OpenShift Container Platform 4.18

OCI へのインストール

Oracle Cloud Infrastructure への OpenShift Container Platform のインストール

Last Updated: 2025-11-20

OpenShift Container Platform 4.18 OCI へのインストール

Oracle Cloud Infrastructure への OpenShift Container Platform のインストール

Abstract

このドキュメントでは、Oracle Cloud Infrastructure に OpenShift Container Platform をインストールする方法を説明します。

Table of Contents

第1章 ASSISTED INSTALLER を使用して ORACLE CLOUD INFRASTRUCTURE (OCI) にクラスターをインストールする

Assisted Installer を使用して、Oracle® Cloud Infrastructure (OCI) にクラスターをインストールできます。この方法はほとんどのユーザーに推奨されます。インターネット接続が必要です。

クラスターを手動でセットアップする場合、他の自動化ツールを使用する場合、または非接続環境で作業する場合は、インストールに Red Hat Agent-based Installer を使用できます。詳細は、Agent-based Installer を使用して Oracle Cloud Infrastructure (OCI) にクラスターをインストールする を参照してください。

注記

Oracle Cloud Infrastructure (OCI) の任意のリージョンと同じように、Dedicated Region (Oracle ドキュメント) に OpenShift Container Platform をデプロイできます。

1.1. ASSISTED INSTALLER と OCI の統合について

専用、ハイブリッド、パブリックおよびマルチクラウド環境をサポートする Oracle® Cloud Infrastructure (OCI) インフラストラクチャー上でクラスターワークロードを実行できます。Red Hat と Oracle はどちらも、OCI 上の OpenShift Container Platform クラスターでの OCI の実行をテスト、検証、サポートしています。

このセクションでは、Assisted Installer を使用して OCI プラットフォームに OpenShift Container Platform クラスターをインストールする方法を説明します。このインストールにより、Oracle Cloud Controller Manager (CCM) や Oracle Container Storage Interface (CSI) などのクラウドネイティブコンポーネントがデプロイされます。また、インスタンスノード、ロードバランサー、ストレージなどの OCI API リソースとクラスターが統合されます。

インストールプロセスでは、Red Hat が提供する OpenShift Container Platform 検出 ISO イメージと、OCI が提供および管理するスクリプトおよびマニフェストを使用します。

1.1.1. インストール前の考慮事項

Oracle Cloud Infrastructure (OCI) に OpenShift Container Platform をインストールする前に、次の設定の選択を検討する必要があります。

デプロイメントプラットフォーム

OpenShift Container Platform と Oracle Cloud Infrastructure (OCI) の統合は、仮想マシン (VM) とベアメタル (BM) マシンの両方で認定されています。iSCSI ブートドライブを使用したベアメタルインストールには、Oracle が提供する Terraform スタックで自動的に作成されるセカンダリーの仮想 NIC が必要です。

仮想マシン (VM) またはベアメタル (BM) マシンを作成する前に、関連する OCI シェイプを特定する必要があります。詳細は、次のリソースを参照してください。

- Cloud instance types (Red Hat Ecosystem Catalog ポータル)

VPU のサイズ設定に関する推奨事項

OCI 上で動作するクラスターワークロードに最適なパフォーマンス条件を確保するために、ブロックボリュームのボリュームパフォーマンスユニット (VPU) がワークロードに適したサイズに設定されていることを確認してください。次のリストを参考に、特定のパフォーマンスニーズに応じて必要な VPU を選択してください。

- テストまたは概念実証環境: 100 GB、20 - 30 VPU。
- 基本的な環境: 500 GB、60 VPU
- 高負荷の実稼働環境: 500 GB 以上、100 以上の VPU

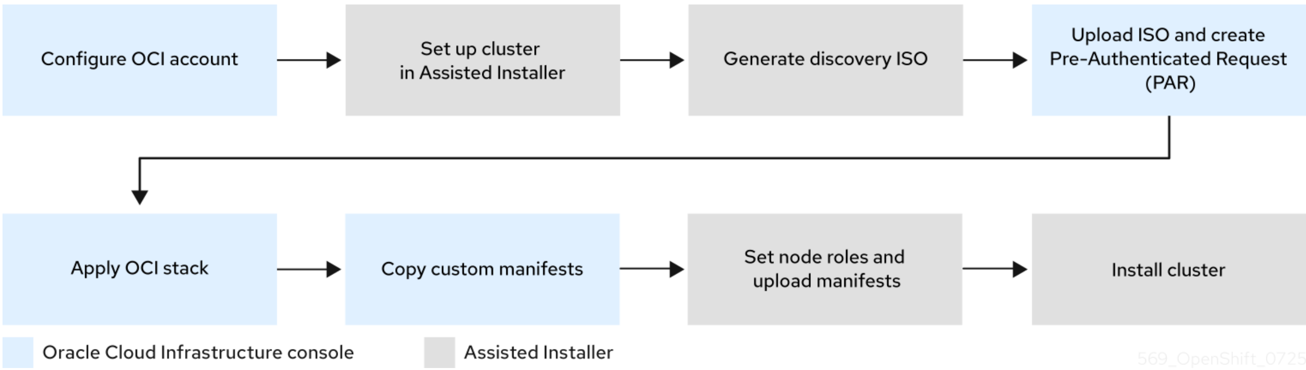
更新やスケーリングアクティビティーに十分な容量を提供できるように、VPU を余分に確保しておくことを検討してください。VPU の詳細は、Volume Performance Units (Oracle ドキュメント) を参照してください。

インスタンスのサイズ設定に関する推奨事項

OpenShift Container Platform ノードのコンピュートインスタンスの CPU、メモリー、VPU、およびボリュームサイズの推奨値を確認してください。詳細は、Instance Sizing Recommendations for OpenShift Container Platform on OCI Nodes (Oracle ドキュメント) を参照してください。

1.1.2. ワークフロー

図1.1 接続環境で Assisted Installer を使用して OCI にクラスターをインストールするための概略的なワークフロー



インターネット接続環境で Assisted Installer を使用して OCI にクラスターをインストールする手順を次に示します。

1. OCI コンソールで、クラスターをホストする OCI アカウントを設定します。
    a. 既存のコンパートメントの下に新しい子コンパートメントを作成します。
    b. 新しいオブジェクトストレージバケットを作成するか、OCI が提供するバケットを使用します。
    c. スタックファイルテンプレートをダウンロードしてローカルに保存します。
2. Assisted Installer コンソールで、クラスターを設定します。
    a. クラスター設定を入力します。
    b. 検出 ISO イメージを生成してダウンロードします。
3. OCI コンソールでインフラストラクチャーを作成します。
    a. 検出 ISO イメージを OCI バケットにアップロードします。
    b. ISO イメージの Pre-Authenticated Request (PAR) を作成します。
    c. スタックファイルテンプレートをアップロードし、それを使用してスタックを作成して適用します。

d. スタックからカスタムマニフェスト YAML ファイルをコピーします。

4. Assisted Installer コンソールで、クラスターのインストールを完了します。

   a. クラスターノードのロールを設定します。

   b. Oracle が提供するマニフェストをアップロードします。

   c. クラスターをインストールします。

重要

OCI リソースをプロビジョニングする手順は、例としてのみ提供されています。他の方法で必要なリソースを作成することも選択できます。スクリプトは単なる例です。独自にプロビジョニングするインフラストラクチャーでクラスターをインストールするには、クラウドプロバイダーおよび OpenShift Container Platform のインストールプロセスを理解している必要があります。OCI 設定にアクセスしてこの手順を完了することも、設定をモデルとして使用して独自のカスタムスクリプトを作成することもできます。

関連情報

- Assisted Installer for OpenShift Container Platform
- Installing a Cluster with Red Hat's Assisted Installer (Oracle ドキュメント)
- OpenShift Container Platform のインターネットアクセス

1.2. OCI 環境の準備

Assisted Installer を使用して OpenShift Container Platform をインストールする前に、必要なリソースを作成し、OCI 環境に設定ファイルをダウンロードします。

前提条件

- クラスターをホストするための OCI アカウントがある。
- ファイアウォールを使用しており、Telemetry サービスを使用する予定の場合は、OpenShift Container Platform が必要なサイトにアクセスできるようにファイアウォールを設定した。

手順

1. 管理者権限を使用して Oracle Cloud Infrastructure (OCI) アカウントにログインします。

2. Accounts and Resources (Oracle ドキュメント) を定義してアカウントを設定します。次のリソースを必ず作成してください。

   a. OCI リソースの整理、アクセスの制限、および使用制限の設定を行うための子コンパートメントを作成します。詳細な手順は、Creating a Compartment (Oracle ドキュメント) を参照してください。

   b. 検出 ISO イメージをアップロードする新しいオブジェクトストレージバケットを作成します。詳細な手順は、Creating an Object Storage Bucket (Oracle ドキュメント) を参照してください。

3. **oracle-quickstart/oci-openshift** リポジトリーから、**create-cluster-vX.X.X.zip** 設定ファイルの最新バージョンをダウンロードします。このファイルは、クラスターのインフラストラクチャーを提供するものであり、次の設定を含んでいます。

    - **Terraform スタック**: OCI 上で OpenShift Container Platform クラスターを作成および管理するための OCI リソースをプロビジョニングする Terraform スタックコード。
    - **カスタムマニフェスト**: OCI 上で OpenShift Container Platform クラスターをインストールするのに必要なマニフェストファイル。

    注記

    マニフェストに変更を加える場合は、Oracle GitHub リポジトリー全体をクローンすると、**custom_manifests** および **terraform-stacks** ディレクトリーに直接アクセスできます。

    詳細は、Configuration Files (Oracle ドキュメント) を参照してください。

1.3. ASSISTED INSTALLER を使用して OCI 互換の検出 ISO イメージを生成する

Assisted Installer Web コンソールでクラスター設定を作成し、検出 ISO イメージを生成します。

前提条件

- OCI 上に子コンパートメントとオブジェクトストレージバケットを作成した。詳細は、**OCI 環境の準備** を参照してください。
- OpenShift Container Platform のインストールおよび更新プロセスの詳細を確認した。

1.3.1. クラスターの作成

クラスターの詳細を設定します。

手順

1. 認証情報を使用して、Assisted Installer Web コンソール にログインします。
2. **Red Hat OpenShift** タイルで、**OpenShift** を選択します。
3. **Red Hat OpenShift Container Platform** タイルで、**Create Cluster** を選択します。
4. **Cluster Type** ページで、**Cloud** タブの最後までスクロールし、**Oracle Cloud Infrastructure (virtual machines)** を選択します。
5. **Create an OpenShift Cluster** ページで、**Interactive** タイルを選択します。
6. **Cluster Details** ページで、次のフィールドに入力します。

フィールド	必要な操作
クラスター名	クラスターの名前 (**oci** など) を指定します。これは、OCI のクラスター名と同じ値です。

フィールド	必要な操作
Base domain	クラスターのベースドメイン (**openshift-demo.devcluster.openshift.com** など) を指定します。 これは、OCI のゾーン DNS サーバーと同じ値である必要があります。
OpenShift のバージョン	* 仮想マシンのみにインストールする場合は、**OpenShift 4.14** 以降のバージョンを指定します。 * ベアメタルマシンを含むインストールの場合は、**OpenShift 4.16** 以降のバージョンを指定します。
CPU architecture	**x86_64** または **Arm64** を指定します。
Integrate with external partner platforms	**Oracle Cloud Infrastructure** を指定します。 この値を指定すると、**Include custom manifests** チェックボックスがデフォルトで選択され、**Custom manifests** ページがウィザードに追加されます。

7. 残りのフィールドはデフォルト設定のままにして、**Next** をクリックします。

8. **Operators** ページで、**Next** をクリックします。

1.3.2. Discovery ISO イメージの生成

Discovery ISO イメージを生成してダウンロードします。

手順

1. **Host Discovery** ページで、**Add hosts** をクリックし、次の手順を実行します。
   a. **Provisioning type** フィールドで、**Minimal image file** を選択します。
   b. **SSH public key** フィールドに、次のコマンドの出力をコピーして、ローカルシステムから SSH 公開鍵を追加します。

   ```
   $ cat ~/.ssh/id_rsa.put
   ```

   SSH 公開鍵は、すべての OpenShift Container Platform コントロールプレーンとコンピュートノードにインストールされます。
   c. **Generate Discovery ISO** をクリックして、検出 ISO イメージファイルを生成します。
   d. **Download Discovery ISO** をクリックして、ファイルをローカルシステムに保存します。

関連情報

- インストールおよび更新

- ファイアウォールの設定

1.4. クラスター用の OCI インフラストラクチャーのプロビジョニング

Assisted Installer を使用して OpenShift Container Platform クラスターの詳細を作成する場合、Terraform スタックでクラスターの詳細を指定します。スタックは、OCI に OpenShift Container Platform クラスターをインストールするために必要なすべての OCI インフラストラクチャーリソースのプロビジョニングを自動化する OCI の機能です。

前提条件

- 検出 ISO イメージをローカルディレクトリーにダウンロードした。詳細は、「Assisted Installer を使用して OCI 互換の検出 ISO イメージを生成する」を参照してください。
- Terraform スタックテンプレートをローカルディレクトリーにダウンロードした。詳細は、「OCI 環境の準備」を参照してください。

手順

1. Oracle Cloud Infrastructure (OCI) アカウントにログインします。
2. 検出 ISO イメージを、ローカルドライブから、作成した新しいオブジェクトストレージバケットにアップロードします。詳細な手順は、Uploading an Object Storage Object to a Bucket (Oracle ドキュメント) を参照してください。
3. アップロードした検出 ISO を見つけて、次の手順を実行します。
   a. 横にあるオプションメニューから ISO の Pre-Authenticated Request (PAR) を作成します。
   b. 生成された URL をコピーします。これは次のステップで OpenShift Image Source URI として使用します。

   詳細な手順は、Creating a Pre-Authenticated Requests in Object Storage (Oracle ドキュメント) を参照してください。
4. Terraform スタックを作成して適用します。

   重要

   Terraform スタックには、クラスターリソースとカスタムマニフェストを作成するためのファイルが含まれています。このスタックにはスクリプトも含まれており、スタックを適用すると、そのスクリプトによって DNS レコード、インスタンス、その他のリソースといった OCI リソースが作成されます。リソースのリストは、OpenShift on OCI (OSO) の **terraform-stacks** フォルダーを参照してください。

   a. Terraform スタックテンプレート terraform-stacks を新しいオブジェクトストレージバケットにアップロードします。
   b. スタックの情報を入力し、**Next** をクリックします。

重要

- **Cluster Name** が Assisted Installer の **Cluster Name** と一致し、**Zone DNS** が Assisted Installer の **Base Domain** と一致していることを確認してください。
- **OpenShift Image Source URI** フィールドに、前のステップで生成した Pre-Authenticated Request の URL リンクを貼り付けてください。
- ベアメタルにインストールするか、仮想マシンにインストールするかに応じて、正しい **Compute Shape** フィールド値が定義されていることを確認してください。正しくない場合は、リストから別のシェイプを選択してください。詳細は、Compute Shapes (Oracle ドキュメント) を参照してください。

c. **Apply** をクリックしてスタックを適用します。

詳細な手順は、Creating OpenShift Container Platform Infrastructure Using Resource Manager (Oracle ドキュメント) を参照してください。

5. Terraform スタックの **Outputs** ページから **dynamic_custom_manifest.yml** ファイルをコピーします。

注記

YAML ファイルには、設定値と連結され、事前にフォーマットされた必要なマニフェストがすべて含まれています。詳細は、カスタムマニフェストの README ファイル を参照してください。

詳細な手順は、Getting the OpenShift Container Platform Custom Manifests for Installation (Oracle ドキュメント) を参照してください。

1.5. ASSISTED INSTALLER の残りの手順を完了する

Oracle® Cloud Infrastructure (OCI) リソースをプロビジョニングし、OpenShift Container Platform カスタムマニフェスト設定ファイルを OCI にアップロードした後、インスタンス OCI を作成する前に、Assisted Installer で残りのクラスターのインストール手順を完了する必要があります。この手順では、ノードロールの割り当てとカスタムマニフェストの追加を行います。

1.5.1. ノードロールの割り当て

ホストの検出後、ノードのロールは、すべてデフォルトで **Auto-assign** と表示されます。各ノードのロールを、**Control Plane node** または **Worker** のいずれかに変更します。

前提条件

- OCI で Terraform スタックを作成して適用した。詳細は、「クラスター用の OCI インフラストラクチャーのプロビジョニング」を参照してください。

手順

1. Assisted Installer ユーザーインターフェイスから、**Host discovery** ページに移動します。

2. **Role** 列で、対象のホスト名ごとに **Control plane node** または **Worker** を選択します。**Next** をクリックします。

注記

1. 次の手順に進む前に、各ノードが **Ready** ステータスになるまで待ちます。
2. ノードを展開して、ハードウェアタイプがベアメタルであることを確認します。

3. **Storage** ページおよび **Networking** ページのデフォルト設定を受け入れます。**Next** をクリックします。

1.5.2. カスタムマニフェストの追加

Oracle が提供する必須のカスタムマニフェストを追加します。詳細は、Custom Manifests (Oracle ドキュメント) を参照してください。

前提条件

- OCI の Terraform スタックから **dynamic_custom_manifest.yml** ファイルをコピーした。詳細は、「クラスター用の OCI インフラストラクチャーのプロビジョニング」を参照してください。

手順

1. **Custom manifests** ページの **Folder** フィールドで、**manifests** を選択します。これは、カスタムマニフェストファイルを保存する Assisted Installer 用のフォルダーです。
2. **File name** フィールドに、ファイル名 (例: **dynamic_custom_manifest.yml**) を入力します。
3. OCI からコピーした **dynamic_custom_manifest.yml** ファイルの内容を貼り付けます。
   a. **Content** セクションで、**Paste content** アイコンをクリックします。
   b. Firefox を使用している場合は、**OK** をクリックしてダイアログボックスを閉じ、**Ctrl+V** を押します。そうでない場合は、このステップをスキップしてください。
4. **Next** をクリックしてカスタムマニフェストを保存します。
5. **Review and create** ページで、**Install cluster** をクリックして、OCI 上に OpenShift Container Platform クラスターを作成します。

クラスターのインストールと初期化操作が完了すると、Assisted Installer によってクラスターのインストール操作が完了したことが示されます。詳細は、「OpenShift Container Platform の Assisted Installer」ドキュメントの「インストールの完了」セクションを参照してください。

関連情報

- Assisted Installer for OpenShift Container Platform

1.6. OCI へのクラスターのインストールが成功したことを確認する

クラスターが Oracle® Cloud Infrastructure (OCI) にインストールされ、適切に動作していることを確認します。

手順

1. Red Hat Hybrid Cloud Console から、**Clusters** > **Assisted Clusters** に移動し、クラスターの名前を選択します。
2. **Installation Progress** ページで、インストールの進行状況バーが 100% になっており、**Installation completed successfully** というメッセージが表示されていることを確認します。
3. **Host inventory** で、すべてのコントロールプレーンとコンピュートノードのステータスが **Installed** であることを確認します。

   注記

   OpenShift Container Platform は、コントロールプレーンノードの 1 つをブートストラップ仮想マシンとして指定します。そのため、別のブートストラップマシンは不要です。

4. Web コンソール URL をクリックして、OpenShift Container Platform Web コンソールにアクセスします。
5. メニューから、**Compute** > **Nodes** を選択します。
6. **Nodes** テーブルからノードを見つけます。
7. **Terminal** タブで、シリアル番号の横に iSCSI が表示されていることを確認します。
8. **Overview** タブで、ノードが **Ready** ステータスになっていることを確認します。
9. **YAML** タブを選択します。
10. **labels** パラメーターを確認し、表示されるラベルが、使用する設定に該当するものであることを確認します。たとえば、**topology.kubernetes.io/region=us-sanjose-1** というラベルからは、ノードがデプロイされた OCI リージョンがわかります。

1.7. インストール後にクラスターにホストを追加する

Assisted Installer を使用してクラスターを作成した後、Red Hat Hybrid Cloud Console を使用してクラスターに新しいホストノードを追加し、そのノードの証明書署名要求 (CRS) を承認できます。

詳細は、Adding Nodes to a Cluster (Oracle ドキュメント) を参照してください。

1.8. OCI でのクラスターのインストールのトラブルシューティング

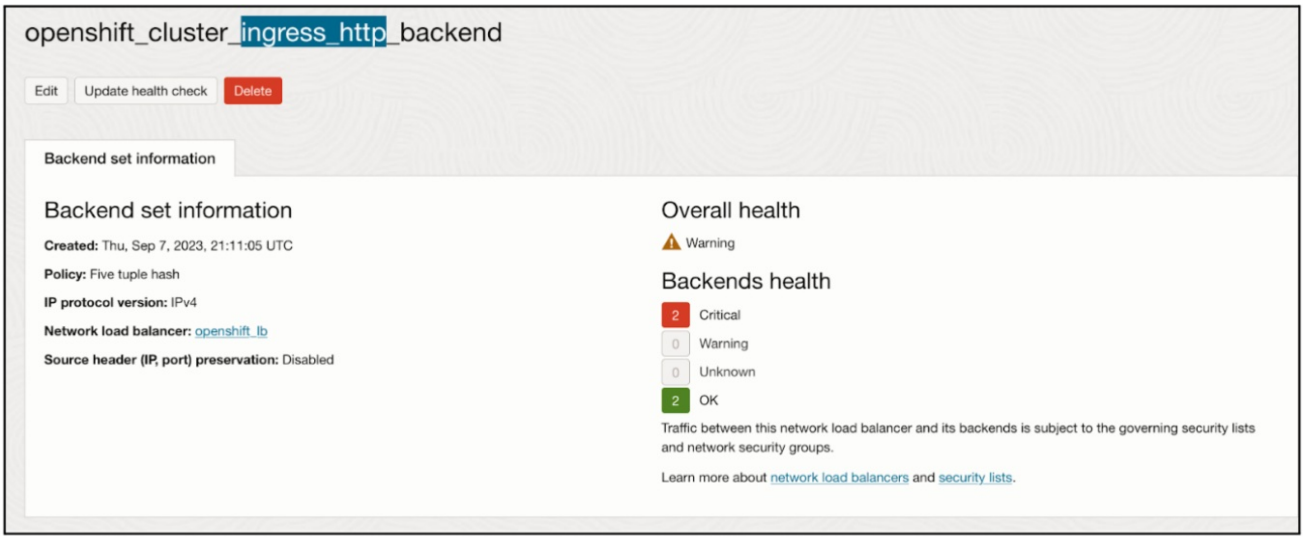
Assisted Installer を使用して OpenShift Container Platform クラスターを Oracle® Cloud Infrastructure (OCI) にインストールする際に問題が発生した場合は、次のセクションを読んで一般的な問題のトラブルシューティングを行ってください。

1.8.1. OCI の Ingress ロードバランサーが健全なステータスでない

この問題は、**Warning** として分類されています。OCI を使用してスタックを作成すると、デフォルト

で 3 つのコンピュートノードのプールが作成され、Ingress ロードバランサーのバックエンドリスナーとして自動的に追加されるためです。デフォルトでは、OpenShift Container Platform は 2 つのルーター Pod をデプロイします。これらの Pod は、OpenShift Container Platform マニフェストファイルのデフォルト値に基づいています。3 つのコンピュートノードで実行できる使用可能なルーター Pod の数 (2 つ) との不一致により、このような **Warning** が発生することが予想されます。

図1.2 OCI の Backend set information タブに表示されるWarning メッセージの例



Ingress ロードバランサーの設定を変更する必要はありません。代わりに、OpenShift Container Platform 上のクラスター内で動作する特定のコンピュートノードに、Ingress ロードバランサーを参照させることができます。これを行うには、OpenShift Container Platform でアノテーションなどの配置メカニズムを使用して、最初に Ingress ロードバランサーにバックエンドリスナーとして設定したコンピュートノード上でのみルーター Pod を実行します。

1.8.2. OCI スタック作成操作が失敗し、Error: 400-InvalidParameter というメッセージが表示される

OCI でスタックを作成しようとすると、ジョブの **Logs** セクションにエラーメッセージが出力されることがあります。以下に例を示します。

```
Error: 400-InvalidParameter, DNS Label oci-demo does not follow Oracle requirements
Suggestion: Please update the parameter(s) in the Terraform config as per error message DNS Label
oci-demo does not follow Oracle requirements
Documentation: https://registry.terraform.io/providers/oracle/oci/latest/docs/resources/core_vcn
```

Hybrid Cloud Console の **Install OpenShift with the Assisted Installer** ページに移動し、**Cluster Details** ステップの **Cluster name** フィールドを確認します。ハイフン (**-**) などの特殊文字は、OCI 命名規則に対応性してないため、名前から削除してください。たとえば、**oci-demo** は **ocidemo** に変更します。

関連情報

- Troubleshooting OpenShift Container Platform on OCI (Oracle ドキュメント)
- Assisted Installer を使用したオンプレミスクラスターのインストール

第2章 AGENT-BASED INSTALLER を使用して ORACLE CLOUD INFRASTRUCTURE (OCI) にクラスターをインストールする

OpenShift Container Platform 4.18 では、Agent-based Installer を使用して Oracle® Cloud Infrastructure (OCI) にクラスターをインストールすると、専用、ハイブリッド、パブリックおよびマルチクラウド環境をサポートするインフラストラクチャー上でクラスターのワークロードを実行できます。

OCI へのクラスターのインストールは、仮想マシン (VM) とベアメタルマシンでサポートされています。

注記

Oracle Cloud Infrastructure (OCI) の任意のリージョンと同じように、Dedicated Region (Oracle ドキュメント) に OpenShift Container Platform をデプロイできます。

2.1. AGENT-BASED INSTALLER と OCI の概要

Agent-based Installer を使用して、OpenShift Container Platform クラスターを Oracle® Cloud Infrastructure (OCI) にインストールできます。Red Hat と Oracle は、OpenShift Container Platform クラスターでの OCI ワークロードの実行をテスト、検証、サポートしています。

Agent-based Installer は、Assisted Installation サービスを使いやすくするだけでなく、接続環境または非接続環境のいずれかにクラスターをインストールする機能を備えています。

次の図は、接続環境と非接続環境のワークフローを示しています。

図2.1 接続環境で Agent-based Installer を使用して OCI にクラスターをインストールするためのワークフロー

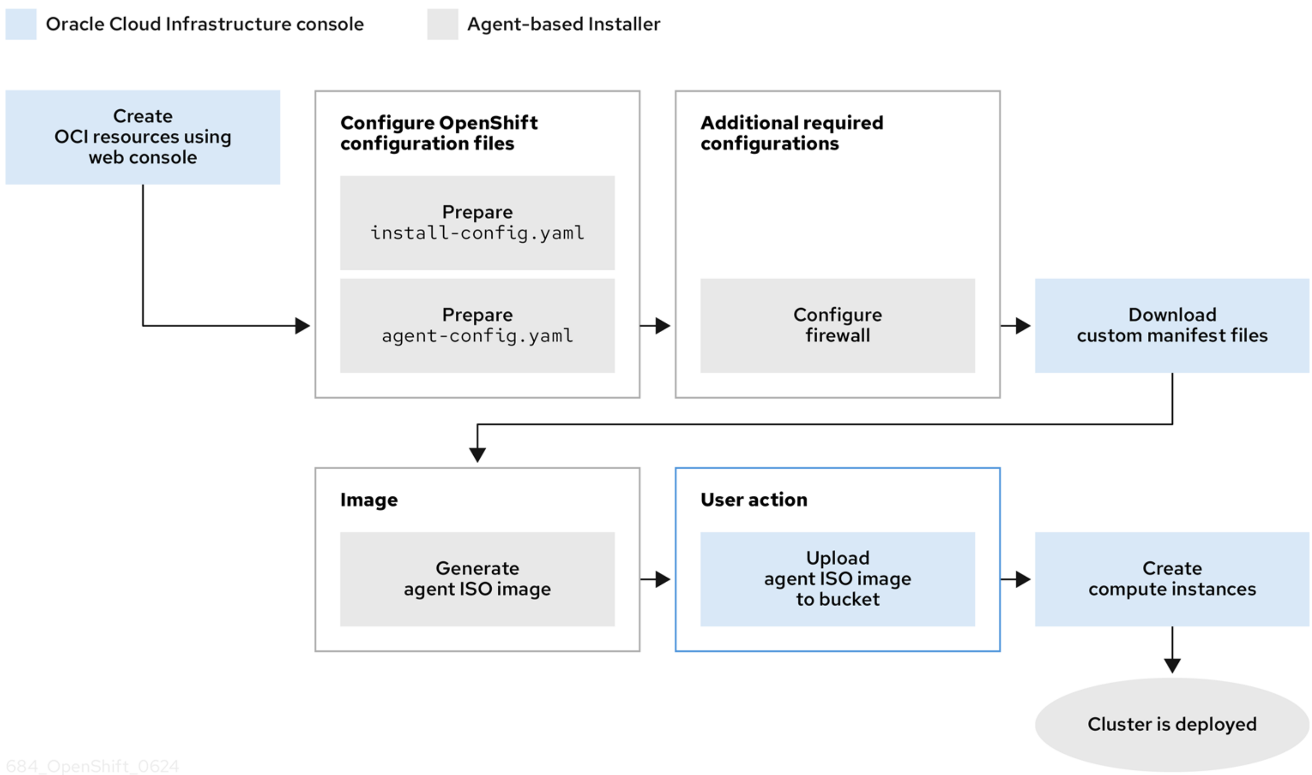
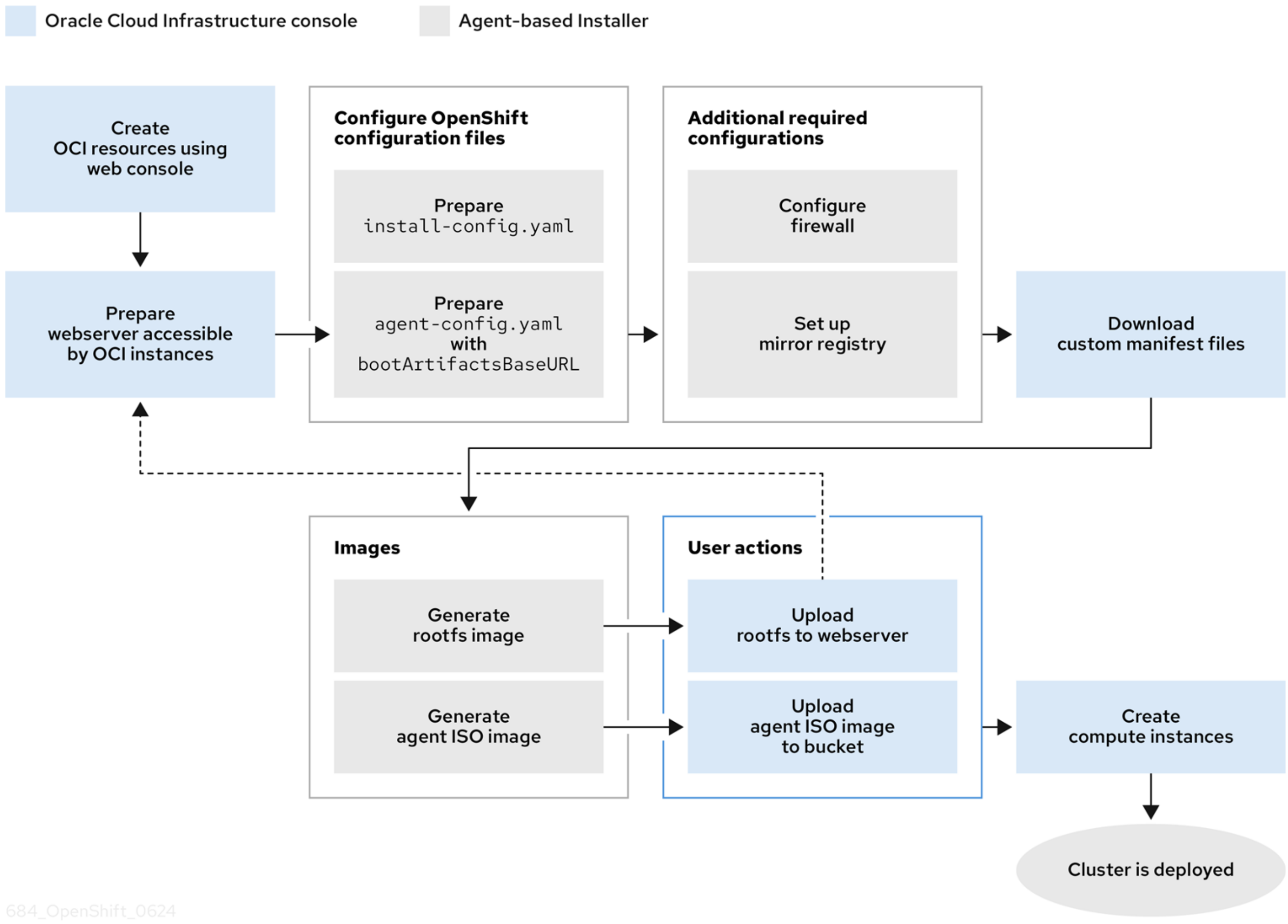


図2.2 非接続環境で Agent-based Installer を使用して OCI にクラスターをインストールするためのワークフロー



OCI は、規制コンプライアンス、パフォーマンス、費用対効果のニーズを満たすサービスを提供します。OCI は、64 ビット **x86** インスタンスと 64 ビット **ARM** インスタンスをサポートします。

注記

ブートディスクには、Nonvolatile Memory Express (NVMe) ドライブまたはソリッドステートドライブ (SSD) を選択することを検討してください。これらのドライブは、低遅延機能と高スループット機能をブートディスクに提供するためです。

OCI で OpenShift Container Platform クラスターを実行すると、次の機能を利用できます。

- コンピュートフレキシブルシェイプ。仮想マシンの Oracle® CPU (OCPU) とメモリーリソースの数をカスタマイズできます。この機能を利用すると、リソースのバランスが取れた環境でクラスターのワークロードが操作を実行できます。Red Hat Ecosystem Catalog ポータルの Oracle ページにアクセスすると、RHEL 認定を受けたすべての OCI シェイプを参照できます。

- ブロックボリュームストレージ。ストレージボリュームのスケーリングと自動チューニングを設定できるため、ブロックボリュームサービスによりパフォーマンスレベルを自動的に調整してパフォーマンスを最適化できます。

重要

OCI および OCVS サービス上で動作するクラスターワークロードに最適なパフォーマンス条件を確保するために、ブロックボリュームのボリュームパフォーマンスユニット (VPU) がワークロードに適したサイズに設定されていることを確認してください。次のリストを参考に、特定のパフォーマンスニーズに応じて必要な VPU を選択してください。

- テストまたは概念実証環境: 100 GB、20 - 30 VPU。
- 基本的な環境: 500 GB、60 VPU
- 高負荷の実稼働環境: 500 GB 以上、100 以上の VPU

更新やスケーリングアクティビティーに十分な容量を提供できるように、VPU を余分に確保しておくことを検討してください。VPU の詳細は、Oracle ドキュメントの「Volume Performance Units」を参照してください。

関連情報

- インストールプロセス
- OpenShift Container Platform のインターネットアクセス
- Agent-based Installer について
- Overview of the Compute Service (Oracle ドキュメント)
- Volume Performance Units (Oracle ドキュメント)
- Instance Sizing Recommendations for OpenShift Container Platform on OCI Nodes (Oracle ドキュメント)

2.2. インストールプロセスのワークフロー

次のワークフローは、Agent-based Installer を使用して OCI に OpenShift Container Platform クラスターをインストールするプロセスの概要を示しています。

1. OCI リソースとサービスを作成します (Oracle)。
2. 非接続環境: OCI インスタンスからアクセスできる Web サーバーを準備します (Red Hat)。
3. Agent-based Installer 用の設定ファイルを準備します (Red Hat)。
4. エージェント ISO イメージを生成します (Red Hat)。
5. 非接続環境: rootfs イメージを Web サーバーにアップロードします (Red Hat)。
6. OpenShift Container Platform のファイアウォールを設定します (Red Hat)。
7. エージェント ISO イメージをストレージバケットにアップロードします (Oracle)。
8. アップロードしたエージェント ISO イメージからカスタムイメージを作成します (Oracle)。
9. OCI でコンピュートインスタンスを作成します (Oracle)。
10. クラスターが OCI 上で稼働していることを確認します (Oracle)。

2.3. OCI インフラストラクチャーのリソースとサービスの作成

仮想マシン (VM) またはベアメタルシェイプ上に OCI 環境を作成する必要があります。この環境を作成すると、OpenShift Container Platform をインストールし、幅広いクラウドオプションと強力なセキュリティーポリシーをサポートするインフラストラクチャーにクラスターをデプロイできます。OCI コンポーネントに関する事前の知識があれば、OCI リソースの概念を理解し、組織のニーズに合わせてリソースを設定する方法を理解するのに役立ちます。

Agent-based Installer 方式で OpenShift Container Platform クラスターを OCI にインストールするには、OCI リソースとサービスを手動で作成する必要があります。

重要

OpenShift Container Platform との互換性を確保するには、各 DNS レコードのレコードタイプとして **A** を設定し、次のようにレコードに名前を付ける必要があります。

- **api.<cluster_name>.<base_domain>**。これは API ロードバランサーの **apiVIP** パラメーターをターゲットとしています。
- **api-int.<cluster_name>.<base_domain>**。これは API ロードバランサーの **apiVIP** パラメーターをターゲットとしています。
- ***.apps.<cluster_name>.<base_domain>**。これは Ingress ロードバランサーの **ingressVIP** パラメーターをターゲットとしています。

api.* および **api-int.*** DNS レコードは、コントロールプレーンマシンに関連しています。そのため、インストールした OpenShift Container Platform クラスター内のすべてのノードがこれらの DNS レコードにアクセスできることを確認する必要があります。

前提条件

- OpenShift Container Platform クラスターをホストするために OCI アカウントを設定しました。Prerequisites (Oracle ドキュメント) を参照してください。

手順

- 必要な OCI リソースとサービスを作成します。
  接続環境でのインストールは、Provisioning Cluster Infrastructure Using Terraform (Oracle ドキュメント) を参照してください。

  非接続環境でのインストールは、Provisioning OCI Resources for the Agent-based Installer in Disconnected Environments (Oracle ドキュメント) を参照してください。

関連情報

- Learn About Oracle Cloud Basics (Oracle ドキュメント)

2.4. OCI にクラスターをインストールするための設定ファイルの作成

Agent-based Installer を使用して起動可能な ISO イメージを生成できるように、**install-config.yaml** 設定ファイルと **agent-config.yaml** 設定ファイルを作成する必要があります。エージェントベースのインストールは、Assisted Discovery Agent と Assisted Service を含む起動可能な ISO で構成されます。これらのコンポーネントは、クラスターのインストールを実行するために両方とも必要ですが、後者のコンポーネントはいずれか 1 つのホストでのみ実行されます。

注記

Agent-based Installer を使用して、ゼロタッチプロビジョニング (ZTP) カスタムリソースを生成または受け入れることもできます。

前提条件

- OpenShift Container Platform のインストールおよび更新プロセスの詳細を確認した。
- クラスターのインストール方法の選択とその方法の準備に関するユーザー向けドキュメントを確認した。
- 「Agent-based Installer を使用したインストールの準備」ドキュメントを確認した。
- Red Hat Hybrid Cloud Console から Agent-based Installer とコマンドラインインターフェイス (CLI) をダウンロードした。
- 非接続環境にインストールする場合は、環境にミラーレジストリーを準備し、リリースイメージをレジストリーにミラーリングした。

  重要

  次のコマンドを実行して、**openshift-install** バイナリーのバージョンが、Red Hat Quay などの共有レジストリーではなく、ローカルイメージコンテナーレジストリーに関連していることを確認してください。

  ```
  $ ./openshift-install version
  ```

  共有レジストリーバイナリーの出力例

  ```
  ./openshift-install 4.18.0
  built from commit ae7977b7d1ca908674a0d45c5c243c766fa4b2ca
  release image registry.ci.openshift.org/origin/release:4.18ocp-release@sha256:0da6316466d60a3a4535d5fed3589feb0391989982fba59d47d4c729912d6363
  release architecture amd64
  ```

- 管理者権限で OpenShift Container Platform にログインしている。

手順

1. 次のコマンドを実行して、設定ファイルを保存するインストールディレクトリーを作成します。

   ```
   $ mkdir ~/<directory_name>
   ```

2. 組織のニーズに合わせて **install-config.yaml** 設定ファイルを設定し、作成したディレクトリーにファイルを保存します。

   外部プラットフォームを設定する install-config.yaml ファイル

   ```
   # install-config.yaml
   apiVersion: v1
   ```

```
baseDomain: <base_domain> 1
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  network type: OVNKubernetes
  machineNetwork:
  - cidr: <ip_address_from_cidr> 2
  serviceNetwork:
  - 172.30.0.0/16
compute:
  - architecture: amd64 3
  hyperthreading: Enabled
  name: worker
  replicas: 0
controlPlane:
  architecture: amd64 4
  hyperthreading: Enabled
  name: master
  replicas: 3
platform:
   external:
    platformName: oci 5
    cloudControllerManager: External
sshKey: <public_ssh_key> 6
pullSecret: '<pull_secret>' 7
# ...
```

1 クラウドプロバイダーのベースドメイン。

2 ネットワーク上で機能するリソースおよびコンポーネントに対して CIDR が割り当てる仮想クラウドネットワーク (VCN) の IP アドレス。

3 4 インフラストラクチャーに応じて、**arm64** または **amd64** のいずれかを選択できます。

5 OpenShift Container Platform が OCI と統合できるように、**OCI** を外部プラットフォームとして設定します。

6 SSH 公開鍵を指定します。

7 OpenShift Container Platform コンポーネントおよびサービス (Quay.io など) のコンテナーイメージをダウンロードするときに認証するために必要なプルシークレット。Red Hat Hybrid Cloud Console の Install OpenShift Container Platform 4 を参照してください。

3. ローカルシステム上に **openshift** という名前のディレクトリーを作成します。これはインストールディレクトリーのサブディレクトリーである必要があります。

重要

install-config.yaml または **agent-config.yaml** 設定ファイルを **openshift** ディレクトリーに移動しないでください。

4. スタックを使用して OCI インフラストラクチャーリソースをプロビジョニングした場合: OCI スタックの **dynamic_custom_manifest** 出力をコピーして、**manifest.yaml** という名前のファイルに貼り付け、そのファイルを **openshift** ディレクトリーに保存します。

5. スタックを使用して OCI インフラストラクチャーリソースをプロビジョニングしなかった場合: カスタムマニフェストをダウンロードして準備し、エージェント ISO イメージを作成します。

    a. Configuration Files (Oracle ドキュメント) に移動し、GitHub のカスタムマニフェストディレクトリーへのリンクをクリックします。

    b. **condensed-manifest.yml** ファイルの内容をコピーし、**openshift** ディレクトリー内のファイルにローカルに保存します。

    c. **condensed-manifest.yml** ファイルで、**TODO** でマークされたセクションを更新して、コンパートメントの Oracle® Cloud Identifier (OCID)、VCN の OCID、ロードバランサーからのサブネットの OCID、およびセキュリティーリストの OCID を指定します。

6. 組織の要件に合わせて **agent-config.yaml** 設定ファイルを設定します。

    IPv4 ネットワーク用のサンプル agent-config.yaml ファイル

    ```
    apiVersion: v1beta1
    metadata:
      name: <cluster_name> 1
      namespace: <cluster_namespace> 2
    rendezvousIP: <ip_address_from_CIDR> 3
    bootArtifactsBaseURL: <server_URL> 4
    # ...
    ```

    1 DNS レコードに指定したクラスター名。

    2 OpenShift Container Platform 上のクラスターの namespace。

    3 ネットワーク IP アドレス形式として IPv4 を使用する場合は、**rendezvousIP** パラメーターを、VCN の Classless Inter-Domain Routing (CIDR) 方式によってネットワークに割り当てられる IPv4 アドレスに必ず設定してください。また、ISO を使用して起動したインスタンスプール内の少なくとも 1 つのインスタンスが、**rendezvousIP** パラメーターに設定した IP アドレス値と一致していることを確認してください。

    4 rootfs イメージをアップロードするサーバーの URL。このパラメーターは、非接続環境でのみ必要です。

7. インストールディレクトリーで次のコマンドを入力して、rootfs イメージを除外した最小限の ISO イメージを生成します。

    ```
    $ ./openshift-install agent create image --log-level debug
    ```

    このコマンドは次の操作も実行します。

    - サブディレクトリー **./<installation_directory>/auth directory:** を作成し、そのサブディレクトリーに **kubeadmin-password** ファイルと **kubeconfig** ファイルを配置します。

    - **agent-config.yaml** 設定ファイルで指定した IP アドレスに基づいて、**rendezvousIP** ファイルを作成します。

- オプション: **agent-config.yaml** および **install-config.yaml** 設定ファイルに加えた変更は、すべてゼロタッチプロビジョニング (ZTP) カスタムリソースにインポートされます。

重要

Agent-based Installer は Red Hat Enterprise Linux CoreOS (RHCOS) を使用します。後のステップで説明する rootfs イメージは、オペレーティングシステムの起動、回復、修復に必要です。

8. 非接続環境のみ: rootfs イメージを Web サーバーにアップロードします。

    a. 最小限の ISO イメージを作成したときに生成された **./<installation_directory>/boot-artifacts** ディレクトリーに移動します。

    b. 任意の Hypertext Transfer Protocol デーモン (**httpd**) などの優先 Web サーバーを使用して、**agent-config.yaml** ファイルの **bootArtifactsBaseURL** パラメーターに指定された場所に rootfs イメージをアップロードします。
    たとえば、**bootArtifactsBaseURL** パラメーターに **http://192.168.122.20** と指定されている場合、生成された rootfs イメージをこの場所にアップロードして、Agent-based Installer が **http://192.168.122.20/agent.x86_64-rootfs.img** からイメージにアクセスできるようにします。Agent-based Installer は、外部プラットフォームの最小限の ISO を起動した後、**http://192.168.122.20/agent.x86_64-rootfs.img** の場所から rootfs イメージをシステムメモリーにダウンロードします。

注記

また、Agent-based Installer は、Operator がクラスターのノードを起動するときに rootfs イメージをシステムメモリーにダウンロードするために、**bootArtifactsBaseURL** の値を最小限の ISO イメージの設定に追加します。

重要

1 GB を超える完全な ISO イメージには、rootfs イメージが含まれていることに注意してください。このイメージは、通常 **150** MB 未満の最小 ISO イメージよりも大きくなります。

関連情報

- OpenShift Container Platform のインストール
- クラスターのインストールタイプの選択
- Agent-based Installer を使用したインストールの準備
- Agent-based Installer のダウンロード
- mirror registry for Red Hat OpenShift を使用したミラーレジストリーの作成
- OpenShift Container Platform イメージリポジトリーのミラーリング
- オプション: ZTP マニフェストの使用

2.5. OPENSHIFT CONTAINER PLATFORM のファイアウォールの設定

OpenShift Container Platform をインストールする前に、ファイアウォールを、OpenShift Container Platform が必要とするサイトへのアクセスを付与するように設定する必要があります。ファイアウォールを使用する場合は、OpenShift Container Platform が機能するために必要なサイトにアクセスできるように、ファイアウォールに追加の設定を行います。

非接続環境の場合は、Red Hat と Oracle の両方のコンテンツをミラーリングする必要があります。このような環境では、ファイアウォールを特定のポートとレジストリーに公開するためのファイアウォールルールを作成する必要があります。

注記

ご使用の環境で OpenShift Container Platform クラスターの前に専用のロードバランサーがある場合は、ファイアウォールとロードバランサーの間の許可リストを確認して、クラスターに対する不要なネットワーク制限を回避してください。

手順

1. ファイアウォールの許可リストに次のレジストリー URL を設定します。

URL	ポート	機能
registry.redhat.io	443	コアコンテナーイメージを指定します。
access.redhat.com	443	コンテナークライアントが **registry.access.redhat.com** から取得したイメージを検証するのに必要な署名ストアをホストします。ファイアウォール環境では、このリソースが許可リストに含まれていることを確認してください。
registry.access.redhat.com	443	コアコンテナーイメージを含め、Red Hat Ecosystem Catalog に保存されているすべてのコンテナーイメージをホストします。
quay.io	443	コアコンテナーイメージを指定します。
cdn.quay.io	443	コアコンテナーイメージを指定します。
cdn01.quay.io	443	コアコンテナーイメージを指定します。
cdn02.quay.io	443	コアコンテナーイメージを指定します。
cdn03.quay.io	443	コアコンテナーイメージを指定します。
cdn04.quay.io	443	コアコンテナーイメージを指定します。
cdn05.quay.io	443	コアコンテナーイメージを指定します。

URL	ポート	機能
cdn06.quay.io	443	コアコンテナーイメージを指定します。
sso.redhat.com	443	https://console.redhat.com サイトは、**sso.redhat.com** からの認証を使用します。
icr.io	443	IBM Cloud Pak コンテナーイメージを提供します。このドメインは、IBM Cloud Paks を使用する場合にのみ必要です。
cp.icr.io	443	IBM Cloud Pak コンテナーイメージを提供します。このドメインは、IBM Cloud Paks を使用する場合にのみ必要です。

- 許可リストでは、**cdn.quay.io** と **cdn0[1-6].quay.io** の代わりにワイルドカード ***.quay.io** を使用できます。
- ワイルドカード ***.access.redhat.com** を使用すると、設定を簡素化し、**registry.access.redhat.com** を含むすべてのサブドメインを許可できます。
- **quay.io** などのサイトを許可リストに追加するには、***.quay.io** などのワイルドカードエントリーを拒否リストに加えないでください。ほとんどの場合、イメージレジストリーはコンテンツ配信ネットワーク (CDN) を使用してイメージを提供します。ファイアウォールがアクセスをブロックすると、最初のダウンロード要求が **cdn01.quay.io** などのホスト名にリダイレクトされるときに、イメージのダウンロードが拒否されます。

2. ファイアウォールの許可リストを設定し、ビルドに必要な言語またはフレームワークのリソースを提供するサイトをリストに含めます。

3. Telemetry を無効にしていない場合は、以下の URL へのアクセスを許可して Red Hat Insights にアクセスできるようにする必要があります。

URL	ポート	機能
cert-api.access.redhat.com	443	Telemetry で必須
api.access.redhat.com	443	Telemetry で必須
infogw.api.openshift.com	443	Telemetry で必須
console.redhat.com	443	Telemetry および **insights-operator** で必須

4. ファイアウォールの許可リストを設定し、次のレジストリー URL をリストに含めます。

URL	ポート	機能
api.openshift.com	443	クラスタートークンの両方が必要であり、クラスターに更新が利用可能かどうかを確認するために必要です。
rhcos.mirror.openshift.com	443	Red Hat Enterprise Linux CoreOS (RHCOS) イメージをダウンロードするために必要。

5. ファイアウォールの許可リストを設定し、次の外部 URL をリストに含めます。各リポジトリー URL は OCI コンテナーをホストします。パフォーマンスの問題を軽減するために、イメージをミラーリングするリポジトリーの数をできる限り少なくすることを検討してください。

URL	ポート	機能
k8s.gcr.io	port	コミュニティーベースのイメージレジストリーのコンテナーイメージをホストする Kubernetes レジストリー。このイメージレジストリーは、カスタム Google Container Registry (GCR) ドメインでホストされています。
ghcr.io	port	Open Container Initiative イメージを保存および管理できる GitHub イメージレジストリー。プライベート、内部、パブリックパッケージを公開、インストール、削除するには、アクセストークンが必要です。
storage.googleapis.com	443	リリースイメージ署名のソース。ただし、Cluster Version Operator には単一の機能ソースのみが必要です。
registry.k8s.io	port	**k8s.gcr.io** イメージレジストリーを置き換えます。これは、**k8s.gcr.io** イメージレジストリーが他のプラットフォームやベンダーをサポートしていないためです。

2.6. OCI でのクラスターの実行

Oracle® Cloud Infrastructure (OCI) でクラスターを実行するには、生成されたエージェント ISO イメージを OCI のデフォルトの Object Storage バケットにアップロードする必要があります。さらに、OCI 上でクラスターを実行するために OpenShift Container Platform と OCI が相互に通信できるように、提供されたベースイメージからコンピュートインスタンスを作成する必要があります。

注記

OCI は、次の OpenShift Container Platform クラスタートポロジーをサポートしています。

- シングルノードへの OpenShift Container Platform クラスターのインストール
- 少なくとも 3 つのコントロールプレーンインスタンスと 2 つのコンピュートインスタンスを持つ高可用性クラスター
- 少なくとも 3 つのコントロールプレーンインスタンスを持つコンパクトな 3 ノードクラスター

前提条件

- エージェント ISO イメージを生成した。「OCI にクラスターをインストールするための設定ファイルの作成」を参照してください。

手順

1. エージェント ISO イメージを Oracle のデフォルトの Object Storage バケットにアップロードし、エージェント ISO イメージをカスタムイメージとしてこのバケットにインポートします。カスタムイメージが Unified Extensible Firmware Interface (UEFI) モードで起動するように設定されていることを確認します。詳細は、Creating the OpenShift Container Platform ISO Image (Oracle ドキュメント) を参照してください。
2. クラスタートポロジー用に提供されたベースイメージからコンピュートインスタンスを作成します。Creating the OpenShift Container Platform cluster on OCI (Oracle ドキュメント) を参照してください。

重要

コンピュートインスタンスを作成する前に、クラスターに十分なメモリーとディスクリソースがあることを確認してください。さらに、少なくとも 1 つのコンピュートインスタンスが、**agent-config.yaml** ファイルの **rendezvousIP** に記載されているアドレスと同じ IP アドレスを持っていることを確認してください。

関連情報

- 各トポロジーに推奨されるリソース
- Instance Sizing Recommendations for OpenShift Container Platform on OCI Nodes (Oracle ドキュメント)
- Troubleshooting OpenShift Container Platform on OCI (Oracle ドキュメント)

2.7. エージェントベースのクラスターのインストールが OCI 上で動作していることを確認する

クラスターが Oracle® Cloud Infrastructure (OCI) にインストールされ、適切に動作していることを確認します。

前提条件

- 必要な OCI リソースとサービスをすべて作成した。「OCI インフラストラクチャーのリソースとサービスの作成」を参照してください。
- **install-config.yaml** 設定ファイルと **agent-config.yaml** 設定ファイルを作成した。「OCI にクラスターをインストールするための設定ファイルの作成」を参照してください。
- エージェント ISO イメージをデフォルトの Oracle Object Storage バケットにアップロードし、OCI 上にコンピュートインスタンスを作成した。詳細は、「OCI でのクラスターの実行」を参照してください。

手順

OpenShift Container Platform クラスター内の自己管理ノードにコンピュートインスタンスをデプロイした後、以下のいずれかの方法でクラスターのステータスを監視できます。

- OpenShift Container Platform CLI から次のコマンドを入力します。

  ```
  $ ./openshift-install agent wait-for install-complete --log-level debug
  ```

  ブートストラップノードが動作する **rendezvous** ホストノードの状態を確認します。ホストが再起動すると、ホストはクラスターの一部となります。

- **kubeconfig** API を使用して、さまざまな OpenShift Container Platform コンポーネントのステータスを確認します。**KUBECONFIG** 環境変数に、クラスターの **kubeconfig** 設定ファイルの相対パスを設定します。

  ```
  $  export KUBECONFIG=~/auth/kubeconfig
  ```

  クラスターの各自己管理ノードのステータスを確認します。CCM は、各ノードにラベルを適用して、ノードを OCI 上のクラスターで実行するよう指定します。

  ```
  $ oc get nodes -A
  ```

  出力例

  ```
  NAME                                   STATUS ROLES                 AGE VERSION
  main-0.private.agenttest.oraclevcn.com Ready  control-plane, master 7m  v1.27.4+6eeca63
  main-1.private.agenttest.oraclevcn.com Ready  control-plane, master 15m v1.27.4+d7fa83f
  main-2.private.agenttest.oraclevcn.com Ready  control-plane, master 15m v1.27.4+d7fa83f
  ```

  クラスターの各 Operator のステータスを確認します。CCM Operator のステータスは、クラスターが実行中であることを示す適切な指標です。

  ```
  $ oc get co
  ```

  出力例 (一部のみ記載)

  ```
  NAME           VERSION     AVAILABLE  PROGRESSING    DEGRADED   SINCE
  MESSAGE
  authentication 4.18.0-0    True       False          False      6m18s
  baremetal      4.18.0-0    True       False          False      2m42s
  network        4.18.0-0    True       True           False      5m58s  Progressing: …
     …
  ```

2.8. 関連情報

- 失敗したエージェントベースのインストールからログデータを収集する
- オンプレミスクラスターにワーカーノードを追加する

第3章 AGENT-BASED INSTALLER を使用した ORACLE COMPUTE CLOUD@CUSTOMER へのクラスターのインストール

Agent-based Installer を使用して Oracle Compute Cloud@Customer にクラスターをインストールすることで、Oracle® Cloud Infrastructure (OCI) サービスを引き続き使用しながら、オンプレミスインフラストラクチャーでクラスターワークロードを実行できるようになります。

3.1. インストールプロセスのワークフロー

以下のワークフローは、Agent-based Installer を使用して Compute Cloud@Customer に OpenShift Container Platform クラスターをインストールするプロセスの概要を示しています。

1. Compute Cloud@Customer のリソースとサービス (Oracle) を作成します。
2. Agent-based Installer 用の設定ファイルを準備します (Red Hat)。
3. エージェント ISO イメージを生成します (Red Hat)。
4. ISO イメージを Oracle Cloud Infrastructure (OCI) イメージに変換し、OCI Home Region Bucket にアップロードしてから、アップロードしたイメージを Compute Cloud@Customer システムにインポートします (Oracle)。
5. 非接続環境: OCI インスタンスからアクセスできる Web サーバーを準備します (Red Hat)。
6. 非接続環境: rootfs イメージを Web サーバーにアップロードします (Red Hat)。
7. OpenShift Container Platform のファイアウォールを設定します (Red Hat)。
8. コントロールプレーンノードを作成し、ロードバランサーを設定します (Oracle)。
9. コンピュートノードを作成し、ロードバランサーを設定します (Oracle)。
10. クラスターが OCI 上で稼働していることを確認します (Oracle)。

3.2. ORACLE COMPUTE CLOUD@CUSTOMER インフラストラクチャーのリソースとサービスの作成

仮想マシン (VM) シェイプ上に Compute Cloud@Customer 環境を作成する必要があります。この環境を作成すると、OpenShift Container Platform をインストールし、幅広いクラウドオプションと強力なセキュリティーポリシーをサポートするインフラストラクチャーにクラスターをデプロイできます。OCI コンポーネントに関する事前の知識があれば、OCI リソースの概念を理解し、組織のニーズに合わせてリソースを設定する方法を理解するのに役立ちます。

重要

OpenShift Container Platform との互換性を確保するには、各 DNS レコードのレコードタイプとして **A** を設定し、次のようにレコードに名前を付ける必要があります。

- **api.<cluster_name>.<base_domain>**。これは API ロードバランサーの **apiVIP** パラメーターをターゲットとしています。
- **api-int.<cluster_name>.<base_domain>**。これは API ロードバランサーの **apiVIP** パラメーターをターゲットとしています。
- ***.apps.<cluster_name>.<base_domain>**。これは Ingress ロードバランサーの **ingressVIP** パラメーターをターゲットとしています。

api.* および **api-int.*** DNS レコードは、コントロールプレーンマシンに関連しています。そのため、インストールした OpenShift Container Platform クラスター内のすべてのノードがこれらの DNS レコードにアクセスできることを確認する必要があります。

前提条件

- OpenShift Container Platform クラスターをホストするために OCI アカウントを設定しました。OpenShift Cluster Setup with Agent Based Installer on Compute Cloud@Customer (Oracle ドキュメント) の「Access and Considerations」を参照してください。

手順

- 必要な Compute Cloud@Customer リソースとサービスを作成します。
詳細は、OpenShift Cluster Setup with Agent Based Installer on Compute Cloud@Customer (Oracle ドキュメント) の「Terraform Script Execution」を参照してください。

関連情報

- Learn About Oracle Cloud Basics (Oracle ドキュメント)

3.3. COMPUTE CLOUD@CUSTOMER にクラスターをインストールするための設定ファイルの作成

Agent-based Installer を使用して起動可能な ISO イメージを生成できるように、**install-config.yaml** 設定ファイルと **agent-config.yaml** 設定ファイルを作成する必要があります。エージェントベースのインストールは、Assisted Discovery Agent と Assisted Service を含む起動可能な ISO で構成されます。これらのコンポーネントは、クラスターのインストールを実行するために両方とも必要ですが、後者のコンポーネントはいずれか 1 つのホストでのみ実行されます。

注記

Agent-based Installer を使用して、ゼロタッチプロビジョニング (ZTP) カスタムリソースを生成または受け入れることもできます。

前提条件

- OpenShift Container Platform のインストールおよび更新プロセスの詳細を確認した。
- クラスターのインストール方法の選択とその方法の準備に関するユーザー向けドキュメントを確認した。

- 「Agent-based Installer を使用したインストールの準備」ドキュメントを確認した。
- Red Hat Hybrid Cloud Console から Agent-based Installer とコマンドラインインターフェイス (CLI) をダウンロードした。
- 非接続環境にインストールする場合は、環境にミラーレジストリーを準備し、リリースイメージをレジストリーにミラーリングした。

重要

次のコマンドを実行して、**openshift-install** バイナリーのバージョンが、Red Hat Quay などの共有レジストリーではなく、ローカルイメージコンテナーレジストリーに関連していることを確認してください。

```
$ ./openshift-install version
```

共有レジストリーバイナリーの出力例

```
./openshift-install 4.18.0
built from commit ae7977b7d1ca908674a0d45c5c243c766fa4b2ca
release image registry.ci.openshift.org/origin/release:4.18ocp-
release@sha256:0da6316466d60a3a4535d5fed3589feb0391989982fba59d47d
4c729912d6363
release architecture amd64
```

- 管理者権限で OpenShift Container Platform にログインしている。

手順

1. 次のコマンドを実行して、設定ファイルを保存するインストールディレクトリーを作成します。

```
$ mkdir ~/<directory_name>
```

2. 組織のニーズに合わせて **install-config.yaml** 設定ファイルを設定し、作成したディレクトリーにファイルを保存します。

外部プラットフォームを設定する install-config.yaml ファイル

```
# install-config.yaml
apiVersion: v1
baseDomain: <base_domain> 1
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  network type: OVNKubernetes
  machineNetwork:
  - cidr: <ip_address_from_cidr> 2
  serviceNetwork:
  - 172.30.0.0/16
compute:
  - architecture: amd64 3
```

```
    hyperthreading: Enabled
    name: worker
    replicas: 0
  controlPlane:
    architecture: amd64 (4)
    hyperthreading: Enabled
    name: master
    replicas: 3
  platform:
    external:
      platformName: oci (5)
      cloudControllerManager: External
  sshKey: <public_ssh_key> (6)
  pullSecret: '<pull_secret>' (7)
  # ...
```

1. クラウドプロバイダーのベースドメイン。
2. ネットワーク上で機能するリソースおよびコンポーネントに対して CIDR が割り当てる仮想クラウドネットワーク (VCN) の IP アドレス。
3. 4. インフラストラクチャーに応じて、**arm64** または **amd64** のいずれかを選択できます。
5. OpenShift Container Platform が OCI と統合できるように、**OCI** を外部プラットフォームとして設定します。
6. SSH 公開鍵を指定します。
7. OpenShift Container Platform コンポーネントおよびサービス (Quay.io など) のコンテナーイメージをダウンロードするときに認証するために必要なプルシークレット。Red Hat Hybrid Cloud Console の Install OpenShift Container Platform 4 を参照してください。

3. ローカルシステム上に **openshift** という名前のディレクトリーを作成します。これはインストールディレクトリーのサブディレクトリーである必要があります。

重要

install-config.yaml または **agent-config.yaml** 設定ファイルを **openshift** ディレクトリーに移動しないでください。

4. Oracle カスタムマニフェストファイルを設定します。
   a. OpenShift Cluster Setup with Agent Based Installer on Compute Cloud@Customer (Oracle ドキュメント) の「Prepare the OpenShift Master Images」にアクセスします。
   b. **oci-ccm.yml**、**oci-csi.yml**、**machineconfig-ccm.yml** ファイルをコピーして、**openshift** ディレクトリーに貼り付けます。
   c. **oci-ccm.yml** ファイルと **oci-csi.yml** ファイルを編集して、コンパートメントの Oracle® Cloud Identifier (OCID)、VCN の OCID、ロードバランサーからのサブネットの OCID、セキュリティーリストの OCID、および **c3-cert.pem** セクションを指定します。
5. 組織の要件に合わせて **agent-config.yaml** 設定ファイルを設定します。

IPv4 ネットワーク用のサンプル agent-config.yaml ファイル

```
apiVersion: v1beta1
metadata:
  name: <cluster_name> 1
  namespace: <cluster_namespace> 2
rendezvousIP: <ip_address_from_CIDR> 3
bootArtifactsBaseURL: <server_URL> 4
# ...
```

1. DNS レコードに指定したクラスター名。
2. OpenShift Container Platform 上のクラスターの namespace。
3. ネットワーク IP アドレス形式として IPv4 を使用する場合は、**rendezvousIP** パラメーターを、VCN の Classless Inter-Domain Routing (CIDR) 方式によってネットワークに割り当てられる IPv4 アドレスに必ず設定してください。また、ISO を使用して起動したインスタンスプール内の少なくとも 1 つのインスタンスが、**rendezvousIP** パラメーターに設定した IP アドレス値と一致していることを確認してください。
4. rootfs イメージをアップロードするサーバーの URL。このパラメーターは、非接続環境でのみ必要です。

6. インストールディレクトリーで次のコマンドを入力して、rootfs イメージを除外した最小限の ISO イメージを生成します。

```
$ ./openshift-install agent create image --log-level debug
```

このコマンドは次の操作も実行します。

- サブディレクトリー **./<installation_directory>/auth directory:** を作成し、そのサブディレクトリーに **kubeadmin-password** ファイルと **kubeconfig** ファイルを配置します。
- **agent-config.yaml** 設定ファイルで指定した IP アドレスに基づいて、 **rendezvousIP** ファイルを作成します。
- オプション: **agent-config.yaml** および **install-config.yaml** 設定ファイルに加えた変更は、すべてゼロタッチプロビジョニング (ZTP) カスタムリソースにインポートされます。

重要

Agent-based Installer は Red Hat Enterprise Linux CoreOS (RHCOS) を使用します。後のステップで説明する rootfs イメージは、オペレーティングシステムの起動、回復、修復に必要です。

7. 非接続環境のみ: rootfs イメージを Web サーバーにアップロードします。

   a. 最小限の ISO イメージを作成したときに生成された **./<installation_directory>/boot-artifacts** ディレクトリーに移動します。

   b. 任意の Hypertext Transfer Protocol デーモン (**httpd**) などの優先 Web サーバーを使用して、**agent-config.yaml** ファイルの **bootArtifactsBaseURL** パラメーターに指定された場所に rootfs イメージをアップロードします。

たとえば、**bootArtifactsBaseURL** パラメーターに **http://192.168.122.20** と指定されている場合、生成された rootfs イメージをこの場所にアップロードして、Agent-based Installer が **http://192.168.122.20/agent.x86_64-rootfs.img** からイメージにアクセスできるようにします。Agent-based Installer は、外部プラットフォームの最小限の ISO を起動した後、**http://192.168.122.20/agent.x86_64-rootfs.img** の場所から rootfs イメージをシステムメモリーにダウンロードします。

注記

また、Agent-based Installer は、Operator がクラスターのノードを起動するときに rootfs イメージをシステムメモリーにダウンロードするために、**bootArtifactsBaseURL** の値を最小限の ISO イメージの設定に追加します。

重要

1 GB を超える完全な ISO イメージには、rootfs イメージが含まれていることに注意してください。このイメージは、通常 **150** MB 未満の最小 ISO イメージよりも大きくなります。

関連情報

- OpenShift Container Platform のインストール
- クラスターのインストールタイプの選択
- Agent-based Installer を使用したインストールの準備
- Agent-based Installer のダウンロード
- mirror registry for Red Hat OpenShift を使用したミラーレジストリーの作成
- OpenShift Container Platform イメージリポジトリーのミラーリング
- オプション: ZTP マニフェストの使用

3.4. OPENSHIFT CONTAINER PLATFORM のファイアウォールの設定

OpenShift Container Platform をインストールする前に、ファイアウォールを、OpenShift Container Platform が必要とするサイトへのアクセスを付与するように設定する必要があります。ファイアウォールを使用する場合は、OpenShift Container Platform が機能するために必要なサイトにアクセスできるように、ファイアウォールに追加の設定を行います。

ワーカーノードと比較して、コントローラーノードのみで実行されるサービスには、特別な設定上の考慮事項はありません。

注記

ご使用の環境で OpenShift Container Platform クラスターの前に専用のロードバランサーがある場合は、ファイアウォールとロードバランサーの間の許可リストを確認して、クラスターに対する不要なネットワーク制限を回避してください。

手順

1. ファイアウォールの許可リストに次のレジストリー URL を設定します。

URL	ポート	機能
registry.redhat.io	443	コアコンテナーイメージを指定します。
access.redhat.com	443	コンテナークライアントが **registry.access.redhat.com** から取得したイメージを検証するのに必要な署名ストアをホストします。ファイアウォール環境では、このリソースが許可リストに含まれていることを確認してください。
registry.access.redhat.com	443	コアコンテナーイメージを含め、Red Hat Ecosystem Catalog に保存されているすべてのコンテナーイメージをホストします。
quay.io	443	コアコンテナーイメージを指定します。
cdn.quay.io	443	コアコンテナーイメージを指定します。
cdn01.quay.io	443	コアコンテナーイメージを指定します。
cdn02.quay.io	443	コアコンテナーイメージを指定します。
cdn03.quay.io	443	コアコンテナーイメージを指定します。
cdn04.quay.io	443	コアコンテナーイメージを指定します。
cdn05.quay.io	443	コアコンテナーイメージを指定します。
cdn06.quay.io	443	コアコンテナーイメージを指定します。
sso.redhat.com	443	**https://console.redhat.com** サイトは、**sso.redhat.com** からの認証を使用します。
icr.io	443	IBM Cloud Pak コンテナーイメージを提供します。このドメインは、IBM Cloud Paks を使用する場合にのみ必要です。
cp.icr.io	443	IBM Cloud Pak コンテナーイメージを提供します。このドメインは、IBM Cloud Paks を使用する場合にのみ必要です。

- 許可リストでは、**cdn.quay.io** と **cdn0[1-6].quay.io** の代わりにワイルドカード ***.quay.io** を使用できます。

- ワイルドカード ***.access.redhat.com** を使用すると、設定を簡素化し、**registry.access.redhat.com** を含むすべてのサブドメインを許可できます。

- **quay.io** などのサイトを許可リストに追加するには、***.quay.io** などのワイルドカードエントリーを拒否リストに加えないでください。ほとんどの場合、イメージレジストリーはコンテンツ配信ネットワーク (CDN) を使用してイメージを提供します。ファイアウォールがアクセスをブロックすると、最初のダウンロード要求が **cdn01.quay.io** などのホスト名にリダイレクトされるときに、イメージのダウンロードが拒否されます。

2. ファイアウォールの許可リストを設定し、ビルドに必要な言語またはフレームワークのリソースを提供するサイトをリストに含めます。

3. Telemetry を無効にしていない場合は、以下の URL へのアクセスを許可して Red Hat Insights にアクセスできるようにする必要があります。

URL	ポート	機能
cert-api.access.redhat.com	443	Telemetry で必須
api.access.redhat.com	443	Telemetry で必須
infogw.api.openshift.com	443	Telemetry で必須
console.redhat.com	443	Telemetry および **insights-operator** で必須

4. Alibaba Cloud、Amazon Web Services (AWS)、Microsoft Azure、または Google Cloud を使用してクラスターをホストする場合は、そのクラウドのクラウドプロバイダー API と DNS を提供する URL へのアクセスを許可する必要があります。

クラウド	URL	ポート	機能
Alibaba	***.aliyuncs.com**	443	Alibaba Cloud のサービスとリソースにアクセスするために必要です。Alibaba の endpoints_config.go ファイル を参照して、使用するリージョンを許可する正確なエンドポイントを確認してください。
AWS	**aws.amazon.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.amazonaws.com** または、AWS API にワイルドカードを使用しない場合は、次の URL を許可リストに含める必要があります。	443	AWS サービスおよびリソースへのアクセスに必要です。AWS ドキュメントの AWS Service Endpoints を参照して、使用するリージョンを許可する正確なエンドポイントを確認してください。

クラウド	URL	ポート	機能
	ec2.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	events.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	iam.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	route53.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.s3.amazonaws.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.s3.<aws_region>.amazonaws.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.s3.dualstack.<aws_region>.amazonaws.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	sts.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	sts.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	tagging.us-east-1.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。このエンドポイントは、クラスターがデプロイされているリージョンに関係なく、常に **us-east-1** です。
	ec2.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	elasticloadbalancing.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	servicequotas.<aws_region>.amazonaws.com	443	必須。サービスをデプロイするためのクォータを確認するのに使用されます。

クラウド	URL	ポート	機能
	tagging.<aws_region>.amazonaws.com	443	タグの形式で AWS リソースに関するメタデータを割り当てることができます。
	***.cloudfront.net**	443	CloudFront へのアクセスを提供するために使用されます。AWS Security Token Service (STS) およびプライベート S3 バケットを使用する場合は、CloudFront へのアクセスを提供する必要があります。
GCP	***.googleapis.com**	443	Google Cloud のサービスとリソースへのアクセスに必要。Google Cloud ドキュメントの Cloud Endpoints を確認して、API を許可するエンドポイントを見つけます。
	accounts.google.com	443	Google Cloud アカウントにアクセスするために必要。
Microsoft Azure	**management.azure.com**	443	Microsoft Azure のサービスとリソースにアクセスするために必要です。Microsoft Azure ドキュメントの Microsoft Azure REST API reference を参照して、お使いの API を許可するエンドポイントを確認してください。
	***.blob.core.windows.net**	443	Ignition ファイルのダウンロードに必要です。
	login.microsoftonline.com	443	Microsoft Azure のサービスとリソースにアクセスするために必要です。Microsoft Azure ドキュメントの Azure REST API reference を参照して、お使いの API を許可するエンドポイントを確認してください。

5. 以下の URL を許可リストに指定します。

URL	ポート	機能
***.apps.<cluster_name>.<base_domain>**	443	Ingress ワイルドカードをインストール時に設定しない限り、デフォルトのクラスタールートへのアクセスに必要です。

URL	ポート	機能
api.openshift.com	443	クラスタートークンの両方が必要であり、クラスターに更新が利用可能かどうかを確認するために必要です。
console.redhat.com	443	クラスタートークンに必要です。
mirror.openshift.com	443	ミラーリングされたインストールのコンテンツおよびイメージへのアクセスに必要です。Cluster Version Operator には単一の機能ソースのみが必要ですが、このサイトはリリースイメージ署名のソースでもあります。
quayio-production-s3.s3.amazonaws.com	443	AWS で Quay イメージコンテンツにアクセスするために必要です。
rhcos.mirror.openshift.com	443	Red Hat Enterprise Linux CoreOS (RHCOS) イメージをダウンロードするために必要です。
sso.redhat.com	443	**https://console.redhat.com** サイトは、**sso.redhat.com** からの認証を使用します。
storage.googleapis.com/openshift-release	443	リリースイメージ署名のソース。ただし、Cluster Version Operator には単一の機能ソースのみが必要です。

Operator にはヘルスチェックを実行するためのルートアクセスが必要です。具体的には、認証および Web コンソール Operator は 2 つのルートに接続し、ルートが機能することを確認します。クラスター管理者として操作を実行しており、***.apps.<cluster_name>.<base_domain>** を許可しない場合は、これらのルートを許可します。

- **oauth-openshift.apps.<cluster_name>.<base_domain>**
- **canary-openshift-ingress-canary.apps.<cluster_name>.<base_domain>**
- **console-openshift-console.apps.<cluster_name>.<base_domain>**、またはフィールドが空でない場合に **consoles.operator/cluster** オブジェクトの **spec.route.hostname** フィールドに指定されるホスト名

6. オプションのサードパーティーコンテンツに対する次の URL を許可リストに追加します。

URL	ポート	機能
registry.connect.redhat.com	443	すべてのサードパーティーのイメージと認定 Operator に必要です。

7. デフォルトの Red Hat Network Time Protocol (NTP) サーバーを使用する場合は、以下の URL を許可します。
   - **1.rhel.pool.ntp.org**
   - **2.rhel.pool.ntp.org**
   - **3.rhel.pool.ntp.org**

注記

デフォルトの Red Hat NTP サーバーを使用しない場合は、プラットフォームの NTP サーバーを確認し、ファイアウォールでこれを許可します。

3.5. COMPUTE CLOUD@CUSTOMER でのクラスターの実行

Oracle® Compute Cloud@Customer でクラスターを実行するには、まず生成されたエージェント ISO イメージを OCI イメージに変換し、OCI Home Region Bucket にアップロードしてから、アップロードしたイメージを Compute Cloud@Customer システムにインポートする必要があります。

注記

Compute Cloud@Customer は、次の OpenShift Container Platform クラスタートポロジーをサポートしています。

- シングルノードへの OpenShift Container Platform クラスターのインストール
- 少なくとも 3 つのコントロールプレーンインスタンスと 2 つのコンピュートインスタンスを持つ高可用性クラスター
- 少なくとも 3 つのコントロールプレーンインスタンスを持つコンパクトな 3 ノードクラスター

前提条件

- エージェント ISO イメージを生成した。「Compute Cloud@Customer にクラスターをインストールするための設定ファイルの作成」セクションを参照してください。

手順

1. エージェント ISO イメージを OCI イメージに変換し、OCI Home Region Bucket にアップロードしてから、アップロードしたイメージを Compute Cloud@Customer システムにインポートします。手順は、OpenShift Cluster Setup with Agent Based Installer on Compute Cloud@Customer (Oracle ドキュメント) の「Prepare the OpenShift Master Images」を参照してください。
2. Compute Cloud@Customer にコントロールプレーンインスタンスを作成します。手順は、OpenShift Cluster Setup with Agent Based Installer on Compute Cloud@Customer (Oracle ドキュメント) の「Create control plane instances on C3 and Master Node LB Backend Sets」を参照してください。
3. クラスタートポロジー用に提供されたベースイメージからコンピュートインスタンスを作成します。手順は、OpenShift Cluster Setup with Agent Based Installer on Compute Cloud@Customer (Oracle ドキュメント) の「Add worker nodes」を参照してください。

重要

コンピュートインスタンスを作成する前に、クラスターに十分なメモリーとディスクリソースがあることを確認してください。さらに、少なくとも 1 つのコンピュートインスタンスが、**agent-config.yaml** ファイルの **rendezvousIP** に記載されているアドレスと同じ IP アドレスを持っていることを確認してください。

3.6. エージェントベースのクラスターインストールが COMPUTE CLOUD@CUSTOMER 上で動作していることを確認する

クラスターが Compute Cloud@Customer にインストールされ、適切に動作していることを確認します。

前提条件

- 必要なすべての Oracle® Compute Cloud@Customer リソースとサービスを作成した。「Oracle Compute Cloud@Customer インフラストラクチャーのリソースとサービスの作成」セクションを参照してください。
- **install-config.yaml** 設定ファイルと **agent-config.yaml** 設定ファイルを作成した。「Compute Cloud@Customer にクラスターをインストールするための設定ファイルの作成」セクションを参照してください。
- エージェント ISO イメージをデフォルトの Oracle Object Storage バケットにアップロードし、Compute Cloud@Customer 上にコンピュートインスタンスを作成した。詳細は、「Compute Cloud@Customer でのクラスターの実行」を参照してください。

手順

OpenShift Container Platform クラスター内の自己管理ノードにコンピュートインスタンスをデプロイした後、以下のいずれかの方法でクラスターのステータスを監視できます。

- OpenShift Container Platform CLI から次のコマンドを入力します。

  ```
  $ ./openshift-install agent wait-for install-complete --log-level debug
  ```

  ブートストラップノードが動作する **rendezvous** ホストノードの状態を確認します。ホストが再起動すると、ホストはクラスターの一部となります。

- **kubeconfig** API を使用して、さまざまな OpenShift Container Platform コンポーネントのステータスを確認します。**KUBECONFIG** 環境変数に、クラスターの **kubeconfig** 設定ファイルの相対パスを設定します。

  ```
  $  export KUBECONFIG=~/auth/kubeconfig
  ```

  クラスターの各自己管理ノードのステータスを確認します。CCM は、各ノードにラベルを適用して、ノードを OCI 上のクラスターで実行するよう指定します。

  ```
  $ oc get nodes -A
  ```

  出力例

  ```
  NAME                                STATUS ROLES                 AGE VERSION
  main-0.private.agenttest.oraclevcn.com Ready  control-plane, master 7m  v1.27.4+6eeca63
  ```

```
main-1.private.agenttest.oraclevcn.com Ready  control-plane, master 15m v1.27.4+d7fa83f
main-2.private.agenttest.oraclevcn.com Ready  control-plane, master 15m v1.27.4+d7fa83f
```

クラスターの各 Operator のステータスを確認します。CCM Operator のステータスは、クラスターが実行中であることを示す適切な指標です。

```
$ oc get co
```

出力例 (一部のみ記載)

```
NAME           VERSION     AVAILABLE  PROGRESSING    DEGRADED   SINCE
MESSAGE
authentication 4.18.0-0    True       False          False      6m18s
baremetal      4.18.0-0    True       False          False      2m42s
network        4.18.0-0    True       True           False      5m58s  Progressing: …
    …
```

3.7. 関連情報

- 失敗したエージェントベースのインストールからログデータを収集する
- オンプレミスクラスターにワーカーノードを追加する

第4章 AGENT-BASED INSTALLER を使用した ORACLE PRIVATE CLOUD APPLIANCE へのクラスターのインストール

Agent-based Installer を使用して Oracle® Private Cloud Appliance にクラスターをインストールすることで、Oracle® Cloud Infrastructure (OCI) サービスを引き続き使用しながら、オンプレミスインフラストラクチャーでクラスターワークロードを実行できるようになります。

4.1. インストールプロセスのワークフロー

次のワークフローは、Agent-based Installer を使用して Private Cloud Appliance に OpenShift Container Platform クラスターをインストールするプロセスの概要を示しています。

1. Private Cloud Appliance のリソースとサービスを作成します (Oracle)。
2. Agent-based Installer 用の設定ファイルを準備します (Red Hat)。
3. エージェント ISO イメージを生成します (Red Hat)。
4. ISO イメージを Oracle Cloud Infrastructure (OCI) イメージに変換し、OCI Home Region Bucket にアップロードしてから、アップロードしたイメージを Private Cloud Appliance システム (Oracle) にインポートします。
5. 非接続環境: OCI インスタンスからアクセスできる Web サーバーを準備します (Red Hat)。
6. 非接続環境: rootfs イメージを Web サーバーにアップロードします (Red Hat)。
7. OpenShift Container Platform のファイアウォールを設定します (Red Hat)。
8. コントロールプレーンノードを作成し、ロードバランサーを設定します (Oracle)。
9. コンピュートノードを作成し、ロードバランサーを設定します (Oracle)。
10. クラスターが OCI 上で稼働していることを確認します (Oracle)。

4.2. ORACLE PRIVATE CLOUD APPLIANCE インフラストラクチャーのリソースとサービスの作成

仮想マシン (VM) シェイプ上に Private Cloud Appliance 環境を作成する必要があります。この環境を作成すると、OpenShift Container Platform をインストールし、幅広いクラウドオプションと強力なセキュリティーポリシーをサポートするインフラストラクチャーにクラスターをデプロイできます。OCI コンポーネントに関する事前の知識があれば、OCI リソースの概念を理解し、組織のニーズに合わせてリソースを設定する方法を理解するのに役立ちます。

重要

OpenShift Container Platform との互換性を確保するには、各 DNS レコードのレコードタイプとして **A** を設定し、次のようにレコードに名前を付ける必要があります。

- **api.<cluster_name>.<base_domain>**。これは API ロードバランサーの **apiVIP** パラメーターをターゲットとしています。
- **api-int.<cluster_name>.<base_domain>**。これは API ロードバランサーの **apiVIP** パラメーターをターゲットとしています。
- ***.apps.<cluster_name>.<base_domain>**。これは Ingress ロードバランサーの **ingressVIP** パラメーターをターゲットとしています。

api.* および **api-int.*** DNS レコードは、コントロールプレーンマシンに関連しています。そのため、インストールした OpenShift Container Platform クラスター内のすべてのノードがこれらの DNS レコードにアクセスできることを確認する必要があります。

前提条件

- OpenShift Container Platform クラスターをホストするために OCI アカウントを設定しました。OpenShift Cluster Setup with Agent Based Installer on Private Cloud Appliance (Oracle ドキュメント) の「Access and Considerations」を参照してください。

手順

- Private Cloud Appliance の必要なリソースとサービスを作成します。
  詳細は、OpenShift Cluster Setup with Agent Based Installer on Private Cloud Appliance (Oracle ドキュメント) の「Terraform Script Execution」を参照してください。

関連情報

- Learn About Oracle Cloud Basics (Oracle ドキュメント)

4.3. PRIVATE CLOUD APPLIANCE にクラスターをインストールするための設定ファイルの作成

Agent-based Installer を使用して起動可能な ISO イメージを生成できるように、**install-config.yaml** 設定ファイルと **agent-config.yaml** 設定ファイルを作成する必要があります。エージェントベースのインストールは、Assisted Discovery Agent と Assisted Service を含む起動可能な ISO で構成されます。これらのコンポーネントは、クラスターのインストールを実行するために両方とも必要ですが、後者のコンポーネントはいずれか 1 つのホストでのみ実行されます。

注記

Agent-based Installer を使用して、ゼロタッチプロビジョニング (ZTP) カスタムリソースを生成または受け入れることもできます。

前提条件

- OpenShift Container Platform のインストールおよび更新プロセスの詳細を確認した。
- クラスターのインストール方法の選択とその方法の準備に関するユーザー向けドキュメントを確認した。

- 「Agent-based Installer を使用したインストールの準備」ドキュメントを確認した。
- Red Hat Hybrid Cloud Console から Agent-based Installer とコマンドラインインターフェイス (CLI) をダウンロードした。
- 非接続環境にインストールする場合は、環境にミラーレジストリーを準備し、リリースイメージをレジストリーにミラーリングした。

> **重要**
>
> 次のコマンドを実行して、**openshift-install** バイナリーのバージョンが、Red Hat Quay などの共有レジストリーではなく、ローカルイメージコンテナーレジストリーに関連していることを確認してください。
>
> ```
> $ ./openshift-install version
> ```
>
> **共有レジストリーバイナリーの出力例**
>
> ```
> ./openshift-install 4.18.0
> built from commit ae7977b7d1ca908674a0d45c5c243c766fa4b2ca
> release image registry.ci.openshift.org/origin/release:4.18ocp-release@sha256:0da6316466d60a3a4535d5fed3589feb0391989982fba59d47d4c729912d6363
> release architecture amd64
> ```

- 管理者権限で OpenShift Container Platform にログインしている。

手順

1. 次のコマンドを実行して、設定ファイルを保存するインストールディレクトリーを作成します。

```
$ mkdir ~/<directory_name>
```

2. 組織のニーズに合わせて **install-config.yaml** 設定ファイルを設定し、作成したディレクトリーにファイルを保存します。

外部プラットフォームを設定する install-config.yaml ファイル

```
# install-config.yaml
apiVersion: v1
baseDomain: <base_domain> 1
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  network type: OVNKubernetes
  machineNetwork:
  - cidr: <ip_address_from_cidr> 2
  serviceNetwork:
  - 172.30.0.0/16
compute:
  - architecture: amd64 3
```

```
    hyperthreading: Enabled
    name: worker
    replicas: 0
  controlPlane:
    architecture: amd64 (4)
    hyperthreading: Enabled
    name: master
    replicas: 3
  platform:
     external:
      platformName: oci (5)
      cloudControllerManager: External
  sshKey: <public_ssh_key> (6)
  pullSecret: '<pull_secret>' (7)
  # ...
```

1. クラウドプロバイダーのベースドメイン。
2. ネットワーク上で機能するリソースおよびコンポーネントに対して CIDR が割り当てる仮想クラウドネットワーク (VCN) の IP アドレス。
3. 4. インフラストラクチャーに応じて、**arm64** または **amd64** のいずれかを選択できます。
5. OpenShift Container Platform が OCI と統合できるように、**OCI** を外部プラットフォームとして設定します。
6. SSH 公開鍵を指定します。
7. OpenShift Container Platform コンポーネントおよびサービス (Quay.io など) のコンテナーイメージをダウンロードするときに認証するために必要なプルシークレット。Red Hat Hybrid Cloud Console の Install OpenShift Container Platform 4 を参照してください。

3. ローカルシステム上に **openshift** という名前のディレクトリーを作成します。これはインストールディレクトリーのサブディレクトリーである必要があります。

重要

install-config.yaml または **agent-config.yaml** 設定ファイルを **openshift** ディレクトリーに移動しないでください。

4. Oracle カスタムマニフェストファイルを設定します。
   a. OpenShift Cluster Setup with Agent Based Installer on Private Cloud Appliance (Oracle ドキュメント) の「Prepare the OpenShift Master Images」にアクセスします。
   b. **oci-ccm.yml**、**oci-csi.yml**、**machineconfig-ccm.yml** ファイルをコピーして、**openshift** ディレクトリーに貼り付けます。
   c. **oci-ccm.yml** ファイルと **oci-csi.yml** ファイルを編集して、コンパートメントの Oracle® Cloud Identifier (OCID)、VCN の OCID、ロードバランサーからのサブネットの OCID、セキュリティーリストの OCID、および **c3-cert.pem** セクションを指定します。
5. 組織の要件に合わせて **agent-config.yaml** 設定ファイルを設定します。

IPv4 ネットワーク用のサンプル agent-config.yaml ファイル

```
apiVersion: v1beta1
metadata:
  name: <cluster_name> 1
  namespace: <cluster_namespace> 2
rendezvousIP: <ip_address_from_CIDR> 3
bootArtifactsBaseURL: <server_URL> 4
# ...
```

1. DNS レコードに指定したクラスター名。
2. OpenShift Container Platform 上のクラスターの namespace。
3. ネットワーク IP アドレス形式として IPv4 を使用する場合は、**rendezvousIP** パラメーターを、VCN の Classless Inter-Domain Routing (CIDR) 方式によってネットワークに割り当てられる IPv4 アドレスに必ず設定してください。また、ISO を使用して起動したインスタンスプール内の少なくとも 1 つのインスタンスが、**rendezvousIP** パラメーターに設定した IP アドレス値と一致していることを確認してください。
4. rootfs イメージをアップロードするサーバーの URL。このパラメーターは、非接続環境でのみ必要です。

6. インストールディレクトリーで次のコマンドを入力して、rootfs イメージを除外した最小限の ISO イメージを生成します。

```
$ ./openshift-install agent create image --log-level debug
```

このコマンドは次の操作も実行します。

- サブディレクトリー **./<installation_directory>/auth directory:** を作成し、そのサブディレクトリーに **kubeadmin-password** ファイルと **kubeconfig** ファイルを配置します。
- **agent-config.yaml** 設定ファイルで指定した IP アドレスに基づいて、 **rendezvousIP** ファイルを作成します。
- オプション: **agent-config.yaml** および **install-config.yaml** 設定ファイルに加えた変更は、すべてゼロタッチプロビジョニング (ZTP) カスタムリソースにインポートされます。

重要

Agent-based Installer は Red Hat Enterprise Linux CoreOS (RHCOS) を使用します。後のステップで説明する rootfs イメージは、オペレーティングシステムの起動、回復、修復に必要です。

7. 非接続環境のみ: rootfs イメージを Web サーバーにアップロードします。
   a. 最小限の ISO イメージを作成したときに生成された **./<installation_directory>/boot-artifacts** ディレクトリーに移動します。
   b. 任意の Hypertext Transfer Protocol デーモン (**httpd**) などの優先 Web サーバーを使用して、**agent-config.yaml** ファイルの **bootArtifactsBaseURL** パラメーターに指定された場所に rootfs イメージをアップロードします。

たとえば、**bootArtifactsBaseURL** パラメーターに **http://192.168.122.20** と指定されている場合、生成された rootfs イメージをこの場所にアップロードして、Agent-based Installer が **http://192.168.122.20/agent.x86_64-rootfs.img** からイメージにアクセスできるようにします。Agent-based Installer は、外部プラットフォームの最小限の ISO を起動した後、**http://192.168.122.20/agent.x86_64-rootfs.img** の場所から rootfs イメージをシステムメモリーにダウンロードします。

注記

また、Agent-based Installer は、Operator がクラスターのノードを起動するときに rootfs イメージをシステムメモリーにダウンロードするために、**bootArtifactsBaseURL** の値を最小限の ISO イメージの設定に追加します。

重要

1 GB を超える完全な ISO イメージには、rootfs イメージが含まれていることに注意してください。このイメージは、通常 **150** MB 未満の最小 ISO イメージよりも大きくなります。

関連情報

- OpenShift Container Platform のインストール
- クラスターのインストールタイプの選択
- Agent-based Installer を使用したインストールの準備
- Agent-based Installer のダウンロード
- mirror registry for Red Hat OpenShift を使用したミラーレジストリーの作成
- OpenShift Container Platform イメージリポジトリーのミラーリング
- オプション: ZTP マニフェストの使用

4.4. OPENSHIFT CONTAINER PLATFORM のファイアウォールの設定

OpenShift Container Platform をインストールする前に、ファイアウォールを、OpenShift Container Platform が必要とするサイトへのアクセスを付与するように設定する必要があります。ファイアウォールを使用する場合は、OpenShift Container Platform が機能するために必要なサイトにアクセスできるように、ファイアウォールに追加の設定を行います。

ワーカーノードと比較して、コントローラーノードのみで実行されるサービスには、特別な設定上の考慮事項はありません。

注記

ご使用の環境で OpenShift Container Platform クラスターの前に専用のロードバランサーがある場合は、ファイアウォールとロードバランサーの間の許可リストを確認して、クラスターに対する不要なネットワーク制限を回避してください。

手順

1. ファイアウォールの許可リストに次のレジストリー URL を設定します。

URL	ポート	機能
registry.redhat.io	443	コアコンテナーイメージを指定します。
access.redhat.com	443	コンテナークライアントが **registry.access.redhat.com** から取得したイメージを検証するのに必要な署名ストアをホストします。ファイアウォール環境では、このリソースが許可リストに含まれていることを確認してください。
registry.access.redhat.com	443	コアコンテナーイメージを含め、Red Hat Ecosystem Catalog に保存されているすべてのコンテナーイメージをホストします。
quay.io	443	コアコンテナーイメージを指定します。
cdn.quay.io	443	コアコンテナーイメージを指定します。
cdn01.quay.io	443	コアコンテナーイメージを指定します。
cdn02.quay.io	443	コアコンテナーイメージを指定します。
cdn03.quay.io	443	コアコンテナーイメージを指定します。
cdn04.quay.io	443	コアコンテナーイメージを指定します。
cdn05.quay.io	443	コアコンテナーイメージを指定します。
cdn06.quay.io	443	コアコンテナーイメージを指定します。
sso.redhat.com	443	**https://console.redhat.com** サイトは、**sso.redhat.com** からの認証を使用します。
icr.io	443	IBM Cloud Pak コンテナーイメージを提供します。このドメインは、IBM Cloud Paks を使用する場合にのみ必要です。
cp.icr.io	443	IBM Cloud Pak コンテナーイメージを提供します。このドメインは、IBM Cloud Paks を使用する場合にのみ必要です。

- 許可リストでは、**cdn.quay.io** と **cdn0[1-6].quay.io** の代わりにワイルドカード ***.quay.io** を使用できます。

- ワイルドカード ***.access.redhat.com** を使用すると、設定を簡素化し、**registry.access.redhat.com** を含むすべてのサブドメインを許可できます。
- **quay.io** などのサイトを許可リストに追加するには、***.quay.io** などのワイルドカードエントリーを拒否リストに加えないでください。ほとんどの場合、イメージレジストリーはコンテンツ配信ネットワーク (CDN) を使用してイメージを提供します。ファイアウォールがアクセスをブロックすると、最初のダウンロード要求が **cdn01.quay.io** などのホスト名にリダイレクトされるときに、イメージのダウンロードが拒否されます。

2. ファイアウォールの許可リストを設定し、ビルドに必要な言語またはフレームワークのリソースを提供するサイトをリストに含めます。

3. Telemetry を無効にしていない場合は、以下の URL へのアクセスを許可して Red Hat Insights にアクセスできるようにする必要があります。

URL	ポート	機能
cert-api.access.redhat.com	443	Telemetry で必須
api.access.redhat.com	443	Telemetry で必須
infogw.api.openshift.com	443	Telemetry で必須
console.redhat.com	443	Telemetry および **insights-operator** で必須

4. Alibaba Cloud、Amazon Web Services (AWS)、Microsoft Azure、または Google Cloud を使用してクラスターをホストする場合は、そのクラウドのクラウドプロバイダー API と DNS を提供する URL へのアクセスを許可する必要があります。

クラウド	URL	ポート	機能
Alibaba	***.aliyuncs.com**	443	Alibaba Cloud のサービスとリソースにアクセスするために必要です。Alibaba の endpoints_config.go ファイル を参照して、使用するリージョンを許可する正確なエンドポイントを確認してください。
AWS	**aws.amazon.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.amazonaws.com** または、AWS API にワイルドカードを使用しない場合は、次の URL を許可リストに含める必要があります。	443	AWS サービスおよびリソースへのアクセスに必要です。AWS ドキュメントの AWS Service Endpoints を参照して、使用するリージョンを許可する正確なエンドポイントを確認してください。

クラウド	URL	ポート	機能
	ec2.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	events.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	iam.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	route53.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.s3.amazonaws.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.s3.<aws_region>.amazonaws.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	***.s3.dualstack.<aws_region>.amazonaws.com**	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	sts.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	sts.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	tagging.us-east-1.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。このエンドポイントは、クラスターがデプロイされているリージョンに関係なく、常に **us-east-1** です。
	ec2.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	elasticloadbalancing.<aws_region>.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび管理に使用されます。
	servicequotas.<aws_region>.amazonaws.com	443	必須。サービスをデプロイするためのクォータを確認するのに使用されます。

クラウド	URL	ポート	機能
	tagging.<aws_region>.amazonaws.com	443	タグの形式で AWS リソースに関するメタデータを割り当てることができます。
	***.cloudfront.net**	443	CloudFront へのアクセスを提供するために使用されます。AWS Security Token Service (STS) およびプライベート S3 バケットを使用する場合は、CloudFront へのアクセスを提供する必要があります。
GCP	***.googleapis.com**	443	Google Cloud のサービスとリソースへのアクセスに必要。Google Cloud ドキュメントの Cloud Endpoints を確認して、API を許可するエンドポイントを見つけます。
	accounts.google.com	443	Google Cloud アカウントにアクセスするために必要。
Microsoft Azure	**management.azure.com**	443	Microsoft Azure のサービスとリソースにアクセスするために必要です。Microsoft Azure ドキュメントの Microsoft Azure REST API reference を参照して、お使いの API を許可するエンドポイントを確認してください。
	***.blob.core.windows.net**	443	Ignition ファイルのダウンロードに必要です。
	login.microsoftonline.com	443	Microsoft Azure のサービスとリソースにアクセスするために必要です。Microsoft Azure ドキュメントの Azure REST API reference を参照して、お使いの API を許可するエンドポイントを確認してください。

5. 以下の URL を許可リストに指定します。

URL	ポート	機能
***.apps.<cluster_name>.<base_domain>**	443	Ingress ワイルドカードをインストール時に設定しない限り、デフォルトのクラスタールートへのアクセスに必要です。

URL	ポート	機能
api.openshift.com	443	クラスタートークンの両方が必要であり、クラスターに更新が利用可能かどうかを確認するために必要です。
console.redhat.com	443	クラスタートークンに必要です。
mirror.openshift.com	443	ミラーリングされたインストールのコンテンツおよびイメージへのアクセスに必要です。Cluster Version Operator には単一の機能ソースのみが必要ですが、このサイトはリリースイメージ署名のソースでもあります。
quayio-production-s3.s3.amazonaws.com	443	AWS で Quay イメージコンテンツにアクセスするために必要です。
rhcos.mirror.openshift.com	443	Red Hat Enterprise Linux CoreOS (RHCOS) イメージをダウンロードするために必要です。
sso.redhat.com	443	**https://console.redhat.com** サイトは、**sso.redhat.com** からの認証を使用します。
storage.googleapis.com/openshift-release	443	リリースイメージ署名のソース。ただし、Cluster Version Operator には単一の機能ソースのみが必要です。

Operator にはヘルスチェックを実行するためのルートアクセスが必要です。具体的には、認証および Web コンソール Operator は 2 つのルートに接続し、ルートが機能することを確認します。クラスター管理者として操作を実行しており、***.apps.<cluster_name>.<base_domain>** を許可しない場合は、これらのルートを許可します。

- **oauth-openshift.apps.<cluster_name>.<base_domain>**
- **canary-openshift-ingress-canary.apps.<cluster_name>.<base_domain>**
- **console-openshift-console.apps.<cluster_name>.<base_domain>**、またはフィールドが空でない場合に **consoles.operator/cluster** オブジェクトの **spec.route.hostname** フィールドに指定されるホスト名

6. オプションのサードパーティーコンテンツに対する次の URL を許可リストに追加します。

URL	ポート	機能
registry.connect.redhat.com	443	すべてのサードパーティーのイメージと認定 Operator に必要です。

7. デフォルトの Red Hat Network Time Protocol (NTP) サーバーを使用する場合は、以下の URL を許可します。
   - **1.rhel.pool.ntp.org**
   - **2.rhel.pool.ntp.org**
   - **3.rhel.pool.ntp.org**

注記

デフォルトの Red Hat NTP サーバーを使用しない場合は、プラットフォームの NTP サーバーを確認し、ファイアウォールでこれを許可します。

4.5. PRIVATE CLOUD APPLIANCE でのクラスターの実行

Oracle® Private Cloud Appliance でクラスターを実行するには、まず生成されたエージェント ISO イメージを OCI イメージに変換し、OCI Home Region Bucket にアップロードしてから、アップロードしたイメージを Private Cloud Appliance システムにインポートする必要があります。

注記

Private Cloud Appliance は、次の OpenShift Container Platform クラスタートポロジーをサポートしています。

- シングルノードへの OpenShift Container Platform クラスターのインストール
- 少なくとも 3 つのコントロールプレーンインスタンスと 2 つのコンピュートインスタンスを持つ高可用性クラスター
- 少なくとも 3 つのコントロールプレーンインスタンスを持つコンパクトな 3 ノードクラスター

前提条件

- エージェント ISO イメージを生成した。「Private Cloud Appliance にクラスターをインストールするための設定ファイルの作成」セクションを参照してください。

手順

1. エージェント ISO イメージを OCI イメージに変換し、OCI Home Region Bucket にアップロードしてから、アップロードしたイメージを Private Cloud Appliance システムにインポートします。手順は、OpenShift Cluster Setup with Agent Based Installer on Private Cloud Appliance (Oracle ドキュメント) の「Prepare the OpenShift Master Images」を参照してください。
2. Private Cloud Appliance にコントロールプレーンインスタンスを作成します。手順は、OpenShift Cluster Setup with Agent Based Installer on Private Cloud Appliance (Oracle ドキュメント) の「Create control plane instances on PCA and Master Node LB Backend Sets」を参照してください。
3. クラスタートポロジー用に提供されたベースイメージからコンピュートインスタンスを作成します。手順は、OpenShift Cluster Setup with Agent Based Installer on Private Cloud Appliance (Oracle ドキュメント) の「Add worker nodes」を参照してください。

> **重要**
>
> コンピュートインスタンスを作成する前に、クラスターに十分なメモリーとディスクリソースがあることを確認してください。さらに、少なくとも 1 つのコンピュートインスタンスが、**agent-config.yaml** ファイルの **rendezvousIP** に記載されているアドレスと同じ IP アドレスを持っていることを確認してください。

4.6. エージェントベースのクラスターインストールが PRIVATE CLOUD APPLIANCE 上で動作していることを確認する

クラスターが Private Cloud Appliance にインストールされ、適切に動作していることを確認します。

前提条件

- 必要なすべての Oracle® Private Cloud Appliance リソースとサービスを作成した。「Oracle Private Cloud Appliance インフラストラクチャーのリソースとサービスの作成」セクションを参照してください。
- **install-config.yaml** 設定ファイルと **agent-config.yaml** 設定ファイルを作成した。「Private Cloud Appliance にクラスターをインストールするための設定ファイルの作成」セクションを参照してください。
- エージェント ISO イメージをデフォルトの Oracle Object Storage バケットにアップロードし、Private Cloud Appliance にコンピュートインスタンスを作成した。詳細は、「Private Cloud Appliance でのクラスターの実行」を参照してください。

手順

OpenShift Container Platform クラスター内の自己管理ノードにコンピュートインスタンスをデプロイした後、以下のいずれかの方法でクラスターのステータスを監視できます。

- OpenShift Container Platform CLI から次のコマンドを入力します。

  ```
  $ ./openshift-install agent wait-for install-complete --log-level debug
  ```

  ブートストラップノードが動作する **rendezvous** ホストノードの状態を確認します。ホストが再起動すると、ホストはクラスターの一部となります。

- **kubeconfig** API を使用して、さまざまな OpenShift Container Platform コンポーネントのステータスを確認します。**KUBECONFIG** 環境変数に、クラスターの **kubeconfig** 設定ファイルの相対パスを設定します。

  ```
  $  export KUBECONFIG=~/auth/kubeconfig
  ```

  クラスターの各自己管理ノードのステータスを確認します。CCM は、各ノードにラベルを適用して、ノードを OCI 上のクラスターで実行するよう指定します。

  ```
  $ oc get nodes -A
  ```

  出力例

  ```
  NAME                                         STATUS ROLES                AGE VERSION
  main-0.private.agenttest.oraclevcn.com Ready  control-plane, master 7m  v1.27.4+6eeca63
  main-1.private.agenttest.oraclevcn.com Ready  control-plane, master 15m v1.27.4+d7fa83f
  ```

```
main-2.private.agenttest.oraclevcn.com Ready  control-plane, master 15m v1.27.4+d7fa83f
```

クラスターの各 Operator のステータスを確認します。CCM Operator のステータスは、クラスターが実行中であることを示す適切な指標です。

```
$ oc get co
```

出力例 (一部のみ記載)

```
NAME           VERSION     AVAILABLE  PROGRESSING    DEGRADED   SINCE
MESSAGE
authentication 4.18.0-0    True       False          False      6m18s
baremetal      4.18.0-0    True       False          False      2m42s
network        4.18.0-0    True       True           False      5m58s  Progressing: …
   …
```

4.7. 関連情報

- 失敗したエージェントベースのインストールからログデータを収集する
- オンプレミスクラスターにワーカーノードを追加する

第5章 ASSISTED INSTALLER を使用した ORACLE COMPUTE CLOUD@CUSTOMER へのクラスターのインストール

Oracle® Compute Cloud@Customer (C3) を使用すると、データセンターの高性能クラウドインフラストラクチャー上で Oracle® Cloud Infrastructure (OCI) サービスを使用して、アプリケーションとミドルウェアを実行できます。

5.1. 概要

Assisted Installer を使用して、Oracle Compute Cloud@Customer に OpenShift Container Platform をインストールできます。

別のインストール方法は、「Agent-based Installer を使用した Oracle® Compute Cloud@Customer へのクラスターのインストール」を参照してください。

インストール前の考慮事項

- インストールが Oracle の指定された前提条件を満たしていることを確認します。詳細は、Oracle ドキュメント の「Access and Considerations」セクションを参照してください。
- インフラストラクチャーが認定済みのものであり、互換性のあるクラウドインスタンスタイプを使用していることを確認します。詳細は、Oracle Cloud Infrastructure を参照してください。
- 必ず仮想マシン上でインストールを実行します。

インストールプロセス

インストールプロセスでは、OpenShift Container Platform クラスターの指定コンパートメント内に踏み台ホストが構築されます。踏み台ホストは、次の 2 つの Terraform スクリプトを実行するために使用されます。

- 最初のスクリプトは、Compute Cloud@Customer システムの OCI ホームリージョンに IAM リソース (2 つの動的グループと 1 つのポリシー) を構築します。
- 2 番目のスクリプトは、OpenShift Container Platform クラスターをサポートするためのインフラストラクチャーリソースを、Compute Cloud@Customer システム上に構築します。リソースには、OpenShift Container Platform VCN、パブリックサブネットとプライベートサブネット、ロードバランサー、インターネット GW、NAT GW、DNS サーバーが含まれます。スクリプトには、クラスターを形成するコントロールプレーンノードとコンピュートノードをアクティブ化するために必要なすべてのリソースが含まれています。

踏み台ホストは、OpenShift Container Platform の指定コンパートメントにインストールされ、Compute Cloud@Customer 親テナンシー内の指定された Compute Cloud@Customer DRG サブネットまたはインターネット GW サブネットを介して通信するように設定されます。

インストールプロセスでは、その後、クラスターを形成する外部および内部ロードバランサーとともに、3 つのコントロールプレーン (マスター) ノードと 3 つのコンピュート (ワーカー) ノードがプロビジョニングされます。これは、Oracle Cloud Infrastructure (OCI) の標準実装です。

主なステップ

手順の主なステップは次のとおりです。

1. Compute Cloud@Customer の踏み台サーバーを準備します。
2. ホームリージョンを介して Terraform スクリプトを実行します。

3. Oracle Cloud Infrastructure (OCI) 用の OpenShift Container Platform イメージを準備します。

4. Compute Cloud@Customer リージョンを介して Terraform スクリプトを実行します。

5. Assisted Installer Web コンソールを使用してクラスターをインストールします。

5.2. OCI 踏み台サーバーの準備

踏み台ホストを実装することで、Oracle Compute Cloud@Customer リソースへのアクセスをセキュアかつ効率的に管理して、プライベートインスタンスの保護を維持し、インスタンスへのアクセス元を制御されたセキュアなエントリーポイントに限定できます。

前提条件

- Oracle ドキュメント の「Bastion server - prerequisites」セクションを参照してください。

手順

1. 踏み台サーバーをインストールします。詳細は、Oracle ドキュメント の「Bastion Installation」セクションを参照してください。

2. Terraform スクリプトを実行するために使用する Terraform アプリケーションをインストールします。詳細は、Oracle ドキュメント の「Terraform Installation」セクションを参照してください。

3. OCI コマンドラインインターフェイス (CLI) をインストールして設定します。詳細は、Oracle ドキュメント の「Installing and Configuring the OCI CLI」セクションを参照してください。

関連情報

- Quick start - Installing the CLI (Oracle ドキュメント)

5.3. ホームリージョンを介した TERRAFORM スクリプトの実行

Terraform スクリプト **createInfraResources.tf** と **terraform.tfvars** を踏み台サーバーにコピーします。次に、**createInfraResources.tf** スクリプトを実行して、Compute Cloud@Customer OCI ホームリージョンに Dynamic Group Identity リソースを作成します。このリソースには、動的グループ、ポリシー、タグが含まれます。

前提条件

- 動的グループとポリシーを作成するためのテナント権限がある。ない場合は、この手順中に手動でプロビジョニングできます。

手順

1. SSH 経由で踏み台サーバーに接続します。

2. **OpenShift\createResourceOnHomeRegion** フォルダーを作成します。

3. C3_PCA GitHub リポジトリーから **createInfraResources.tf** ファイルと **terraform.tfvars** ファイルを **createResourceOnHomeRegion** フォルダーにコピーします。

4. ソース環境にアクセスできること、および C3 証明書がエクスポートされていることを確認します。

5. **createInfraResources.tf** Terraform スクリプトを実行します。

詳細な手順は、Oracle ドキュメント の「Terraform Script Execution Part-1 (Run Script via Home Region)」セクションを参照してください。

5.4. OCI イメージの準備

Red Hat ポータルの Assisted Installer で OpenShift Container Platform ISO イメージを生成します。次に、イメージを Oracle Cloud Infrastructure (OCI) 互換イメージに変換し、Oracle Compute Cloud@Customer 環境の **Custom Images** ページにアップロードします。

イメージは、踏み台サーバーや Oracle Solution Center などの環境ではなく、ラップトップ上で生成、変換、アップロードできます。

5.4.1. Assisted Installer でのイメージの生成

クラスターを作成し、検出 ISO イメージをダウンロードします。

手順

1. 認証情報を使用して、Assisted Installer Web コンソール にログインします。

2. **Red Hat OpenShift** タイルで、**OpenShift** を選択します。

3. **Red Hat OpenShift Container Platform** タイルで、**Create Cluster** を選択します。

4. **Cluster Type** ページで、**Cloud** タブの最後までスクロールし、**Oracle Cloud Infrastructure (virtual machines)** を選択します。

5. **Create an OpenShift Cluster** ページで、**Interactive** タイルを選択します。

6. **Cluster Details** ページで、次のフィールドに入力します。

フィールド	必要な操作
クラスター名	OpenShift Container Platform クラスターの名前を指定します。この名前は、Terraform スクリプトを使用してリソースを作成するときに使用した名前と同じです。名前は 1 - 54 文字にする必要があります。小文字の英数字またはハイフン (-) を使用できますが、先頭と末尾は小文字または数字にする必要があります。
Base domain	クラスターのベースドメインを指定します。これは、Compute Cloud@Customer で実行される Terraform スクリプトの **zone_dns** 変数に使用する値です。この値をメモしておきます。
OpenShift のバージョン	**OpenShift 4.16.20** を選択します。すぐに表示されない場合は、ドロップダウンメニューの最後までスクロールし、**Show all available versions** を選択して、検索ボックスにバージョンを入力します。

フィールド	必要な操作
Integrate with external partner platforms	**Oracle Cloud Infrastructure** を選択します。 この値を指定すると、**Include custom manifests** チェックボックスがデフォルトで選択され、**Custom manifests** ページがウィザードに追加されます。

7. 残りのフィールドはデフォルト設定のままにして、**Next** をクリックします。

8. **Operators** ページで、**Next** をクリックします。

9. **Host Discovery** ページで、**Add hosts** をクリックし、次の手順を実行します。

   注記

   最小限の ISO イメージは、Oracle Cloud Infrastructure (OCI) の必須の **Provisioning type** であり、変更できません。

   a. **SSH public key** フィールドに、次のコマンドの出力をコピーして SSH 公開鍵を追加します。

   ```
   $ cat ~/.ssh/id_rsa.put
   ```

   SSH 公開鍵は、すべての OpenShift Container Platform コントロールプレーンとコンピュートノードにインストールされます。

   b. **Show proxy settings** チェックボックスをクリックします。

   c. 先ほど設定した踏み台サーバーの **/etc/environment** ファイルからプロキシー変数を追加します。

   ```
   http_proxy=http://www-proxy.<your_domain>.com:80
   https_proxy=http://www-proxy.<your_domain>.com:80
   no_proxy=localhost,127.0.0.1,1,2,3,4,5,6,7,8,9,0,.<your_domain>.com
   #(ie.oracle.com,.oraclecorp.com)
   ```

   d. **Generate Discovery ISO** をクリックして、検出 ISO イメージファイルを生成します。

10. **Download Discovery ISO** をクリックして、ファイルをローカルシステムに保存します。ISO ファイルをダウンロードした後、必要に応じてファイル名を変更できます (例: **discovery_image_<your_cluster_name>.iso**)。

5.4.2. イメージの変換と Oracle Compute Cloud@Customer へのアップロード

ISO イメージを OCI イメージに変換し、OCI ホームリージョンのオブジェクトストアから Compute Cloud@Customer システムにアップロードします。

手順

1. イメージを ISO から OCI に変換します。

2. OCI イメージを OCI バケットにアップロードし、Pre-Authenticated Request (PAR) URL を生成します。

3. OCI イメージを Compute Cloud@Customer ポータルにインポートします。

4. 次のステップで使用するために、イメージの Oracle Cloud Identifier (OCID) をコピーします。

詳細な手順は、Oracle ドキュメント の「OpenShift Image Preparation」のステップ 6 - 8 を参照してください。

5.5. C3 リージョンを介した TERRAFORM スクリプトの実行

terraform.tfvars Terraform スクリプトを実行して、Compute Cloud@Customer 上にすべてのインフラストラクチャーリソースを作成します。これらのリソースには、OpenShift Container Platform VCN、パブリックおよびプライベートサブネット、ロードバランサー、インターネット GW、NAT GW、DNS サーバーが含まれます。

この手順では、3 つのコントロールプレーン (マスター) ノードと 3 つのコンピュート (ワーカー) ノードで構成されるクラスターをデプロイします。デプロイ後、ノードの名前を変更して再起動する必要があります。このプロセスにより、ノードが一時的に複製されるため、次の手順で手動でクリーンアップする必要があります。

手順

1. SSH 経由で踏み台サーバーに接続します。

2. C3 証明書の場所を設定し、証明書をエクスポートします。

3. **terraform.tfvars** スクリプトを実行して、3 つのコントロールプレーンノードと 3 つのコンピュートノードを作成します。

4. コントロールプレーンとコンピュートノードのラベルを更新します。

5. Compute Cloud@Customer ポータルでインスタンスを 1 つずつ停止して再起動します。

詳細な手順は、Oracle ドキュメント の「Terraform Script Execution - Part 2」セクションを参照してください。

5.6. ASSISTED INSTALLER WEB コンソールを使用したインストールの完了

インフラストラクチャーを設定すると、インスタンスが実行され、Red Hat に登録する準備が整います。

5.6.1. ノードロールの割り当て

Terraform スクリプトが正常に完了すると、クラスターに 12 個のホストがリストされます。3 つのコントロールプレーンホストと 3 つのコンピュートホストのステータスは "Disconnected" です。3 つのコントロールプレーンホストと 3 つのコンピュートホストのステータスは "Insufficient" です。

Disconnected のホストを削除し、残りのホストにロールを割り当てます。

手順

1. Assisted Installer Web コンソール からクラスターを選択し、**Host discovery** ページに移動します。
2. 各ホストのオプションボタンをクリックし、**Remove host** を選択して、"Disconnected" ステータスの 6 つのホストを削除します。残りのホストのステータスが "Insufficient" から "Ready" に変わります。このプロセスには最大 3 分かかる場合があります。
3. **Role** 列から、ブートサイズが 1.10 TB の 3 つのノードに **Control plane** ロールを割り当てます。ブートサイズが 100 GB の 3 つのノードに **Worker** ロールを割り当てます。
4. 名前が 63 文字未満のホストの名前を変更します。ホストのオプションボタンをクリックし、**Change hostname** を選択します。これを行わないと、クラスターのインストールが失敗します。
5. **Next** をクリックします。
6. **Storage** ページで、**Next** をクリックします。

5.6.2. ネットワークの設定

Networking ページで、**Some validations failed** ステータスが表示されたホストの NTP ソースを追加します。

手順

1. **Host inventory** テーブルで、このステータスが表示されている各ホストの **Some validations failed** リンクをクリックします。
2. **Add NTP sources** をクリックし、いずれかのノードに IP アドレス **169.254.169.254** を追加します。
3. すべての **Some validations failed** の表示が消えるまで 2 - 3 分待ちます。
4. **Next** を選択します。

5.6.3. カスタムマニフェストの追加

Oracle が提供する 4 つの必須カスタムマニフェストを作成、変更、アップロードします。

- **C3/custom_manifests_C3/manifests** フォルダーには、次のマニフェストが必須です。
  - **oci-ccm.yml**
  - **oci-csi.yml**
- **C3/custom_manifests_C3/openshift** フォルダーには、次のマニフェストが必須です。
  - **machineconfig-ccm.yml**
  - **machineconfig-csi.yml**

前提条件

- カスタムマニフェストを準備します。詳細は、Oracle ドキュメント の「Install the Cluster using the RH Assisted Installer UI」セクションのステップ 8 を参照してください。

手順

1. **Custom manifests** ページに移動します。
2. **oci-ccm.yml** および **oci-csi.yml** マニフェストファイルをアップロードして保存します。
   a. **Folder** フィールドで、**manifests** を選択します。
   b. **File name** フィールドに **oci-ccm.yml** と入力します。
   c. **Content** セクションで、**Browse** をクリックします。
   d. **C3/custom_ manifest_C3/manifests** フォルダーから oci-ccm.yml ファイルを選択します。
   e. **Add another manifest** をクリックし、**oci-csi.yml** ファイルに対して上記のサブステップを繰り返します。
3. **machineconfig-ccm.yml** および **machineconfig-csi.yml** マニフェストファイルをアップロードして保存します。
   a. **Add another manifest** をクリックします。
   b. **Folder** フィールドで、**openshift** を選択します。
   c. **File name** フィールドに **machineconfig-ccm.yml** と入力します。
   d. **Content** セクションで、**Browse** をクリックします。
   e. **C3/custom_ manifest_C3/openshift** フォルダーから machineconfig-ccm.yml ファイルを選択します。
   f. **Add another manifest** をクリックし、**machineconfig-csi.yml** ファイルに対して上記のサブステップを繰り返します。
4. **Next** をクリックしてカスタムマニフェストを保存します。
5. **Review and create** ページで、**Install cluster** をクリックして、OpenShift Container Platform クラスターを作成します。このプロセスには約 30 分かかります。

5.7. ORACLE COMPUTE CLOUD@CUSTOMER WEB コンソールから OPENSHIFT CONTAINER PLATFORM を開く

Oracle Compute Cloud@Customer から OpenShift Container Platform コンソールにアクセスする手順は、Oracle ドキュメント の「Install the Cluster using the RH Assisted Installer UI」セクションのステップ 15 - 17 を参照してください。