OpenShift Container Platform 4.13

IBM Cloud VPC へのインストール

OpenShift Container Platform IBM Cloud のインストール

Last Updated: 2025-11-10

OpenShift Container Platform 4.13 IBM Cloud VPC へのインストール

OpenShift Container Platform IBM Cloud のインストール

Legal Notice

Abstract

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

Table of Contents

第1章 IBM CLOUD VPC へのインストールの準備 **4**
1.1. 前提条件 4
1.2. IBM CLOUD VPC に OPENSHIFT CONTAINER PLATFORM をインストールするための要件 4
1.3. IBM CLOUD VPC に OPENSHIFT CONTAINER PLATFORM をインストールする方法の選択 4
1.4. 次のステップ 5

第2章 IBM CLOUD アカウントの設定 **6**
2.1. 前提条件 6
2.2. IBM CLOUD VPC のクォータと制限 6
2.3. DNS 解決の設定 7
2.4. IBM CLOUD VPC IAM ポリシーと API キー 10
2.5. サポート対象の IBM CLOUD VPC リージョン 12
2.6. 次のステップ 12

第3章 IBM CLOUD VPC 用の IAM の設定 **13**
3.1. 管理者レベルのシークレットを KUBE-SYSTEM プロジェクトに保存する代替方法 13
3.2. CLOUD CREDENTIAL OPERATOR ユーティリティーの設定 13
3.3. 次のステップ 14
3.4. 関連情報 15

第4章 カスタマイズを使用した IBM CLOUD VPC へのクラスターのインストール **16**
4.1. 前提条件 16
4.2. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス 16
4.3. クラスターノードの SSH アクセス用のキーペアの生成 16
4.4. インストールプログラムの取得 18
4.5. API キーのエクスポート 19
4.6. インストール設定ファイルの作成 19
4.7. IAM を手動で作成する 35
4.8. クラスターのデプロイ 38
4.9. バイナリーのダウンロードによる OPENSHIFT CLI のインストール 40
4.10. CLI の使用によるクラスターへのログイン 42
4.11. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス 42
4.12. 次のステップ 43

第5章 ネットワークをカスタマイズして IBM CLOUD VPC にクラスターをインストールする **44**
5.1. 前提条件 44
5.2. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス 44
5.3. クラスターノードの SSH アクセス用のキーペアの生成 44
5.4. インストールプログラムの取得 46
5.5. API キーのエクスポート 47
5.6. インストール設定ファイルの作成 47
5.7. IAM を手動で作成する 64
5.8. ネットワーク設定フェーズ 67
5.9. 高度なネットワーク設定の指定 68
5.10. CLUSTER NETWORK OPERATOR (CNO) の設定 69
5.11. クラスターのデプロイ 77
5.12. バイナリーのダウンロードによる OPENSHIFT CLI のインストール 78
5.13. CLI の使用によるクラスターへのログイン 80
5.14. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス 81
5.15. 次のステップ 81

第6章 クラスターの IBM CLOUD VPC の既存 VPC へのインストール **82**

6.1. 前提条件 82
6.2. カスタム VPC の使用について 82
6.3. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス 83
6.4. クラスターノードの SSH アクセス用のキーペアの生成 84
6.5. インストールプログラムの取得 85
6.6. API キーのエクスポート 86
6.7. インストール設定ファイルの作成 87
6.8. IAM を手動で作成する 104
6.9. クラスターのデプロイ 107
6.10. バイナリーのダウンロードによる OPENSHIFT CLI のインストール 108
6.11. CLI の使用によるクラスターへのログイン 110
6.12. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス 111
6.13. 次のステップ 111

第7章 プライベートクラスターを IBM CLOUD VPC にインストールする 112
7.1. 前提条件 112
7.2. プライベートクラスター 112
7.3. IBM CLOUD VPC 内のプライベートクラスター 113
7.4. カスタム VPC の使用について 113
7.5. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス 115
7.6. クラスターノードの SSH アクセス用のキーペアの生成 115
7.7. インストールプログラムの取得 117
7.8. API キーのエクスポート 118
7.9. インストール設定ファイルの手動作成 118
7.10. IAM を手動で作成する 135
7.11. クラスターのデプロイ 138
7.12. バイナリーのダウンロードによる OPENSHIFT CLI のインストール 139
7.13. CLI の使用によるクラスターへのログイン 141
7.14. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス 142
7.15. 次のステップ 142

第8章 IBM CLOUD VPC でのクラスターのアンインストール 143
8.1. インストーラーでプロビジョニングされるインフラストラクチャーを使用するクラスターの削除 143

第1章 IBM CLOUD VPC へのインストールの準備

このセクションに記載されているインストールワークフローは、IBM Cloud VPC インフラストラクチャー環境向けです。現時点では、IBM Cloud Classic はサポートされていません。Classic インフラストラクチャーと VPC インフラストラクチャーの違いの詳細は、IBM ドキュメント を参照してください。

1.1. 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ている。
- クラスターインストール方法の選択およびそのユーザー向けの準備 を確認している。

1.2. IBM CLOUD VPC に OPENSHIFT CONTAINER PLATFORM をインストールするための要件

OpenShift Container Platform VPC を IBM Cloud にインストールする前に、サービスアカウントを作成し、IBM Cloud アカウントを設定する必要があります。アカウントの作成、API サービスの有効化、DNS の設定、IBM Cloud アカウント制限、およびサポートされる IBM Cloud VPC リージョンの詳細については、IBM Cloud アカウントの設定 を参照してください。

クラスターを IBM Cloud VPC にインストールするときは、クラウドの認証情報を手動で管理する必要があります。これは、クラスターをインストールする前に、手動モードの Cloud Credential Operator (CCO) を設定して実行します。詳細は、IBM Cloud VPC 用の IAM の設定 を参照してください。

1.3. IBM CLOUD VPC に OPENSHIFT CONTAINER PLATFORM をインストールする方法の選択

インストーラーがプロビジョニングしたインフラストラクチャーを使用して、IBM Cloud VPC に OpenShift Container Platform をインストールできます。このプロセスでは、インストールプログラムを使用して、クラスターの基盤となるインフラストラクチャーをプロビジョニングします。現時点では、ユーザーによってプロビジョニングされたインフラストラクチャーを使用した IBM Cloud VPC への OpenShift Container Platform のインストールはサポートされていません。

インストーラーがプロビジョニングしたインストールプロセスの詳細については、インストールプロセス を参照してください。

1.3.1. インストーラーでプロビジョニングされるインフラストラクチャーへのクラスターのインストール

以下のいずれかの方法を使用して、OpenShift Container Platform インストールプログラムによってプロビジョニングされた IBM Cloud VPC インフラストラクチャーにクラスターをインストールできます。

- **カスタマイズされたクラスターの IBM Cloud VPC へのインストール**: インストールプログラムがプロビジョニングする IBM Cloud VPC インフラストラクチャーにカスタマイズされたクラスターをインストールできます。インストールプログラムは、インストールの段階で一部のカスタマイズを適用できるようにします。その他の数多くのカスタマイズオプションは、インストール後 に利用できます。
- **ネットワークをカスタマイズして IBM Cloud VPC にクラスターをインストールする**: インストール中に OpenShift Container Platform ネットワーク設定をカスタマイズして、クラスターが既存の IP アドレス割り当てと共存し、ネットワーク要件に準拠できるようにすることができ

ます。

- **IBM Cloud VPC 上のクラスターの既存の VPC へのインストール**: 既存の IBM Virtual Private Cloud (VPC) に OpenShift Container Platform をインストールできます。このインストール方法は、新規アカウントまたはインフラストラクチャーを作成する際の制限など、会社のガイドラインによる制約がある場合に使用できます。

- **既存の VPC へのプライベートクラスター** のインストール: 既存の Virtual Private Cloud (VPC) にプライベートクラスターをインストールできます。この方法を使用して、インターネット上に表示されない内部ネットワークに OpenShift Container Platform をデプロイすることができます。

1.4. 次のステップ

- IBM Cloud アカウントの設定

第2章 IBM CLOUD アカウントの設定

OpenShift Container Platform をインストールする前に、IBM Cloud アカウントを設定する必要があります。

2.1. 前提条件

- サブスクリプションのある IBM Cloud アカウントを持っている。無料または試用版の IBM Cloud アカウントに OpenShift Container Platform をインストールすることはできません。

2.2. IBM CLOUD VPC のクォータと制限

OpenShift Container Platform クラスターは多数の IBM Cloud VPC コンポーネントを使用し、デフォルトのクォータと制限は OpenShift Container Platform クラスターをインストールする機能に影響を与えます。特定のクラスター設定を使用する場合、特定のリージョンにクラスターをデプロイするか、アカウントから複数のクラスターを実行する場合は、IBM Cloud アカウントに追加のリソースを要求する必要がある場合があります。

デフォルトの IBM Cloud VPC クォータとサービス制限の包括的なリストについては、IBM Cloud のドキュメント Quotas and service limits を参照してください。

Virtual Private Cloud (VPC)

各 OpenShift Container Platform クラスターは、独自の VPC を作成します。リージョンごとの VPC のデフォルトのクォータは 10 で、10 個のクラスターを許可します。1 つのリージョンに 10 を超えるクラスターを含めるには、このクオータを増やす必要があります。

アプリケーションロードバランサー

デフォルトでは、各クラスターは 3 つのアプリケーションロードバランサー (ALB) を作成します。

- マスター API サーバーの内部ロードバランサー
- マスター API サーバーの外部ロードバランサー
- ルーターのロードバランサー

追加の **LoadBalancer** サービスオブジェクトを作成して、追加の ALB を作成できます。VPC ALB のデフォルトのクォータは、リージョンごとに 50 です。50 を超える ALB を使用するには、このクオータを増やす必要があります。

VPC ALB がサポートされています。従来の ALB は、IBM Cloud VPC ではサポートされていません。

フローティング IP アドレス

デフォルトでは、インストールプログラムは、コントロールプレーンとコンピューティングマシンをリージョン内のすべてのアベイラビリティーゾーンに分散して、高可用性設定でクラスターをプロビジョニングします。各アベイラビリティーゾーンで、パブリックゲートウェイが作成され、個別のフローティング IP アドレスが必要になります。

フローティング IP アドレスのデフォルトのクォータは、アベイラビリティーゾーンごとに 20 アドレスです。デフォルトのクラスター設定では、3 つのフローティング IP アドレスが生成されます。

- **us-east-1** プライマリーゾーンの 2 つのフローティング IP アドレス。ブートストラップノードに関連付けられている IP アドレスは、インストール後に削除されます。
- **us-east-2** セカンダリーゾーンの 1 つのフローティング IP アドレス。

- **us-east-3**セカンダリーゾーンの 1 つのフローティング IP アドレス。

IBM Cloud VPC は、アカウント内のリージョンごとに最大 19 個のクラスターをサポートできます。19 を超えるデフォルトクラスターを計画している場合は、このクオータを増やす必要があります。

Virtual Server Instances (VSI)

デフォルトでは、クラスターは **bx2-4x16** プロファイルを使用して VSI を作成します。これには、デフォルトで次のリソースが含まれます。

- 仮想 CPU 4 個
- 16 GB RAM

次のノードが作成されます。

- インストールの完了後に削除される 1 台の **bx2-4x16** ブートストラップマシン
- 3 つの **bx2-4x16** コントロールプレーンノード
- 3 つの **bx2-4x16** コンピュートノード

詳細については、IBM Cloud のドキュメント supported profiles を参照してください。

表2.1 VSI コンポーネントのクオータと制限

VSI コンポーネント	デフォルトの IBM Cloud VPC クォータ	デフォルトのクラスター設定	クラスターの最大数
仮想 CPU	リージョンごとに 200 の vCPU	28 の vCPU、またはブートストラップの削除後は 24 個の vCPU	リージョンごとに 8
RAM	リージョンあたり 1600 GB	112 GB、またはブートストラップの削除後は 96 GB	リージョンごとに 16
ストレージ	リージョンごとに 18 TB	1050 GB、またはブートストラップの削除後は 900 GB	リージョンごとに 19

表に記載されているリソースを超える予定がある場合は、IBM Cloud アカウントのクォータを増やす必要があります。

ブロックストレージボリューム

VPC マシンごとに、ブートボリューム用にブロックストレージデバイスが接続されます。デフォルトのクラスター設定では、7 台の VPC マシンが作成され、7 つのブロックストレージボリュームが作成されます。IBM Cloud VPC ストレージクラスの追加の Kubernetes 永続ボリューム要求 (PVC) は、追加のブロックストレージボリュームを作成します。VPC ブロックストレージボリュームのデフォルトのクォータは、リージョンごとに 300 です。300 を超えるボリュームを使用するには、このクオータを増やす必要があります。

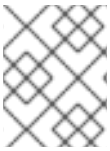
2.3. DNS 解決の設定

DNS 解決の設定方法は、インストールする OpenShift Container Platform クラスターのタイプによって異なります。

- パブリッククラスターをインストールする場合は、IBM Cloud Internet Services (CIS) を使用します。
- プライベートクラスターをインストールする場合は、IBM Cloud DNS サービス (DNS サービス) を使用します

2.3.1. DNS 解決のための IBM Cloud Internet Services の使用

インストールプログラムは、IBM Cloud Internet Services (CIS) を使用してクラスター DNS 解決を設定し、パブリッククラスターの名前検索を提供します。



注記

この製品は IPv6 をサポートしていないため、デュアルスタックまたは IPv6 環境は使用できません。

クラスターと同じアカウントの CIS にドメインゾーンを作成する必要があります。また、ゾーンがドメインに対して権限を持っていることを確認する必要があります。これは、root ドメインまたはサブドメインを使用して行うことができます。

前提条件

- IBM Cloud CLI をインストールしている。
- 既存のドメインとレジストラがあります。詳細については、IBM の ドキュメント を参照してください。

手順

1. クラスターで使用する CIS インスタンスを作成します。
   a. CIS プラグインをインストールします。

```
$ ibmcloud plugin install cis
```

   b. CIS インスタンスを作成します。

```
$ ibmcloud cis instance-create <instance_name> standard 1
```

   1 CIS がクラスターサブドメインとその DNS レコードを管理するには、少なくとも **Standard** プランが必要です。

2. 既存のドメインを CIS インスタンスに接続します。
   a. CIS のコンテキストインスタンスを設定します。

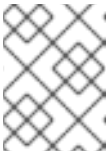
```
$ ibmcloud cis instance-set <instance_name> 1
```

   1 インスタンスクラウドのリソース名。

   b. CIS のドメインを追加します。

```
$ ibmcloud cis domain-add <domain_name> 1
```

1 完全修飾ドメイン名。設定する予定に応じて、ドメイン名として root ドメインまたはサブドメインのいずれかの値を使用できます。



注記

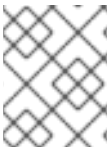
root ドメインは、**openshiftcorp.com** の形式を使用します。サブドメインは、**clusters.openshiftcorp.com** の形式を使用します。

3. CIS Web コンソール を開き、**Overview** ページに移動して、CIS ネームサーバーをメモします。これらのネームサーバーは、次のステップで使用されます。
4. ドメインのレジストラーまたは DNS プロバイダーでドメインまたはサブドメインのネームサーバーを設定します。詳細は、IBM Cloud の ドキュメント を参照してください。

2.3.2. DNS 解決のための IBM Cloud DNS サービスの使用

インストールプログラムは、IBM Cloud DNS サービスを使用してクラスター DNS 解決を設定し、プライベートクラスターの名前ルックアップを提供します。

クラスターの DNS サービスインスタンスを作成し、DNS サービスインスタンスに DNS ゾーンを追加して、DNS 解決を設定します。ゾーンがドメインに対して権限を持っていることを確認してください。これは、root ドメインまたはサブドメインを使用して行うことができます。



注記

IBM Cloud VPC は IPv6 をサポートしていないため、デュアルスタックまたは IPv6 環境は使用できません。

前提条件

- IBM Cloud CLI をインストールしている。
- 既存のドメインとレジストラがあります。詳細については、IBM の ドキュメント を参照してください。

手順

1. クラスターで使用する DNS サービスインスタンスを作成します。
   a. 次のコマンドを実行して、DNS サービスプラグインをインストールします。

```
$ ibmcloud plugin install cloud-dns-services
```

   b. 次のコマンドを実行して、DNS サービスインスタンスを作成します。

```
$ ibmcloud dns instance-create <instance-name> standard-dns 1
```

1 DNS Services がクラスターサブドメインとその DNS レコードを管理するには、少なくとも **Standard** プランが必要です。

2. DNS サービスインスタンスの DNS ゾーンを作成します。

   a. 次のコマンドを実行して、ターゲットのオペレーティング DNS サービスインスタンスを設定します。

   ```
   $ ibmcloud dns instance-target <instance-name>
   ```

   b. 次のコマンドを実行して、DNS サービスインスタンスに DNS ゾーンを追加します。

   ```
   $ ibmcloud dns zone-create <zone-name> 1
   ```

   1 完全修飾ゾーン名。設定する予定に応じて、ゾーン名として root ドメインまたはサブドメインのいずれかの値を使用できます。root ドメインは、**openshiftcorp.com** の形式を使用します。サブドメインは、**clusters.openshiftcorp.com** の形式を使用します。

3. 作成した DNS ゾーンの名前を記録します。インストールプロセスの一環として、クラスターをデプロイする前に、**install-config.yaml** ファイルを更新する必要があります。DNS ゾーンの名前を **baseDomain** パラメーターの値として使用します。

注記

許可されたネットワークを管理したり、"A" DNS リソースレコードを設定したりする必要はありません。必要に応じて、インストールプログラムはこれらのリソースを自動的に設定します。

2.4. IBM CLOUD VPC IAM ポリシーと API キー

OpenShift Container Platform を IBMCloud アカウントにインストールするには、インストールプログラムに IAM API キーが必要です。これにより、IBM Cloud サービス API にアクセスするための認証と認証が提供されます。必要なポリシーを含む既存の IAM API キーを使用するか、新しいポリシーを作成できます。

IBM Cloud IAM の概要については、IBM Cloud の ドキュメント を参照してください。

2.4.1. 必要なアクセスポリシー

必要なアクセスポリシーを IBM Cloud アカウントに割り当てる必要があります。

表2.2 必要なアクセスポリシー

サービスのタイプ	サービス	アクセスポリシーの範囲	プラットフォームアクセス	サービスアクセス
アカウント管理	IAM ID サービス	すべてのリソースまたはリソースのサブセット [1]	エディター、Operator、ビューアー、管理者	サービス ID 作成者

サービスのタイプ	サービス	アクセスポリシーの範囲	プラットフォームアクセス	サービスアクセス
アカウント管理 [2]	アイデンティティーおよびアクセス管理	すべてのリソース	エディター、Operator、ビューアー、管理者	
アカウント管理	リソースグループのみ	アカウント内のすべてのリソースグループ	Administrator	
IAM services	Cloud Object Storage	すべてのリソースまたはリソースのサブセット [1]	エディター、Operator、ビューアー、管理者	リーダー、ライター、マネージャー、コンテンツリーダー、オブジェクトリーダー、オブジェクトライター
IAM services	インターネットサービス	すべてのリソースまたはリソースのサブセット [1]	エディター、Operator、ビューアー、管理者	リーダー、ライター、マネージャー
IAM services	DNS Services	すべてのリソースまたはリソースのサブセット [1]	エディター、Operator、ビューアー、管理者	リーダー、ライター、マネージャー
IAM services	VPC インフラストラクチャーサービス	すべてのリソースまたはリソースのサブセット [1]	エディター、Operator、ビューアー、管理者	リーダー、ライター、マネージャー

1. ポリシーアクセススコープは、アクセスを割り当てる粒度に基づいて設定する必要があります。スコープは、**すべてのリソース** または **選択した属性に基づくリソース** に設定できます。

2. オプション: このアクセスポリシーは、インストールプログラムでリソースグループを作成する場合にのみ必要です。リソースグループの詳細については、IBM の ドキュメント を参照してください。

2.4.2. アクセスポリシーの割り当て

IBM Cloud VPC IAM では、アクセスポリシーをさまざまなサブジェクトにアタッチできます。

- アクセスグループ (推奨)
- サービス ID
- User

推奨される方法は、アクセスグループ で IAM アクセスポリシーを定義することです。これにより、OpenShift Container Platform に必要なすべてのアクセスを整理し、ユーザーとサービス ID をこのグループにオンボードできます。必要に応じて、ユーザーとサービス ID に直接アクセスを割り当てることもできます。

2.4.3. API キーの作成

IBM Cloud アカウントのユーザー API キーまたはサービス ID API キーを作成する必要があります。

前提条件

- 必要なアクセスポリシーを IBM Cloud アカウントに割り当てている。
- IAM アクセスポリシーをアクセスグループまたはその他の適切なリソースにアタッチしている。

手順

- IAM アクセスポリシーの定義方法に応じて、API キーを作成します。
  たとえば、アクセスポリシーをユーザーに割り当てた場合は、ユーザー API キー を作成する必要があります。アクセスポリシーをサービス ID に割り当てた場合は、サービス ID API キー を作成する必要があります。アクセスポリシーがアクセスグループに割り当てられている場合は、どちらの API キータイプも使用できます。IBM Cloud VPC API キーの詳細は、Understanding API keys を参照してください。

2.5. サポート対象の IBM CLOUD VPC リージョン

OpenShift Container Platform クラスターを以下のリージョンにデプロイできます。

- **au-syd** (Sydney, Australia)
- **br-sao** (Sao Paulo, Brazil)
- **ca-tor** (Toronto, Canada)
- **eu-de** (Frankfurt, Germany)
- **eu-gb** (London, United Kingdom)
- **jp-osa** (Osaka, Japan)
- **jp-tok** (Tokyo, Japan)
- **us-east** (Washington DC, United States)
- **us-south** (Dallas, United States)

2.6. 次のステップ

- IBM Cloud VPC 用の IAM の設定

第3章 IBM CLOUD VPC 用の IAM の設定

クラウドアイデンティティーおよびアクセス管理 (IAM) API に到達できない環境では、クラスターのインストール前に Cloud Credential Operator (CCO) を手動モードに配置する必要があります。

3.1. 管理者レベルのシークレットを KUBE-SYSTEM プロジェクトに保存する代替方法

Cloud Credential Operator (CCO) は、クラウドプロバイダーの認証情報を Kubernetes カスタムリソース定義 (CRD) として管理します。**credentialsMode** パラメーターの異なる値を **install-config.yaml** ファイルに設定し、組織のセキュリティー要件に応じて CCO を設定できます。

管理者レベルのクレデンシャルシークレットをクラスター **kube-system** プロジェクトに格納することは、IBM Cloud ではサポートされていません。したがって、OpenShift Container Platform をインストールするときは、CCO の **credentialsMode** パラメーターを **Manual** に設定し、クラウドクレデンシャルを手動で管理する必要があります。

手動モードを使用すると、クラスターに管理者レベルの認証情報を保存する必要なく、各クラスターコンポーネントに必要なパーミッションのみを指定できます。お使いの環境でクラウドプロバイダーのパブリック IAM エンドポイントへの接続がない場合も、このモードを使用できます。ただし、各アップグレードについて、パーミッションを新規リリースイメージを使用して手動で調整する必要があります。また、それらを要求するすべてのコンポーネントについて認証情報を手動で指定する必要があります。

関連情報

- Cloud Credential Operator について

3.2. CLOUD CREDENTIAL OPERATOR ユーティリティーの設定

Cloud Credential Operator (CCO) が手動モードで動作しているときにクラスターの外部からクラウドクレデンシャルを作成および管理するには、CCO ユーティリティー (**ccoctl**) バイナリーを抽出して準備します。

注記

ccoctl ユーティリティーは、Linux 環境で実行する必要がある Linux バイナリーです。

前提条件

- クラスター管理者のアクセスを持つ OpenShift Container Platform アカウントを使用できる。
- OpenShift CLI (**oc**) がインストールされている。

手順

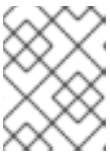
1. 以下のコマンドを実行して、OpenShift Container Platform リリースイメージを取得します。

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

2. 以下のコマンドを実行して、OpenShift Container Platform リリースイメージから CCO コンテナーイメージを取得します。

```
$ CCO_IMAGE=$(oc adm release info --image-for='cloud-credential-operator'
```

```
$RELEASE_IMAGE -a ~/.pull-secret)
```



注記

$RELEASE_IMAGE のアーキテクチャーが、**ccoctl** ツールを使用する環境のアーキテクチャーと一致していることを確認してください。

3. 以下のコマンドを実行して、OpenShift Container Platform リリースイメージ内の CCO コンテナーイメージから **ccoctl** バイナリーを抽出します。

```
$ oc image extract $CCO_IMAGE --file="/usr/bin/ccoctl" -a ~/.pull-secret
```

4. 次のコマンドを実行して、権限を変更して **ccoctl** を実行可能にします。

```
$ chmod 775 ccoctl
```

検証

- **ccoctl** が使用できることを確認するには、help ファイルを表示します。コマンドを実行するときは、相対ファイル名を使用します。以下に例を示します。

```
$ ./ccoctl.rhel9
```

出力例

```
OpenShift credentials provisioning tool

Usage:
  ccoctl [command]

Available Commands:
  alibabacloud Manage credentials objects for alibaba cloud
  aws          Manage credentials objects for AWS cloud
  gcp          Manage credentials objects for Google cloud
  help         Help about any command
  ibmcloud     Manage credentials objects for IBM Cloud
  nutanix      Manage credentials objects for Nutanix

Flags:
  -h, --help   help for ccoctl

Use "ccoctl [command] --help" for more information about a command.
```

関連情報

- IBM Cloud VPC の API キーのローテーション

3.3. 次のステップ

- カスタマイズを使用した IBM Cloud VPC へのクラスターのインストール

3.4. 関連情報

- 手動で維持された認証情報でクラスターを更新する準備

第4章 カスタマイズを使用した IBM CLOUD VPC へのクラスターのインストール

OpenShift Container Platform バージョン 4.13 では、インストールプログラムが IBM Cloud VPC でプロビジョニングするインフラストラクチャーにカスタマイズされたクラスターをインストールできます。インストールをカスタマイズするには、クラスターをインストールする前に、**install-config.yaml** ファイルでパラメーターを変更します。

4.1. 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ている。
- クラスターインストール方法の選択およびそのユーザー向けの準備 を確認している。
- クラスターをホストするように IBM Cloud アカウントを設定 している。
- ファイアウォールを使用する場合は、クラスターがアクセスを必要とするサイトを許可するようにファイアウォールを設定する必要がある。
- クラスターをインストールする前に、**ccoctl** ユーティリティーを設定している。詳細は、IBM Cloud VPC 用の IAM の設定 を参照してください。

4.2. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス

OpenShift Container Platform 4.13 では、クラスターをインストールするためにインターネットアクセスが必要になります。

インターネットへのアクセスは以下を実行するために必要です。

- OpenShift Cluster Manager Hybrid Cloud Console にアクセスし、インストールプログラムをダウンロードし、サブスクリプション管理を実行します。クラスターにインターネットアクセスがあり、Telemetry を無効にしない場合、そのサービスは有効なサブスクリプションでクラスターを自動的に使用します。
- クラスターのインストールに必要なパッケージを取得するために Quay.io にアクセスします。
- クラスターの更新を実行するために必要なパッケージを取得します。

重要

クラスターでインターネットに直接アクセスできない場合、プロビジョニングする一部のタイプのインフラストラクチャーでネットワークが制限されたインストールを実行できます。このプロセスで、必要なコンテンツをダウンロードし、これを使用してミラーレジストリーにインストールパッケージを設定します。インストールタイプに応じて、クラスターのインストール環境でインターネットアクセスが不要となる場合があります。クラスターを更新する前に、ミラーレジストリーのコンテンツを更新します。

4.3. クラスターノードの SSH アクセス用のキーペアの生成

OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定できます。キーは、Ignition 設定ファイルを介して Red Hat Enterprise Linux CoreOS (RHCOS) ノードに渡され、ノードへの SSH アクセスを認証するために使用されます。このキーは各

ノードの **core** ユーザーの ~/**.ssh/authorized_keys** リストに追加され、パスワードなしの認証が可能になります。

キーがノードに渡されると、キーペアを使用して RHCOS ノードにユーザー **core** として SSH を実行できます。SSH 経由でノードにアクセスするには、秘密鍵のアイデンティティーをローカルユーザーの SSH で管理する必要があります。

インストールのデバッグまたは障害復旧を実行するためにクラスターノードに対して SSH を実行する場合は、インストールプロセスの間に SSH 公開鍵を指定する必要があります。**./openshift-install gather** コマンドでは、SSH 公開鍵がクラスターノードに配置されている必要もあります。

重要

障害復旧およびデバッグが必要な実稼働環境では、この手順を省略しないでください。

注記

AWS キーペア などのプラットフォームに固有の方法で設定したキーではなく、ローカルキーを使用する必要があります。

手順

1. クラスターノードへの認証に使用するローカルマシンに既存の SSH キーペアがない場合は、これを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ ssh-keygen -t ed25519 -N '' -f <path>/<file_name> 1
```

1 新しい SSH キーのパスとファイル名 (~/**.ssh/id_ed25519** など) を指定します。既存のキーペアがある場合は、公開鍵が ~/**.ssh** ディレクトリーにあることを確認します。

2. 公開 SSH キーを表示します。

```
$ cat <path>/<file_name>.pub
```

たとえば、次のコマンドを実行して ~/**.ssh/id_ed25519.pub** 公開鍵を表示します。

```
$ cat ~/.ssh/id_ed25519.pub
```

3. ローカルユーザーの SSH エージェントに SSH 秘密鍵 ID が追加されていない場合は、それを追加します。キーの SSH エージェント管理は、クラスターノードへのパスワードなしの SSH 認証、または **./openshift-install gather** コマンドを使用する場合は必要になります。

注記

一部のディストリビューションでは、~/**.ssh/id_rsa** および ~/**.ssh/id_dsa** などのデフォルトの SSH 秘密鍵のアイデンティティーは自動的に管理されます。

a. **ssh-agent** プロセスがローカルユーザーに対して実行されていない場合は、バックグラウンドタスクとして開始します。

```
$ eval "$(ssh-agent -s)"
```

出力例

```
Agent pid 31874
```

4. SSH プライベートキーを **ssh-agent** に追加します。

```
$ ssh-add <path>/<file_name> 1
```

1 **~/.ssh/id_ed25519** などの、SSH プライベートキーのパスおよびファイル名を指定します。

出力例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

次のステップ

- OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定します。

4.4. インストールプログラムの取得

OpenShift Container Platform をインストールする前に、インストールに使用しているホストにインストールファイルをダウンロードします。

前提条件

- 500 MB のローカルディスク領域がある Linux または macOS を実行するコンピューターが必要です。

手順

1. OpenShift Cluster Manager サイトの インフラストラクチャープロバイダー ページにアクセスします。Red Hat アカウントがある場合は、認証情報を使用してログインします。アカウントがない場合はこれを作成します。
2. インフラストラクチャープロバイダーを選択します。
3. インストールタイプのページに移動し、ホストオペレーティングシステムとアーキテクチャーに対応するインストールプログラムをダウンロードして、インストール設定ファイルを保存するディレクトリーにファイルを配置します。

重要

インストールプログラムは、クラスターのインストールに使用するコンピューターにいくつかのファイルを作成します。クラスターのインストール完了後は、インストールプログラムおよびインストールプログラムが作成するファイルを保持する必要があります。ファイルはいずれもクラスターを削除するために必要になります。

重要

インストールプログラムで作成されたファイルを削除しても、クラスターがインストール時に失敗した場合でもクラスターは削除されません。クラスターを削除するには、特定のクラウドプロバイダー用の OpenShift Container Platform のアンインストール手順を実行します。

4. インストールプログラムを展開します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar -xvf openshift-install-linux.tar.gz
```

5. Red Hat OpenShift Cluster Manager からインストールプルシークレット をダウンロードします。このプルシークレットを使用し、OpenShift Container Platform コンポーネントのコンテナーイメージを提供する Quay.io など、組み込まれた各種の認証局によって提供されるサービスで認証できます。

4.5. API キーのエクスポート

作成した API キーをグローバル変数として設定する必要があります。インストールプログラムは、起動時に変数を取り込み、API キーを設定します。

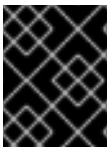
前提条件

- IBM Cloud アカウント用にユーザー API キーまたはサービス ID API キーのいずれかを作成している。

手順

- アカウントの API キーをグローバル変数としてエクスポートします。

```
$ export IC_API_KEY=<api_key>
```



重要

変数名は指定どおりに正確に設定する必要があります。インストールプログラムは、起動時に変数名が存在することを想定しています。

4.6. インストール設定ファイルの作成

IBM Cloud にインストールする OpenShift Container Platform クラスターをカスタマイズできます。

前提条件

- OpenShift Container Platform インストールプログラム、およびクラスターのプルシークレットを取得する。
- サブスクリプションレベルでサービスプリンシパルのパーミッションを取得する。

手順

1. **install-config.yaml** ファイルを作成します。

a. インストールプログラムが含まれるディレクトリーに切り替え、以下のコマンドを実行します。

```
$ ./openshift-install create install-config --dir <installation_directory> 1
```

1 **<installation_directory>** の場合、インストールプログラムが作成するファイルを保存するためにディレクトリー名を指定します。

ディレクトリーを指定する場合:

- ディレクトリーに **execute** 権限があることを確認します。この権限は、インストールディレクトリーで Terraform バイナリーを実行するために必要です。
- 空のディレクトリーを使用します。ブートストラップ X.509 証明書などの一部のインストールアセットは有効期限が短いため、インストールディレクトリーを再利用しないでください。別のクラスターインストールの個別のファイルを再利用する必要がある場合は、それらをディレクトリーにコピーすることができます。ただし、インストールアセットのファイル名はリリース間で変更される可能性があります。インストールファイルを以前のバージョンの OpenShift Container Platform からコピーする場合は注意してください。

注記

古い設定の再利用を回避するために、~/**.powervs** ディレクトリーは必ず削除してください。以下のコマンドを実行します。

```
$ rm -rf ~/.powervs
```

b. プロンプト時に、クラウドの設定の詳細情報を指定します。

i. オプション: クラスターマシンにアクセスするために使用する SSH キーを選択します。

注記

インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。

ii. ターゲットとするプラットフォームとして **ibmcloud** を選択します。

iii. クラスターをデプロイするリージョンを選択します。

iv. クラスターをデプロイするベースドメインを選択します。ベースドメインは、クラスターに作成したパブリック DNS ゾーンに対応します。

v. クラスターの記述名を入力します。

vi. Red Hat OpenShift Cluster Manager からプルシークレット を貼り付けます。

2. **install-config.yaml** ファイルを変更します。利用可能なパラメーターの詳細は、「インストール設定パラメーター」のセクションを参照してください。

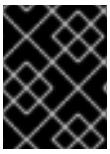
3. **install-config.yaml** ファイルをバックアップし、複数のクラスターをインストールするのに使用できるようにします。

重要

install-config.yaml ファイルはインストールプロセス時に使用されます。このファイルを再利用する必要がある場合は、この段階でこれをバックアップしてください。

4.6.1. インストール設定パラメーター

OpenShift Container Platform クラスターをデプロイする前に、クラスターをホストするクラウドプラットフォームでアカウントを記述し、クラスターのプラットフォームをオプションでカスタマイズするためにパラメーターの値を指定します。**install-config.yaml** インストール設定ファイルを作成する際に、コマンドラインで必要なパラメーターの値を指定します。クラスターをカスタマイズする場合、**install-config.yaml** ファイルを変更して、プラットフォームについての詳細情報を指定できます。



重要

インストール後は、これらのパラメーターを **install-config.yaml** ファイルで変更することはできません。

4.6.1.1. 必須設定パラメーター

必須のインストール設定パラメーターは、以下の表で説明されています。

表4.1 必須パラメーター

パラメーター	説明	値
apiVersion	**install-config.yaml** コンテンツの API バージョン。現在のバージョンは **v1** です。インストールプログラムは、古い API バージョンもサポートしている場合があります。	String
baseDomain	クラウドプロバイダーのベースドメイン。ベースドメインは、OpenShift Container Platform クラスターコンポーネントへのルートを作成するために使用されます。クラスターの完全な DNS 名は、**<metadata.name>.<baseDomain>** 形式を使用する **baseDomain** と **metadata.name** パラメーターの値を組み合わせたものです。	**example.com** などの完全修飾ドメインまたはサブドメイン名。

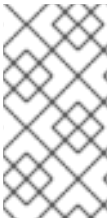
パラメーター	説明	値
metadata	Kubernetes リソース **ObjectMeta**。ここからは **name** パラメーターのみが消費されます。	オブジェクト
metadata.name	クラスターの名前。クラスターの DNS レコードはすべて **{{.metadata.name}}.{{.baseDomain}}** のサブドメインです。	**dev** などの小文字、ハイフン (**-**)、およびピリオド (**.**) が含まれる文字列。
platform	インストールを実行する特定のプラットフォームの設定: **alibabacloud**、**aws**、**baremetal**、**azure**、**gcp**、**ibmcloud**、**Nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**。**platform.<platform>** パラメーターに関する追加情報は、以下の表で特定のプラットフォームを参照してください。	オブジェクト

pullSecret	Red Hat OpenShift Cluster Manager からプルシークレット を取得して、Quay.io などのサービスから OpenShift Container Platform コンポーネントのコンテナーイメージをダウンロードすることを認証します。	<pre>{
		  "auths":{
		  "cloud.openshift.com":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  },
		  "quay.io":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  }
		  }
		}</pre>

4.6.1.2. ネットワーク設定パラメーター

既存のネットワークインフラストラクチャーの要件に基づいて、インストール設定をカスタマイズできます。たとえば、クラスターネットワークの IP アドレスブロックを拡張するか、デフォルトとは異なる IP アドレスブロックを指定できます。

IPv4 アドレスのみがサポートされます。



注記

Globalnet は、Red Hat OpenShift Data Foundation ディザスターリカバリーソリューションではサポートされていません。局地的なディザスターリカバリーのシナリオでは、各クラスター内のクラスターとサービスネットワークに重複しない範囲のプライベート IP アドレスを使用するようにしてください。

表4.2 ネットワークパラメーター

パラメーター	説明	値
networking	クラスターのネットワークの設定。	Object  **注記** インストール後に **networking** オブジェクトで指定したパラメーターを変更することはできません。
networking.networkType	インストールする Red Hat OpenShift Networking ネットワークプラグイン。	**OpenShiftSDN** または **OVNKubernetes** のいずれか。**OpenShiftSDN** は、すべての Linux ネットワークの Container Network Interface (CNI)プラグインです。**OVNKubernetes** は、Linux ネットワークと、Linux サーバーと Windows サーバーの両方を含む Linux ネットワークおよびハイブリッドネットワーク用の CNI プラグインです。デフォルトの値は **OVNkubernetes** です。

networking.clusterNetwork	Pod の IP アドレスブロック。
	
	デフォルト値は **10.128.0.0/14** で、ホストの接頭辞は **/23** です。
	
	複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。
		オブジェクトの配列。以下に例を示します。
		
		`networking:`
		`  clusterNetwork:`
		`  - cidr: 10.128.0.0/14`
		`    hostPrefix: 23`

networking.clusterNetwork.cidr	**networking.clusterNetwork** を使用する場合に必須です。IP アドレスブロック。 IPv4 ネットワーク	CIDR (Classless Inter-Domain Routing) 表記の IP アドレスブロック。IPv4 ブロックの接頭辞長は **0** から **32** の間になります。

パラメーター	説明	値
networking.clusterNetwork.hostPrefix	それぞれの個別ノードに割り当てるサブネット接頭辞長。たとえば、**hostPrefix** が **23** に設定される場合、各ノードに指定の **cidr** から **/23** サブネットが割り当てられます。**hostPrefix** 値の **23** は、510 (2^(32 - 23) - 2) Pod IP アドレスを提供します。	サブネット接頭辞。 デフォルト値は **23** です。

networking.serviceNetwork	サービスの IP アドレスブロック。デフォルト値は **172.30.0.0/16** です。
	
	OpenShift SDN および OVN-Kubernetes ネットワークプラグインは、サービスネットワークの単一 IP アドレスブロックのみをサポートします。
		CIDR 形式の IP アドレスブロックを持つ配列。以下に例を示します。
		
		`networking:`
		`  serviceNetwork:`
		`  - 172.30.0.0/16`

networking.machineNetwork	マシンの IP アドレスブロック。
	
	複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。
		オブジェクトの配列。以下に例を示します。
		
		`networking:`
		`  machineNetwork:`
		`  - cidr: 10.0.0.0/16`

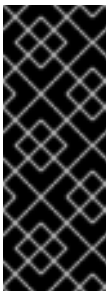
networking.machineNetwork.cidr	**networking.machineNetwork** を使用する場合に必須です。IP アドレスブロック。libvirt と IBM Power Virtual Server を除くすべてのプラットフォームのデフォルト値は **10.0.0.0/16** です。libvirt の場合、デフォルト値は **192.168.126.0/24** です。IBM Power Virtual Server の場合、デフォルト値は **192.168.0.0/24** です。	CIDR 表記の IP ネットワークブロック。 例: **10.0.0.0/16** **注記** 優先される NIC が置かれている CIDR に一致する **networking.machineNetwork** を設定します。

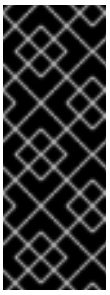
4.6.1.3. オプションの設定パラメーター

オプションのインストール設定パラメーターは、以下の表で説明されています。

表4.3 オプションのパラメーター

パラメーター	説明	値
additionalTrustBundle	ノードの信頼済み証明書ストアに追加される PEM でエンコードされた X.509 証明書バンドル。この信頼バンドルは、プロキシーが設定されている場合にも使用することができます。	String
capabilities	オプションのコアクラスターコンポーネントのインストールを制御します。オプションのコンポーネントを無効にすることで、OpenShift Container Platform クラスターのフットプリントを削減できます。詳細は、**インストール** の「クラスター機能ページ」を参照してください。	文字列配列
capabilities.baselineCapabilitySet	有効にするオプション機能の初期セットを選択します。有効な値は **None**、**v4.11**、**v4.12**、**vCurrent** です。デフォルト値は **vCurrent** です。	文字列
capabilities.additionalEnabledCapabilities	オプションの機能のセットを、**baselineCapabilitySet** で指定したものを超えて拡張します。このパラメーターで複数の機能を指定できます。	String array
cpuPartitioningMode	ワークロードパーティション設定を使用して、OpenShift Container Platform サービス、クラスター管理ワークロード、およびインフラストラクチャー Pod を分離し、予約された CPU セットで実行できます。ワークロードパーティショニングは、インストール中にのみ有効にできます。インストール後に無効にすることはできません。このフィールドはワークロードのパーティショニングを有効にしますが、特定の CPU を使用するようにワークロードを設定するわけではありません。詳細は、**スケーラビリティとパフォーマンス** セクションの **ワークロードパーティショニング** ページを参照してください。	**None** または **AllNodes**。デフォルト値は **None** です。
compute	コンピュートノードを形成するマシンの設定。	**MachinePool** オブジェクトの配列。

パラメーター	説明	値
compute.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String
compute: hyperthreading:	コンピュートマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。  **重要** 同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
compute.name	**compute** を使用する場合に必須です。マシンプールの名前。	**worker**
compute.platform	**compute** を使用する場合に必須です。このパラメーターを使用して、ワーカーマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **controlPlane.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
compute.replicas	プロビジョニングするコンピュートマシン (ワーカーマシンとしても知られる) の数。	**2** 以上の正の整数。デフォルト値は **3** です。
featureSet	機能セットのクラスターを有効にします。機能セットは、デフォルトで有効にされない OpenShift Container Platform 機能のコレクションです。インストール中に機能セットを有効にする方法の詳細は、「機能ゲートの使用による各種機能の有効化」を参照してください。	文字列。**TechPreviewNoUpgrade** など、有効にする機能セットの名前。

パラメーター	説明	値
controlPlane	コントロールプレーンを形成するマシンの設定。	**MachinePool** オブジェクトの配列。
controlPlane.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String
controlPlane: hyperthreading:	コントロールプレーンマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。  **重要** 同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
controlPlane.name	**controlPlane** を使用する場合に必須です。マシンプールの名前。	**master**
controlPlane.platform	**controlPlane** を使用する場合に必須です。このパラメーターを使用して、コントロールプレーンマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **compute.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
controlPlane.replicas	プロビジョニングするコントロールプレーンマシンの数。	サポートされる値は **3** のみです (これはデフォルト値です)。

パラメーター	説明	値
credentialsMode	Cloud Credential Operator (CCO) モード。CCO は、モードが指定されていない場合に指定される認証情報の機能を動的に判別しようとします。この場合、複数のモードがサポートされるプラットフォームで mint モードが優先されます。  **注記** すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**Cluster Operators リファレンス** の **Cloud Credential Operator** を参照してください。  **注記** AWS アカウントでサービスコントロールポリシー (SCP) が有効になっている場合は、**credentialsMode** パラメーターを **Mint**、**Passthrough** または **Manual** に設定する必要があります。	**Mint**、**Passthrough**、**Manual**、または空の文字列 (**""**)。
imageContentSources	release-image コンテンツのソースおよびリポジトリー。	オブジェクトの配列。この表の以下の行で説明されているように、**source** およびオプションで **mirrors** が含まれます。
imageContentSources.source	**imageContentSources** を使用する場合に必須です。ユーザーが参照するリポジトリーを指定します (例: イメージプル仕様)。	文字列
imageContentSources.mirrors	同じイメージが含まれる可能性のあるリポジトリーを 1 つ以上指定します。	文字列の配列。

パラメーター	説明	値
publish	Kubernetes API、OpenShift ルートなどのクラスターのユーザーに表示されるエンドポイントをパブリッシュまたは公開する方法。	**Internal** または **External**。プライベートクラスターをデプロイするには、**publish** を **Internal** に設定します。これはインターネットからアクセスできません。デフォルト値は **External** です。
sshKey	クラスターマシンへのアクセスを認証するための SSH キー。  **注記** インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。	たとえば、**sshKey: ssh-ed25519 AAAA..** です。

1. すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**認証と認可** コンテンツの「クラウドプロバイダーの認証情報の管理」を参照してください。

4.6.1.4. 追加の IBM Cloud VPC 設定パラメーター

追加の IBM Cloud VPC 設定パラメーターについて、以下の表で説明します。

表4.4 追加の IBM Cloud VPC パラメーター

パラメーター	説明	値
platform.ibmcloud.resourceGroupName	既存のリソースグループの名前。デフォルトでは、installer-provisioned VPC およびクラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。クラスターを既存の VPC にデプロイする場合、installer-provisioned クラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。プロビジョニングした VPC リソースは、**networkResourceGroupName** パラメーターを使用して指定したリソースグループに存在する必要があります。いずれの場合も、クラスターコンポーネントはリソースグループ内のすべてのリソースの所有権を引き受けるため、このリソースグループは単一のクラスターインストールのみに使用する必要があります。[1]	文字列 (例: **existing_resource_group**)。

パラメーター	説明	値
platform.ibmcloud.networkResourceGroupName	既存のリソースグループの名前。このリソースには、クラスターがデプロイされる既存の VPC とサブネットが含まれます。このパラメーターは、プロビジョニングした VPC にクラスターをデプロイする際に必要です。	文字列 (例: **existing_network_resource_group**)。
platform.ibmcloud.dedicatedHosts.profile	作成する新しい専用ホスト。**platform.ibmcloud.dedicatedHosts.name** に値を指定する場合、このパラメーターは必須ではありません。	**cx2-host-152x304**などの有効な IBM Cloud VPC 専用ホストプロファイル。[2]
platform.ibmcloud.dedicatedHosts.name	既存の専用ホスト。**platform.ibmcloud.dedicatedHosts.profile** に値を指定する場合、このパラメーターは必須ではありません。	文字列、たとえば **my-dedicated-host-name**。
platform.ibmcloud.type	すべての IBM Cloud VPC マシンのインスタンスタイプ。	**bx2-8x32** などの有効な IBM Cloud VPC インスタンスタイプ。[2]
platform.ibmcloud.vpcName	クラスターをデプロイする既存 VPC の名前。	文字列。
platform.ibmcloud.controlPlaneSubnets	コントロールプレーンマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。	文字列配列

パラメーター	説明	値
platform.ibmcloud.computeSubnets	コンピュートマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。サブネット ID はサポートされていません。	文字列配列

1. 既存のリソースグループを定義するか、インストーラーが作成するかによって、クラスターがアンインストールされたときにリソースグループがどのように扱われるかが決まります。リソースグループを定義すると、インストーラーはインストーラーがプロビジョニングしたすべてのリソースを削除しますが、リソースグループはそのままにします。インストールの一部としてリソースグループが作成された場合、インストーラーは、インストーラーがプロビジョニングしたすべてのリソースとリソースグループを削除します。
2. 自身のニーズに最適なプロファイルを判別するには、IBM ドキュメントの Instance Profiles を参照してください。

4.6.2. クラスターインストールの最小リソース要件

それぞれのクラスターマシンは、以下の最小要件を満たしている必要があります。

表4.5 最小リソース要件

マシン	オペレーティングシステム	仮想 CPU	仮想 RAM	ストレージ	1秒あたりの入出力 (IOPS)
ブートストラップ	RHCOS	4	16 GB	100 GB	300
コントロールプレーン	RHCOS	4	16 GB	100 GB	300
Compute	RHCOS	2	8 GB	100 GB	300

注記

OpenShift Container Platform バージョン 4.13 の時点で、RHCOS は RHEL バージョン 9.2 に基づいており、マイクロアーキテクチャーの要件を更新します。次のリストには、各アーキテクチャーに必要な最小限の命令セットアーキテクチャー (ISA) が含まれています。

- x86-64 アーキテクチャーには x86-64-v2 ISA が必要
- ARM64 アーキテクチャーには ARMv8.0-A ISA が必要
- IBM Power アーキテクチャーには Power 9 ISA が必要
- s390x アーキテクチャーには z14 ISA が必要

詳細は、RHEL アーキテクチャー を参照してください。

プラットフォームのインスタンスタイプがクラスターマシンの最小要件を満たす場合、これは OpenShift Container Platform で使用することがサポートされます。

関連情報

- ストレージの最適化

4.6.3. IBM Cloud VPC 用にカスタマイズされた install-config.yaml ファイルのサンプル

install-config.yaml ファイルをカスタマイズして、OpenShift Container Platform クラスターのプラットフォームについての詳細を指定するか、必要なパラメーターの値を変更することができます。

重要

このサンプルの YAML ファイルは参照用にのみ提供されます。インストールプログラムを使用して **install-config.yaml** ファイルを取得し、変更する必要があります。

```
apiVersion: v1
baseDomain: example.com (1)
controlPlane: (2) (3)
  hyperthreading: Enabled (4)
  name: master
  platform:
    ibmcloud: {}
  replicas: 3
compute: (5) (6)
- hyperthreading: Enabled (7)
  name: worker
  platform:
    ibmcloud: {}
  replicas: 3
metadata:
  name: test-cluster (8)
networking:
  clusterNetwork:
```

```
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes 9
  serviceNetwork:
  - 172.30.0.0/16
platform:
  ibmcloud:
    region: us-south 10
credentialsMode: Manual
publish: External
pullSecret: '{"auths": ...}' 11
fips: false 12
sshKey: ssh-ed25519 AAAA... 13
```

1 8 10 11 必須。インストールプログラムはこの値の入力を求めるプロンプトを出します。

2 5 これらのパラメーターおよび値を指定しない場合、インストールプログラムはデフォルトの値を指定します。

3 6 **controlPlane** セクションは単一マッピングですが、**compute** セクションはマッピングのシーケンスになります。複数の異なるデータ構造の要件を満たすには、**compute** セクションの最初の行はハイフン **-** で始め、**controlPlane** セクションの最初の行はハイフンで始めることができません。1 つのコントロールプレーンプールのみが使用されます。

4 7 ハイパースレッディングとも呼ばれる同時マルチスレッドを有効または無効にします。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。パラメーター値を **Disabled** に設定するとこれを無効にすることができます。一部のクラスターマシンで同時マルチスレッドを無効にする場合は、これをすべてのクラスターマシンで無効にする必要があります。

重要

同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。同時マルチスレッドを無効にする場合は、マシンに対して **n1-standard-8** などの大規模なマシンタイプを使用します。

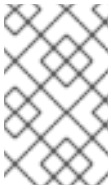
9 インストールするクラスターネットワークプラグイン。サポートされている値は **OVNKubernetes** と **OpenShiftSDN** です。デフォルトの値は **OVNkubernetes** です。

12 FIPS モードを有効または無効にします。デフォルトでは、FIPS モードは有効にされません。

重要

OpenShift Container Platform 4.13 は Red Hat Enterprise Linux (RHEL) 9.2 をベースにしています。FIPS 検証用に RHEL 9.2 暗号化モジュールがまだ送信されていません。詳細は、4.13 **OpenShift Container Platform リリースノート** の "About this release" を参照してください。

13 オプション: クラスター内のマシンにアクセスするのに使用する **sshKey** 値をオプションで指定できます。



注記

インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。

4.6.4. インストール時のクラスター全体のプロキシーの設定

実稼働環境では、インターネットへの直接アクセスを拒否し、代わりに HTTP または HTTPS プロキシーを使用することができます。プロキシー設定を **install-config.yaml** ファイルで行うことにより、新規の OpenShift Container Platform クラスターをプロキシーを使用するように設定できます。

前提条件

- 既存の **install-config.yaml** ファイルがある。
- クラスターがアクセスする必要のあるサイトを確認済みで、それらのいずれかがプロキシーをバイパスする必要があるかどうかを判別している。デフォルトで、すべてのクラスター Egress トラフィック (クラスターをホストするクラウドに関するクラウドプロバイダー API に対する呼び出しを含む) はプロキシーされます。プロキシーを必要に応じてバイパスするために、サイトを **Proxy** オブジェクトの **spec.noProxy** フィールドに追加している。

注記

Proxy オブジェクトの **status.noProxy** フィールドには、インストール設定の **networking.machineNetwork[].cidr**、**networking.clusterNetwork[].cidr**、および **networking.serviceNetwork[]** フィールドの値が設定されます。

Amazon Web Services (AWS)、Google Cloud、Microsoft Azure、および Red Hat OpenStack Platform (RHOSP)へのインストールの場合、**Proxy** オブジェクトの **status.noProxy** フィールドには、インスタンスメタデータのエンドポイント(**169.254.169.254**)も設定されます。

手順

1. **install-config.yaml** ファイルを編集し、プロキシー設定を追加します。以下に例を示します。

```
apiVersion: v1
baseDomain: my.domain.com
proxy:
  httpProxy: http://<username>:<pswd>@<ip>:<port> 1
  httpsProxy: https://<username>:<pswd>@<ip>:<port> 2
  noProxy: example.com 3
additionalTrustBundle: | 4
    -----BEGIN CERTIFICATE-----
    <MY_TRUSTED_CA_CERT>
    -----END CERTIFICATE-----
additionalTrustBundlePolicy: <policy_to_add_additionalTrustBundle> 5
```

1. クラスター外の HTTP 接続を作成するために使用するプロキシー URL。URL スキームは **http** である必要があります。

2 クラスター外で HTTPS 接続を作成するために使用するプロキシー URL。

3 プロキシーから除外するための宛先ドメイン名、IP アドレス、または他のネットワーク CIDR のコンマ区切りのリスト。サブドメインのみと一致するように、ドメインの前に **.** を付けます。たとえば、**.y.com** は **x.y.com** に一致しますが、**y.com** には一致しません。***** を使用し、すべての宛先のプロキシーをバイパスします。

4 指定されている場合、インストールプログラムは HTTPS 接続のプロキシーに必要な 1 つ以上の追加の CA 証明書が含まれる **user-ca-bundle** という名前の設定マップを **openshift-config** namespace に生成します。次に Cluster Network Operator は、これらのコンテンツを Red Hat Enterprise Linux CoreOS (RHCOS) 信頼バンドルにマージする **trusted-ca-bundle** 設定マップを作成し、この設定マップは **Proxy** オブジェクトの **trustedCA** フィールドで参照されます。**additionalTrustBundle** フィールドは、プロキシーのアイデンティティー証明書が RHCOS 信頼バンドルからの認証局によって署名されない限り必要になります。

5 オプション: **trustedCA** フィールドの **user-ca-bundle** 設定マップを参照する **Proxy** オブジェクトの設定を決定するポリシー。許可される値は **Proxyonly** および **Always** です。**Proxyonly** を使用して、**http/https** プロキシーが設定されている場合にのみ **user-ca-bundle** 設定マップを参照します。**Always** を使用して、常に **user-ca-bundle** 設定マップを参照します。デフォルト値は **Proxyonly** です。

注記

インストールプログラムは、プロキシーの **readinessEndpoints** フィールドをサポートしません。

注記

インストーラーがタイムアウトした場合は、インストーラーの **wait-for** コマンドを使用してデプロイメントを再起動してからデプロイメントを完了します。以下に例を示します。

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

2. ファイルを保存し、OpenShift Container Platform のインストール時にこれを参照します。

インストールプログラムは、指定の **install-config.yaml** ファイルのプロキシー設定を使用する **cluster** という名前のクラスター全体のプロキシーを作成します。プロキシー設定が指定されていない場合、**cluster Proxy** オブジェクトが依然として作成されますが、これには **spec** がありません。

注記

cluster という名前の **Proxy** オブジェクトのみがサポートされ、追加のプロキシーを作成することはできません。

4.7. IAM を手動で作成する

クラスターをインストールするには、Cloud Credential Operator (CCO) が手動モードで動作する必要があります。インストールプログラムは CCO を手動モードに設定しますが、クラウドプロバイダーの ID とアクセス管理シークレットを指定する必要があります。

Cloud Credential Operator (CCO) ユーティリティー (**ccoctl**) を使用して、必要な IBM Cloud VPC リソースを作成できます。

前提条件

- **ccoctl** バイナリーを設定している。
- 既存の **install-config.yaml** ファイルがある。

手順

1. **install-config.yaml** 設定ファイルを編集し、**credentialsMode** パラメーターが **Manual** に設定されるようにします。

   サンプル install-config.yaml 設定ファイル

   ```
   apiVersion: v1
   baseDomain: cluster1.example.com
   credentialsMode: Manual (1)
   compute:
   - architecture: amd64
     hyperthreading: Enabled
   ```

   (1) この行は、**credentialsMode** パラメーターを **Manual** に設定するために追加されます。

2. マニフェストを生成するには、インストールプログラムが含まれるディレクトリーから以下のコマンドを実行します。

   ```
   $ ./openshift-install create manifests --dir <installation_directory>
   ```

3. インストールプログラムが含まれているディレクトリーから、**openshift-install** バイナリーが使用するようにビルドされている OpenShift Container Platform リリースイメージを取得します。

   ```
   $ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
   ```

4. OpenShift Container Platform リリースイメージから **CredentialsRequest** オブジェクトを抽出します。

   ```
   $ oc adm release extract \
     --from=$RELEASE_IMAGE \
     --credentials-requests \
     --cloud=<provider_name> \(1)
     --to=<path_to_credential_requests_directory> (2)
   ```

   (1) プロバイダーの名前。例: **ibmcloud** または **powervs**

   (2) 認証情報の要求が保存されるディレクトリー。

   このコマンドにより、それぞれの **CredentialsRequest** オブジェクトに YAML ファイルが作成されます。

サンプル CredentialsRequest オブジェクト

```
apiVersion: cloudcredential.openshift.io/v1
kind: CredentialsRequest
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: openshift-image-registry-ibmcos
  namespace: openshift-cloud-credential-operator
spec:
  secretRef:
    name: installer-cloud-credentials
    namespace: openshift-image-registry
  providerSpec:
    apiVersion: cloudcredential.openshift.io/v1
    kind: IBMCloudProviderSpec
    policies:
    - attributes:
      - name: serviceName
        value: cloud-object-storage
      roles:
      - crn:v1:bluemix:public:iam::::role:Viewer
      - crn:v1:bluemix:public:iam::::role:Operator
      - crn:v1:bluemix:public:iam::::role:Editor
      - crn:v1:bluemix:public:iam::::serviceRole:Reader
      - crn:v1:bluemix:public:iam::::serviceRole:Writer
    - attributes:
      - name: resourceType
        value: resource-group
      roles:
      - crn:v1:bluemix:public:iam::::role:Viewer
```

5. クラスターでクラスター機能を使用して 1 つ以上のオプションコンポーネントを無効にする場合は、無効なコンポーネントの **CredentialsRequest** カスタムリソースを削除します。

IBM Cloud VPC 上の OpenShift Container Platform 4.13 の credrequests ディレクトリーの内容の例

```
0000_26_cloud-controller-manager-operator_15_credentialsrequest-ibm.yaml 1
0000_30_machine-api-operator_00_credentials-request.yaml 2
0000_50_cluster-image-registry-operator_01-registry-credentials-request-ibmcos.yaml 3
0000_50_cluster-ingress-operator_00-ingress-credentials-request.yaml 4
0000_50_cluster-storage-operator_03_credentials_request_ibm.yaml 5
```

1. Cloud Controller Manager Operator CR が必要です。
2. Machine API Operator CR が必要です。
3. Image Registry Operator CR が必要です。
4. Ingress Operator CR が必要です。
5. Storage Operator CR はオプションのコンポーネントであり、クラスターで無効になっている場合があります。

6. 各認証情報リクエストのサービス ID を作成し、定義されたポリシーを割り当て、API キーを作成し、シークレットを生成します。

```
$ ccoctl ibmcloud create-service-id \
  --credentials-requests-dir <path_to_credential_requests_directory> \ 1
  --name <cluster_name> \ 2
  --output-dir <installation_directory> \
  --resource-group-name <resource_group_name> 3
```

1 認証情報の要求が保存されるディレクトリー。

2 OpenShift Container Platform クラスターの名前。

3 オプション: アクセスポリシーのスコープに使用されるリソースグループの名前。

注記

クラスターで **TechPreviewNoUpgrade** 機能セットによって有効化されたテクノロジープレビュー機能を使用している場合は、**--enable-tech-preview** パラメーターを含める必要があります。

間違ったリソースグループ名が指定された場合、ブートストラップフェーズ中にインストールが失敗します。正しいリソースグループ名を見つけるには、次のコマンドを実行します。

```
$ grep resourceGroupName <installation_directory>/manifests/cluster-infrastructure-02-config.yml
```

検証

- クラスターの **manifests** ディレクトリーに適切なシークレットが生成されていることを確認してください。

4.8. クラスターのデプロイ

互換性のあるクラウドプラットフォームに OpenShift Container Platform をインストールできます。

重要

インストールプログラムの **create cluster** コマンドは、初期インストール時に 1 回だけ実行できます。

前提条件

- クラスターをホストするクラウドプラットフォームでアカウントを設定します。
- OpenShift Container Platform インストールプログラム、およびクラスターのプルシークレットを取得する。
- ホスト上のクラウドプロバイダーアカウントに、クラスターをデプロイするための適切な権限があることを確認してください。アカウントの権限が正しくないと、インストールプロセスが失敗し、不足している権限を示すエラーメッセージが表示されます。

手順

- インストールプログラムが含まれるディレクトリーに切り替え、クラスターのデプロイメントを初期化します。

```
$ ./openshift-install create cluster --dir <installation_directory> \ 1
    --log-level=info 2
```

1. **<installation_directory>** に、カスタマイズした **./install-config.yaml** ファイルの場所を指定します。
2. 異なるインストールの詳細情報を表示するには、**info** ではなく、**warn**、**debug**、または **error** を指定します。

検証

クラスターのデプロイが正常に完了すると、次のようになります。

- ターミナルには、Web コンソールへのリンクや **kubeadmin** ユーザーの認証情報など、クラスターにアクセスするための指示が表示されます。
- 認証情報は **<installation_directory>/.openshift_install.log** にも出力されます。

重要

インストールプログラム、またはインストールプログラムが作成するファイルを削除することはできません。これらはいずれもクラスターを削除するために必要になります。

出力例

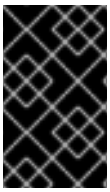
```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- インストールプログラムが生成する Ignition 設定ファイルには、24 時間が経過すると期限切れになり、その後に更新される証明書が含まれます。証明書を更新する前にクラスターが停止し、24 時間経過した後にクラスターを再起動すると、クラスターは期限切れの証明書を自動的に復元します。例外として、kubelet 証明書を回復するために保留状態の **node-bootstrapper** 証明書署名要求 (CSR) を手動で承認する必要があります。詳細は、**コントロールプレーン証明書の期限切れの状態からのリカバリー** に関するドキュメントを参照してください。
- 24 時間証明書はクラスターのインストール後 16 時間から 22 時間にローテーションするため、Ignition 設定ファイルは、生成後 12 時間以内に使用することを推奨します。12 時間以内に Ignition 設定ファイルを使用することにより、インストール中に証明書の更新が実行された場合のインストールの失敗を回避できます。

4.9. バイナリーのダウンロードによる OPENSHIFT CLI のインストール

コマンドラインインターフェイスを使用して OpenShift Container Platform と対話するために CLI (**oc**) をインストールすることができます。**oc** は Linux、Windows、または macOS にインストールできます。



重要

以前のバージョンの **oc** をインストールしている場合、これを使用して OpenShift Container Platform 4.13 のすべてのコマンドを実行することはできません。新規バージョンの **oc** をダウンロードし、インストールします。

Linux への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Linux にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **Product Variant** ドロップダウンリストからアーキテクチャーを選択します。
3. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
4. **OpenShift v4.13 Linux Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
5. アーカイブを展開します。

```
$ tar xvf <file>
```

6. **oc** バイナリーを、**PATH** にあるディレクトリーに配置します。
PATH を確認するには、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

Windows への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Windows にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 Windows Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
4. ZIP プログラムでアーカイブを解凍します。
5. **oc** バイナリーを、**PATH** にあるディレクトリーに移動します。
   PATH を確認するには、コマンドプロンプトを開いて以下のコマンドを実行します。

```
C:\> path
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
C:\> oc <command>
```

macOS への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを macOS にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 macOS Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。

注記

macOS arm64 の場合は、**OpenShift v4.13 macOS arm64 Client** エントリーを選択します。

4. アーカイブを展開し、解凍します。
5. **oc** バイナリーをパスにあるディレクトリーに移動します。

PATH を確認するには、ターミナルを開き、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

4.10. CLI の使用によるクラスターへのログイン

クラスター **kubeconfig** ファイルをエクスポートし、デフォルトシステムユーザーとしてクラスターにログインできます。**kubeconfig** ファイルには、クライアントを正しいクラスターおよび API サーバーに接続するために CLI で使用されるクラスターに関する情報が含まれます。このファイルはクラスターに固有のファイルであり、OpenShift Container Platform のインストール時に作成されます。

前提条件

- OpenShift Container Platform クラスターをデプロイしていること。
- **oc** CLI がインストールされている。

手順

1. **kubeadmin** 認証情報をエクスポートします。

```
$ export KUBECONFIG=<installation_directory>/auth/kubeconfig 1
```

1 **<installation_directory>** には、インストールファイルを保存したディレクトリーへのパスを指定します。

2. エクスポートされた設定を使用して、**oc** コマンドを正常に実行できることを確認します。

```
$ oc whoami
```

出力例

```
system:admin
```

関連情報

- Web コンソールへのアクセス

4.11. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス

OpenShift Container Platform 4.13 では、クラスターの健全性および正常に実行された更新についてのメトリクスを提供するためにデフォルトで実行される Telemetry サービスにもインターネットアクセスが必要です。クラスターがインターネットに接続されている場合、Telemetry は自動的に実行され、クラスターは OpenShift Cluster Manager Hybrid Cloud Console に登録されます。

OpenShift Cluster Manager インベントリーが正常である (Telemetry によって自動的に維持、または OpenShift Cluster Manager Hybrid Cloud Console を使用して手動で維持) ことを確認した後に、subscription watch を使用 して、アカウントまたはマルチクラスターレベルで OpenShift Container Platform サブスクリプションを追跡します。

関連情報

- リモートヘルスモニタリングについて

4.12. 次のステップ

- クラスターをカスタマイズします。
- 必要に応じて、リモートヘルスレポート にすることができます。

第5章 ネットワークをカスタマイズして IBM CLOUD VPC にクラスターをインストールする

OpenShift Container Platform バージョン 4.13 では、インストールプログラムが IBM Cloud VPC でプロビジョニングするインフラストラクチャーに、カスタマイズされたネットワーク設定でクラスターをインストールできます。ネットワーク設定をカスタマイズすることにより、クラスターは環境内の既存の IP アドレスの割り当てと共存でき、既存の MTU および VXLAN 設定と統合できます。インストールをカスタマイズするには、クラスターをインストールする前に、**install-config.yaml** ファイルでパラメーターを変更します。

大半のネットワーク設定パラメーターはインストール時に設定する必要があり、実行中のクラスターで変更できるのは **kubeProxy** 設定パラメーターのみになります。

5.1. 前提条件

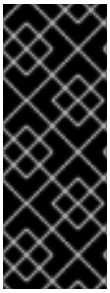
- OpenShift Container Platform のインストールおよび更新 プロセスの詳細を確認している。
- クラスターインストール方法の選択およびそのユーザー向けの準備 を確認している。
- クラスターをホストするように IBM Cloud アカウントを設定 している。
- ファイアウォールを使用する場合は、クラスターがアクセスを必要とするサイトを許可するようにファイアウォールを設定する必要がある。
- クラスターをインストールする前に、**ccoctl** ユーティリティーを設定している。詳細は、IBM Cloud VPC 用の IAM の設定 を参照してください。

5.2. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス

OpenShift Container Platform 4.13 では、クラスターをインストールするためにインターネットアクセスが必要になります。

インターネットへのアクセスは以下を実行するために必要です。

- OpenShift Cluster Manager Hybrid Cloud Console にアクセスし、インストールプログラムをダウンロードし、サブスクリプション管理を実行します。クラスターにインターネットアクセスがあり、Telemetry を無効にしない場合、そのサービスは有効なサブスクリプションでクラスターを自動的に使用します。
- クラスターのインストールに必要なパッケージを取得するために Quay.io にアクセスします。
- クラスターの更新を実行するために必要なパッケージを取得します。



重要

クラスターでインターネットに直接アクセスできない場合、プロビジョニングする一部のタイプのインフラストラクチャーでネットワークが制限されたインストールを実行できます。このプロセスで、必要なコンテンツをダウンロードし、これを使用してミラーレジストリーにインストールパッケージを設定します。インストールタイプに応じて、クラスターのインストール環境でインターネットアクセスが不要となる場合があります。クラスターを更新する前に、ミラーレジストリーのコンテンツを更新します。

5.3. クラスターノードの SSH アクセス用のキーペアの生成

OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定できます。キーは、Ignition 設定ファイルを介して Red Hat Enterprise Linux CoreOS (RHCOS) ノードに渡され、ノードへの SSH アクセスを認証するために使用されます。このキーは各ノードの **core** ユーザーの ~/**.ssh/authorized_keys** リストに追加され、パスワードなしの認証が可能になります。

キーがノードに渡されると、キーペアを使用して RHCOS ノードにユーザー **core** として SSH を実行できます。SSH 経由でノードにアクセスするには、秘密鍵のアイデンティティーをローカルユーザーの SSH で管理する必要があります。

インストールのデバッグまたは障害復旧を実行するためにクラスターノードに対して SSH を実行する場合は、インストールプロセスの間に SSH 公開鍵を指定する必要があります。**./openshift-install gather** コマンドでは、SSH 公開鍵がクラスターノードに配置されている必要もあります。

重要

障害復旧およびデバッグが必要な実稼働環境では、この手順を省略しないでください。

注記

AWS キーペア などのプラットフォームに固有の方法で設定したキーではなく、ローカルキーを使用する必要があります。

手順

1. クラスターノードへの認証に使用するローカルマシンに既存の SSH キーペアがない場合は、これを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ ssh-keygen -t ed25519 -N '' -f <path>/<file_name> 1
```

1 新しい SSH キーのパスとファイル名 (~/**.ssh/id_ed25519** など) を指定します。既存のキーペアがある場合は、公開鍵が ~/**.ssh** ディレクトリーにあることを確認します。

2. 公開 SSH キーを表示します。

```
$ cat <path>/<file_name>.pub
```

たとえば、次のコマンドを実行して ~/**.ssh/id_ed25519.pub** 公開鍵を表示します。

```
$ cat ~/.ssh/id_ed25519.pub
```

3. ローカルユーザーの SSH エージェントに SSH 秘密鍵 ID が追加されていない場合は、それを追加します。キーの SSH エージェント管理は、クラスターノードへのパスワードなしの SSH 認証、または **./openshift-install gather** コマンドを使用する場合は必要になります。

注記

一部のディストリビューションでは、~/**.ssh/id_rsa** および ~/**.ssh/id_dsa** などのデフォルトの SSH 秘密鍵のアイデンティティーは自動的に管理されます。

a. **ssh-agent** プロセスがローカルユーザーに対して実行されていない場合は、バックグラウンドタスクとして開始します。

```
$ eval "$(ssh-agent -s)"
```

出力例

```
Agent pid 31874
```

4. SSH プライベートキーを **ssh-agent** に追加します。

```
$ ssh-add <path>/<file_name> 1
```

1 ~/**.ssh/id_ed25519** などの、SSH プライベートキーのパスおよびファイル名を指定します。

出力例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

次のステップ

- OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定します。

5.4. インストールプログラムの取得

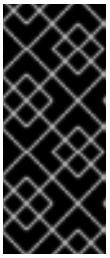
OpenShift Container Platform をインストールする前に、インストールに使用しているホストにインストールファイルをダウンロードします。

前提条件

- 500 MB のローカルディスク領域がある Linux または macOS を実行するコンピューターが必要です。

手順

1. OpenShift Cluster Manager サイトの インフラストラクチャープロバイダー ページにアクセスします。Red Hat アカウントがある場合は、認証情報を使用してログインします。アカウントがない場合はこれを作成します。
2. インフラストラクチャープロバイダーを選択します。
3. インストールタイプのページに移動し、ホストオペレーティングシステムとアーキテクチャーに対応するインストールプログラムをダウンロードして、インストール設定ファイルを保存するディレクトリーにファイルを配置します。



重要

インストールプログラムは、クラスターのインストールに使用するコンピューターにいくつかのファイルを作成します。クラスターのインストール完了後は、インストールプログラムおよびインストールプログラムが作成するファイルを保持する必要があります。ファイルはいずれもクラスターを削除するために必要になります。

重要

インストールプログラムで作成されたファイルを削除しても、クラスターがインストール時に失敗した場合でもクラスターは削除されません。クラスターを削除するには、特定のクラウドプロバイダー用の OpenShift Container Platform のアンインストール手順を実行します。

4. インストールプログラムを展開します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar -xvf openshift-install-linux.tar.gz
```

5. Red Hat OpenShift Cluster Manager からインストールプルシークレット をダウンロードします。このプルシークレットを使用し、OpenShift Container Platform コンポーネントのコンテナーイメージを提供する Quay.io など、組み込まれた各種の認証局によって提供されるサービスで認証できます。

5.5. API キーのエクスポート

作成した API キーをグローバル変数として設定する必要があります。インストールプログラムは、起動時に変数を取り込み、API キーを設定します。

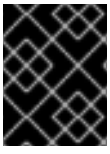
前提条件

- IBM Cloud アカウント用にユーザー API キーまたはサービス ID API キーのいずれかを作成している。

手順

- アカウントの API キーをグローバル変数としてエクスポートします。

```
$ export IC_API_KEY=<api_key>
```



重要

変数名は指定どおりに正確に設定する必要があります。インストールプログラムは、起動時に変数名が存在することを想定しています。

5.6. インストール設定ファイルの作成

IBM Cloud にインストールする OpenShift Container Platform クラスターをカスタマイズできます。

前提条件

- OpenShift Container Platform インストールプログラム、およびクラスターのプルシークレットを取得する。
- サブスクリプションレベルでサービスプリンシパルのパーミッションを取得する。

手順

1. **install-config.yaml** ファイルを作成します。

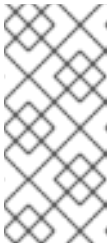
   a. インストールプログラムが含まれるディレクトリーに切り替え、以下のコマンドを実行します。

   ```
   $ ./openshift-install create install-config --dir <installation_directory> 1
   ```

   1 **<installation_directory>** の場合、インストールプログラムが作成するファイルを保存するためにディレクトリー名を指定します。

   ディレクトリーを指定する場合:

   - ディレクトリーに **execute** 権限があることを確認します。この権限は、インストールディレクトリーで Terraform バイナリーを実行するために必要です。
   - 空のディレクトリーを使用します。ブートストラップ X.509 証明書などの一部のインストールアセットは有効期限が短いため、インストールディレクトリーを再利用しないでください。別のクラスターインストールの個別のファイルを再利用する必要がある場合は、それらをディレクトリーにコピーすることができます。ただし、インストールアセットのファイル名はリリース間で変更される可能性があります。インストールファイルを以前のバージョンの OpenShift Container Platform からコピーする場合は注意してください。

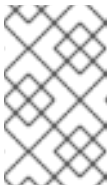
   注記

   古い設定の再利用を回避するために、~/**.powervs** ディレクトリーは必ず削除してください。以下のコマンドを実行します。

   ```
   $ rm -rf ~/.powervs
   ```

   b. プロンプト時に、クラウドの設定の詳細情報を指定します。

      i. オプション: クラスターマシンにアクセスするために使用する SSH キーを選択します。

      注記

      インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。

      ii. ターゲットとするプラットフォームとして **ibmcloud** を選択します。

      iii. クラスターをデプロイするリージョンを選択します。

      iv. クラスターをデプロイするベースドメインを選択します。ベースドメインは、クラスターに作成したパブリック DNS ゾーンに対応します。

v. クラスターの記述名を入力します。

vi. Red Hat OpenShift Cluster Manager からプルシークレット を貼り付けます。

2. **install-config.yaml** ファイルを変更します。利用可能なパラメーターの詳細は、「インストール設定パラメーター」のセクションを参照してください。

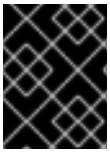
3. **install-config.yaml** ファイルをバックアップし、複数のクラスターをインストールするのに使用できるようにします。

重要

install-config.yaml ファイルはインストールプロセス時に使用されます。このファイルを再利用する必要がある場合は、この段階でこれをバックアップしてください。

5.6.1. インストール設定パラメーター

OpenShift Container Platform クラスターをデプロイする前に、クラスターをホストするクラウドプラットフォームでアカウントを記述し、クラスターのプラットフォームをオプションでカスタマイズするためにパラメーターの値を指定します。**install-config.yaml** インストール設定ファイルを作成する際に、コマンドラインで必要なパラメーターの値を指定します。クラスターをカスタマイズする場合、**install-config.yaml** ファイルを変更して、プラットフォームについての詳細情報を指定できます。



重要

インストール後は、これらのパラメーターを **install-config.yaml** ファイルで変更することはできません。

5.6.1.1. 必須設定パラメーター

必須のインストール設定パラメーターは、以下の表で説明されています。

表5.1 必須パラメーター

パラメーター	説明	値
apiVersion	**install-config.yaml** コンテンツの API バージョン。現在のバージョンは **v1** です。インストールプログラムは、古い API バージョンもサポートしている場合があります。	文字列

パラメーター	説明	値
baseDomain	クラウドプロバイダーのベースドメイン。ベースドメインは、OpenShift Container Platform クラスターコンポーネントへのルートを作成するために使用されます。クラスターの完全な DNS 名は、**<metadata.name>.<baseDomain>** 形式を使用する **baseDomain** と **metadata.name** パラメーターの値を組み合わせたものです。	**example.com** などの完全修飾ドメインまたはサブドメイン名。
metadata	Kubernetes リソース **ObjectMeta**。ここからは **name** パラメーターのみが消費されます。	オブジェクト
metadata.name	クラスターの名前。クラスターの DNS レコードはすべて **{{.metadata.name}}.{{.baseDomain}}** のサブドメインです。	**dev** などの小文字、ハイフン (**-**)、およびピリオド (**.**) が含まれる文字列。
platform	インストールを実行する特定のプラットフォームの設定: **alibabacloud**、**aws**、**baremetal**、**azure**、**gcp**、**ibmcloud**、**Nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**。**platform.<platform>** パラメーターに関する追加情報は、以下の表で特定のプラットフォームを参照してください。	オブジェクト

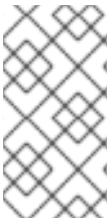
パラメーター	説明	値

pullSecret	Red Hat OpenShift Cluster Manager からプルシークレット を取得して、Quay.io などのサービスから OpenShift Container Platform コンポーネントのコンテナーイメージをダウンロードすることを認証します。	<pre>{
		  "auths":{
		  "cloud.openshift.com":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  },
		  "quay.io":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  }
		  }
		}</pre>

5.6.1.2. ネットワーク設定パラメーター

既存のネットワークインフラストラクチャーの要件に基づいて、インストール設定をカスタマイズできます。たとえば、クラスターネットワークの IP アドレスブロックを拡張するか、デフォルトとは異なる IP アドレスブロックを指定できます。

IPv4 アドレスのみがサポートされます。



注記

Globalnet は、Red Hat OpenShift Data Foundation ディザスターリカバリーソリューションではサポートされていません。局地的なディザスターリカバリーのシナリオでは、各クラスター内のクラスターとサービスネットワークに重複しない範囲のプライベート IP アドレスを使用するようにしてください。

表5.2 ネットワークパラメーター

パラメーター	説明	値
networking	クラスターのネットワークの設定。	オブジェクト  **注記** インストール後に **networking** オブジェクトで指定したパラメーターを変更することはできません。

パラメーター	説明	値
networking.networkType	インストールする Red Hat OpenShift Networking ネットワークプラグイン。	**OpenShiftSDN** または **OVNKubernetes** のいずれか。**OpenShiftSDN** は、すべての Linux ネットワークの Container Network Interface (CNI)プラグインです。**OVNKubernetes** は、Linux ネットワークと、Linux サーバーと Windows サーバーの両方を含む Linux ネットワークおよびハイブリッドネットワーク用の CNI プラグインです。デフォルトの値は **OVNkubernetes** です。
networking.clusterNetwork	Pod の IP アドレスブロック。 デフォルト値は **10.128.0.0/14** で、ホストの接頭辞は **/23** です。 複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。	オブジェクトの配列。以下に例を示します。 networking: clusterNetwork: - cidr: 10.128.0.0/14 hostPrefix: 23
networking.clusterNetwork.cidr	**networking.clusterNetwork** を使用する場合に必須です。IP アドレスブロック。 IPv4 ネットワーク	CIDR (Classless Inter-Domain Routing) 表記の IP アドレスブロック。IPv4 ブロックの接頭辞長は **0** から **32** の間になります。
networking.clusterNetwork.hostPrefix	それぞれの個別ノードに割り当てるサブネット接頭辞長。たとえば、**hostPrefix** が **23** に設定される場合、各ノードに指定の **cidr** から **/23** サブネットが割り当てられます。**hostPrefix** 値の **23** は、510 (2^(32 - 23) - 2) Pod IP アドレスを提供します。	サブネット接頭辞。 デフォルト値は **23** です。
networking.serviceNetwork	サービスの IP アドレスブロック。デフォルト値は **172.30.0.0/16** です。 OpenShift SDN および OVN-Kubernetes ネットワークプラグインは、サービスネットワークの単一 IP アドレスブロックのみをサポートします。	CIDR 形式の IP アドレスブロックを持つ配列。以下に例を示します。 networking: serviceNetwork: - 172.30.0.0/16

パラメーター	説明	値
networking.machineNetwork	マシンの IP アドレスブロック。 複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。	オブジェクトの配列。以下に例を示します。 networking: machineNetwork: - cidr: 10.0.0.0/16
networking.machineNetwork.cidr	**networking.machineNetwork** を使用する場合に必須です。IP アドレスブロック。libvirt と IBM Power Virtual Server を除くすべてのプラットフォームのデフォルト値は **10.0.0.0/16** です。libvirt の場合、デフォルト値は **192.168.126.0/24** です。IBM Power Virtual Server の場合、デフォルト値は **192.168.0.0/24** です。	CIDR 表記の IP ネットワークブロック。 例: **10.0.0.0/16** **注記** 優先される NIC が置かれている CIDR に一致する **networking.machineNetwork** を設定します。

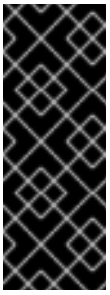
5.6.1.3. オプションの設定パラメーター

オプションのインストール設定パラメーターは、以下の表で説明されています。

表5.3 オプションのパラメーター

パラメーター	説明	値
additionalTrustBundle	ノードの信頼済み証明書ストアに追加される PEM でエンコードされた X.509 証明書バンドル。この信頼バンドルは、プロキシーが設定されている場合にも使用することができます。	文字列
capabilities	オプションのコアクラスターコンポーネントのインストールを制御します。オプションのコンポーネントを無効にすることで、OpenShift Container Platform クラスターのフットプリントを削減できます。詳細は、**インストール** の「クラスター機能ページ」を参照してください。	文字列配列

パラメーター	説明	値
capabilities.baselineCapabilitySet	有効にするオプション機能の初期セットを選択します。有効な値は **None**、**v4.11**、**v4.12**、**vCurrent** です。デフォルト値は **vCurrent** です。	文字列
capabilities.additionalEnabledCapabilities	オプションの機能のセットを、**baselineCapabilitySet** で指定したものを超えて拡張します。このパラメーターで複数の機能を指定できます。	文字列配列
cpuPartitioningMode	ワークロードパーティション設定を使用して、OpenShift Container Platform サービス、クラスター管理ワークロード、およびインフラストラクチャー Pod を分離し、予約された CPU セットで実行できます。ワークロードパーティショニングは、インストール中にのみ有効にできます。インストール後に無効にすることはできません。このフィールドはワークロードのパーティショニングを有効にしますが、特定の CPU を使用するようにワークロードを設定するわけではありません。詳細は、**スケーラビリティとパフォーマンス** セクションの **ワークロードパーティショニング** ページを参照してください。	**None** または **AllNodes**。デフォルト値は **None** です。
compute	コンピュートノードを形成するマシンの設定。	**MachinePool** オブジェクトの配列。
compute.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String

パラメーター	説明	値
compute: hyperthreading:	コンピュートマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時スレッドはマシンのコアのパフォーマンスを上げるために有効にされます。  **重要** 同時スレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
compute.name	**compute** を使用する場合に必須です。マシンプールの名前。	**worker**
compute.platform	**compute** を使用する場合に必須です。このパラメーターを使用して、ワーカーマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **controlPlane.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
compute.replicas	プロビジョニングするコンピュートマシン (ワーカーマシンとしても知られる) の数。	**2** 以上の正の整数。デフォルト値は **3** です。
featureSet	機能セットのクラスターを有効にします。機能セットは、デフォルトで有効にされない OpenShift Container Platform 機能のコレクションです。インストール中に機能セットを有効にする方法の詳細は、「機能ゲートの使用による各種機能の有効化」を参照してください。	文字列。**TechPreviewNoUpgrade** など、有効にする機能セットの名前。
controlPlane	コントロールプレーンを形成するマシンの設定。	**MachinePool** オブジェクトの配列。

パラメーター	説明	値
controlPlane.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String
controlPlane: hyperthreading:	コントロールプレーンマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時スレッドはマシンのコアのパフォーマンスを上げるために有効にされます。  **重要** 同時スレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
controlPlane.name	**controlPlane** を使用する場合に必須です。マシンプールの名前。	**master**
controlPlane.platform	**controlPlane** を使用する場合に必須です。このパラメーターを使用して、コントロールプレーンマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **compute.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
controlPlane.replicas	プロビジョニングするコントロールプレーンマシンの数。	サポートされる値は **3** のみです (これはデフォルト値です)。

パラメーター	説明	値
credentialsMode	Cloud Credential Operator (CCO) モード。CCO は、モードが指定されていない場合に指定される認証情報の機能を動的に判別しようとします。この場合、複数のモードがサポートされるプラットフォームで mint モードが優先されます。  **注記** すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**Cluster Operators リファレンス** の **Cloud Credential Operator** を参照してください。  **注記** AWS アカウントでサービスコントロールポリシー (SCP) が有効になっている場合は、**credentialsMode** パラメーターを **Mint**、**Passthrough** または **Manual** に設定する必要があります。	**Mint**、**Passthrough**、**Manual**、または空の文字列 (**""**)。
imageContentSources	release-image コンテンツのソースおよびリポジトリー。	オブジェクトの配列。この表の以下の行で説明されているように、**source** およびオプションで **mirrors** が含まれます。
imageContentSources.source	**imageContentSources** を使用する場合に必須です。ユーザーが参照するリポジトリーを指定します (例: イメージプル仕様)。	文字列
imageContentSources.mirrors	同じイメージが含まれる可能性のあるリポジトリーを 1 つ以上指定します。	文字列の配列。

パラメーター	説明	値
publish	Kubernetes API、OpenShift ルートなどのクラスターのユーザーに表示されるエンドポイントをパブリッシュまたは公開する方法。	**Internal** または **External**。プライベートクラスターをデプロイするには、**publish** を **Internal** に設定します。これはインターネットからアクセスできません。デフォルト値は **External** です。
sshKey	クラスターマシンへのアクセスを認証するための SSH キー。 **注記** インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。	たとえば、**sshKey: ssh-ed25519 AAAA..** です。

1. すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**認証と認可** コンテンツの「クラウドプロバイダーの認証情報の管理」を参照してください。

5.6.1.4. 追加の IBM Cloud VPC 設定パラメーター

追加の IBM Cloud VPC 設定パラメーターについて、以下の表で説明します。

表5.4 追加の IBM Cloud VPC パラメーター

パラメーター	説明	値
platform.ibmcloud.resourceGroupName	既存のリソースグループの名前。デフォルトでは、installer-provisioned VPC およびクラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。クラスターを既存の VPC にデプロイする場合、installer-provisioned クラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。プロビジョニングした VPC リソースは、**networkResourceGroupName** パラメーターを使用して指定したリソースグループに存在する必要があります。いずれの場合も、クラスターコンポーネントはリソースグループ内のすべてのリソースの所有権を引き受けるため、このリソースグループは単一のクラスターインストールのみに使用する必要があります。[1]	文字列 (例: **existing_resource_group**)。

パラメーター	説明	値
platform.ibmcloud.networkResourceGroupName	既存のリソースグループの名前。このリソースには、クラスターがデプロイされる既存の VPC とサブネットが含まれます。このパラメーターは、プロビジョニングした VPC にクラスターをデプロイする際に必要です。	文字列 (例: **existing_network_resource_group**)。
platform.ibmcloud.dedicatedHosts.profile	作成する新しい専用ホスト。**platform.ibmcloud.dedicatedHosts.name** に値を指定する場合、このパラメーターは必須ではありません。	**cx2-host-152x304**などの有効な IBM Cloud VPC 専用ホストプロファイル。[2]
platform.ibmcloud.dedicatedHosts.name	既存の専用ホスト。**platform.ibmcloud.dedicatedHosts.profile** に値を指定する場合、このパラメーターは必須ではありません。	文字列、たとえば **my-dedicated-host-name**。
platform.ibmcloud.type	すべての IBM Cloud VPC マシンのインスタンスタイプ。	**bx2-8x32** などの有効な IBM Cloud VPC インスタンスタイプ。[2]
platform.ibmcloud.vpcName	クラスターをデプロイする既存 VPC の名前。	文字列。
platform.ibmcloud.controlPlaneSubnets	コントロールプレーンマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。	文字列配列

パラメーター	説明	値
platform.ibmcloud.computeSubnets	コンピュートマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。サブネット ID はサポートされていません。	文字列配列

1. 既存のリソースグループを定義するか、インストーラーが作成するかによって、クラスターがアンインストールされたときにリソースグループがどのように扱われるかが決まります。リソースグループを定義すると、インストーラーはインストーラーがプロビジョニングしたすべてのリソースを削除しますが、リソースグループはそのままにします。インストールの一部としてリソースグループが作成された場合、インストーラーは、インストーラーがプロビジョニングしたすべてのリソースとリソースグループを削除します。
2. 自身のニーズに最適なプロファイルを判別するには、IBM ドキュメントの Instance Profiles を参照してください。

5.6.2. クラスターインストールの最小リソース要件

それぞれのクラスターマシンは、以下の最小要件を満たしている必要があります。

表5.5 最小リソース要件

マシン	オペレーティングシステム	仮想 CPU	仮想 RAM	ストレージ	1秒あたりの入出力 (IOPS)
ブートストラップ	RHCOS	4	16 GB	100 GB	300
コントロールプレーン	RHCOS	4	16 GB	100 GB	300
Compute	RHCOS	2	8 GB	100 GB	300

注記

OpenShift Container Platform バージョン 4.13 の時点で、RHCOS は RHEL バージョン 9.2 に基づいており、マイクロアーキテクチャーの要件を更新します。次のリストには、各アーキテクチャーに必要な最小限の命令セットアーキテクチャー (ISA) が含まれています。

- x86-64 アーキテクチャーには x86-64-v2 ISA が必要
- ARM64 アーキテクチャーには ARMv8.0-A ISA が必要
- IBM Power アーキテクチャーには Power 9 ISA が必要
- s390x アーキテクチャーには z14 ISA が必要

詳細は、RHEL アーキテクチャー を参照してください。

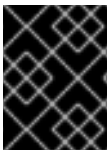
プラットフォームのインスタンスタイプがクラスターマシンの最小要件を満たす場合、これは OpenShift Container Platform で使用することがサポートされます。

関連情報

- ストレージの最適化

5.6.3. IBM Cloud VPC 用にカスタマイズされた install-config.yaml ファイルのサンプル

install-config.yaml ファイルをカスタマイズして、OpenShift Container Platform クラスターのプラットフォームについての詳細を指定するか、必要なパラメーターの値を変更することができます。



重要

このサンプルの YAML ファイルは参照用にのみ提供されます。インストールプログラムを使用して **install-config.yaml** ファイルを取得し、変更する必要があります。

```
apiVersion: v1
baseDomain: example.com 1
controlPlane: 2 3
  hyperthreading: Enabled 4
  name: master
  platform:
    ibmcloud: {}
  replicas: 3
compute: 5 6
- hyperthreading: Enabled 7
  name: worker
  platform:
    ibmcloud: {}
  replicas: 3
metadata:
  name: test-cluster 8
networking: 9
  clusterNetwork:
```

```
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes 10
  serviceNetwork:
  - 172.30.0.0/16
platform:
  ibmcloud:
    region: us-south 11
credentialsMode: Manual
publish: External
pullSecret: '{"auths": ...}' 12
fips: false 13
sshKey: ssh-ed25519 AAAA... 14
```

1 8 11 12 必須。インストールプログラムはこの値の入力を求めるプロンプトを出します。

2 5 9 これらのパラメーターおよび値を指定しない場合、インストールプログラムはデフォルトの値を指定します。

3 6 **controlPlane** セクションは単一マッピングですが、**compute** セクションはマッピングのシーケンスになります。複数の異なるデータ構造の要件を満たすには、**compute** セクションの最初の行はハイフン **-** で始め、**controlPlane** セクションの最初の行はハイフンで始めることができません。1 つのコントロールプレーンプールのみが使用されます。

4 7 ハイパースレッディングとも呼ばれる同時マルチスレッドを有効または無効にします。デフォルトでは、同時スレッドはマシンのコアのパフォーマンスを上げるために有効にされます。パラメーター値を **Disabled** に設定するとこれを無効にすることができます。一部のクラスターマシンで同時マルチスレッドを無効にする場合は、これをすべてのクラスターマシンで無効にする必要があります。

重要

同時スレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。同時マルチスレッドを無効にする場合は、マシンに対して **n1-standard-8** などの大規模なマシンタイプを使用します。

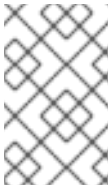
10 インストールするクラスターネットワークプラグイン。サポートされている値は **OVNKubernetes** と **OpenShiftSDN** です。デフォルトの値は **OVNkubernetes** です。

13 FIPS モードを有効または無効にします。デフォルトでは、FIPS モードは有効にされません。

重要

OpenShift Container Platform 4.13 は Red Hat Enterprise Linux (RHEL) 9.2 をベースにしています。FIPS 検証用に RHEL 9.2 暗号化モジュールがまだ送信されていません。詳細は、4.13 **OpenShift Container Platform リリースノート** の "About this release" を参照してください。

14 オプション: クラスター内のマシンにアクセスするのに使用する **sshKey** 値をオプションで指定できます。



注記

インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。

5.6.4. インストール時のクラスター全体のプロキシーの設定

実稼働環境では、インターネットへの直接アクセスを拒否し、代わりに HTTP または HTTPS プロキシーを使用することができます。プロキシー設定を **install-config.yaml** ファイルで行うことにより、新規の OpenShift Container Platform クラスターをプロキシーを使用するように設定できます。

前提条件

- 既存の **install-config.yaml** ファイルがある。
- クラスターがアクセスする必要のあるサイトを確認済みで、それらのいずれかがプロキシーをバイパスする必要があるかどうかを判別している。デフォルトで、すべてのクラスター Egress トラフィック (クラスターをホストするクラウドに関するクラウドプロバイダー API に対する呼び出しを含む) はプロキシーされます。プロキシーを必要に応じてバイパスするために、サイトを **Proxy** オブジェクトの **spec.noProxy** フィールドに追加している。

注記

Proxy オブジェクトの **status.noProxy** フィールドには、インストール設定の **networking.machineNetwork[].cidr**、**networking.clusterNetwork[].cidr**、および **networking.serviceNetwork[]** フィールドの値が設定されます。

Amazon Web Services (AWS)、Google Cloud、Microsoft Azure、および Red Hat OpenStack Platform (RHOSP)へのインストールの場合、**Proxy** オブジェクトの **status.noProxy** フィールドには、インスタンスメタデータのエンドポイント(**169.254.169.254**)も設定されます。

手順

1. **install-config.yaml** ファイルを編集し、プロキシー設定を追加します。以下に例を示します。

```
apiVersion: v1
baseDomain: my.domain.com
proxy:
  httpProxy: http://<username>:<pswd>@<ip>:<port> 1
  httpsProxy: https://<username>:<pswd>@<ip>:<port> 2
  noProxy: example.com 3
additionalTrustBundle: | 4
    -----BEGIN CERTIFICATE-----
    <MY_TRUSTED_CA_CERT>
    -----END CERTIFICATE-----
additionalTrustBundlePolicy: <policy_to_add_additionalTrustBundle> 5
```

1. クラスター外の HTTP 接続を作成するために使用するプロキシー URL。URL スキームは **http** である必要があります。

2 クラスター外で HTTPS 接続を作成するために使用するプロキシー URL。

3 プロキシーから除外するための宛先ドメイン名、IP アドレス、または他のネットワーク CIDR のコンマ区切りのリスト。サブドメインのみと一致するように、ドメインの前に **.** を付けます。たとえば、**.y.com** は **x.y.com** に一致しますが、**y.com** には一致しません。***** を使用し、すべての宛先のプロキシーをバイパスします。

4 指定されている場合、インストールプログラムは HTTPS 接続のプロキシーに必要な 1 つ以上の追加の CA 証明書が含まれる **user-ca-bundle** という名前の設定マップを **openshift-config** namespace に生成します。次に Cluster Network Operator は、これらのコンテンツを Red Hat Enterprise Linux CoreOS (RHCOS) 信頼バンドルにマージする **trusted-ca-bundle** 設定マップを作成し、この設定マップは **Proxy** オブジェクトの **trustedCA** フィールドで参照されます。**additionalTrustBundle** フィールドは、プロキシーのアイデンティティー証明書が RHCOS 信頼バンドルからの認証局によって署名されない限り必要になります。

5 オプション： **trustedCA** フィールドの **user-ca-bundle** 設定マップを参照する **Proxy** オブジェクトの設定を決定するポリシー。許可される値は **Proxyonly** および **Always** です。**Proxyonly** を使用して、**http/https** プロキシーが設定されている場合にのみ **user-ca-bundle** 設定マップを参照します。**Always** を使用して、常に **user-ca-bundle** 設定マップを参照します。デフォルト値は **Proxyonly** です。

注記

インストールプログラムは、プロキシーの **readinessEndpoints** フィールドをサポートしません。

注記

インストーラーがタイムアウトした場合は、インストーラーの **wait-for** コマンドを使用してデプロイメントを再起動してからデプロイメントを完了します。以下に例を示します。

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

2. ファイルを保存し、OpenShift Container Platform のインストール時にこれを参照します。

インストールプログラムは、指定の **install-config.yaml** ファイルのプロキシー設定を使用する **cluster** という名前のクラスター全体のプロキシーを作成します。プロキシー設定が指定されていない場合、**cluster Proxy** オブジェクトが依然として作成されますが、これには **spec** がありません。

注記

cluster という名前の **Proxy** オブジェクトのみがサポートされ、追加のプロキシーを作成することはできません。

5.7. IAM を手動で作成する

クラスターをインストールするには、Cloud Credential Operator (CCO) が手動モードで動作する必要があります。インストールプログラムは CCO を手動モードに設定しますが、クラウドプロバイダーの ID とアクセス管理シークレットを指定する必要があります。

Cloud Credential Operator (CCO) ユーティリティー (**ccoctl**) を使用して、必要な IBM Cloud VPC リソースを作成できます。

前提条件

- **ccoctl** バイナリーを設定している。
- 既存の **install-config.yaml** ファイルがある。

手順

1. **install-config.yaml** 設定ファイルを編集し、**credentialsMode** パラメーターが **Manual** に設定されるようにします。

   サンプル install-config.yaml 設定ファイル

   ```
   apiVersion: v1
   baseDomain: cluster1.example.com
   credentialsMode: Manual (1)
   compute:
   - architecture: amd64
     hyperthreading: Enabled
   ```

   (1) この行は、**credentialsMode** パラメーターを **Manual** に設定するために追加されます。

2. マニフェストを生成するには、インストールプログラムが含まれるディレクトリーから以下のコマンドを実行します。

   ```
   $ ./openshift-install create manifests --dir <installation_directory>
   ```

3. インストールプログラムが含まれているディレクトリーから、**openshift-install** バイナリーが使用するようにビルドされている OpenShift Container Platform リリースイメージを取得します。

   ```
   $ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
   ```

4. OpenShift Container Platform リリースイメージから **CredentialsRequest** オブジェクトを抽出します。

   ```
   $ oc adm release extract \
     --from=$RELEASE_IMAGE \
     --credentials-requests \
     --cloud=<provider_name> \(1)
     --to=<path_to_credential_requests_directory> (2)
   ```

   (1) プロバイダーの名前。例: **ibmcloud** または **powervs**

   (2) 認証情報の要求が保存されるディレクトリー。

   このコマンドにより、それぞれの **CredentialsRequest** オブジェクトに YAML ファイルが作成されます。

サンプル CredentialsRequest オブジェクト

```
apiVersion: cloudcredential.openshift.io/v1
kind: CredentialsRequest
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: openshift-image-registry-ibmcos
  namespace: openshift-cloud-credential-operator
spec:
  secretRef:
    name: installer-cloud-credentials
    namespace: openshift-image-registry
  providerSpec:
    apiVersion: cloudcredential.openshift.io/v1
    kind: IBMCloudProviderSpec
    policies:
    - attributes:
      - name: serviceName
        value: cloud-object-storage
      roles:
      - crn:v1:bluemix:public:iam::::role:Viewer
      - crn:v1:bluemix:public:iam::::role:Operator
      - crn:v1:bluemix:public:iam::::role:Editor
      - crn:v1:bluemix:public:iam::::serviceRole:Reader
      - crn:v1:bluemix:public:iam::::serviceRole:Writer
    - attributes:
      - name: resourceType
        value: resource-group
      roles:
      - crn:v1:bluemix:public:iam::::role:Viewer
```

5. クラスターでクラスター機能を使用して 1 つ以上のオプションコンポーネントを無効にする場合は、無効なコンポーネントの **CredentialsRequest** カスタムリソースを削除します。

IBM Cloud VPC 上の OpenShift Container Platform 4.13 の credrequests ディレクトリーの内容の例

```
0000_26_cloud-controller-manager-operator_15_credentialsrequest-ibm.yaml 1
0000_30_machine-api-operator_00_credentials-request.yaml 2
0000_50_cluster-image-registry-operator_01-registry-credentials-request-ibmcos.yaml 3
0000_50_cluster-ingress-operator_00-ingress-credentials-request.yaml 4
0000_50_cluster-storage-operator_03_credentials_request_ibm.yaml 5
```

1. Cloud Controller Manager Operator CR が必要です。
2. Machine API Operator CR が必要です。
3. Image Registry Operator CR が必要です。
4. Ingress Operator CR が必要です。
5. Storage Operator CR はオプションのコンポーネントであり、クラスターで無効になっている場合があります。

6. 各認証情報リクエストのサービス ID を作成し、定義されたポリシーを割り当て、API キーを作成し、シークレットを生成します。

```
$ ccoctl ibmcloud create-service-id \
  --credentials-requests-dir <path_to_credential_requests_directory> \ 1
  --name <cluster_name> \ 2
  --output-dir <installation_directory> \
  --resource-group-name <resource_group_name> 3
```

1 認証情報の要求が保存されるディレクトリー。

2 OpenShift Container Platform クラスターの名前。

3 オプション: アクセスポリシーのスコープに使用されるリソースグループの名前。

注記

クラスターで **TechPreviewNoUpgrade** 機能セットによって有効化されたテクノロジープレビュー機能を使用している場合は、**--enable-tech-preview** パラメーターを含める必要があります。

間違ったリソースグループ名が指定された場合、ブートストラップフェーズ中にインストールが失敗します。正しいリソースグループ名を見つけるには、次のコマンドを実行します。

```
$ grep resourceGroupName <installation_directory>/manifests/cluster-infrastructure-02-config.yml
```

検証

- クラスターの **manifests** ディレクトリーに適切なシークレットが生成されていることを確認してください。

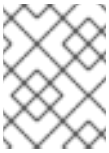
5.8. ネットワーク設定フェーズ

OpenShift Container Platform をインストールする前に、ネットワーク設定をカスタマイズできる 2 つのフェーズがあります。

フェーズ 1

マニフェストファイルを作成する前に、**install-config.yaml** ファイルで以下のネットワーク関連のフィールドをカスタマイズできます。

- **networking.networkType**
- **networking.clusterNetwork**
- **networking.serviceNetwork**
- **networking.machineNetwork**
  詳細は、「インストール設定パラメーター」を参照してください。



注記

優先されるサブネットが配置されている Classless Inter-Domain Routing (CIDR) と一致するように **networking.machineNetwork** を設定します。

重要

CIDR 範囲 **172.17.0.0/16** は **libVirt** によって予約されています。クラスター内のネットワークに **172.17.0.0/16** CIDR 範囲と重複する他の CIDR 範囲を使用することはできません。

フェーズ 2

openshift-install create manifests を実行してマニフェストファイルを作成した後に、変更するフィールドのみでカスタマイズされた Cluster Network Operator マニフェストを定義できます。マニフェストを使用して、高度なネットワーク設定を指定できます。

フェーズ 2 では、**install-config.yaml** ファイルのフェーズ 1 で指定した値をオーバーライドすることはできません。ただし、フェーズ 2 でネットワークプラグインをカスタマイズできます。

5.9. 高度なネットワーク設定の指定

ネットワークプラグインに高度なネットワーク設定を使用し、クラスターを既存のネットワーク環境に統合することができます。高度なネットワーク設定は、クラスターのインストール前にのみ指定することができます。

重要

インストールプロブラムで作成される OpenShift Container Platform マニフェストファイルを変更してネットワーク設定をカスタマイズすることは、サポートされていません。以下の手順のように、作成するマニフェストファイルを適用することがサポートされています。

前提条件

- **install-config.yaml** ファイルを作成し、これに対する変更を完了している。

手順

1. インストールプログラムが含まれるディレクトリーに切り替え、マニフェストを作成します。

```
$ ./openshift-install create manifests --dir <installation_directory> 1
```

1 **<installation_directory>** は、クラスターの **install-config.yaml** ファイルが含まれるディレクトリーの名前を指定します。

2. **cluster-network-03-config.yml** という名前の、高度なネットワーク設定用のスタブマニフェストファイルを **<installation_directory>/manifests/** ディレクトリーに作成します。

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
```

```
spec:
```

3. 次の例のように、**cluster-network-03-config.yml** ファイルでクラスターの高度なネットワーク設定を指定します。

   OpenShift SDN ネットワークプロバイダーに異なる VXLAN ポートを指定します。

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  defaultNetwork:
    openshiftSDNConfig:
      vxlanPort: 4800
```

4. オプション: **manifests/cluster-network-03-config.yml** ファイルをバックアップします。インストールプログラムは、Ignition 設定ファイルの作成時に **manifests/** ディレクトリーを使用します。

5.10. CLUSTER NETWORK OPERATOR (CNO) の設定

クラスターネットワークの設定は、Cluster Network Operator (CNO) 設定の一部として指定され、**cluster** という名前のカスタムリソース (CR) オブジェクトに保存されます。CR は **operator.openshift.io** API グループの **Network** API のフィールドを指定します。

CNO 設定は、**Network.config.openshift.io** API グループの **Network** API からクラスターのインストール時に以下のフィールドを継承し、これらのフィールドは変更できません。

clusterNetwork

Pod IP アドレスの割り当てに使用する IP アドレスプール。

serviceNetwork

サービスの IP アドレスプール。

defaultNetwork.type

OpenShift SDN や OVN-Kubernetes などのクラスターネットワークプラグイン。

defaultNetwork オブジェクトのフィールドを **cluster** という名前の CNO オブジェクトに設定することにより、クラスターのクラスターネットワークプラグイン設定を指定できます。

5.10.1. Cluster Network Operator 設定オブジェクト

Cluster Network Operator (CNO) のフィールドは以下の表で説明されています。

表5.6 Cluster Network Operator 設定オブジェクト

フィールド	型	説明
metadata.name	**string**	CNO オブジェクトの名前。この名前は常に **cluster** です。

フィールド	型	説明
spec.clusterNetwork	**array**	Pod IP アドレスの割り当て、サブネット接頭辞の長さのクラスター内の個別ノードへの割り当てに使用される IP アドレスのブロックを指定するリストです。以下に例を示します。 spec: clusterNetwork: - cidr: 10.128.0.0/19 hostPrefix: 23 - cidr: 10.128.32.0/19 hostPrefix: 23 マニフェストを作成する前に、このフィールドを **install-config.yaml** ファイルでのみカスタマイズすることができます。この値は、マニフェストファイルでは読み取り専用です。
spec.serviceNetwork	**array**	サービスの IP アドレスのブロック。OpenShift SDN および OVN-Kubernetes ネットワークプラグインは、サービスネットワークの単一 IP アドレスブロックのみをサポートします。以下に例を示します。 spec: serviceNetwork: - 172.30.0.0/14 マニフェストを作成する前に、このフィールドを **install-config.yaml** ファイルでのみカスタマイズすることができます。この値は、マニフェストファイルでは読み取り専用です。
spec.defaultNetwork	**object**	クラスターネットワークのネットワークプラグインを設定します。
spec.kubeProxyConfig	**object**	このオブジェクトのフィールドは、kube-proxy 設定を指定します。OVN-Kubernetes クラスターネットワークプラグインを使用している場合、kube-proxy 設定は機能しません。

重要

複数のネットワークにオブジェクトをデプロイする必要があるクラスターの場合は、**install-config.yaml** ファイルで定義されている各ネットワークタイプの **clusterNetwork.hostPrefix** パラメーターに、必ず同じ値を指定してください。**clusterNetwork.hostPrefix** パラメーターにそれぞれ異なる値を設定すると、OVN-Kubernetes ネットワークプラグインに影響が及び、異なるノード間のオブジェクトトラフィックをプラグインが効果的にルーティングできなくなる可能性があります。

defaultNetwork オブジェクト設定
defaultNetwork オブジェクトの値は、以下の表で定義されます。

表5.7 defaultNetwork オブジェクト

フィールド	型	説明
type	**string**	**OpenShiftSDN** または **OVNKubernetes** のいずれか。Red Hat OpenShift Networking ネットワークプラグインは、インストール中に選択されます。この値は、クラスターのインストール後は変更できません。  **注記** OpenShift Container Platform は、デフォルトで OVN-Kubernetes ネットワークプラグインを使用します。
openshiftSDNConfig	**object**	このオブジェクトは、OpenShift SDN ネットワークプラグインに対してのみ有効です。
ovnKubernetesConfig	**object**	このオブジェクトは、OVN-Kubernetes ネットワークプラグインに対してのみ有効です。

OpenShift SDN ネットワークプラグインの設定
以下の表では、OpenShift SDN ネットワークプラグインの設定フィールドを説明します。

表5.8 openshiftSDNConfig オブジェクト

フィールド	型	説明
mode	**string**	OpenShift SDN のネットワーク分離モードを設定します。デフォルト値は **NetworkPolicy** です。 **Multitenant** および **Subnet** の値は、OpenShift Container Platform 3.x との後方互換性を維持するために利用できますが、その使用は推奨されていません。この値は、クラスターのインストール後は変更できません。

フィールド	型	説明
mtu	**integer**	VXLAN オーバーレイネットワークの最大転送単位 (MTU)。これは、プライマリーネットワークインターフェイスの MTU に基づいて自動的に検出されます。通常、検出された MTU を上書きする必要はありません。 自動検出した値が予想される値ではない場合は、ノード上のプライマリーネットワークインターフェイスの MTU が正しいことを確認します。このオプションを使用して、ノード上のプライマリーネットワークインターフェイスの MTU 値を変更することはできません。 クラスターで異なるノードに異なる MTU 値が必要な場合、この値をクラスター内の最小の MTU 値よりも **50** 小さく設定する必要があります。たとえば、クラスター内の一部のノードでは MTU が **9001** であり、MTU が **1500** のクラスターもある場合には、この値を **1450** に設定する必要があります。 クラスターインストール時またはインストール後のタスクとして値を設定できます。詳細は、OpenShift Container Platform Networking ドキュメントの "Changing the MTU for the cluster network" を参照してください。
vxlanPort	**integer**	すべての VXLAN パケットに使用するポート。デフォルト値は **4789** です。この値は、クラスターのインストール後は変更できません。 別の VXLAN ネットワークの一部である既存ノードと共に仮想化環境で実行している場合は、これを変更する必要がある可能性があります。たとえば、OpenShift SDN オーバーレイを VMware NSX-T 上で実行する場合は、両方の SDN が同じデフォルトの VXLAN ポート番号を使用するため、VXLAN の別のポートを選択する必要があります。 Amazon Web Services (AWS) では、VXLAN にポート **9000** とポート **9999** 間の代替ポートを選択できます。

OVN-Kubernetes ネットワークプラグインの設定
次の表では、OVN-Kubernetes ネットワークプラグインの設定フィールドを説明します。

表5.9 ovnKubernetesConfig オブジェクト

フィールド	型	説明

フィールド	型	説明
mtu	**integer**	Geneve (Generic Network Virtualization Encapsulation) オーバーレイネットワークの MTU (maximum transmission unit)。これは、プライマリーネットワークインターフェイスの MTU に基づいて自動的に検出されます。通常、検出された MTU を上書きする必要はありません。 自動検出した値が予想される値ではない場合は、ノード上のプライマリーネットワークインターフェイスの MTU が正しいことを確認します。このオプションを使用して、ノード上のプライマリーネットワークインターフェイスの MTU 値を変更することはできません。 クラスターで異なるノードに異なる MTU 値が必要な場合、この値をクラスター内の最小の MTU 値よりも **100** 小さく設定する必要があります。たとえば、クラスター内の一部のノードでは MTU が **9001** であり、MTU が **1500** のクラスターもある場合には、この値を **1400** に設定する必要があります。
genevePort	**integer**	すべての Geneve パケットに使用するポート。デフォルト値は **6081** です。この値は、クラスターのインストール後は変更できません。
ipsecConfig	**object**	IPsec 暗号化を有効にするために空のオブジェクトを指定します。
policyAuditConfig	**object**	ネットワークポリシー監査ロギングをカスタマイズする設定オブジェクトを指定します。指定されていない場合は、デフォルトの監査ログ設定が使用されます。
gatewayConfig	**object**	オプション: Egress トラフィックのノードゲートウェイへの送信方法をカスタマイズするための設定オブジェクトを指定します。  **注記** Egress トラフィックの移行中は、Cluster Network Operator (CNO) が変更を正常にロールアウトするまで、ワークロードとサービストラフィックに多少の中断が発生することが予想されます。

フィールド	型	説明
v4InternalSubnet	既存のネットワーククインフラストラクチャーが **100.64.0.0/16** IPv4 サブネットと重複している場合は、OVN-Kubernetes による内部使用のために別の IP アドレス範囲を指定できます。IP アドレス範囲が、OpenShift Container Platform インストールで使用される他のサブネットと重複しないようにする必要があります。IP アドレス範囲は、クラスターに追加できるノードの最大数より大きくする必要があります。たとえば、**clusterNetwork.cidr** 値が **10.128.0.0/14** で、**clusterNetwork.hostPrefix** 値が **/23** の場合、ノードの最大数は **2^(23-14)=512** です。 このフィールドは、インストール後に変更できません。	デフォルト値は **100.64.0.0/16** です。

フィールド	型	説明
v6InternalSubnet	既存のネットワークインフラストラクチャーが **fd98::/48** IPv6 サブネットと重複する場合は、OVN-Kubernetes による内部使用のために別の IP アドレス範囲を指定できます。IP アドレス範囲が、OpenShift Container Platform インストールで使用される他のサブネットと重複しないようにする必要があります。IP アドレス範囲は、クラスターに追加できるノードの最大数より大きくする必要があります。 このフィールドは、インストール後に変更できません。	デフォルト値は **fd98::/48** です。

表5.10 **policyAuditConfig** object

フィールド	型	説明
rateLimit	integer	ノードごとに毎秒生成されるメッセージの最大数。デフォルト値は、1秒あたり **20** メッセージです。
maxFileSize	integer	監査ログの最大サイズ (バイト単位)。デフォルト値は **50000000** (50MB) です。
maxLogFiles	integer	保持されるログファイルの最大数。

フィールド	型	説明
比較先	string	以下の追加の監査ログターゲットのいずれかになります。 **libc** ホスト上の journald プロセスの libc **syslog()** 関数。 **udp:<host>:<port>** syslog サーバー。**<host>:<port>** を syslog サーバーのホストおよびポートに置き換えます。 **unix:<file>** **<file>** で指定された Unix ドメインソケットファイル。 **null** 監査ログを追加のターゲットに送信しないでください。
syslogFacility	string	RFC5424 で定義される **kern** などの syslog ファシリティー。デフォルト値は **local0** です。

表5.11 gatewayConfig オブジェクト

フィールド	型	説明
routingViaHost	**boolean**	Pod からホストネットワークスタックへの Egress トラフィックを送信するには、このフィールドを **true** に設定します。インストールおよびアプリケーションがカーネルルーティングテーブルに手動設定されたルートに依存するなど非常に特化されている場合には、Egress トラフィックをホストネットワークスタックにルーティングすることを推奨します。デフォルトでは、Egress トラフィックは OVN で処理され、クラスターを終了するために処理され、トラフィックはカーネルルーティングテーブルの特殊なルートによる影響を受けません。デフォルト値は **false** です。 このフィールドで、Open vSwitch ハードウェアオフロード機能との対話が可能になりました。このフィールドを **true** に設定すると、egress トラフィックがホストネットワークスタックで処理されるため、パフォーマンス的に、オフロードによる利点は得られません。

IPsec が有効な OVN-Kubernetes 設定の例

```
defaultNetwork:
  type: OVNKubernetes
  ovnKubernetesConfig:
    mtu: 1400
    genevePort: 6081
    ipsecConfig: {}
```

kubeProxyConfig オブジェクト設定
kubeProxyConfig オブジェクトの値は以下の表で定義されます。

表5.12 kubeProxyConfig オブジェクト

フィールド	型	説明
iptablesSyncPeriod	**string**	**iptables** ルールの更新期間。デフォルト値は **30s** です。有効な接尾辞には、**s**、**m**、および **h** などが含まれ、これらについては、Go **time** パッケージ ドキュメントで説明されています。 **注記** OpenShift Container Platform 4.3 以降で強化されたパフォーマンスの向上により、**iptablesSyncPeriod** パラメーターを調整する必要はなくなりました。
proxyArguments.iptables-min-sync-period	**array**	**iptables** ルールを更新する前の最小期間。このフィールドにより、更新の頻度が高くなり過ぎないようにできます。有効な接尾辞には、**s**、**m**、および **h** などが含まれ、これらについては、Go **time** パッケージ で説明されています。デフォルト値: kubeProxyConfig: proxyArguments: iptables-min-sync-period: - 0s

5.11. クラスターのデプロイ

互換性のあるクラウドプラットフォームに OpenShift Container Platform をインストールできます。

重要

インストールプログラムの **create cluster** コマンドは、初期インストール時に 1 回だけ実行できます。

前提条件

- クラスターをホストするクラウドプラットフォームでアカウントを設定します。
- OpenShift Container Platform インストールプログラム、およびクラスターのプルシークレットを取得する。
- ホスト上のクラウドプロバイダーアカウントに、クラスターをデプロイするための適切な権限があることを確認してください。アカウントの権限が正しくないと、インストールプロセスが失敗し、不足している権限を示すエラーメッセージが表示されます。

手順

- インストールプログラムが含まれるディレクトリーに切り替え、クラスターのデプロイメントを初期化します。

```
$ ./openshift-install create cluster --dir <installation_directory> \ 1
    --log-level=info 2
```

1. **<installation_directory>** に、カスタマイズした **./install-config.yaml** ファイルの場所を指定します。
2. 異なるインストールの詳細情報を表示するには、**info** ではなく、**warn**、**debug**、または **error** を指定します。

検証

クラスターのデプロイが正常に完了すると、次のようになります。

- ターミナルには、Web コンソールへのリンクや **kubeadmin** ユーザーの認証情報など、クラスターにアクセスするための指示が表示されます。
- 認証情報は **<installation_directory>/.openshift_install.log** にも出力されます。

重要

インストールプログラム、またはインストールプログラムが作成するファイルを削除することはできません。これらはいずれもクラスターを削除するために必要になります。

出力例

```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- インストールプログラムが生成する Ignition 設定ファイルには、24 時間が経過すると期限切れになり、その後に更新される証明書が含まれます。証明書を更新する前にクラスターが停止し、24 時間経過した後にクラスターを再起動すると、クラスターは期限切れの証明書を自動的に復元します。例外として、kubelet 証明書を回復するために保留状態の **node-bootstrapper** 証明書署名要求 (CSR) を手動で承認する必要があります。詳細は、**コントロールプレーン証明書の期限切れの状態からのリカバリー** に関するドキュメントを参照してください。
- 24 時間証明書はクラスターのインストール後 16 時間から 22 時間にローテーションするため、Ignition 設定ファイルは、生成後 12 時間以内に使用することを推奨します。12 時間以内に Ignition 設定ファイルを使用することにより、インストール中に証明書の更新が実行された場合のインストールの失敗を回避できます。

5.12. バイナリーのダウンロードによる OPENSHIFT CLI のインストール

コマンドラインインターフェイスを使用して OpenShift Container Platform と対話するために CLI (**oc**) をインストールすることができます。**oc** は Linux、Windows、または macOS にインストールできます。

重要

以前のバージョンの **oc** をインストールしている場合、これを使用して OpenShift Container Platform 4.13 のすべてのコマンドを実行することはできません。新規バージョンの **oc** をダウンロードし、インストールします。

Linux への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Linux にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **Product Variant** ドロップダウンリストからアーキテクチャーを選択します。
3. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
4. **OpenShift v4.13 Linux Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
5. アーカイブを展開します。

```
$ tar xvf <file>
```

6. **oc** バイナリーを、**PATH** にあるディレクトリーに配置します。
PATH を確認するには、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

Windows への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Windows にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 Windows Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。

4. ZIP プログラムでアーカイブを解凍します。
5. **oc** バイナリーを、**PATH** にあるディレクトリーに移動します。
   PATH を確認するには、コマンドプロンプトを開いて以下のコマンドを実行します。

```
C:\> path
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
C:\> oc <command>
```

macOS への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを macOS にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 macOS Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。

注記

macOS arm64 の場合は、**OpenShift v4.13 macOS arm64 Client** エントリーを選択します。

4. アーカイブを展開し、解凍します。
5. **oc** バイナリーをパスにあるディレクトリーに移動します。
   PATH を確認するには、ターミナルを開き、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

5.13. CLI の使用によるクラスターへのログイン

クラスター **kubeconfig** ファイルをエクスポートし、デフォルトシステムユーザーとしてクラスターにログインできます。**kubeconfig** ファイルには、クライアントを正しいクラスターおよび API サーバーに接続するために CLI で使用されるクラスターに関する情報が含まれます。このファイルはクラスターに固有のファイルであり、OpenShift Container Platform のインストール時に作成されます。

前提条件

前提条件

- OpenShift Container Platform クラスターをデプロイしていること。
- **oc** CLI がインストールされている。

手順

1. **kubeadmin** 認証情報をエクスポートします。

```
$ export KUBECONFIG=<installation_directory>/auth/kubeconfig 1
```

1 **<installation_directory>** には、インストールファイルを保存したディレクトリーへのパスを指定します。

2. エクスポートされた設定を使用して、**oc** コマンドを正常に実行できることを確認します。

```
$ oc whoami
```

出力例

```
system:admin
```

関連情報

- Web コンソールへのアクセス

5.14. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス

OpenShift Container Platform 4.13 では、クラスターの健全性および正常に実行された更新についてのメトリクスを提供するためにデフォルトで実行される Telemetry サービスにもインターネットアクセスが必要です。クラスターがインターネットに接続されている場合、Telemetry は自動的に実行され、クラスターは OpenShift Cluster Manager Hybrid Cloud Console に登録されます。

OpenShift Cluster Manager インベントリーが正常である (Telemetry によって自動的に維持、または OpenShift Cluster Manager Hybrid Cloud Console を使用して手動で維持) ことを確認した後に、subscription watch を使用 して、アカウントまたはマルチクラスターレベルで OpenShift Container Platform サブスクリプションを追跡します。

関連情報

- リモートヘルスモニタリングについて

5.15. 次のステップ

- クラスターをカスタマイズします。
- 必要に応じて、リモートヘルスレポート にすることができます。

第6章 クラスターの IBM CLOUD VPC の既存 VPC へのインストール

OpenShift Container Platform バージョン 4.13 では、クラスターを IBM Cloud VPC の既存の Virtual Private Cloud (VPC) にインストールできます。インストールプログラムは、カスタマイズ可能な残りの必要なインフラストラクチャーをプロビジョニングします。インストールをカスタマイズするには、クラスターをインストールする前に、**install-config.yaml** ファイルでパラメーターを変更します。

6.1. 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ている。
- クラスターインストール方法の選択およびそのユーザー向けの準備 を確認している。
- クラスターをホストするように IBM Cloud アカウントを設定 している。
- ファイアウォールを使用する場合は、クラスターがアクセスを必要とするサイトを許可するようにファイアウォールを設定する必要がある。
- クラスターをインストールする前に、**ccoctl** ユーティリティーを設定している。詳細は、IBM Cloud VPC 用の IAM の設定 を参照してください。

6.2. カスタム VPC の使用について

OpenShift Container Platform 4.13 では、クラスターを既存の IBM Virtual Private Cloud (VPC) のサブネットにデプロイできます。OpenShift Container Platform を既存の VPC にデプロイすると、新規アカウントの制限を回避したり、会社のガイドラインによる運用上の制約をより容易に遵守することが可能になる場合があります。VPC を作成するために必要なインフラストラクチャーの作成パーミッションを取得できない場合は、このインストールオプションを使用します。

インストールプログラムは既存のサブネットにある他のコンポーネントを認識できないため、サブネットの CIDR などを選択できません。クラスターをインストールするサブネットのネットワークを設定する必要があります。

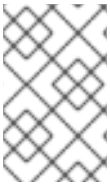
6.2.1. VPC を使用するための要件

クラスターをインストールする前に、既存の VPC およびそのサブネットを適切に設定する必要があります。インストールプログラムでは、次のコンポーネントは作成されません。

- NAT ゲートウェイ
- サブネット
- ルートテーブル
- VPC ネットワーク

インストールプログラムには、以下の機能はありません。

- 使用するクラスターのネットワーク範囲を細分化します。
- サブネットのルートテーブルを設定します。
- DHCP などの VPC オプションの設定



注記

インストールプログラムでは、クラウド提供の DNS サーバーを使用する必要があります。カスタム DNS サーバーの使用はサポートされていないため、インストールが失敗します。

6.2.2. VPC 検証

VPC とすべてのサブネットは、既存のリソースグループ内にある必要があります。クラスターはこのリソースグループにデプロイされます。

インストールの一環として、**install-config.yaml** ファイルで以下を指定します。

- リソースグループの名前
- VPC の名前
- コントロールプレーンマシンおよびコンピュートマシンのサブネット

指定するサブネットが適切であることを確認するには、インストールプログラムが以下を確認します。

- 指定したサブネットがすべて存在します。
- リージョン内の各アベイラビリティーゾーンに、以下を指定します。
  - コントロールプレーンマシンの 1 つのサブネット。
  - コンピュートマシン用に 1 つのサブネット。
- 指定したマシン CIDR にはコンピュートマシンおよびコントロールプレーンマシンのサブネットが含まれます。

注記

サブネット ID はサポートされていません。

6.2.3. クラスター間の分離

OpenShift Container Platform を既存のネットワークにデプロイする場合、クラスターサービスの分離の規模は以下の方法で縮小されます。

- 複数の OpenShift Container Platform クラスターを同じ VPC にインストールできます。
- ICMP Ingress はネットワーク全体で許可されます。
- TCP ポート 22 Ingress (SSH) はネットワーク全体に対して許可されます。
- コントロールプレーンの TCP 6443 Ingress (Kubernetes API) はネットワーク全体に対して許可されます。
- コントロールプレーンの TCP 22623 Ingress (MCS) はネットワーク全体に対して許可されます。

6.3. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス

OpenShift Container Platform 4.13 では、クラスターをインストールするためにインターネットアクセスが必要になります。

インターネットへのアクセスは以下を実行するために必要です。

- OpenShift Cluster Manager Hybrid Cloud Console にアクセスし、インストールプログラムをダウンロードし、サブスクリプション管理を実行します。クラスターにインターネットアクセスがあり、Telemetry を無効にしない場合、そのサービスは有効なサブスクリプションでクラスターを自動的に使用します。
- クラスターのインストールに必要なパッケージを取得するために Quay.io にアクセスします。
- クラスターの更新を実行するために必要なパッケージを取得します。

重要

クラスターでインターネットに直接アクセスできない場合、プロビジョニングする一部のタイプのインフラストラクチャーでネットワークが制限されたインストールを実行できます。このプロセスで、必要なコンテンツをダウンロードし、これを使用してミラーレジストリーにインストールパッケージを設定します。インストールタイプに応じて、クラスターのインストール環境でインターネットアクセスが不要となる場合があります。クラスターを更新する前に、ミラーレジストリーのコンテンツを更新します。

6.4. クラスターノードの SSH アクセス用のキーペアの生成

OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定できます。キーは、Ignition 設定ファイルを介して Red Hat Enterprise Linux CoreOS (RHCOS) ノードに渡され、ノードへの SSH アクセスを認証するために使用されます。このキーは各ノードの **core** ユーザーの **~/.ssh/authorized_keys** リストに追加され、パスワードなしの認証が可能になります。

キーがノードに渡されると、キーペアを使用して RHCOS ノードにユーザー **core** として SSH を実行できます。SSH 経由でノードにアクセスするには、秘密鍵のアイデンティティーをローカルユーザーの SSH で管理する必要があります。

インストールのデバッグまたは障害復旧を実行するためにクラスターノードに対して SSH を実行する場合は、インストールプロセスの間に SSH 公開鍵を指定する必要があります。**./openshift-install gather** コマンドでは、SSH 公開鍵がクラスターノードに配置されている必要もあります。

重要

障害復旧およびデバッグが必要な実稼働環境では、この手順を省略しないでください。

注記

AWS キーペア などのプラットフォームに固有の方法で設定したキーではなく、ローカルキーを使用する必要があります。

手順

1. クラスターノードへの認証に使用するローカルマシンに既存の SSH キーペアがない場合は、これを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ ssh-keygen -t ed25519 -N '' -f <path>/<file_name> 1
```

1 新しい SSH キーのパスとファイル名 (~/**.ssh/id_ed25519** など) を指定します。既存のキーペアがある場合は、公開鍵が ~/**.ssh** ディレクトリーにあることを確認します。

2. 公開 SSH キーを表示します。

```
$ cat <path>/<file_name>.pub
```

たとえば、次のコマンドを実行して ~/**.ssh/id_ed25519.pub** 公開鍵を表示します。

```
$ cat ~/.ssh/id_ed25519.pub
```

3. ローカルユーザーの SSH エージェントに SSH 秘密鍵 ID が追加されていない場合は、それを追加します。キーの SSH エージェント管理は、クラスターノードへのパスワードなしの SSH 認証、または **./openshift-install gather** コマンドを使用する場合は必要になります。

注記

一部のディストリビューションでは、~/**.ssh/id_rsa** および ~/**.ssh/id_dsa** などのデフォルトの SSH 秘密鍵のアイデンティティーは自動的に管理されます。

a. **ssh-agent** プロセスがローカルユーザーに対して実行されていない場合は、バックグラウンドタスクとして開始します。

```
$ eval "$(ssh-agent -s)"
```

出力例

```
Agent pid 31874
```

4. SSH プライベートキーを **ssh-agent** に追加します。

```
$ ssh-add <path>/<file_name> 1
```

1 ~/**.ssh/id_ed25519** などの、SSH プライベートキーのパスおよびファイル名を指定します。

出力例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

次のステップ

- OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定します。

6.5. インストールプログラムの取得

OpenShift Container Platform をインストールする前に、インストールに使用しているホストにインストールファイルをダウンロードします。

前提条件

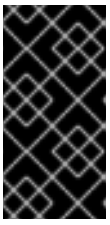
- 500 MB のローカルディスク領域がある Linux または macOS を実行するコンピューターが必要です。

手順

1. OpenShift Cluster Manager サイトの インフラストラクチャープロバイダー ページにアクセスします。Red Hat アカウントがある場合は、認証情報を使用してログインします。アカウントがない場合はこれを作成します。
2. インフラストラクチャープロバイダーを選択します。
3. インストールタイプのページに移動し、ホストオペレーティングシステムとアーキテクチャーに対応するインストールプログラムをダウンロードして、インストール設定ファイルを保存するディレクトリーにファイルを配置します。

重要

インストールプログラムは、クラスターのインストールに使用するコンピューターにいくつかのファイルを作成します。クラスターのインストール完了後は、インストールプログラムおよびインストールプログラムが作成するファイルを保持する必要があります。ファイルはいずれもクラスターを削除するために必要になります。



重要

インストールプログラムで作成されたファイルを削除しても、クラスターがインストール時に失敗した場合でもクラスターは削除されません。クラスターを削除するには、特定のクラウドプロバイダー用の OpenShift Container Platform のアンインストール手順を実行します。

4. インストールプログラムを展開します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar -xvf openshift-install-linux.tar.gz
```

5. Red Hat OpenShift Cluster Manager からインストールプルシークレット をダウンロードします。このプルシークレットを使用し、OpenShift Container Platform コンポーネントのコンテナーイメージを提供する Quay.io など、組み込まれた各種の認証局によって提供されるサービスで認証できます。

6.6. API キーのエクスポート

作成した API キーをグローバル変数として設定する必要があります。インストールプログラムは、起動時に変数を取り込み、API キーを設定します。

前提条件

- IBM Cloud アカウント用にユーザー API キーまたはサービス ID API キーのいずれかを作成している。

手順

- アカウントの API キーをグローバル変数としてエクスポートします。

```
$ export IC_API_KEY=<api_key>
```

重要

変数名は指定どおりに正確に設定する必要があります。インストールプログラムは、起動時に変数名が存在することを想定しています。

6.7. インストール設定ファイルの作成

IBM Cloud にインストールする OpenShift Container Platform クラスターをカスタマイズできます。

前提条件

- OpenShift Container Platform インストールプログラム、およびクラスターのプルシークレットを取得する。
- サブスクリプションレベルでサービスプリンシパルのパーミッションを取得する。

手順

1. **install-config.yaml** ファイルを作成します。
   a. インストールプログラムが含まれるディレクトリーに切り替え、以下のコマンドを実行します。

```
$ ./openshift-install create install-config --dir <installation_directory> 1
```

1 **<installation_directory>** の場合、インストールプログラムが作成するファイルを保存するためにディレクトリー名を指定します。

ディレクトリーを指定する場合:

- ディレクトリーに **execute** 権限があることを確認します。この権限は、インストールディレクトリーで Terraform バイナリーを実行するために必要です。
- 空のディレクトリーを使用します。ブートストラップ X.509 証明書などの一部のインストールアセットは有効期限が短いため、インストールディレクトリーを再利用しないでください。別のクラスターインストールの個別のファイルを再利用する必要がある場合は、それらをディレクトリーにコピーすることができます。ただし、インストールアセットのファイル名はリリース間で変更される可能性があります。インストールファイルを以前のバージョンの OpenShift Container Platform からコピーする場合は注意してください。

注記

古い設定の再利用を回避するために、~/**.powervs** ディレクトリーは必ず削除してください。以下のコマンドを実行します。

```
$ rm -rf ~/.powervs
```

b. プロンプト時に、クラウドの設定の詳細情報を指定します。

i. オプション: クラスターマシンにアクセスするために使用する SSH キーを選択します。

注記

インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。

ii. ターゲットとするプラットフォームとして **ibmcloud** を選択します。

iii. クラスターをデプロイするリージョンを選択します。

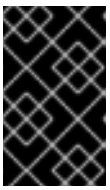
iv. クラスターをデプロイするベースドメインを選択します。ベースドメインは、クラスターに作成したパブリック DNS ゾーンに対応します。

v. クラスターの記述名を入力します。

vi. Red Hat OpenShift Cluster Manager からプルシークレット を貼り付けます。

2. **install-config.yaml** ファイルを変更します。利用可能なパラメーターの詳細は、「インストール設定パラメーター」のセクションを参照してください。

3. **install-config.yaml** ファイルをバックアップし、複数のクラスターをインストールするのに使用できるようにします。



重要

install-config.yaml ファイルはインストールプロセス時に使用されます。このファイルを再利用する必要がある場合は、この段階でこれをバックアップしてください。

6.7.1. インストール設定パラメーター

OpenShift Container Platform クラスターをデプロイする前に、クラスターをホストするクラウドプラットフォームでアカウントを記述し、クラスターのプラットフォームをオプションでカスタマイズするためにパラメーターの値を指定します。**install-config.yaml** インストール設定ファイルを作成する際に、コマンドラインで必要なパラメーターの値を指定します。クラスターをカスタマイズする場合、**install-config.yaml** ファイルを変更して、プラットフォームについての詳細情報を指定できます。

重要

インストール後は、これらのパラメーターを **install-config.yaml** ファイルで変更することはできません。

6.7.1.1. 必須設定パラメーター

必須のインストール設定パラメーターは、以下の表で説明されています。

表6.1 必須パラメーター

パラメーター	説明	値
apiVersion	**install-config.yaml** コンテンツの API バージョン。現在のバージョンは **v1** です。インストールプログラムは、古い API バージョンもサポートしている場合があります。	文字列
baseDomain	クラウドプロバイダーのベースドメイン。ベースドメインは、OpenShift Container Platform クラスターコンポーネントへのルートを作成するために使用されます。クラスターの完全な DNS 名は、**<metadata.name>.<baseDomain>** 形式を使用する **baseDomain** と **metadata.name** パラメーターの値を組み合わせたものです。	**example.com** などの完全修飾ドメインまたはサブドメイン名。
metadata	Kubernetes リソース **ObjectMeta**。ここからは **name** パラメーターのみが消費されます。	オブジェクト
metadata.name	クラスターの名前。クラスターの DNS レコードはすべて **{{.metadata.name}}.{{.baseDomain}}** のサブドメインです。	**dev** などの小文字、ハイフン (**-**)、およびピリオド (**.**) が含まれる文字列。
platform	インストールを実行する特定のプラットフォームの設定: **alibabacloud**、**aws**、**baremetal**、**azure**、**gcp**、**ibmcloud**、**Nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**。**platform.<platform>** パラメーターに関する追加情報は、以下の表で特定のプラットフォームを参照してください。	オブジェクト

パラメーター	説明	値

pullSecret	Red Hat OpenShift Cluster Manager からプルシークレット を取得して、Quay.io などのサービスから OpenShift Container Platform コンポーネントのコンテナーイメージをダウンロードすることを認証します。	<pre>{
		  "auths":{
		  "cloud.openshift.com":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  },
		  "quay.io":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  }
		  }
		}</pre>

6.7.1.2. ネットワーク設定パラメーター

既存のネットワークインフラストラクチャーの要件に基づいて、インストール設定をカスタマイズできます。たとえば、クラスターネットワークの IP アドレスブロックを拡張するか、デフォルトとは異なる IP アドレスブロックを指定できます。

IPv4 アドレスのみがサポートされます。

注記

Globalnet は、Red Hat OpenShift Data Foundation ディザスターリカバリーソリューションではサポートされていません。局地的なディザスターリカバリーのシナリオでは、各クラスター内のクラスターとサービスネットワークに重複しない範囲のプライベート IP アドレスを使用するようにしてください。

表6.2 ネットワークパラメーター

パラメーター	説明	値
networking	クラスターのネットワークの設定。	Object  **注記** インストール後に **networking** オブジェクトで指定したパラメーターを変更することはできません。

パラメーター	説明	値
networking.networkType	インストールする Red Hat OpenShift Networking ネットワークプラグイン。	**OpenShiftSDN** または **OVNKubernetes** のいずれか。**OpenShiftSDN** は、すべての Linux ネットワークの Container Network Interface (CNI)プラグインです。**OVNKubernetes** は、Linux ネットワークと、Linux サーバーと Windows サーバーの両方を含む Linux ネットワークおよびハイブリッドネットワーク用の CNI プラグインです。デフォルトの値は **OVNkubernetes** です。
networking.clusterNetwork	Pod の IP アドレスブロック。 デフォルト値は **10.128.0.0/14** で、ホストの接頭辞は **/23** です。 複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。	オブジェクトの配列。以下に例を示します。 networking: clusterNetwork: - cidr: 10.128.0.0/14 hostPrefix: 23
networking.clusterNetwork.cidr	**networking.clusterNetwork** を使用する場合に必須です。IP アドレスブロック。 IPv4 ネットワーク	CIDR (Classless Inter-Domain Routing) 表記の IP アドレスブロック。IPv4 ブロックの接頭辞長は **0** から **32** の間になります。
networking.clusterNetwork.hostPrefix	それぞれの個別ノードに割り当てるサブネット接頭辞長。たとえば、**hostPrefix** が **23** に設定される場合、各ノードに指定の **cidr** から **/23** サブネットが割り当てられます。**hostPrefix** 値の **23** は、510 (2^(32 - 23) - 2) Pod IP アドレスを提供します。	サブネット接頭辞。 デフォルト値は **23** です。
networking.serviceNetwork	サービスの IP アドレスブロック。デフォルト値は **172.30.0.0/16** です。 OpenShift SDN および OVN-Kubernetes ネットワークプラグインは、サービスネットワークの単一 IP アドレスブロックのみをサポートします。	CIDR 形式の IP アドレスブロックを持つ配列。以下に例を示します。 networking: serviceNetwork: - 172.30.0.0/16

パラメーター	説明	値
networking.machineNetwork	マシンの IP アドレスブロック。 複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。	オブジェクトの配列。以下に例を示します。 networking: machineNetwork: - cidr: 10.0.0.0/16
networking.machineNetwork.cidr	**networking.machineNetwork** を使用する場合に必須です。IP アドレスブロック。libvirt と IBM Power Virtual Server を除くすべてのプラットフォームのデフォルト値は **10.0.0.0/16** です。libvirt の場合、デフォルト値は **192.168.126.0/24** です。IBM Power Virtual Server の場合、デフォルト値は **192.168.0.0/24** です。CIDR には、**platform.ibmcloud.controlPlaneSubnets** および **platform.ibmcloud.computeSubnets** で定義されたサブネットが含まれている必要があります。	CIDR 表記の IP ネットワークブロック。 例: **10.0.0.0/16** **注記** 優先される NIC が置かれている CIDR に一致する **networking.machineNetwork** を設定します。

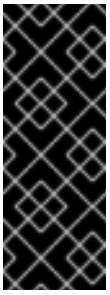
6.7.1.3. オプションの設定パラメーター

オプションのインストール設定パラメーターは、以下の表で説明されています。

表6.3 オプションのパラメーター

パラメーター	説明	値
additionalTrustBundle	ノードの信頼済み証明書ストアに追加される PEM でエンコードされた X.509 証明書バンドル。この信頼バンドルは、プロキシーが設定されている場合にも使用することができます。	String
capabilities	オプションのコアクラスターコンポーネントのインストールを制御します。オプションのコンポーネントを無効にすることで、OpenShift Container Platform クラスターのフットプリントを削減できます。詳細は、**インストール** の「クラスター機能ページ」を参照してください。	文字列配列

パラメーター	説明	値
capabilities.baselineCapabilitySet	有効にするオプション機能の初期セットを選択します。有効な値は **None**、**v4.11**、**v4.12**、**vCurrent** です。デフォルト値は **vCurrent** です。	文字列
capabilities.additionalEnabledCapabilities	オプションの機能のセットを、**baselineCapabilitySet** で指定したものを超えて拡張します。このパラメーターで複数の機能を指定できます。	String array
cpuPartitioningMode	ワークロードパーティション設定を使用して、OpenShift Container Platform サービス、クラスター管理ワークロード、およびインフラストラクチャー Pod を分離し、予約された CPU セットで実行できます。ワークロードパーティショニングは、インストール中にのみ有効にできます。インストール後に無効にすることはできません。このフィールドはワークロードのパーティショニングを有効にしますが、特定の CPU を使用するようにワークロードを設定するわけではありません。詳細は、**スケーラビリティとパフォーマンス** セクションの **ワークロードパーティショニング** ページを参照してください。	**None** または **AllNodes**。デフォルト値は **None** です。
compute	コンピュートノードを形成するマシンの設定。	**MachinePool** オブジェクトの配列。
compute.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String

パラメーター	説明	値
compute: hyperthreading:	コンピュートマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。  **重要** 同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
compute.name	**compute** を使用する場合に必須です。マシンプールの名前。	**worker**
compute.platform	**compute** を使用する場合に必須です。このパラメーターを使用して、ワーカーマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **controlPlane.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
compute.replicas	プロビジョニングするコンピュートマシン (ワーカーマシンとしても知られる) の数。	**2** 以上の正の整数。デフォルト値は **3** です。
featureSet	機能セットのクラスターを有効にします。機能セットは、デフォルトで有効にされない OpenShift Container Platform 機能のコレクションです。インストール中に機能セットを有効にする方法の詳細は、「機能ゲートの使用による各種機能の有効化」を参照してください。	文字列。**TechPreviewNoUpgrade** など、有効にする機能セットの名前。
controlPlane	コントロールプレーンを形成するマシンの設定。	**MachinePool** オブジェクトの配列。

パラメーター	説明	値
controlPlane.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String
controlPlane: hyperthreading:	コントロールプレーンマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。  **重要** 同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
controlPlane.name	**controlPlane** を使用する場合に必須です。マシンプールの名前。	**master**
controlPlane.platform	**controlPlane** を使用する場合に必須です。このパラメーターを使用して、コントロールプレーンマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **compute.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
controlPlane.replicas	プロビジョニングするコントロールプレーンマシンの数。	サポートされる値は **3** のみです (これはデフォルト値です)。

パラメーター	説明	値
credentialsMode	Cloud Credential Operator (CCO) モード。CCO は、モードが指定されていない場合に指定される認証情報の機能を動的に判別しようとします。この場合、複数のモードがサポートされるプラットフォームで mint モードが優先されます。  **注記** すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**Cluster Operators リファレンス** の **Cloud Credential Operator** を参照してください。  **注記** AWS アカウントでサービスコントロールポリシー (SCP) が有効になっている場合は、**credentialsMode** パラメーターを **Mint**、**Passthrough** または **Manual** に設定する必要があります。	**Mint**、**Passthrough**、**Manual**、または空の文字列 (**""**)。
imageContentSources	release-image コンテンツのソースおよびリポジトリー。	オブジェクトの配列。この表の以下の行で説明されているように、**source** およびオプションで **mirrors** が含まれます。
imageContentSources.source	**imageContentSources** を使用する場合に必須です。ユーザーが参照するリポジトリーを指定します (例: イメージプル仕様)。	文字列
imageContentSources.mirrors	同じイメージが含まれる可能性のあるリポジトリーを 1 つ以上指定します。	文字列の配列。

パラメーター	説明	値
publish	Kubernetes API、OpenShift ルートなどのクラスターのユーザーに表示されるエンドポイントをパブリッシュまたは公開する方法。	**Internal** または **External**。プライベートクラスターをデプロイするには、**publish** を **Internal** に設定します。これはインターネットからアクセスできません。デフォルト値は **External** です。
sshKey	クラスターマシンへのアクセスを認証するための SSH キー。 **注記** インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。	たとえば、**sshKey: ssh-ed25519 AAAA..** です。

1. すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**認証と認可** コンテンツの「クラウドプロバイダーの認証情報の管理」を参照してください。

6.7.1.4. 追加の IBM Cloud VPC 設定パラメーター

追加の IBM Cloud VPC 設定パラメーターについて、以下の表で説明します。

表6.4 追加の IBM Cloud VPC パラメーター

パラメーター	説明	値
platform.ibmcloud.resourceGroupName	既存のリソースグループの名前。デフォルトでは、installer-provisioned VPC およびクラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。クラスターを既存の VPC にデプロイする場合、installer-provisioned クラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。プロビジョニングした VPC リソースは、**networkResourceGroupName** パラメーターを使用して指定したリソースグループに存在する必要があります。いずれの場合も、クラスターコンポーネントはリソースグループ内のすべてのリソースの所有権を引き受けるため、このリソースグループは単一のクラスターインストールのみに使用する必要があります。[1]	文字列 (例: **existing_resource_group**)。

パラメーター	説明	値
platform.ibmcloud.networkResourceGroupName	既存のリソースグループの名前。このリソースには、クラスターがデプロイされる既存の VPC とサブネットが含まれます。このパラメーターは、プロビジョニングした VPC にクラスターをデプロイする際に必要です。	文字列 (例: **existing_network_resource_group**)。
platform.ibmcloud.dedicatedHosts.profile	作成する新しい専用ホスト。**platform.ibmcloud.dedicatedHosts.name** に値を指定する場合、このパラメーターは必須ではありません。	**cx2-host-152x304**などの有効な IBM Cloud VPC 専用ホストプロファイル。[2]
platform.ibmcloud.dedicatedHosts.name	既存の専用ホスト。**platform.ibmcloud.dedicatedHosts.profile** に値を指定する場合、このパラメーターは必須ではありません。	文字列、たとえば **my-dedicated-host-name**。
platform.ibmcloud.type	すべての IBM Cloud VPC マシンのインスタンスタイプ。	**bx2-8x32** などの有効な IBM Cloud VPC インスタンスタイプ。[2]
platform.ibmcloud.vpcName	クラスターをデプロイする既存 VPC の名前。	文字列。
platform.ibmcloud.controlPlaneSubnets	コントロールプレーンマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。	文字列配列

パラメーター	説明	値
platform.ibmcloud.computeSubnets	コンピュートマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。サブネット ID はサポートされていません。	文字列配列

1. 既存のリソースグループを定義するか、インストーラーが作成するかによって、クラスターがアンインストールされたときにリソースグループがどのように扱われるかが決まります。リソースグループを定義すると、インストーラーはインストーラーがプロビジョニングしたすべてのリソースを削除しますが、リソースグループはそのままにします。インストールの一部としてリソースグループが作成された場合、インストーラーは、インストーラーがプロビジョニングしたすべてのリソースとリソースグループを削除します。
2. 自身のニーズに最適なプロファイルを判別するには、IBM ドキュメントの Instance Profiles を参照してください。

6.7.2. クラスターインストールの最小リソース要件

それぞれのクラスターマシンは、以下の最小要件を満たしている必要があります。

表6.5 最小リソース要件

マシン	オペレーティングシステム	仮想 CPU	仮想 RAM	ストレージ	1秒あたりの入出力 (IOPS)
ブートストラップ	RHCOS	4	16 GB	100 GB	300
コントロールプレーン	RHCOS	4	16 GB	100 GB	300
Compute	RHCOS	2	8 GB	100 GB	300

注記

OpenShift Container Platform バージョン 4.13 の時点で、RHCOS は RHEL バージョン 9.2 に基づいており、マイクロアーキテクチャーの要件を更新します。次のリストには、各アーキテクチャーに必要な最小限の命令セットアーキテクチャー (ISA) が含まれています。

- x86-64 アーキテクチャーには x86-64-v2 ISA が必要
- ARM64 アーキテクチャーには ARMv8.0-A ISA が必要
- IBM Power アーキテクチャーには Power 9 ISA が必要
- s390x アーキテクチャーには z14 ISA が必要

詳細は、RHEL アーキテクチャー を参照してください。

プラットフォームのインスタンスタイプがクラスターマシンの最小要件を満たす場合、これは OpenShift Container Platform で使用することがサポートされます。

関連情報

- ストレージの最適化

6.7.3. IBM Cloud VPC 用にカスタマイズされた install-config.yaml ファイルのサンプル

install-config.yaml ファイルをカスタマイズして、OpenShift Container Platform クラスターのプラットフォームについての詳細を指定するか、必要なパラメーターの値を変更することができます。

重要

このサンプルの YAML ファイルは参照用にのみ提供されます。インストールプログラムを使用して **install-config.yaml** ファイルを取得し、変更する必要があります。

```
apiVersion: v1
baseDomain: example.com 1
controlPlane: 2 3
  hyperthreading: Enabled 4
  name: master
  platform:
    ibmcloud: {}
  replicas: 3
compute: 5 6
- hyperthreading: Enabled 7
  name: worker
  platform:
    ibmcloud: {}
  replicas: 3
metadata:
  name: test-cluster 8
networking:
  clusterNetwork:
```

```
  - cidr: 10.128.0.0/14 9
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes 10
  serviceNetwork:
  - 172.30.0.0/16
platform:
  ibmcloud:
    region: eu-gb 11
    resourceGroupName: eu-gb-example-network-rg 12
    networkResourceGroupName: eu-gb-example-existing-network-rg 13
    vpcName: eu-gb-example-network-1 14
    controlPlaneSubnets: 15
      - eu-gb-example-network-1-cp-eu-gb-1
      - eu-gb-example-network-1-cp-eu-gb-2
      - eu-gb-example-network-1-cp-eu-gb-3
    computeSubnets: 16
      - eu-gb-example-network-1-compute-eu-gb-1
      - eu-gb-example-network-1-compute-eu-gb-2
      - eu-gb-example-network-1-compute-eu-gb-3
credentialsMode: Manual
publish: External
pullSecret: '{"auths": ...}' 17
fips: false 18
sshKey: ssh-ed25519 AAAA... 19
```

1 8 11 17 必須。インストールプログラムはこの値の入力を求めるプロンプトを出します。

2 5 これらのパラメーターおよび値を指定しない場合、インストールプログラムはデフォルトの値を指定します。

3 6 **controlPlane** セクションは単一マッピングですが、**compute** セクションはマッピングのシーケンスになります。複数の異なるデータ構造の要件を満たすには、**compute** セクションの最初の行はハイフン **-** で始め、**controlPlane** セクションの最初の行はハイフンで始めることができません。1 つのコントロールプレーンプールのみが使用されます。

4 7 ハイパースレッディングとも呼ばれる同時マルチスレッドを有効または無効にします。デフォルトでは、同時スレッドはマシンのコアのパフォーマンスを上げるために有効にされます。パラメーター値を **Disabled** に設定するとこれを無効にすることができます。一部のクラスターマシンで同時マルチスレッドを無効にする場合は、これをすべてのクラスターマシンで無効にする必要があります。

重要

同時スレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。同時マルチスレッドを無効にする場合は、マシンに対して **n1-standard-8** などの大規模なマシンタイプを使用します。

9 マシン CIDR にはコンピュートマシンおよびコントロールプレーンマシンのサブネットが含まれている必要があります。

10 インストールするクラスターネットワークプラグイン。サポートされている値は **OVNKubernetes** と **OpenShiftSDN** です。デフォルトの値は **OVNkubernetes** です。

12 既存のリソースグループの名前。すべての installer-provisioned クラスターリソースは、このリソースグループにデプロイされます。定義されていない場合は、クラスターに新しいリソースグループが作成されます。

13 既存の Virtual Private Cloud (VPC) を含むリソースグループの名前を指定します。既存の VPC およびサブネットはこのリソースグループにある必要があります。クラスターはこの VPC にインストールされます。

14 既存 VPC の名前を指定します。

15 コントロールプレーンマシンをデプロイする既存のサブネット名を指定します。サブネットは、指定した VPC に属している必要があります。リージョン内の各アベイラビリティーゾーンのサブネットを指定します。

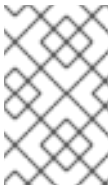
16 コンピュートマシンをデプロイする既存のサブネット名を指定します。サブネットは、指定した VPC に属している必要があります。リージョン内の各アベイラビリティーゾーンのサブネットを指定します。

18 FIPS モードを有効または無効にします。デフォルトでは、FIPS モードは有効にされません。

重要

OpenShift Container Platform 4.13 は Red Hat Enterprise Linux (RHEL) 9.2 をベースにしています。FIPS 検証用に RHEL 9.2 暗号化モジュールがまだ送信されていません。詳細は、4.13 **OpenShift Container Platform リリースノート** の "About this release" を参照してください。

19 オプション: クラスター内のマシンにアクセスするのに使用する **sshKey** 値をオプションで指定できます。



注記

インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。

6.7.4. インストール時のクラスター全体のプロキシーの設定

実稼働環境では、インターネットへの直接アクセスを拒否し、代わりに HTTP または HTTPS プロキシーを使用することができます。プロキシー設定を **install-config.yaml** ファイルで行うことにより、新規の OpenShift Container Platform クラスターをプロキシーを使用するように設定できます。

前提条件

- 既存の **install-config.yaml** ファイルがある。
- クラスターがアクセスする必要のあるサイトを確認済みで、それらのいずれかがプロキシーをバイパスする必要があるかどうかを判別している。デフォルトで、すべてのクラスター Egress トラフィック (クラスターをホストするクラウドに関するクラウドプロバイダー API に対する

呼び出しを含む) はプロキシーされます。プロキシーを必要に応じてバイパスするために、サイトを **Proxy** オブジェクトの **spec.noProxy** フィールドに追加している。

注記

Proxy オブジェクトの **status.noProxy** フィールドには、インストール設定の **networking.machineNetwork[].cidr**、**networking.clusterNetwork[].cidr**、および **networking.serviceNetwork[]** フィールドの値が設定されます。

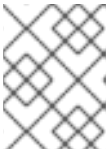
Amazon Web Services (AWS)、Google Cloud、Microsoft Azure、および Red Hat OpenStack Platform (RHOSP)へのインストールの場合、**Proxy** オブジェクトの **status.noProxy** フィールドには、インスタンスメタデータのエンドポイント(**169.254.169.254**)も設定されます。

手順

1. **install-config.yaml** ファイルを編集し、プロキシー設定を追加します。以下に例を示します。

```
apiVersion: v1
baseDomain: my.domain.com
proxy:
  httpProxy: http://<username>:<pswd>@<ip>:<port> 1
  httpsProxy: https://<username>:<pswd>@<ip>:<port> 2
  noProxy: example.com 3
additionalTrustBundle: | 4
    -----BEGIN CERTIFICATE-----
    <MY_TRUSTED_CA_CERT>
    -----END CERTIFICATE-----
additionalTrustBundlePolicy: <policy_to_add_additionalTrustBundle> 5
```

1. クラスター外の HTTP 接続を作成するために使用するプロキシー URL。URL スキームは **http** である必要があります。
2. クラスター外で HTTPS 接続を作成するために使用するプロキシー URL。
3. プロキシーから除外するための宛先ドメイン名、IP アドレス、または他のネットワーク CIDR のコンマ区切りのリスト。サブドメインのみと一致するように、ドメインの前に **.** を付けます。たとえば、**.y.com** は **x.y.com** に一致しますが、**y.com** には一致しません。***** を使用し、すべての宛先のプロキシーをバイパスします。
4. 指定されている場合、インストールプログラムは HTTPS 接続のプロキシーに必要な 1 つ以上の追加の CA 証明書が含まれる **user-ca-bundle** という名前の設定マップを **openshift-config** namespace に生成します。次に Cluster Network Operator は、これらのコンテンツを Red Hat Enterprise Linux CoreOS (RHCOS) 信頼バンドルにマージする **trusted-ca-bundle** 設定マップを作成し、この設定マップは **Proxy** オブジェクトの **trustedCA** フィールドで参照されます。**additionalTrustBundle** フィールドは、プロキシーのアイデンティティー証明書が RHCOS 信頼バンドルからの認証局によって署名されない限り必要になります。
5. オプション： **trustedCA** フィールドの **user-ca-bundle** 設定マップを参照する **Proxy** オブジェクトの設定を決定するポリシー。許可される値は **Proxyonly** および **Always** です。**Proxyonly** を使用して、**http/https** プロキシーが設定されている場合にのみ **user-ca-bundle** 設定マップを参照します。**Always** を使用して、常に **user-ca-bundle** 設定マップを参照します。デフォルト値は **Proxyonly** です。



注記

インストールプログラムは、プロキシーの **readinessEndpoints** フィールドをサポートしません。

注記

インストーラーがタイムアウトした場合は、インストーラーの **wait-for** コマンドを使用してデプロイメントを再起動してからデプロイメントを完了します。以下に例を示します。

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

2. ファイルを保存し、OpenShift Container Platform のインストール時にこれを参照します。

インストールプログラムは、指定の **install-config.yaml** ファイルのプロキシー設定を使用する **cluster** という名前のクラスター全体のプロキシーを作成します。プロキシー設定が指定されていない場合、**cluster Proxy** オブジェクトが依然として作成されますが、これには **spec** がありません。

注記

cluster という名前の **Proxy** オブジェクトのみがサポートされ、追加のプロキシーを作成することはできません。

6.8. IAM を手動で作成する

クラスターをインストールするには、Cloud Credential Operator (CCO) が手動モードで動作する必要があります。インストールプログラムは CCO を手動モードに設定しますが、クラウドプロバイダーの ID とアクセス管理シークレットを指定する必要があります。

Cloud Credential Operator (CCO) ユーティリティー (**ccoctl**) を使用して、必要な IBM Cloud VPC リソースを作成できます。

前提条件

- **ccoctl** バイナリーを設定している。
- 既存の **install-config.yaml** ファイルがある。

手順

1. **install-config.yaml** 設定ファイルを編集し、**credentialsMode** パラメーターが **Manual** に設定されるようにします。

   サンプル install-config.yaml 設定ファイル

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Manual (1)
compute:
- architecture: amd64
  hyperthreading: Enabled
```

1 この行は、**credentialsMode** パラメーターを **Manual** に設定するために追加されます。

2. マニフェストを生成するには、インストールプログラムが含まれるディレクトリーから以下のコマンドを実行します。

```
$ ./openshift-install create manifests --dir <installation_directory>
```

3. インストールプログラムが含まれているディレクトリーから、**openshift-install** バイナリーが使用するようにビルドされている OpenShift Container Platform リリースイメージを取得します。

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

4. OpenShift Container Platform リリースイメージから **CredentialsRequest** オブジェクトを抽出します。

```
$ oc adm release extract \
  --from=$RELEASE_IMAGE \
  --credentials-requests \
  --cloud=<provider_name> \1
  --to=<path_to_credential_requests_directory> 2
```

1 プロバイダーの名前。例: **ibmcloud** または **powervs**

2 認証情報の要求が保存されるディレクトリー。

このコマンドにより、それぞれの **CredentialsRequest** オブジェクトに YAML ファイルが作成されます。

サンプル CredentialsRequest オブジェクト

```
apiVersion: cloudcredential.openshift.io/v1
kind: CredentialsRequest
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: openshift-image-registry-ibmcos
  namespace: openshift-cloud-credential-operator
spec:
  secretRef:
    name: installer-cloud-credentials
    namespace: openshift-image-registry
  providerSpec:
    apiVersion: cloudcredential.openshift.io/v1
    kind: IBMCloudProviderSpec
    policies:
    - attributes:
      - name: serviceName
        value: cloud-object-storage
      roles:
      - crn:v1:bluemix:public:iam::::role:Viewer
      - crn:v1:bluemix:public:iam::::role:Operator
      - crn:v1:bluemix:public:iam::::role:Editor
```

```
    - crn:v1:bluemix:public:iam::::serviceRole:Reader
    - crn:v1:bluemix:public:iam::::serviceRole:Writer
  - attributes:
    - name: resourceType
      value: resource-group
    roles:
    - crn:v1:bluemix:public:iam::::role:Viewer
```

5. クラスターでクラスター機能を使用して 1 つ以上のオプションコンポーネントを無効にする場合は、無効なコンポーネントの **CredentialsRequest** カスタムリソースを削除します。

IBM Cloud VPC 上の OpenShift Container Platform 4.13 の credrequests ディレクトリーの内容の例

```
0000_26_cloud-controller-manager-operator_15_credentialsrequest-ibm.yaml 1
0000_30_machine-api-operator_00_credentials-request.yaml 2
0000_50_cluster-image-registry-operator_01-registry-credentials-request-ibmcos.yaml 3
0000_50_cluster-ingress-operator_00-ingress-credentials-request.yaml 4
0000_50_cluster-storage-operator_03_credentials_request_ibm.yaml 5
```

1. Cloud Controller Manager Operator CR が必要です。
2. Machine API Operator CR が必要です。
3. Image Registry Operator CR が必要です。
4. Ingress Operator CR が必要です。
5. Storage Operator CR はオプションのコンポーネントであり、クラスターで無効になっている場合があります。

6. 各認証情報リクエストのサービス ID を作成し、定義されたポリシーを割り当て、API キーを作成し、シークレットを生成します。

```
$ ccoctl ibmcloud create-service-id \
  --credentials-requests-dir <path_to_credential_requests_directory> \ 1
  --name <cluster_name> \ 2
  --output-dir <installation_directory> \
  --resource-group-name <resource_group_name> 3
```

1. 認証情報の要求が保存されるディレクトリー。
2. OpenShift Container Platform クラスターの名前。
3. オプション: アクセスポリシーのスコープに使用されるリソースグループの名前。

注記

クラスターで **TechPreviewNoUpgrade** 機能セットによって有効化されたテクノロジープレビュー機能を使用している場合は、**--enable-tech-preview** パラメーターを含める必要があります。

間違ったリソースグループ名が指定された場合、ブートストラップフェーズ中にインストールが失敗します。正しいリソースグループ名を見つけるには、次のコマンドを実行します。

```
$ grep resourceGroupName <installation_directory>/manifests/cluster-
infrastructure-02-config.yml
```

検証

- クラスターの **manifests** ディレクトリーに適切なシークレットが生成されていることを確認してください。

6.9. クラスターのデプロイ

互換性のあるクラウドプラットフォームに OpenShift Container Platform をインストールできます。

重要

インストールプログラムの **create cluster** コマンドは、初期インストール時に 1 回だけ実行できます。

前提条件

- クラスターをホストするクラウドプラットフォームでアカウントを設定します。
- OpenShift Container Platform インストールプログラム、およびクラスターのプルシークレットを取得する。
- ホスト上のクラウドプロバイダーアカウントに、クラスターをデプロイするための適切な権限があることを確認してください。アカウントの権限が正しくないと、インストールプロセスが失敗し、不足している権限を示すエラーメッセージが表示されます。

手順

- インストールプログラムが含まれるディレクトリーに切り替え、クラスターのデプロイメントを初期化します。

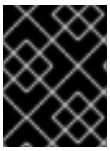
```
$ ./openshift-install create cluster --dir <installation_directory> \ 1
    --log-level=info 2
```

1. **<installation_directory>** に、カスタマイズした **./install-config.yaml** ファイルの場所を指定します。
2. 異なるインストールの詳細情報を表示するには、**info** ではなく、**warn**、**debug**、または **error** を指定します。

検証

クラスターのデプロイが正常に完了すると、次のようになります。

- ターミナルには、Web コンソールへのリンクや **kubeadmin** ユーザーの認証情報など、クラスターにアクセスするための指示が表示されます。
- 認証情報は **<installation_directory>/.openshift_install.log** にも出力されます。



重要

インストールプログラム、またはインストールプログラムが作成するファイルを削除することはできません。これらはいずれもクラスターを削除するために必要になります。

出力例

```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- インストールプログラムが生成する Ignition 設定ファイルには、24 時間が経過すると期限切れになり、その後に更新される証明書が含まれます。証明書を更新する前にクラスターが停止し、24 時間経過した後にクラスターを再起動すると、クラスターは期限切れの証明書を自動的に復元します。例外として、kubelet 証明書を回復するために保留状態の **node-bootstrapper** 証明書署名要求 (CSR) を手動で承認する必要があります。詳細は、**コントロールプレーン証明書の期限切れの状態からのリカバリー** に関するドキュメントを参照してください。
- 24 時間証明書はクラスターのインストール後 16 時間から 22 時間にローテーションするため、Ignition 設定ファイルは、生成後 12 時間以内に使用することを推奨します。12 時間以内に Ignition 設定ファイルを使用することにより、インストール中に証明書の更新が実行された場合のインストールの失敗を回避できます。

6.10. バイナリーのダウンロードによる OPENSHIFT CLI のインストール

コマンドラインインターフェイスを使用して OpenShift Container Platform と対話するために CLI (**oc**) をインストールすることができます。**oc** は Linux、Windows、または macOS にインストールできます。

重要

以前のバージョンの **oc** をインストールしている場合、これを使用して OpenShift Container Platform 4.13 のすべてのコマンドを実行することはできません。新規バージョンの **oc** をダウンロードし、インストールします。

Linux への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Linux にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **Product Variant** ドロップダウンリストからアーキテクチャーを選択します。
3. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
4. **OpenShift v4.13 Linux Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
5. アーカイブを展開します。

```
$ tar xvf <file>
```

6. **oc** バイナリーを、**PATH** にあるディレクトリーに配置します。
PATH を確認するには、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

Windows への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Windows にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 Windows Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
4. ZIP プログラムでアーカイブを解凍します。
5. **oc** バイナリーを、**PATH** にあるディレクトリーに移動します。
PATH を確認するには、コマンドプロンプトを開いて以下のコマンドを実行します。

```
C:\> path
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

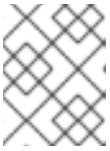
```
C:\> oc <command>
```

macOS への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを macOS にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 macOS Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。



注記

macOS arm64 の場合は、**OpenShift v4.13 macOS arm64 Client** エントリーを選択します。

4. アーカイブを展開し、解凍します。
5. **oc** バイナリーをパスにあるディレクトリーに移動します。
PATH を確認するには、ターミナルを開き、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

6.11. CLI の使用によるクラスターへのログイン

クラスター **kubeconfig** ファイルをエクスポートし、デフォルトシステムユーザーとしてクラスターにログインできます。**kubeconfig** ファイルには、クライアントを正しいクラスターおよび API サーバーに接続するために CLI で使用されるクラスターに関する情報が含まれます。このファイルはクラスターに固有のファイルであり、OpenShift Container Platform のインストール時に作成されます。

前提条件

- OpenShift Container Platform クラスターをデプロイしていること。
- **oc** CLI がインストールされている。

手順

1. **kubeadmin** 認証情報をエクスポートします。

```
$ export KUBECONFIG=<installation_directory>/auth/kubeconfig 1
```

1 **<installation_directory>** には、インストールファイルを保存したディレクトリーへのパスを指定します。

2. エクスポートされた設定を使用して、**oc** コマンドを正常に実行できることを確認します。

```
$ oc whoami
```

出力例

```
system:admin
```

関連情報

- Web コンソールへのアクセス

6.12. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス

OpenShift Container Platform 4.13 では、クラスターの健全性および正常に実行された更新についてのメトリクスを提供するためにデフォルトで実行される Telemetry サービスにもインターネットアクセスが必要です。クラスターがインターネットに接続されている場合、Telemetry は自動的に実行され、クラスターは OpenShift Cluster Manager Hybrid Cloud Console に登録されます。

OpenShift Cluster Manager インベントリーが正常である (Telemetry によって自動的に維持、または OpenShift Cluster Manager Hybrid Cloud Console を使用して手動で維持) ことを確認した後に、subscription watch を使用 して、アカウントまたはマルチクラスターレベルで OpenShift Container Platform サブスクリプションを追跡します。

関連情報

- リモートヘルスモニタリングについて

6.13. 次のステップ

- クラスターをカスタマイズします。
- オプション： リモートヘルスレポート。

第7章 プライベートクラスターを IBM CLOUD VPC にインストールする

OpenShift Container Platform バージョン 4.13 では、プライベートクラスターを既存の VPC にインストールできます。インストールプログラムは、カスタマイズ可能な残りの必要なインフラストラクチャーをプロビジョニングします。インストールをカスタマイズするには、クラスターをインストールする前に、**install-config.yaml** ファイルでパラメーターを変更します。

7.1. 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ている。
- クラスターインストール方法の選択およびそのユーザー向けの準備 を確認している。
- クラスターをホストするように IBM Cloud アカウントを設定 している。
- ファイアウォールを使用する場合は、クラスターがアクセスを必要とするサイトを許可するようにファイアウォールを設定する必要がある。
- クラスターをインストールする前に、**ccoctl** ユーティリティーを設定している。詳細は、IBM Cloud VPC 用の IAM の設定 を参照してください。

7.2. プライベートクラスター

外部エンドポイントを公開しないプライベート OpenShift Container Platform クラスターをデプロイすることができます。プライベートクラスターは内部ネットワークからのみアクセスでき、インターネット上では表示されません。

デフォルトで、OpenShift Container Platform はパブリックにアクセス可能な DNS およびエンドポイントを使用できるようにプロビジョニングされます。プライベートクラスターは、クラスターのデプロイ時に DNS、Ingress コントローラー、および API サーバーを private に設定します。つまり、クラスターリソースは内部ネットワークからのみアクセスでき、インターネット上では表示されません。

重要

クラスターにパブリックサブネットがある場合、管理者により作成されたロードバランサーサービスはパブリックにアクセスできる可能性があります。クラスターのセキュリティーを確保するには、これらのサービスに明示的にプライベートアノテーションが付けられていることを確認してください。

プライベートクラスターをデプロイするには、以下を行う必要があります。

- 要件を満たす既存のネットワークを使用します。クラスターリソースはネットワーク上の他のクラスター間で共有される可能性があります。
- IBM Cloud DNS Services を使用して DNS ゾーンを作成し、それをクラスターの基本ドメインとして指定します。詳しくは、IBM Cloud DNS サービスを使用して DNS 解決を設定するを参照してください。
- 以下にアクセスできるマシンからデプロイ。
  - プロビジョニングするクラウドの API サービス。
  - プロビジョニングするネットワーク上のホスト。

- インストールメディアを取得するインターネット。

これらのアクセス要件を満たし、所属する会社のガイドラインに準拠したすべてのマシンを使用することができます。たとえば、このマシンには、クラウドネットワーク上の bastion ホスト、または VPN 経由でネットワークにアクセスできるマシンを使用できます。

7.3. IBM CLOUD VPC 内のプライベートクラスター

IBM Cloud VPC 上にプライベートクラスターを作成するには、既存のプライベート VPC とサブネットを提供してクラスターをホストする必要があります。インストールプログラムは、クラスターが必要とする DNS レコードを解決できる必要もあります。インストールプログラムは、内部トラフィック用としてのみ Ingress Operator および API サーバーを設定します。

クラスターは、IBM Cloud VPC API にアクセスするために引き続きインターネットにアクセスする必要があります。

以下のアイテムは、プライベートクラスターのインストール時に必要ではなく、作成されません。

- パブリックサブネット
- パブリック Ingress をサポートするパブリックネットワークロードバランサー
- クラスターの **baseDomain** に一致するパブリック DNS ゾーン

インストールプログラムは、プライベート DNS ゾーンおよびクラスターに必要なレコードを作成するために指定する **baseDomain** を使用します。クラスターは、Operator がクラスターのパブリックレコードを作成せず、すべてのクラスターマシンが指定するプライベートサブネットに配置されるように設定されます。

7.3.1. 制限事項

IBM Cloud VPC 上のプライベートクラスターには、クラスターのデプロイメントに使用された既存の VPC に関連する制限のみが適用されます。

7.4. カスタム VPC の使用について

OpenShift Container Platform 4.13 では、クラスターを既存の IBM Virtual Private Cloud (VPC) のサブネットにデプロイできます。OpenShift Container Platform を既存の VPC にデプロイすると、新規アカウントの制限を回避したり、会社のガイドラインによる運用上の制約をより容易に遵守することが可能になる場合があります。VPC を作成するために必要なインフラストラクチャーの作成パーミッションを取得できない場合は、このインストールオプションを使用します。

インストールプログラムは既存のサブネットにある他のコンポーネントを認識できないため、サブネットの CIDR などを選択できません。クラスターをインストールするサブネットのネットワークを設定する必要があります。

7.4.1. VPC を使用するための要件

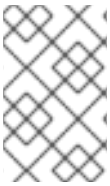
クラスターをインストールする前に、既存の VPC およびそのサブネットを適切に設定する必要があります。インストールプログラムでは、次のコンポーネントは作成されません。

- NAT ゲートウェイ
- サブネット

- ルートテーブル
- VPC ネットワーク

インストールプログラムには、以下の機能はありません。

- 使用するクラスターのネットワーク範囲を細分化します。
- サブネットのルートテーブルを設定します。
- DHCP などの VPC オプションの設定



注記

インストールプログラムでは、クラウド提供の DNS サーバーを使用する必要があります。カスタム DNS サーバーの使用はサポートされていないため、インストールが失敗します。

7.4.2. VPC 検証

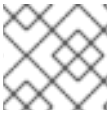
VPC とすべてのサブネットは、既存のリソースグループ内にある必要があります。クラスターはこのリソースグループにデプロイされます。

インストールの一環として、**install-config.yaml** ファイルで以下を指定します。

- リソースグループの名前
- VPC の名前
- コントロールプレーンマシンおよびコンピュートマシンのサブネット

指定するサブネットが適切であることを確認するには、インストールプログラムが以下を確認します。

- 指定したサブネットがすべて存在します。
- リージョン内の各アベイラビリティーゾーンに、以下を指定します。
  - コントロールプレーンマシンの 1 つのサブネット。
  - コンピュートマシン用に 1 つのサブネット。
- 指定したマシン CIDR にはコンピュートマシンおよびコントロールプレーンマシンのサブネットが含まれます。



注記

サブネット ID はサポートされていません。

7.4.3. クラスター間の分離

OpenShift Container Platform を既存のネットワークにデプロイする場合、クラスターサービスの分離の規模は以下の方法で縮小されます。

- 複数の OpenShift Container Platform クラスターを同じ VPC にインストールできます。
- ICMP Ingress はネットワーク全体で許可されます。

- TCP ポート 22 Ingress (SSH) はネットワーク全体に対して許可されます。
- コントロールプレーンの TCP 6443 Ingress (Kubernetes API) はネットワーク全体に対して許可されます。
- コントロールプレーンの TCP 22623 Ingress (MCS) はネットワーク全体に対して許可されます。

7.5. OPENSHIFT CONTAINER PLATFORM のインターネットアクセス

OpenShift Container Platform 4.13 では、クラスターをインストールするためにインターネットアクセスが必要になります。

インターネットへのアクセスは以下を実行するために必要です。

- OpenShift Cluster Manager Hybrid Cloud Console にアクセスし、インストールプログラムをダウンロードし、サブスクリプション管理を実行します。クラスターにインターネットアクセスがあり、Telemetry を無効にしない場合、そのサービスは有効なサブスクリプションでクラスターを自動的に使用します。
- クラスターのインストールに必要なパッケージを取得するために Quay.io にアクセスします。
- クラスターの更新を実行するために必要なパッケージを取得します。

重要

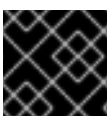
クラスターでインターネットに直接アクセスできない場合、プロビジョニングする一部のタイプのインフラストラクチャーでネットワークが制限されたインストールを実行できます。このプロセスで、必要なコンテンツをダウンロードし、これを使用してミラーレジストリーにインストールパッケージを設定します。インストールタイプに応じて、クラスターのインストール環境でインターネットアクセスが不要となる場合があります。クラスターを更新する前に、ミラーレジストリーのコンテンツを更新します。

7.6. クラスターノードの SSH アクセス用のキーペアの生成

OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定できます。キーは、Ignition 設定ファイルを介して Red Hat Enterprise Linux CoreOS (RHCOS) ノードに渡され、ノードへの SSH アクセスを認証するために使用されます。このキーは各ノードの **core** ユーザーの **~/.ssh/authorized_keys** リストに追加され、パスワードなしの認証が可能になります。

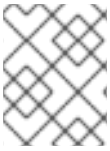
キーがノードに渡されると、キーペアを使用して RHCOS ノードにユーザー **core** として SSH を実行できます。SSH 経由でノードにアクセスするには、秘密鍵のアイデンティティーをローカルユーザーの SSH で管理する必要があります。

インストールのデバッグまたは障害復旧を実行するためにクラスターノードに対して SSH を実行する場合は、インストールプロセスの間に SSH 公開鍵を指定する必要があります。**./openshift-install gather** コマンドでは、SSH 公開鍵がクラスターノードに配置されている必要もあります。



重要

障害復旧およびデバッグが必要な実稼働環境では、この手順を省略しないでください。



注記

AWS キーペア などのプラットフォームに固有の方法で設定したキーではなく、ローカルキーを使用する必要があります。

手順

1. クラスターノードへの認証に使用するローカルマシンに既存の SSH キーペアがない場合は、これを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ ssh-keygen -t ed25519 -N '' -f <path>/<file_name> 1
```

1 新しい SSH キーのパスとファイル名 (~/**.ssh/id_ed25519** など) を指定します。既存のキーペアがある場合は、公開鍵が ~/**.ssh** ディレクトリーにあることを確認します。

2. 公開 SSH キーを表示します。

```
$ cat <path>/<file_name>.pub
```

たとえば、次のコマンドを実行して ~/**.ssh/id_ed25519.pub** 公開鍵を表示します。

```
$ cat ~/.ssh/id_ed25519.pub
```

3. ローカルユーザーの SSH エージェントに SSH 秘密鍵 ID が追加されていない場合は、それを追加します。キーの SSH エージェント管理は、クラスターノードへのパスワードなしの SSH 認証、または **./openshift-install gather** コマンドを使用する場合は必要になります。

注記

一部のディストリビューションでは、~/**.ssh/id_rsa** および ~/**.ssh/id_dsa** などのデフォルトの SSH 秘密鍵のアイデンティティーは自動的に管理されます。

a. **ssh-agent** プロセスがローカルユーザーに対して実行されていない場合は、バックグラウンドタスクとして開始します。

```
$ eval "$(ssh-agent -s)"
```

出力例

```
Agent pid 31874
```

4. SSH プライベートキーを **ssh-agent** に追加します。

```
$ ssh-add <path>/<file_name> 1
```

1 ~/**.ssh/id_ed25519** などの、SSH プライベートキーのパスおよびファイル名を指定します。

出力例

```
Identity added: /home/<you>/<path>/<file_name> (<computer_name>)
```

次のステップ

- OpenShift Container Platform をインストールする際に、SSH パブリックキーをインストールプログラムに指定します。

7.7. インストールプログラムの取得

OpenShift Container Platform をインストールする前に、クラウドネットワーク上の踏み台ホスト、または VPN 経由でネットワークにアクセスできるマシンにインストールファイルをダウンロードします。

プライベートクラスターのインストール要件の詳細は、「プライベートクラスター」を参照してください。

前提条件

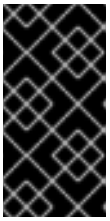
- Linux を実行するマシン (例: 500 MB のローカルディスク領域のある Red Hat Enterprise Linux 8) が必要です。

手順

1. OpenShift Cluster Manager サイトの インフラストラクチャープロバイダー ページにアクセスします。Red Hat アカウントがある場合は、認証情報を使用してログインします。アカウントがない場合はこれを作成します。
2. インフラストラクチャープロバイダーを選択します。
3. インストールタイプのページに移動し、ホストオペレーティングシステムとアーキテクチャーに対応するインストールプログラムをダウンロードして、インストール設定ファイルを保存するディレクトリーにファイルを配置します。

重要

インストールプログラムは、クラスターのインストールに使用するコンピューターにいくつかのファイルを作成します。クラスターのインストール完了後は、インストールプログラムおよびインストールプログラムが作成するファイルを保持する必要があります。ファイルはいずれもクラスターを削除するために必要になります。



重要

インストールプログラムで作成されたファイルを削除しても、クラスターがインストール時に失敗した場合でもクラスターは削除されません。クラスターを削除するには、特定のクラウドプロバイダー用の OpenShift Container Platform のアンインストール手順を実行します。

4. インストールプログラムを展開します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar -xvf openshift-install-linux.tar.gz
```

5. Red Hat OpenShift Cluster Manager からインストールプルシークレット をダウンロードします。このプルシークレットを使用し、OpenShift Container Platform コンポーネントのコンテナーイメージを提供する Quay.io など、組み込まれた各種の認証局によって提供されるサービスで認証できます。

7.8. API キーのエクスポート

作成した API キーをグローバル変数として設定する必要があります。インストールプログラムは、起動時に変数を取り込み、API キーを設定します。

前提条件

- IBM Cloud アカウント用にユーザー API キーまたはサービス ID API キーのいずれかを作成している。

手順

- アカウントの API キーをグローバル変数としてエクスポートします。

```
$ export IC_API_KEY=<api_key>
```

重要

変数名は指定どおりに正確に設定する必要があります。インストールプログラムは、起動時に変数名が存在することを想定しています。

7.9. インストール設定ファイルの手動作成

クラスターをインストールするには、インストール設定ファイルを手動で作成する必要があります。

前提条件

- インストールプログラムで使用するための SSH 公開鍵がローカルマシン上に存在する。この鍵は、デバッグや障害復旧のために、クラスターノードへの SSH 認証に使用できます。
- OpenShift Container Platform インストールプログラムとクラスターのプルシークレットを取得している。

手順

1. 必要なインストールアセットを保存するためのインストールディレクトリーを作成します。

```
$ mkdir <installation_directory>
```

重要

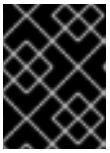
このディレクトリーは必ず作成してください。ブートストラップ X.509 証明書などの一部のインストールアセットは、有効期限が短いため、インストールディレクトリーを再利用しないでください。別のクラスターインストールの個別のファイルを再利用する必要がある場合は、それらをディレクトリーにコピーすることができます。ただし、インストールアセットのファイル名はリリース間で変更される可能性があります。インストールファイルを以前のバージョンの OpenShift Container Platform からコピーする場合は注意してください。

2. 提供されているサンプルの **install-config.yaml** ファイルテンプレートをカスタマイズし、ファイルを **<installation_directory>** に保存します。

注記

この設定ファイルの名前を **install-config.yaml** と付ける必要があります。

3. 多くのクラスターのインストールに使用できるように、**install-config.yaml** ファイルをバックアップします。

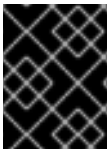


重要

インストールプロセスの次のステップで **install-config.yaml** ファイルを使用するため、今すぐこのファイルをバックアップしてください。

7.9.1. インストール設定パラメーター

OpenShift Container Platform クラスターをデプロイする前に、クラスターをホストするクラウドプラットフォームでアカウントを記述し、クラスターのプラットフォームをオプションでカスタマイズするためにパラメーターの値を指定します。**install-config.yaml** インストール設定ファイルを作成する際に、コマンドラインで必要なパラメーターの値を指定します。クラスターをカスタマイズする場合、**install-config.yaml** ファイルを変更して、プラットフォームについての詳細情報を指定できます。



重要

インストール後は、これらのパラメーターを **install-config.yaml** ファイルで変更することはできません。

7.9.1.1. 必須設定パラメーター

必須のインストール設定パラメーターは、以下の表で説明されています。

表7.1 必須パラメーター

パラメーター	説明	値
apiVersion	**install-config.yaml** コンテンツの API バージョン。現在のバージョンは **v1** です。インストールプログラムは、古い API バージョンもサポートしている場合があります。	String

パラメーター	説明	値
baseDomain	クラウドプロバイダーのベースドメイン。ベースドメインは、OpenShift Container Platform クラスターコンポーネントへのルートを作成するために使用されます。クラスターの完全な DNS 名は、**baseDomain** と **<metadata.name>.<baseDomain>** 形式を使用する **metadata.name** パラメーターの値の組み合わせです。	**example.com** などの完全修飾ドメインまたはサブドメイン名。
metadata	Kubernetes リソース **ObjectMeta**。ここからは **name** パラメーターのみが消費されます。	オブジェクト
metadata.name	クラスターの名前。クラスターの DNS レコードはすべて **{{.metadata.name}}.{{.baseDomain}}** のサブドメインです。	**dev** などの小文字、ハイフン (**-**)、およびピリオド (**.**) が含まれる文字列。
platform	インストールを実行する特定のプラットフォームの設定: **alibabacloud**、**aws**、**baremetal**、**azure**、**gcp**、**ibmcloud**、**Nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**。**platform.<platform>** パラメーターに関する追加情報は、以下の表で特定のプラットフォームを参照してください。	オブジェクト

パラメーター	説明	値

pullSecret	Red Hat OpenShift Cluster Manager からプルシークレット を取得して、Quay.io などのサービスから OpenShift Container Platform コンポーネントのコンテナーイメージをダウンロードすることを認証します。	<pre>{
		  "auths":{
		  "cloud.openshift.com":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  },
		  "quay.io":{
		  "auth":"b3Blb=",
		  "email":"you@example.com"
		  }
		  }
		}</pre>

7.9.1.2. ネットワーク設定パラメーター

既存のネットワークインフラストラクチャーの要件に基づいて、インストール設定をカスタマイズできます。たとえば、クラスターネットワークの IP アドレスブロックを拡張するか、デフォルトとは異なる IP アドレスブロックを指定できます。

IPv4 アドレスのみがサポートされます。

注記

Globalnet は、Red Hat OpenShift Data Foundation ディザスターリカバリーソリューションではサポートされていません。局地的なディザスターリカバリーのシナリオでは、各クラスター内のクラスターとサービスネットワークに重複しない範囲のプライベート IP アドレスを使用するようにしてください。

表7.2 ネットワークパラメーター

パラメーター	説明	値
networking	クラスターのネットワークの設定。	オブジェクト  **注記** インストール後に **networking** オブジェクトで指定したパラメーターを変更することはできません。

パラメーター	説明	値
networking.networkType	インストールする Red Hat OpenShift Networking ネットワークプラグイン。	**OpenShiftSDN** または **OVNKubernetes** のいずれか。**OpenShiftSDN** は、すべての Linux ネットワークの Container Network Interface (CNI)プラグインです。**OVNKubernetes** は、Linux ネットワークと、Linux サーバーと Windows サーバーの両方を含む Linux ネットワークおよびハイブリッドネットワーク用の CNI プラグインです。デフォルトの値は **OVNkubernetes** です。

networking.clusterNetwork	Pod の IP アドレスブロック。
	
	デフォルト値は **10.128.0.0/14** で、ホストの接頭辞は **/23** です。
	
	複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。
		オブジェクトの配列。以下に例を示します。
		
		`networking:`
		`  clusterNetwork:`
		`  - cidr: 10.128.0.0/14`
		`    hostPrefix: 23`

networking.clusterNetwork.cidr	**networking.clusterNetwork** を使用する場合に必須です。IP アドレスブロック。 IPv4 ネットワーク	CIDR (Classless Inter-Domain Routing) 表記の IP アドレスブロック。IPv4 ブロックの接頭辞長は **0** から **32** の間になります。
networking.clusterNetwork.hostPrefix	それぞれの個別ノードに割り当てるサブネット接頭辞長。たとえば、**hostPrefix** が **23** に設定される場合、各ノードに指定の **cidr** から **/23** サブネットが割り当てられます。**hostPrefix** 値の **23** は、510 (2^(32 - 23) - 2) Pod IP アドレスを提供します。	サブネット接頭辞。 デフォルト値は **23** です。

networking.serviceNetwork	サービスの IP アドレスブロック。デフォルト値は **172.30.0.0/16** です。
	
	OpenShift SDN および OVN-Kubernetes ネットワークプラグインは、サービスネットワークの単一 IP アドレスブロックのみをサポートします。
		CIDR 形式の IP アドレスブロックを持つ配列。以下に例を示します。
		
		`networking:`
		`  serviceNetwork:`
		`  - 172.30.0.0/16`

パラメーター	説明	値
networking.machineNetwork	マシンの IP アドレスブロック。 複数の IP アドレスブロックを指定する場合は、ブロックが重複しないようにしてください。	オブジェクトの配列。以下に例を示します。 networking: machineNetwork: - cidr: 10.0.0.0/16
networking.machineNetwork.cidr	**networking.machineNetwork** を使用する場合に必須です。IP アドレスブロック。libvirt と IBM Power Virtual Server を除くすべてのプラットフォームのデフォルト値は **10.0.0.0/16** です。libvirt の場合、デフォルト値は **192.168.126.0/24** です。IBM Power Virtual Server の場合、デフォルト値は **192.168.0.0/24** です。CIDR には、**platform.ibmcloud.controlPlaneSubnets** および **platform.ibmcloud.computeSubnets** で定義されたサブネットが含まれている必要があります。	CIDR 表記の IP ネットワークブロック。 例: **10.0.0.0/16** **注記** 優先される NIC が置かれている CIDR に一致する **networking.machineNetwork** を設定します。

7.9.1.3. オプションの設定パラメーター

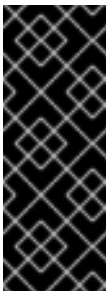
オプションのインストール設定パラメーターは、以下の表で説明されています。

表7.3 オプションのパラメーター

パラメーター	説明	値
additionalTrustBundle	ノードの信頼済み証明書ストアに追加される PEM でエンコードされた X.509 証明書バンドル。この信頼バンドルは、プロキシーが設定されている場合にも使用することができます。	文字列
capabilities	オプションのコアクラスターコンポーネントのインストールを制御します。オプションのコンポーネントを無効にすることで、OpenShift Container Platform クラスターのフットプリントを削減できます。詳細は、**インストール** の「クラスター機能ページ」を参照してください。	文字列配列

パラメーター	説明	値
capabilities.baselineCapabilitySet	有効にするオプション機能の初期セットを選択します。有効な値は **None**、**v4.11**、**v4.12**、**vCurrent** です。デフォルト値は **vCurrent** です。	文字列
capabilities.additionalEnabledCapabilities	オプションの機能のセットを、**baselineCapabilitySet** で指定したものを超えて拡張します。このパラメーターで複数の機能を指定できます。	文字列配列
cpuPartitioningMode	ワークロードパーティション設定を使用して、OpenShift Container Platform サービス、クラスター管理ワークロード、およびインフラストラクチャー Pod を分離し、予約された CPU セットで実行できます。ワークロードパーティショニングは、インストール中にのみ有効にできます。インストール後に無効にすることはできません。このフィールドはワークロードのパーティショニングを有効にしますが、特定の CPU を使用するようにワークロードを設定するわけではありません。詳細は、**スケーラビリティとパフォーマンス** セクションの **ワークロードパーティショニング** ページを参照してください。	**None** または **AllNodes**。デフォルト値は **None** です。
compute	コンピュートノードを形成するマシンの設定。	**MachinePool** オブジェクトの配列。
compute.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String

パラメーター	説明	値
compute: hyperthreading:	コンピュートマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。  **重要** 同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
compute.name	**compute** を使用する場合に必須です。マシンプールの名前。	**worker**
compute.platform	**compute** を使用する場合に必須です。このパラメーターを使用して、ワーカーマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **controlPlane.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
compute.replicas	プロビジョニングするコンピュートマシン (ワーカーマシンとしても知られる) の数。	**2** 以上の正の整数。デフォルト値は **3** です。
featureSet	機能セットのクラスターを有効にします。機能セットは、デフォルトで有効にされない OpenShift Container Platform 機能のコレクションです。インストール中に機能セットを有効にする方法の詳細は、「機能ゲートの使用による各種機能の有効化」を参照してください。	文字列。**TechPreviewNoUpgrade** など、有効にする機能セットの名前。
controlPlane	コントロールプレーンを形成するマシンの設定。	**MachinePool** オブジェクトの配列。

パラメーター	説明	値
controlPlane.architecture	プール内のマシンの命令セットアーキテクチャーを決定します。現在、さまざまなアーキテクチャーのクラスターはサポートされていません。すべてのプールは同じアーキテクチャーを指定する必要があります。有効な値はデフォルト **amd64** です。	String
controlPlane: hyperthreading:	コントロールプレーンマシンで同時マルチスレッドまたは **hyperthreading** を有効/無効にするかどうか。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。  **重要** 同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。	**Enabled** または **Disabled**
controlPlane.name	**controlPlane** を使用する場合に必須です。マシンプールの名前。	**master**
controlPlane.platform	**controlPlane** を使用する場合に必須です。このパラメーターを使用して、コントロールプレーンマシンをホストするクラウドプロバイダーを指定します。このパラメーターの値は **compute.platform** パラメーターの値に一致する必要があります。	**alibabacloud**、**aws**、**azure**、**gcp**、**ibmcloud**、**nutanix**、**openstack**、**ovirt**、**powervs**、**vsphere**、または **{}**
controlPlane.replicas	プロビジョニングするコントロールプレーンマシンの数。	サポートされる値は **3** のみです (これはデフォルト値です)。

パラメーター	説明	値
credentialsMode	Cloud Credential Operator (CCO) モード。CCO は、モードが指定されていない場合に指定される認証情報の機能を動的に判別しようとします。この場合、複数のモードがサポートされるプラットフォームで mint モードが優先されます。  **注記** すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**Cluster Operators リファレンス** の **Cloud Credential Operator** を参照してください。  **注記** AWS アカウントでサービスコントロールポリシー (SCP) が有効になっている場合は、**credentialsMode** パラメーターを **Mint**、**Passthrough** または **Manual** に設定する必要があります。	**Mint**、**Passthrough**、**Manual**、または空の文字列 (**""**)。
imageContentSources	release-image コンテンツのソースおよびリポジトリー。	オブジェクトの配列。この表の以下の行で説明されているように、**source** およびオプションで **mirrors** が含まれます。
imageContentSources.source	**imageContentSources** を使用する場合に必須です。ユーザーが参照するリポジトリーを指定します (例: イメージプル仕様)。	文字列
imageContentSources.mirrors	同じイメージが含まれる可能性のあるリポジトリーを 1 つ以上指定します。	文字列の配列

パラメーター	説明	値
publish	Kubernetes API、OpenShift ルートなどのクラスターのユーザーに表示されるエンドポイントをパブリッシュまたは公開する方法。	**Internal** または **External**。プライベートクラスターをデプロイするには、**publish** を **Internal** に設定します。これはインターネットからアクセスできません。デフォルト値は **External** です。
sshKey	クラスターマシンへのアクセスを認証するための SSH キー。 **注記** インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。	たとえば、**sshKey: ssh-ed25519 AAAA..** です。

1. すべてのクラウドプロバイダーですべての CCO モードがサポートされているわけではありません。CCO モードの詳細は、**認証と認可** コンテンツの「クラウドプロバイダーの認証情報の管理」を参照してください。

7.9.1.4. 追加の IBM Cloud VPC 設定パラメーター

追加の IBM Cloud VPC 設定パラメーターについて、以下の表で説明します。

表7.4 追加の IBM Cloud VPC パラメーター

パラメーター	説明	値
platform.ibmcloud.resourceGroupName	既存のリソースグループの名前。デフォルトでは、installer-provisioned VPC およびクラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。クラスターを既存の VPC にデプロイする場合、installer-provisioned クラスターリソースは、このリソースグループに配置されます。指定しない場合、インストールプログラムはクラスターのリソースグループを作成します。プロビジョニングした VPC リソースは、**networkResourceGroupName** パラメーターを使用して指定したリソースグループに存在する必要があります。いずれの場合も、クラスターコンポーネントはリソースグループ内のすべてのリソースの所有権を引き受けるため、このリソースグループは単一のクラスターインストールのみに使用する必要があります。[1]	文字列 (例: **existing_resource_group**)。

パラメーター	説明	値
platform.ibmcloud.networkResourceGroupName	既存のリソースグループの名前。このリソースには、クラスターがデプロイされる既存の VPC とサブネットが含まれます。このパラメーターは、プロビジョニングした VPC にクラスターをデプロイする際に必要です。	文字列 (例: **existing_network_resource_group**)。
platform.ibmcloud.dedicatedHosts.profile	作成する新しい専用ホスト。**platform.ibmcloud.dedicatedHosts.name** に値を指定する場合、このパラメーターは必須ではありません。	**cx2-host-152x304**などの有効な IBM Cloud VPC 専用ホストプロファイル。[2]
platform.ibmcloud.dedicatedHosts.name	既存の専用ホスト。**platform.ibmcloud.dedicatedHosts.profile** に値を指定する場合、このパラメーターは必須ではありません。	文字列、たとえば **my-dedicated-host-name**。
platform.ibmcloud.type	すべての IBM Cloud VPC マシンのインスタンスタイプ。	**bx2-8x32** などの有効な IBM Cloud VPC インスタンスタイプ。[2]
platform.ibmcloud.vpcName	クラスターをデプロイする既存 VPC の名前。	文字列。
platform.ibmcloud.controlPlaneSubnets	コントロールプレーンマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。	文字列配列

パラメーター	説明	値
platform.ibmcloud.computeSubnets	コンピュートマシンをデプロイする VPC の既存サブネットの名前。各アベイラビリティーゾーンのサブネットを指定します。サブネット ID はサポートされていません。	文字列配列

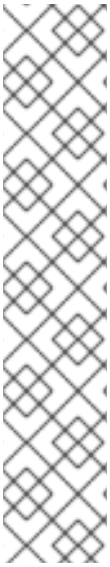
1. 既存のリソースグループを定義するか、インストーラーが作成するかによって、クラスターがアンインストールされたときにリソースグループがどのように扱われるかが決まります。リソースグループを定義すると、インストーラーはインストーラーがプロビジョニングしたすべてのリソースを削除しますが、リソースグループはそのままにします。インストールの一部としてリソースグループが作成された場合、インストーラーは、インストーラーがプロビジョニングしたすべてのリソースとリソースグループを削除します。
2. 自身のニーズに最適なプロファイルを判別するには、IBM ドキュメントの Instance Profiles を参照してください。

7.9.2. クラスターインストールの最小リソース要件

それぞれのクラスターマシンは、以下の最小要件を満たしている必要があります。

表7.5 最小リソース要件

マシン	オペレーティングシステム	仮想 CPU	仮想 RAM	ストレージ	1秒あたりの入出力 (IOPS)
ブートストラップ	RHCOS	4	16 GB	100 GB	300
コントロールプレーン	RHCOS	4	16 GB	100 GB	300
Compute	RHCOS	2	8 GB	100 GB	300



注記

OpenShift Container Platform バージョン 4.13 の時点で、RHCOS は RHEL バージョン 9.2 に基づいており、マイクロアーキテクチャーの要件を更新します。次のリストには、各アーキテクチャーに必要な最小限の命令セットアーキテクチャー (ISA) が含まれています。

- x86-64 アーキテクチャーには x86-64-v2 ISA が必要
- ARM64 アーキテクチャーには ARMv8.0-A ISA が必要
- IBM Power アーキテクチャーには Power 9 ISA が必要
- s390x アーキテクチャーには z14 ISA が必要

詳細は、RHEL アーキテクチャー を参照してください。

プラットフォームのインスタンスタイプがクラスターマシンの最小要件を満たす場合、これは OpenShift Container Platform で使用することがサポートされます。

関連情報

- ストレージの最適化

7.9.3. IBM Cloud VPC 用にカスタマイズされた install-config.yaml ファイルのサンプル

install-config.yaml ファイルをカスタマイズして、OpenShift Container Platform クラスターのプラットフォームについての詳細を指定するか、必要なパラメーターの値を変更することができます。

重要

このサンプルの YAML ファイルは参照用にのみ提供されます。インストールプログラムを使用して **install-config.yaml** ファイルを取得し、変更する必要があります。

```
apiVersion: v1
baseDomain: example.com (1)
controlPlane: (2) (3)
  hyperthreading: Enabled (4)
  name: master
  platform:
    ibmcloud: {}
  replicas: 3
compute: (5) (6)
- hyperthreading: Enabled (7)
  name: worker
  platform:
    ibmcloud: {}
  replicas: 3
metadata:
  name: test-cluster (8)
networking:
  clusterNetwork:
```

```
  - cidr: 10.128.0.0/14 9
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16 10
  networkType: OVNKubernetes 11
  serviceNetwork:
  - 172.30.0.0/16
platform:
  ibmcloud:
    region: eu-gb 12
    resourceGroupName: eu-gb-example-network-rg 13
    networkResourceGroupName: eu-gb-example-existing-network-rg 14
    vpcName: eu-gb-example-network-1 15
    controlPlaneSubnets: 16
      - eu-gb-example-network-1-cp-eu-gb-1
      - eu-gb-example-network-1-cp-eu-gb-2
      - eu-gb-example-network-1-cp-eu-gb-3
    computeSubnets: 17
      - eu-gb-example-network-1-compute-eu-gb-1
      - eu-gb-example-network-1-compute-eu-gb-2
      - eu-gb-example-network-1-compute-eu-gb-3
credentialsMode: Manual
publish: Internal 18
pullSecret: '{"auths": ...}' 19
fips: false 20
sshKey: ssh-ed25519 AAAA... 21
```

1 8 12 19 必須。

2 5 これらのパラメーターおよび値を指定しない場合、インストールプログラムはデフォルトの値を指定します。

3 6 **controlPlane** セクションは単一マッピングですが、**compute** セクションはマッピングのシーケンスになります。複数の異なるデータ構造の要件を満たすには、**compute** セクションの最初の行はハイフン **-** で始め、**controlPlane** セクションの最初の行はハイフンで始めることができません。1 つのコントロールプレーンプールのみが使用されます。

4 7 ハイパースレッディングとも呼ばれる同時マルチスレッドを有効または無効にします。デフォルトでは、同時マルチスレッドはマシンのコアのパフォーマンスを上げるために有効化されます。パラメーター値を **Disabled** に設定するとこれを無効にすることができます。一部のクラスターマシンで同時マルチスレッドを無効にする場合は、これをすべてのクラスターマシンで無効にする必要があります。

重要

同時マルチスレッドを無効にする場合は、容量計画においてマシンパフォーマンスの大幅な低下が考慮に入れられていることを確認します。同時マルチスレッドを無効にする場合は、マシンに対して **n1-standard-8** などの大規模なマシンタイプを使用します。

9 マシン CIDR にはコンピュートマシンおよびコントロールプレーンマシンのサブネットが含まれている必要があります。

10 CIDR には、**platform.ibmcloud.controlPlaneSubnets** および **platform.ibmcloud.computeSubnets** で定義されたサブネットが含まれている必要があります。

11 インストールするクラスターネットワークプラグイン。サポートされている値は **OVNKubernetes** と **OpenShiftSDN** です。デフォルトの値は **OVNkubernetes** です。

13 既存のリソースグループの名前。すべての installer-provisioned クラスターリソースは、このリソースグループにデプロイされます。定義されていない場合は、クラスターに新しいリソースグループが作成されます。

14 既存の Virtual Private Cloud (VPC) を含むリソースグループの名前を指定します。既存の VPC およびサブネットはこのリソースグループにある必要があります。クラスターはこの VPC にインストールされます。

15 既存 VPC の名前を指定します。

16 コントロールプレーンマシンをデプロイする既存のサブネット名を指定します。サブネットは、指定した VPC に属している必要があります。リージョン内の各アベイラビリティーゾーンのサブネットを指定します。

17 コンピュートマシンをデプロイする既存のサブネット名を指定します。サブネットは、指定した VPC に属している必要があります。リージョン内の各アベイラビリティーゾーンのサブネットを指定します。

18 クラスターのユーザーに表示されるエンドポイントをパブリッシュする方法。**publish** を **Internal** に設定して、限定公開クラスターをデプロイします。デフォルト値は **External** です。

20 FIPS モードを有効または無効にします。デフォルトでは、FIPS モードは有効にされません。

重要

OpenShift Container Platform 4.13 は Red Hat Enterprise Linux (RHEL) 9.2 をベースにしています。FIPS 検証用に RHEL 9.2 暗号化モジュールがまだ送信されていません。詳細は、4.13 **OpenShift Container Platform リリースノート** の "About this release" を参照してください。

21 オプション: クラスター内のマシンにアクセスするのに使用する **sshKey** 値をオプションで指定できます。

注記

インストールのデバッグまたは障害復旧を実行する必要のある実稼働用の OpenShift Container Platform クラスターでは、**ssh-agent** プロセスが使用する SSH キーを指定します。

7.9.4. インストール時のクラスター全体のプロキシーの設定

実稼働環境では、インターネットへの直接アクセスを拒否し、代わりに HTTP または HTTPS プロキシーを使用することができます。プロキシー設定を **install-config.yaml** ファイルで行うことにより、新規の OpenShift Container Platform クラスターをプロキシーを使用するように設定できます。

前提条件

- 既存の **install-config.yaml** ファイルがある。
- クラスターがアクセスする必要のあるサイトを確認済みで、それらのいずれかがプロキシーをバイパスする必要があるかどうかを判別している。デフォルトで、すべてのクラスター Egress トラフィック (クラスターをホストするクラウドに関するクラウドプロバイダー API に対する呼び出しを含む) はプロキシーされます。プロキシーを必要に応じてバイパスするために、サイトを **Proxy** オブジェクトの **spec.noProxy** フィールドに追加している。

注記

Proxy オブジェクトの **status.noProxy** フィールドには、インストール設定の **networking.machineNetwork[].cidr**、**networking.clusterNetwork[].cidr**、および **networking.serviceNetwork[]** フィールドの値が設定されます。

Amazon Web Services (AWS)、Google Cloud、Microsoft Azure、および Red Hat OpenStack Platform (RHOSP)へのインストールの場合、**Proxy** オブジェクトの **status.noProxy** フィールドには、インスタンスメタデータのエンドポイント(**169.254.169.254**)も設定されます。

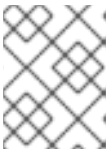
手順

1. **install-config.yaml** ファイルを編集し、プロキシー設定を追加します。以下に例を示します。

```
apiVersion: v1
baseDomain: my.domain.com
proxy:
  httpProxy: http://<username>:<pswd>@<ip>:<port> 1
  httpsProxy: https://<username>:<pswd>@<ip>:<port> 2
  noProxy: example.com 3
additionalTrustBundle: | 4
    -----BEGIN CERTIFICATE-----
    <MY_TRUSTED_CA_CERT>
    -----END CERTIFICATE-----
additionalTrustBundlePolicy: <policy_to_add_additionalTrustBundle> 5
```

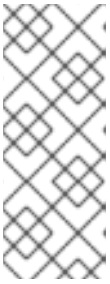
1. クラスター外の HTTP 接続を作成するために使用するプロキシー URL。URL スキームは **http** である必要があります。
2. クラスター外で HTTPS 接続を作成するために使用するプロキシー URL。
3. プロキシーから除外するための宛先ドメイン名、IP アドレス、または他のネットワーク CIDR のコンマ区切りのリスト。サブドメインのみと一致するように、ドメインの前に **.** を付けます。たとえば、**.y.com** は **x.y.com** に一致しますが、**y.com** には一致しません。***** を使用し、すべての宛先のプロキシーをバイパスします。
4. 指定されている場合、インストールプログラムは HTTPS 接続のプロキシーに必要な 1 つ以上の追加の CA 証明書が含まれる **user-ca-bundle** という名前の設定マップを **openshift-config** namespace に生成します。次に Cluster Network Operator は、これらのコンテンツを Red Hat Enterprise Linux CoreOS (RHCOS) 信頼バンドルにマージする **trusted-ca-bundle** 設定マップを作成し、この設定マップは **Proxy** オブジェクトの **trustedCA** フィールドで参照されます。**additionalTrustBundle** フィールドは、プロキシーのアイデンティティー証明書が RHCOS 信頼バンドルからの認証局によって署名されない限り必要になります。

5 オプション: **trustedCA** フィールドの **user-ca-bundle** 設定マップを参照する **Proxy** オブジェクトの設定を決定するポリシー。許可される値は **Proxyonly** および **Always** です。**Proxyonly** を使用して、**http/https** プロキシーが設定されている場合にのみ **user-ca-bundle** 設定マップを参照します。**Always** を使用して、常に **user-ca-bundle** 設定マップを参照します。デフォルト値は **Proxyonly** です。



注記

インストールプログラムは、プロキシーの **readinessEndpoints** フィールドをサポートしません。



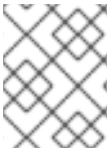
注記

インストーラーがタイムアウトした場合は、インストーラーの **wait-for** コマンドを使用してデプロイメントを再起動してからデプロイメントを完了します。以下に例を示します。

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

2. ファイルを保存し、OpenShift Container Platform のインストール時にこれを参照します。

インストールプログラムは、指定の **install-config.yaml** ファイルのプロキシー設定を使用する **cluster** という名前のクラスター全体のプロキシーを作成します。プロキシー設定が指定されていない場合、**cluster Proxy** オブジェクトが依然として作成されますが、これには **spec** がありません。



注記

cluster という名前の **Proxy** オブジェクトのみがサポートされ、追加のプロキシーを作成することはできません。

7.10. IAM を手動で作成する

クラスターをインストールするには、Cloud Credential Operator (CCO) が手動モードで動作する必要があります。インストールプログラムは CCO を手動モードに設定しますが、クラウドプロバイダーの ID とアクセス管理シークレットを指定する必要があります。

Cloud Credential Operator (CCO) ユーティリティー (**ccoctl**) を使用して、必要な IBM Cloud VPC リソースを作成できます。

前提条件

- **ccoctl** バイナリーを設定している。
- 既存の **install-config.yaml** ファイルがある。

手順

1. **install-config.yaml** 設定ファイルを編集し、**credentialsMode** パラメーターが **Manual** に設定されるようにします。

   サンプル install-config.yaml 設定ファイル

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Manual (1)
compute:
- architecture: amd64
  hyperthreading: Enabled
```

(1) この行は、**credentialsMode** パラメーターを **Manual** に設定するために追加されます。

2. マニフェストを生成するには、インストールプログラムが含まれるディレクトリーから以下のコマンドを実行します。

```
$ ./openshift-install create manifests --dir <installation_directory>
```

3. インストールプログラムが含まれているディレクトリーから、**openshift-install** バイナリーが使用するようにビルドされている OpenShift Container Platform リリースイメージを取得します。

```
$ RELEASE_IMAGE=$(./openshift-install version | awk '/release image/ {print $3}')
```

4. OpenShift Container Platform リリースイメージから **CredentialsRequest** オブジェクトを抽出します。

```
$ oc adm release extract \
  --from=$RELEASE_IMAGE \
  --credentials-requests \
  --cloud=<provider_name> \(1)
  --to=<path_to_credential_requests_directory> (2)
```

(1) プロバイダーの名前。例: **ibmcloud** または **powervs**

(2) 認証情報の要求が保存されるディレクトリー。

このコマンドにより、それぞれの **CredentialsRequest** オブジェクトに YAML ファイルが作成されます。

サンプル CredentialsRequest オブジェクト

```
apiVersion: cloudcredential.openshift.io/v1
kind: CredentialsRequest
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: openshift-image-registry-ibmcos
  namespace: openshift-cloud-credential-operator
spec:
  secretRef:
    name: installer-cloud-credentials
    namespace: openshift-image-registry
  providerSpec:
    apiVersion: cloudcredential.openshift.io/v1
    kind: IBMCloudProviderSpec
```

```
    policies:
    - attributes:
      - name: serviceName
        value: cloud-object-storage
      roles:
      - crn:v1:bluemix:public:iam::::role:Viewer
      - crn:v1:bluemix:public:iam::::role:Operator
      - crn:v1:bluemix:public:iam::::role:Editor
      - crn:v1:bluemix:public:iam::::serviceRole:Reader
      - crn:v1:bluemix:public:iam::::serviceRole:Writer
    - attributes:
      - name: resourceType
        value: resource-group
      roles:
      - crn:v1:bluemix:public:iam::::role:Viewer
```

5. クラスターでクラスター機能を使用して 1 つ以上のオプションコンポーネントを無効にする場合は、無効なコンポーネントの **CredentialsRequest** カスタムリソースを削除します。

IBM Cloud VPC 上の OpenShift Container Platform 4.13 の credrequests ディレクトリーの内容の例

```
0000_26_cloud-controller-manager-operator_15_credentialsrequest-ibm.yaml 1
0000_30_machine-api-operator_00_credentials-request.yaml 2
0000_50_cluster-image-registry-operator_01-registry-credentials-request-ibmcos.yaml 3
0000_50_cluster-ingress-operator_00-ingress-credentials-request.yaml 4
0000_50_cluster-storage-operator_03_credentials_request_ibm.yaml 5
```

1. Cloud Controller Manager Operator CR が必要です。
2. Machine API Operator CR が必要です。
3. Image Registry Operator CR が必要です。
4. Ingress Operator CR が必要です。
5. Storage Operator CR はオプションのコンポーネントであり、クラスターで無効になっている場合があります。

6. 各認証情報リクエストのサービス ID を作成し、定義されたポリシーを割り当て、API キーを作成し、シークレットを生成します。

```
$ ccoctl ibmcloud create-service-id \
  --credentials-requests-dir <path_to_credential_requests_directory> \ 1
  --name <cluster_name> \ 2
  --output-dir <installation_directory> \
  --resource-group-name <resource_group_name> 3
```

1. 認証情報の要求が保存されるディレクトリー。
2. OpenShift Container Platform クラスターの名前。
3. オプション: アクセスポリシーのスコープに使用されるリソースグループの名前。

注記

クラスターで **TechPreviewNoUpgrade** 機能セットによって有効化されたテクノロジープレビュー機能を使用している場合は、**--enable-tech-preview** パラメーターを含める必要があります。

間違ったリソースグループ名が指定された場合、ブートストラップフェーズ中にインストールが失敗します。正しいリソースグループ名を見つけるには、次のコマンドを実行します。

```
$ grep resourceGroupName <installation_directory>/manifests/cluster-infrastructure-02-config.yml
```

検証

- クラスターの **manifests** ディレクトリーに適切なシークレットが生成されていることを確認してください。

7.11. クラスターのデプロイ

互換性のあるクラウドプラットフォームに OpenShift Container Platform をインストールできます。

重要

インストールプログラムの **create cluster** コマンドは、初期インストール時に 1 回だけ実行できます。

前提条件

- クラスターをホストするクラウドプラットフォームでアカウントを設定します。
- OpenShift Container Platform インストールプログラム、およびクラスターのプルシークレットを取得する。
- ホスト上のクラウドプロバイダーアカウントに、クラスターをデプロイするための適切な権限があることを確認してください。アカウントの権限が正しくないと、インストールプロセスが失敗し、不足している権限を示すエラーメッセージが表示されます。

手順

- インストールプログラムが含まれるディレクトリーに切り替え、クラスターのデプロイメントを初期化します。

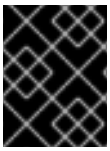
```
$ ./openshift-install create cluster --dir <installation_directory> \ 1
    --log-level=info 2
```

1. **<installation_directory>** に、カスタマイズした **./install-config.yaml** ファイルの場所を指定します。
2. 異なるインストールの詳細情報を表示するには、**info** ではなく、**warn**、**debug**、または **error** を指定します。

検証

クラスターのデプロイが正常に完了すると、次のようになります。

- ターミナルには、Web コンソールへのリンクや **kubeadmin** ユーザーの認証情報など、クラスターにアクセスするための指示が表示されます。
- 認証情報は **<installation_directory>/.openshift_install.log** にも出力されます。



重要

インストールプログラム、またはインストールプログラムが作成するファイルを削除することはできません。これらはいずれもクラスターを削除するために必要になります。

出力例

```
...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/home/myuser/install_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-
console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "password"
INFO Time elapsed: 36m22s
```

重要

- インストールプログラムが生成する Ignition 設定ファイルには、24 時間が経過すると期限切れになり、その後に更新される証明書が含まれます。証明書を更新する前にクラスターが停止し、24 時間経過した後にクラスターを再起動すると、クラスターは期限切れの証明書を自動的に復元します。例外として、kubelet 証明書を回復するために保留状態の **node-bootstrapper** 証明書署名要求 (CSR) を手動で承認する必要があります。詳細は、**コントロールプレーン証明書の期限切れの状態からのリカバリー** に関するドキュメントを参照してください。
- 24 時間証明書はクラスターのインストール後 16 時間から 22 時間にローテーションするため、Ignition 設定ファイルは、生成後 12 時間以内に使用することを推奨します。12 時間以内に Ignition 設定ファイルを使用することにより、インストール中に証明書の更新が実行された場合のインストールの失敗を回避できます。

7.12. バイナリーのダウンロードによる OPENSHIFT CLI のインストール

コマンドラインインターフェイスを使用して OpenShift Container Platform と対話するために CLI (**oc**) をインストールすることができます。**oc** は Linux、Windows、または macOS にインストールできます。

重要

以前のバージョンの **oc** をインストールしている場合、これを使用して OpenShift Container Platform 4.13 のすべてのコマンドを実行することはできません。新規バージョンの **oc** をダウンロードし、インストールします。

Linux への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Linux にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **Product Variant** ドロップダウンリストからアーキテクチャーを選択します。
3. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
4. **OpenShift v4.13 Linux Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
5. アーカイブを展開します。

```
$ tar xvf <file>
```

6. **oc** バイナリーを、**PATH** にあるディレクトリーに配置します。
PATH を確認するには、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

Windows への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを Windows にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 Windows Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。
4. ZIP プログラムでアーカイブを解凍します。
5. **oc** バイナリーを、**PATH** にあるディレクトリーに移動します。
PATH を確認するには、コマンドプロンプトを開いて以下のコマンドを実行します。

```
C:\> path
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
C:\> oc <command>
```

macOS への OpenShift CLI のインストール

以下の手順を使用して、OpenShift CLI (**oc**) バイナリーを macOS にインストールできます。

手順

1. Red Hat カスタマーポータルの OpenShift Container Platform ダウンロードページ に移動します。
2. **バージョン** ドロップダウンリストから適切なバージョンを選択します。
3. **OpenShift v4.13 macOS Client** エントリーの横にある **Download Now** をクリックして、ファイルを保存します。

注記

macOS arm64 の場合は、**OpenShift v4.13 macOS arm64 Client** エントリーを選択します。

4. アーカイブを展開し、解凍します。
5. **oc** バイナリーをパスにあるディレクトリーに移動します。
PATH を確認するには、ターミナルを開き、以下のコマンドを実行します。

```
$ echo $PATH
```

検証

- OpenShift CLI のインストール後に、**oc** コマンドを使用して利用できます。

```
$ oc <command>
```

7.13. CLI の使用によるクラスターへのログイン

クラスター **kubeconfig** ファイルをエクスポートし、デフォルトシステムユーザーとしてクラスターにログインできます。**kubeconfig** ファイルには、クライアントを正しいクラスターおよび API サーバーに接続するために CLI で使用されるクラスターに関する情報が含まれます。このファイルはクラスターに固有のファイルであり、OpenShift Container Platform のインストール時に作成されます。

前提条件

- OpenShift Container Platform クラスターをデプロイしていること。
- **oc** CLI がインストールされている。

手順

1. **kubeadmin** 認証情報をエクスポートします。

```
$ export KUBECONFIG=<installation_directory>/auth/kubeconfig 1
```

1 **<installation_directory>** には、インストールファイルを保存したディレクトリーへのパスを指定します。

2. エクスポートされた設定を使用して、**oc** コマンドを正常に実行できることを確認します。

```
$ oc whoami
```

出力例

```
system:admin
```

関連情報

- Web コンソールへのアクセス

7.14. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス

OpenShift Container Platform 4.13 では、クラスターの健全性および正常に実行された更新についてのメトリクスを提供するためにデフォルトで実行される Telemetry サービスにもインターネットアクセスが必要です。クラスターがインターネットに接続されている場合、Telemetry は自動的に実行され、クラスターは OpenShift Cluster Manager Hybrid Cloud Console に登録されます。

OpenShift Cluster Manager インベントリーが正常である (Telemetry によって自動的に維持、または OpenShift Cluster Manager Hybrid Cloud Console を使用して手動で維持) ことを確認した後に、subscription watch を使用 して、アカウントまたはマルチクラスターレベルで OpenShift Container Platform サブスクリプションを追跡します。

関連情報

- リモートヘルスモニタリングについて

7.15. 次のステップ

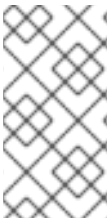
- クラスターをカスタマイズします。
- 必要に応じて、リモートヘルスレポート にすることができます。

第8章 IBM CLOUD VPC でのクラスターのアンインストール

IBM Cloud VPC にデプロイしたクラスターを削除できます。

8.1. インストーラーでプロビジョニングされるインフラストラクチャーを使用するクラスターの削除

installer-provisioned infrastructure を使用するクラスターは、クラウドから削除できます。



注記

アンインストール後に、とくに user-provisioned infrastructure (UPI) クラスターで適切に削除されていないリソースがあるかどうかについて、クラウドプロバイダーを確認します。インストーラーが作成しなかったリソースや、インストーラーがアクセスできないリソースが存在する可能性があります。

前提条件

- クラスターをデプロイするために使用したインストールプログラムのコピーがある。
- クラスター作成時にインストールプログラムが生成したファイルがあります。
- **ccoctl** バイナリーを設定している。
- IBM Cloud CLI をインストールし、VPC インフラストラクチャーサービスプラグインをインストールまたは更新している。詳細は、IBM Cloud VPC CLI ドキュメント の "Prerequisites" を参照してください。

手順

1. 次の条件が満たされている場合、この手順が必要です。
   - インストーラーは、インストールプロセスの一環としてリソースグループを作成しました。
   - クラスターがデプロイされた後、ユーザーまたはお使いのアプリケーションの 1 つが永続ボリューム要求 (PVC) を作成しました。

   この場合、クラスターをアンインストールするときに PVC が削除されないため、リソースグループが正常に削除されない可能性があります。失敗を防ぐには、以下を行います。

   a. CLI を使用して IBM Cloud にログインします。

   b. PVC をリスト表示するには、次のコマンドを実行します。

   ```
   $ ibmcloud is volumes --resource-group-name <infrastructure_id>
   ```

   ボリュームのリストの詳細については、IBM Cloud VPCCLI のドキュメント を参照してください。

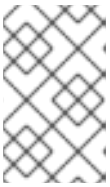
   c. PVC を削除するには、次のコマンドを実行します。

   ```
   $ ibmcloud is volume-delete --force <volume_id>
   ```

ボリュームの削除の詳細については、IBM Cloud VPC CLI のドキュメント を参照してください。

2. インストールプロセスの一環として作成された API キーをエクスポートします。

```
$ export IC_API_KEY=<api_key>
```



注記

変数名は指定どおりに設定する必要があります。インストールプログラムは、クラスターのインストール時に作成されたサービス ID を削除するために、変数名が存在することを想定しています。

3. クラスターをインストールするために使用したコンピューターのインストールプログラムが含まれるディレクトリーから、以下のコマンドを実行します。

```
$ ./openshift-install destroy cluster \
--dir <installation_directory> --log-level info 1 2
```

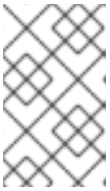
1. **<installation_directory>** には、インストールファイルを保存したディレクトリーへのパスを指定します。
2. 異なる詳細情報を表示するには、**info** ではなく、**warn**、**debug**、または **error** を指定します。

注記

クラスターのクラスター定義ファイルが含まれるディレクトリーを指定する必要があります。クラスターを削除するには、インストールプログラムでこのディレクトリーにある **metadata.json** ファイルが必要になります。

4. クラスター用に作成された手動の CCO クレデンシャルを削除します。

```
$ ccoctl ibmcloud delete-service-id \
    --credentials-requests-dir <path_to_credential_requests_directory> \
    --name <cluster_name>
```



注記

クラスターで **TechPreviewNoUpgrade** 機能セットによって有効化されたテクノロジープレビュー機能を使用している場合は、**--enable-tech-preview** パラメーターを含める必要があります。

5. オプション: **<installation_directory>** ディレクトリーおよび OpenShift Container Platform インストールプログラムを削除します。