 日	2022 年 12 月 18 日
4.8	2021 年 7 月 27 日	2022 年 9 月 27 日

第4章 サポート

OpenShift Dedicated のサポートを取得します。

4.1. 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 Hybrid Cloud Console 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。

4.2. 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、および動画で設定されています。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。

4.3. 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。

4.4. サポートケースの送信

前提条件

- Red Hat OpenShift Cluster Manager にアクセスできる。
- 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、**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 **OpenShift Dedicated**) 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 Cluster Manager Hybrid Cloud Console 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. **Clusters** 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。
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。

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。

4.5. 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。