OpenShift Container Platform 4.12

Nutanix へのインストール

Nutanix への OpenShift Container Platform のインストール

Last Updated: 2025-11-12

OpenShift Container Platform 4.12 Nutanix へのインストール

Nutanix への OpenShift Container Platform のインストール

Legal Notice

Copyright © 2025 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Abstract

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

Table of Contents

第1章 NUTANIX へのインストールの準備

OpenShift Container Platform クラスターをインストールする前に、Nutanix 環境が以下の要件を満たしていることを確認してください。

1.1. NUTANIX バージョン要件

以下の要件を満たす Nutanix 環境に OpenShift Container Platform クラスターをインストールする必要があります。

表1.1 Nutanix 仮想環境のバージョン要件

コンポーネント	必須バージョン
Nutanix AOS	5.20.4 以降、または 6.5.1 以降
Prism Central	2022.4+

1.2. 環境要件

OpenShift Container Platform クラスターをインストールする前に、以下の Nutanix AOS 環境要件を確認してください。

1.2.1. 必要なアカウント特権

インストールプログラムには、クラスターをデプロイし、その日次の操作を維持するために必要な権限のある Nutanix アカウントへのアクセスが必要です。以下のオプションを使用できます。

- 管理者権限を持つローカル Prism Central ユーザーアカウントを使用できます。ローカルアカウントを使用することは、必要な権限を持つアカウントへのアクセスを許可する最も簡単な方法です。
- 組織のセキュリティーポリシーにより、より制限の厳しい権限セットを使用する必要がある場合は、次の表にリストされている権限を使用して、Prism Central でカスタムの Cloud Native ロールを作成します。その後、Prism Central 認証ディレクトリーのメンバーであるユーザーアカウントにロールを割り当てることができます。エンティティーをロールに割り当てるときは、ユーザーが仮想マシンのデプロイに必要な Prism Element とサブネットのみにアクセスできるようにしてください。
  詳細は、カスタムクラウドネイティブロール の作成と ロールの割り当て に関する Nutanix ドキュメントを参照してください。

例1.1 Custom Cloud Native ロールの作成に必要な権限

Nutanix オブジェクト	Nutanix API で必要な権限	説明

Nutanix オブジェクト	Nutanix API で必要な権限	説明
Categories	**Create_Category_Mapping Create_Or_Update_Name_Category Create_Or_Update_Value_Category Delete_Category_Mapping Delete_Name_Category Delete_Value_Category View_Category_Mapping View_Name_Category View_Value_Category**	OpenShift Container Platform マシンに割り当てられたカテゴリーを作成、読み取り、削除します。
Images	**Create_Image Delete_Image View_Image**	OpenShift Container Platform マシンに使用されるオペレーティングシステムイメージを作成、読み取り、削除します。
仮想マシン	**Create_Virtual_Machine Delete_Virtual_Machine View_Virtual_Machine**	OpenShift Container Platform マシンを作成、読み取り、削除します。
クラスター	**View_Cluster**	OpenShift Container Platform マシンをホストする Prism Element クラスターを表示します。
サブネット	**View_Subnet**	OpenShift Container Platform マシンをホストするサブネットを表示します。

1.2.2. クラスターの制限

利用可能なリソースはクラスターによって異なります。Nutanix 環境内で可能なクラスターの数は、主に、使用可能なストレージスペースと、クラスターが作成するリソースに関連する制限、および IP アドレスやネットワークなど、クラスターをデプロイするために必要なリソースによって制限されます。

1.2.3. クラスターリソース

標準クラスターを使用するには、最低 800 GB のストレージが必要です。

installer-provisioned infrastructure を使用する OpenShift Container Platform クラスターをデプロイする場合、インストールプログラムは Nutanix インスタンスに複数のリソースを作成できる必要があります。これらのリソースは 856 GB のストレージを使用しますが、ブートストラップノードはインストールプロセスの一部として破棄されます。

標準的な OpenShift Container Platform インストールでは、以下のリソースを作成します。

- 1 ラベル

- 仮想マシン:
  - 1 ディスクイメージ
  - 1 一時的ブートストラップノード
  - 3 コントロールプレーンノード
  - 3 コンピュートマシン

1.2.4. ネットワーク要件

ネットワークに AHV IP アドレス管理 (IPAM) を使用し、クラスターマシンに永続的な IP アドレスを提供するように設定されていることを確認する必要があります。さらに、OpenShift Container Platform クラスターをインストールする前に以下のネットワークリソースを作します。

- IP アドレス
- DNS レコード

注記

クラスターの各 OpenShift Container Platform ノードは、DHCP を使用して検出可能な Network Time Protocol (NTP) サーバーにアクセスできることが推奨されます。NTP サーバーなしでインストールが可能です。ただし、NTP サーバーは、非同期サーバークロックに通常関連するエラーを防ぎます。

1.2.4.1. 必要な IP アドレス

installer-provisioned installation には、2 つの静的仮想 IP (VIP) アドレスが必要です。

- API の VIP アドレスが必要です。このアドレスは、クラスター API にアクセスするために使用されます。
- Ingress 用の VIP アドレスが必要です。このアドレスは、クラスターの Ingress トラフィックに使用されます。

これらの IP アドレスは、OpenShift Container Platform クラスターをインストールするときに指定します。

1.2.4.2. DNS レコード

OpenShift Container Platform クラスターをホストする Nutanix インスタンスについて 2 つの静的 IP アドレスの DNS レコードを適切な DNS サーバーに作成する必要があります。各レコードで、**<cluster_name>** はクラスター名で、**<base_domain>** は、クラスターのインストール時に指定するクラスターのベースドメインです。

独自の DNS または DHCP サーバーを使用する場合は、ブートストラップ、コントロールプレーン、コンピュートノードなどの各ノードのレコードも作成する必要があります。

完全な DNS レコードは **<component>.<cluster_name>.<base_domain>.** の形式を取ります。

表1.2 必要な DNS レコード

コンポーネント	レコード	説明
API VIP	**api.<cluster_name>.<base_domain>.**	この DNS A/AAAA または CNAME レコードは、コントロールプレーンマシンのロードバランサーを参照する必要があります。このレコードは、クラスター外のクライアントおよびクラスター内のすべてのノードで解決できる必要があります。
Ingress VIP	***.apps.<cluster_name>.<base_domain>.**	Ingress ルーター Pod を実行するマシンをターゲットにするロードバランサーを参照するワイルドカード DNS A/AAAA または CNAME レコードです。このレコードは、クラスター外のクライアントおよびクラスター内のすべてのノードで解決できる必要があります。

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

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。Nutanix にクラスターをインストールするには、インストールプロセスの一部として CCO を **manual** モードに設定する必要があります。

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** を使用する準備ができていることを確認するには、次のコマンドを実行してヘルプファイルを表示します。

```
$ ccoctl --help
```

ccoctl --help の出力

```
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

- 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2章 クラスターの NUTANIX へのインストール

OpenShift Container Platform バージョン 4.20 では、次のいずれかの方法を選択して、Nutanix インスタンスにクラスターをインストールできます。

installer-provisioned infrastructure の使用: installer-provisioned infrastructure を使用するには、次のセクションの手順を使用します。installer-provisioned infrastructure は、接続されたネットワーク環境または切断されたネットワーク環境でのインストールに最適です。installer-provisioned infrastructure には、クラスターの基礎となるインフラストラクチャーをプロビジョニングするインストールプログラムが含まれています。

Assisted Installer の使用: Assisted Installer は console.redhat.com でホストされます。Assisted Installer は、切断された環境では使用できません。Assisted Installer はクラスターの基礎となるインフラストラクチャーをプロビジョニングしないため、Assisted Installer を実行する前にインフラストラクチャーをプロビジョニングする必要があります。Assisted Installer を使用してインストールすると、Nutanix との統合も提供され、自動スケーリングが可能になります。詳細は、Assisted Installer を使用したオンプレミスクラスターのインストール を参照してください。

user-provisioned infrastructure の使用: 任意のプラットフォームへのクラスターのインストール ドキュメントに概説されている関連手順を完了します。

2.1. 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た。
- インストールプログラムで、Prism Central および Prism Element のポート 9440 にアクセスできる。ポート 9440 にアクセスできることを確認した。
- ファイアウォールを使用している場合は、次の前提条件を満たしている。
  - ポート 9440 にアクセスできることを確認した。コントロールプレーンノードがポート 9440 で Prism Central および Prism Element にアクセスできる (インストールが成功するために必要)。
  - OpenShift Container Platform が必要とするサイトへの アクセスを許可する ようにファイアウォールを設定した。これには、Telemetry の使用が含まれます。
- Nutanix 環境でデフォルトの自己署名 SSL 証明書を使用している場合は、CA によって署名された証明書に置き換える。インストールプログラムには、Prism Central API にアクセスするための有効な CA 署名付き証明書が必要です。自己署名証明書の置き換えに関する詳細は、Nutanix AOS Security Guide を参照してください。
  Nutanix 環境で内部 CA を使用して証明書を発行する場合は、インストールプロセスの一部としてクラスター全体のプロキシーを設定する必要があります。詳細は、カスタム PKI の設定 を参照してください。

  重要

  2048 ビット証明書を使用します。Prism Central 2022.x で 4096 ビット証明書を使用すると、インストールに失敗します。

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

OpenShift Container Platform 4.12 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。

2.3. PRISM CENTRAL のインターネットアクセス

Prism Central では、クラスターのインストールに必要な Red Hat Enterprise Linux CoreOS (RHCOS) イメージを取得するためにインターネットアクセスが必要です。Nutanix の RHCOS イメージは、**rhcos.mirror.openshift.com** で入手できます。

2.4. 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。

鍵がノードに渡されたら、鍵ペアを使用して、**core** ユーザーとして RHCOS ノードに SSH 接続できます。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。

注記

FIPS で検証済みまたは進行中のモジュール (Modules in Process) 暗号ライブラリーを使用する OpenShift Container Platform クラスターを **x86_64**、**ppc64le**、および **s390x** アーキテクチャーにインストールする予定の場合は、**ed25519** アルゴリズムを使用するキーは作成しないでください。代わりに、**rsa** アルゴリズムまたは **ecdsa** アルゴリズムを使用するキーを作成します。

2. SSH 公開鍵を表示します。

```
$ 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
```

注記

クラスターが FIPS モードにある場合は、FIPS 準拠のアルゴリズムのみを使用して SSH キーを生成します。鍵は RSA または ECDSA のいずれかである必要があります。

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。

2.5. 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。

2.6. NUTANIX ROOT CA 証明書をシステム信頼に追加する

インストールプログラムは Prism Central API へのアクセスを必要とするため、OpenShift Container Platform クラスターをインストールする前に、Nutanix の信頼された root CA 証明書をシステム信頼に追加する必要があります。

手順

1. Prism Central Web コンソールから、Nutanix root CA 証明書をダウンロードします。
2. Nutanix root CA 証明書を含む圧縮ファイルを抽出します。
3. オペレーティングシステム用のファイルをシステム信頼に追加します。たとえば、Fedora オペレーティングシステムで以下のコマンドを実行します。

```
# cp certs/lin/* /etc/pki/ca-trust/source/anchors
```

4. システム信頼を更新します。たとえば、Fedora オペレーティングシステムで以下のコマンドを実行します。

```
# update-ca-trust extract
```

2.7. インストール設定ファイルの作成

Nutanix 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。
- Nutanix のネットワーク要件を満たしていることを確認する。詳細については、Nutanix へのインストールの準備を参照してください。

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。

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 **nutanix** を選択します。

iii. Prism Central のドメイン名または IP アドレスを入力します。

iv. Prism Central へのログインに使用するポートを入力します。

v. Prism Central へのログインに使用する認証情報を入力します。
インストールプログラムが Prism Central に接続します。

vi. OpenShift Container Platform クラスターを管理する Prism Element を選択します。

vii. 使用するネットワークサブネットを選択します。

viii. コントロールプレーン API のアクセス用に設定した仮想 IP アドレスを入力します。

ix. クラスター Ingress に設定した仮想 IP アドレスを入力します。

x. ベースドメインを入力します。このベースドメインは、DNS レコードで設定したものと同じである必要があります。

xi. クラスターの記述名を入力します。入力するクラスター名は、DNS レコードの設定時に指定したクラスター名と一致する必要があります。

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

2. オプション: **install.config.yaml** ファイル内の 1 つ以上のデフォルト設定パラメーターを更新して、インストールをカスタマイズします。
パラメーターの詳細については、インストール設定パラメーター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。

2.7.1. 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。

注記

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。

2.7.1.1. 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2.1 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。

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。	小文字いちぶハイフン (**-**) の文字列 (**dev** など)。
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**、**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>

2.7.1.2. 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2.2 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。
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、全 Linux ネットワーク用の 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 以外のすべてのプラットフォームでは、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。	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。

2.7.1.3. 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2.3 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る際にも使用できます。	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
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
compute	コンピュートノードを設定するマシンの設定。	**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 **amd64** (デフォルト) です。	文字列

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**、**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設定するマシンの設定。	**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 **amd64** (デフォルト) です。	文字列
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**、**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。モードを指定しないと、CCO は指定された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 (**""**)。

パラメーター	説明	値
fips	FIPS モードを有効または無効にします。デフォルトは **false** (無効) です。FIPS モードが有効にされている場合、OpenShift Container Platform が実行される Red Hat Enterprise Linux CoreOS (RHCOS) マシンがデフォルトの Kubernetes 暗号スイートをバイパスし、代わりに RHCOS で提供される暗号モジュールを使用します。 **重要** クラスターで FIPS モードを有効にするには、FIPS モードで動作するように設定された Red Hat Enterprise Linux (RHEL) コンピューターからインストールプログラムを実行する必要があります。RHEL での FIPS モードの設定の詳細は、FIPS モードでのシステムのインストール を参照してください。FIPS 検証済み/Modules In Process 暗号ライブラリーの使用は、**x86_64**、**ppc64le**、および **s390x** アーキテクチャー上の OpenShift Container Platform デプロイメントでのみサポートされます。 **注記** Azure File ストレージを使用している場合、FIPS モードを有効にすることはできません。	**false** または **true**
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。

パラメーター	説明	値
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。
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**。デフォルト値は **External** です。 このパラメーターを **Internal** に設定することは、クラウド以外のプラットフォームではサポートされません。 **重要** フィールドの値が **Internal** に設定されている場合、クラスターは機能しなくなります。詳細は、BZ#1953035 を参照してください。
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。

2.7.1.4. 追加の Nutanix 設定パラメーター

追加の Nutanix 設定パラメーターは、次の表で説明します。

表2.4 追加の Nutanix クラスターパラメーター

パラメーター	説明	値
platform.nutanix.apiVIP	コントロールプレーン API のアクセス用に設定した仮想 IP (VIP) アドレス。	IP アドレス
platform.nutanix.ingressVIP	クラスター Ingress に設定した仮想 IP (VIP) アドレス。	IP アドレス
platform.nutanix.prismCentral.endpoint.address	Prism Central ドメイン名または IP アドレス。	文字列
platform.nutanix.prismCentral.endpoint.port	Prism Central へのログインに使用されるポート。	文字列
platform.nutanix.prismCentral.password	Prism Central ユーザー名のパスワード。	文字列
platform.nutanix.prismCentral.username	Prism Central へのログインに使用されるユーザー名。	文字列
platform.nutanix.prismElments.endpoint.address	Prism Element ドメイン名または IP アドレス。[1]	文字列
platform.nutanix.prismElments.endpoint.port	Prism Element へのログインに使用されるポート。	文字列
platform.nutanix.prismElements.uuid	Prism Element の Universally Unique Identifier (UUID)。	文字列
platform.nutanix.subnetUUIDs	設定した仮想 IP アドレスと DNS レコードを含む Prism Element ネットワークの UUID。[2]	文字列
platform.nutanix.clusterOSImage	オプション: デフォルトでは、インストールプログラムは Red Hat Enterprise Linux CoreOS (RHCOS) イメージをダウンロードしてインストールします。Prism Central がインターネットにアクセスできない場合は、任意の HTTP サーバーで RHCOS イメージをホストし、インストールプログラムがそのイメージを指すようにすることで、デフォルトの動作をオーバーライドできます。	HTTP または HTTPS の URL (オプションで SHA-256 形式のチェックサムを使用)。例: http://example.com/images/rhcos-47.83.202103221318-0-nutanix.x86_64.qcow2

1. **prismElements** セクションには、Prism Elements (クラスター) のリストが含まれています。Prism Element は、OpenShift Container Platform クラスターをホストするために使用されるすべての Nutanix リソース (仮想マシンやサブネットなど) を包含します。サポートされている Prism Element は 1 つだけです。

2. OpenShift Container Platform クラスターごとに 1 つのサブネットのみがサポートされます。

2.7.2. Nutanix 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関する詳細を指定するか、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、これを変更する必要があります。

```
apiVersion: v1
baseDomain: example.com 1
compute: 2
- hyperthreading: Enabled 3
  name: worker
  replicas: 3
  platform:
    nutanix: 4
      cpus: 2
      coresPerSocket: 2
      memoryMiB: 8196
      osDisk:
        diskSizeGiB: 120
controlPlane: 5
  hyperthreading: Enabled 6
  name: master
  replicas: 3
  platform:
    nutanix: 7
      cpus: 4
      coresPerSocket: 2
      memoryMiB: 16384
      osDisk:
        diskSizeGiB: 120
metadata:
  creationTimestamp: null
  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
```

```yaml
platform:
  nutanix:
    apiVIP: 10.40.142.7 10
    ingressVIP: 10.40.142.8 11
    prismCentral:
      endpoint:
        address: your.prismcentral.domainname 12
        port: 9440 13
      password: <password> 14
      username: <username> 15
    prismElements:
    - endpoint:
        address: your.prismelement.domainname
        port: 9440
      uuid: 0005b0f1-8f43-a0f2-02b7-3cecef193712
    subnetUUIDs:
    - c7938dc6-7659-453e-a688-e26020c68e43
    clusterOSImage: http://example.com/images/rhcos-47.83.202103221318-0-nutanix.x86_64.qcow2
16
credentialsMode: Manual
publish: External
pullSecret: '{"auths": ...}' 17
fips: false 18
sshKey: ssh-ed25519 AAAA... 19
```

1 8 10 11 12 13 14 15 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 **controlPlane** セクションは単一マッピングですが、コンピュート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。どちらのセクションも、現時点では単一のマシンプールを定義しますが、OpenShift Container Platform の今後のバージョンでは、インストール時の複数のコンピュートプールの定義をサポートする可能性があります。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。

3 6 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。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。

4 7 オプション: コンピュートおよびコントロールプレーンマシンのマシンプールパラメーターの追加設定を指定します。

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。

16 オプション: デフォルトでは、インストールプログラムは Red Hat Enterprise Linux CoreOS (RHCOS) イメージをダウンロードしてインストールします。Prism Central がインターネットにア

クセスできない場合は、任意の HTTP サーバーで RHCOS イメージをホストし、インストールプログラムがそのイメージを指すようにすることで、デフォルトの動作をオーバーライドできます。

18 FIPS モードを有効または無効にするかどうか。デフォルトでは、FIPS モードは有効にされません。FIPS モードが有効にされている場合、OpenShift Container Platform が実行される Red Hat Enterprise Linux CoreOS (RHCOS) マシンがデフォルトの Kubernetes 暗号スイートをバイパスし、代わりに RHCOS で提供される暗号モジュールを使用します。

重要

FIPS 検証済みまたは Modules in Process 暗号ライブラリーの使用は、**x86_64**、**ppc64le**、および **s390x** アーキテクチャー上の OpenShift Container Platform デプロイメントでのみサポートされます。

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。

2.7.3. 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。

2.8. 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 4.12 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 v4.12 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 v4.12 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 v4.12 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 v4.12 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>
```

2.9. NUTANIX の IAM の設定

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が手動モード用に CCO を設定する間、ID およびアクセス管理シークレットを指定する必要があります。

前提条件

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

手順

1. 認証情報データを含む YAML ファイルを次の形式で作成します。

   認証情報データの形式

   ```
   credentials:
   - type: basic_auth (1)
     data:
       prismCentral: (2)
         username: <username_for_prism_central>
         password: <password_for_prism_central>
       prismElements: (3)
       - name: <name_of_prism_element>
         username: <username_for_prism_element>
         password: <password_for_prism_element>
   ```

   (1) 認証タイプを指定します。Basic 認証のみがサポートされています。

   (2) Prism Central の認証情報を指定します。

   (3) オプション: Prism Element 認証情報を指定します。

2. 次のコマンドを実行して、インストールファイルのリリースイメージを **$RELEASE_IMAGE** 変数に設定します。

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

3. 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 **CredentialsRequest** カスタムリソース (CR) のリストを抽出します。

   ```
   $ oc adm release extract \
     --from=$RELEASE_IMAGE \
     --credentials-requests \
     --cloud=nutanix \
     --to=<path_to_directory_with_list_of_credentials_requests>/credrequests (1)
   ```

1. コンポーネント **CredentialsRequests** オブジェクトのファイルを含むディレクトリーへのパスを指定します。指定したディレクトリーが存在しない場合は、このコマンドによって作成されます。

サンプル CredentialsRequest オブジェクト

```
apiVersion: cloudcredential.openshift.io/v1
kind: CredentialsRequest
metadata:
  annotations:
    include.release.openshift.io/self-managed-high-availability: "true"
  labels:
    controller-tools.k8s.io: "1.0"
  name: openshift-machine-api-nutanix
  namespace: openshift-cloud-credential-operator
spec:
  providerSpec:
    apiVersion: cloudcredential.openshift.io/v1
    kind: NutanixProviderSpec
  secretRef:
    name: nutanix-credentials
    namespace: openshift-machine-api
```

4. 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。

Nutanix 上の OpenShift Container Platform 4.12 の credrequests ディレクトリーの内容の例

```
0000_30_machine-api-operator_00_credentials-request.yaml (1)
```

1. Machine API Operator CR が必要です。

5. 次のコマンドを実行し、**ccoctl** ツールを使用して **credrequests** ディレクトリー内のすべての **CredentialsRequest** オブジェクトを処理します。

```
$ ccoctl nutanix create-shared-secrets \
--credentials-requests-dir=<path_to_directory_with_list_of_credentials_requests>/credrequests \ (1)
--output-dir=<ccoctl_output_dir> \ (2)
--credentials-source-filepath=<path_to_credentials_file> (3)
```

1. コンポーネント **CredentialsRequests** オブジェクトのファイルを含むディレクトリーへのパスを指定します。
2. **manifests** ディレクトリーの下に、コンポーネント認証情報シークレットのファイルを含むディレクトリーを指定します。デフォルトでは、**ccoctl** ツールは、コマンドが実行されるディレクトリーにオブジェクトを作成します。オブジェクトを別のディレクトリーに作成するには、**--output-dir** フラグを使用します。
3. オプション: 認証情報データ YAML ファイルを含むディレクトリーを指定します。デフォルトでは、**ccoctl** はこのファイルが **<home_directory>/.nutanix/credentials** にあると想

定します。別のディレクトリーを指定するには、**--credentials-source-filepath** フラグを使用します。

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

サンプル install-config.yaml 設定ファイル

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Manual 1
...
```

1 この行を追加して、**credentialsMode** パラメーターを **Manual** に設定します。

7. 次のコマンドを実行して、インストールマニフェストを作成します。

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

1 クラスターの **install-config.yaml** ファイルを含むディレクトリーへのパスを指定します。

8. 次のコマンドを実行して、生成された認証情報ファイルをターゲットマニフェストディレクトリーにコピーします。

```
$ cp <ccoctl_output_dir>/manifests/*credentials.yaml ./<installation_directory>/manifests
```

検証

- **manifests** ディレクトリーに適切なシークレットが存在することを確認します。

```
$ ls ./<installation_directory>/manifests
```

出力例

```
total 64
-rw-r----- 1 <user> <user> 2335 Jul  8 12:22 cluster-config.yaml
-rw-r----- 1 <user> <user>  161 Jul  8 12:22 cluster-dns-02-config.yml
-rw-r----- 1 <user> <user>  864 Jul  8 12:22 cluster-infrastructure-02-config.yml
-rw-r----- 1 <user> <user>  191 Jul  8 12:22 cluster-ingress-02-config.yml
-rw-r----- 1 <user> <user> 9607 Jul  8 12:22 cluster-network-01-crd.yml
-rw-r----- 1 <user> <user>  272 Jul  8 12:22 cluster-network-02-config.yml
-rw-r----- 1 <user> <user>  142 Jul  8 12:22 cluster-proxy-01-config.yaml
-rw-r----- 1 <user> <user>  171 Jul  8 12:22 cluster-scheduler-02-config.yml
-rw-r----- 1 <user> <user>  200 Jul  8 12:22 cvo-overrides.yaml
-rw-r----- 1 <user> <user>  118 Jul  8 12:22 kube-cloud-config.yaml
-rw-r----- 1 <user> <user> 1304 Jul  8 12:22 kube-system-configmap-root-ca.yaml
-rw-r----- 1 <user> <user> 4090 Jul  8 12:22 machine-config-server-tls-secret.yaml
-rw-r----- 1 <user> <user> 3961 Jul  8 12:22 openshift-config-secret-pull-secret.yaml
-rw------- 1 <user> <user>  283 Jul  8 12:24 openshift-machine-api-nutanix-credentials-
credentials.yaml
```

2.10. 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

- 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。

注記

ホストに設定した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十分なパーミッションがない場合、インストールプロセスは停止し、不足しているパーミッションが表示されます。

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。

2.11. デフォルトのストレージコンテナーの設定

クラスターをインストールしたら、Nutanix CSI Operator をインストールし、クラスターのデフォルトのストレージコンテナーを設定する必要があります。

詳細は、CSI Operator のインストール と レジストリーストレージの設定 に関する Nutanix のドキュメントを参照してください。

2.12. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス

OpenShift Container Platform 4.12 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。

2.13. 関連情報

- リモートヘルスモニタリングについて

2.14. 次のステップ

- リモートヘルスレポート
- クラスターのカスタマイズ

第3章 ネットワークが制限された環境での NUTANIX へのクラスターのインストール

OpenShift Container Platform 4.12 では、インストールリリースコンテンツの内部ミラーを作成して、ネットワークが制限された環境の Nutanix 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。

3.1. 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た。
- インストールプログラムで、Prism Central および Prism Element のポート 9440 にアクセスできる。ポート 9440 にアクセスできることを確認した。
- ファイアウォールを使用している場合は、次の前提条件を満たしている。
  - ポート 9440 にアクセスできることを確認した。コントロールプレーンノードがポート 9440 で Prism Central および Prism Element にアクセスできる (インストールが成功するために必要)。
  - OpenShift Container Platform が必要とするサイトへの アクセスを許可する ようにファイアウォールを設定した。これには、Telemetry の使用が含まれます。
- Nutanix 環境でデフォルトの自己署名 SSL/TLS 証明書を使用している場合は、CA によって署名された証明書に置き換える。インストールプログラムには、Prism Central API にアクセスするための有効な CA 署名付き証明書が必要です。自己署名証明書の置き換えに関する詳細は、Nutanix AOS Security Guide を参照してください。
  Nutanix 環境で内部 CA を使用して証明書を発行する場合は、インストールプロセスの一部としてクラスター全体のプロキシーを設定する必要があります。詳細は、カスタム PKI の設定 を参照してください。

  重要

  2048 ビット証明書を使用します。Prism Central 2022.x で 4096 ビット証明書を使用すると、インストールに失敗します。

- Red Hat Quay などのコンテナーイメージレジストリーがある。レジストリーがまだない場合は、**Red Hat OpenShift のミラーレジストリー** を使用してミラーレジストリーを作成できます。
- oc-mirror OpenShift CLI (oc) プラグイン を使用して、必要なすべての OpenShift Container Platform コンテンツと、Nutanix CSI Operator を含むその他のイメージをミラーレジストリーにミラーリングした。

  重要

  インストールメディアはミラーホストにあるため、そのコンピューターを使用してすべてのインストール手順を完了することができます。

3.2. ネットワークが制限された環境でのインストールについて

OpenShift Container Platform 4.12 では、ソフトウェアコンポーネントを取得するためにインターネットへのアクティブな接続を必要としないインストールを実行できます。ネットワークが制限された環境

のインストールは、クラスターのインストール先となるクラウドプラットフォームに応じて、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またはユーザーによって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して実行できます。

クラウドプラットフォーム上でネットワークが制限されたインストールの実行を選択した場合でも、そのクラウド API へのアクセスが必要になります。Amazon Web Service の Route 53 DNS や IAM サービスなどの一部のクラウド機能には、インターネットアクセスが必要です。ネットワークによっては、ベアメタルハードウェア、Nutanix、または VMware vSphere へのインストールに必要なインターネットアクセスが少なくて済む場合があります。

ネットワークが制限されたインストールを完了するには、OpenShift イメージレジストリーのコンテンツをミラーリングし、インストールメディアを含むレジストリーを作成する必要があります。このミラーは、インターネットと制限されたネットワークの両方にアクセスできるミラーホストで、または制限に対応する他の方法を使用して作成できます。

3.2.1. その他の制限

ネットワークが制限された環境のクラスターには、以下の追加の制限および制約があります。

- **ClusterVersion** ステータスには **Unable to retrieve available updates** エラーが含まれます。
- デフォルトでは、必要なイメージストリームタグにアクセスできないため、開発者カタログのコンテンツは使用できません。

3.3. 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。

鍵がノードに渡されたら、鍵ペアを使用して、**core** ユーザーとして RHCOS ノードに SSH 接続できます。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。

注記

FIPS で検証済みまたは進行中のモジュール (Modules in Process) 暗号ライブラリーを使用する OpenShift Container Platform クラスターを **x86_64**、**ppc64le**、および **s390x** アーキテクチャーにインストールする予定の場合は、**ed25519** アルゴリズムを使用するキーは作成しないでください。代わりに、**rsa** アルゴリズムまたは **ecdsa** アルゴリズムを使用するキーを作成します。

2. SSH 公開鍵を表示します。

```
$ 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
```

注記

クラスターが FIPS モードにある場合は、FIPS 準拠のアルゴリズムのみを使用して SSH キーを生成します。鍵は RSA または ECDSA のいずれかである必要があります。

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。

3.4. NUTANIX ROOT CA 証明書をシステム信頼に追加する

インストールプログラムは Prism Central API へのアクセスを必要とするため、OpenShift Container Platform クラスターをインストールする前に、Nutanix の信頼された root CA 証明書をシステム信頼に追加する必要があります。

手順

1. Prism Central Web コンソールから、Nutanix root CA 証明書をダウンロードします。
2. Nutanix root CA 証明書を含む圧縮ファイルを抽出します。
3. オペレーティングシステム用のファイルをシステム信頼に追加します。たとえば、Fedora オペレーティングシステムで以下のコマンドを実行します。

```
# cp certs/lin/* /etc/pki/ca-trust/source/anchors
```

4. システム信頼を更新します。たとえば、Fedora オペレーティングシステムで以下のコマンドを実行します。

```
# update-ca-trust extract
```

3.5. RHCOS クラスターイメージのダウンロード

Prism Central は、クラスターをインストールするために Red Hat Enterprise Linux CoreOS (RHCOS) イメージにアクセスする必要があります。インストールプログラムを使用して、RHCOS イメージを見つけてダウンロードし、内部 HTTP サーバーまたは Nutanix オブジェクトを介して利用できるようにすることができます。

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。ネットワークが制限されたインストールでは、これらのファイルがミラーホスト上に置かれます。

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、以下のコマンドを実行します。

```
$ ./openshift-install coreos print-stream-json
```

2. コマンドの出力を使用して Nutanix イメージの場所を見つけ、リンクをクリックしてダウンロードします。

出力例

```
"nutanix": {
  "release": "411.86.202210041459-0",
  "formats": {
    "qcow2": {
      "disk": {
        "location": "https://rhcos.mirror.openshift.com/art/storage/releases/rhcos-4.11/411.86.202210041459-0/x86_64/rhcos-411.86.202210041459-0-nutanix.x86_64.qcow2",
        "sha256": "42e227cac6f11ac37ee8a2f9528bb3665146566890577fd55f9b950949e5a54b"
```

3. 内部 HTTP サーバーまたは Nutanix オブジェクトを介してイメージを利用できるようにします。

4. ダウンロードしたイメージの場所に注意してください。クラスターをデプロイする前に、インストール設定ファイル (**install-config.yaml**) の **platform** セクションをイメージの場所で更新します。

RHCOS イメージを指定する install-config.yaml ファイルのスニペット

```
platform:
  nutanix:
    clusterOSImage: http://example.com/images/rhcos-411.86.202210041459-0-nutanix.x86_64.qcow2
```

3.6. インストール設定ファイルの作成

Nutanix 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。ネットワークが制限されたインストールでは、これらのファイルがミラーホスト上に置かれます。
- レジストリーをミラーリングしたときに作成された **imageContentSourcePolicy.yaml** ファイルを用意する。
- ダウンロードした Red Hat Enterprise Linux CoreOS (RHCOS) イメージの場所を用意する。
- ミラーレジストリーの証明書の内容を取得する。
- Red Hat Enterprise Linux CoreOS (RHCOS) イメージを取得し、これをアクセス可能な場所にアップロードする。
- Nutanix のネットワーク要件を満たしていることを確認する。詳細については、Nutanix へのインストールの準備を参照してください。

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。

   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 **nutanix** を選択します。

      iii. Prism Central のドメイン名または IP アドレスを入力します。

      iv. Prism Central へのログインに使用するポートを入力します。

      v. Prism Central へのログインに使用する認証情報を入力します。
      インストールプログラムが Prism Central に接続します。

      vi. OpenShift Container Platform クラスターを管理する Prism Element を選択します。

      vii. 使用するネットワークサブネットを選択します。

      viii. コントロールプレーン API のアクセス用に設定した仮想 IP アドレスを入力します。

      ix. クラスター Ingress に設定した仮想 IP アドレスを入力します。

      x. ベースドメインを入力します。このベースドメインは、DNS レコードで設定したものと同じである必要があります。

xi. クラスターの記述名を入力します。入力するクラスター名は、DNS レコードの設定時に指定したクラスター名と一致する必要があります。

xii. 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** ファイルで、**platform.nutanix.clusterOSImage** の値をイメージの場所または名前に設定します。以下に例を示します。

```
platform:
  nutanix:
      clusterOSImage: http://mirror.example.com/images/rhcos-47.83.202103221318-0-nutanix.x86_64.qcow2
```

3. **install-config.yaml** ファイルを編集し、ネットワークが制限された環境でのインストールに必要な追加の情報を提供します。

   a. **pullSecret** の値を更新して、レジストリーの認証情報を追加します。

   ```
   pullSecret: '{"auths":{"<mirror_host_name>:5000": {"auth": "<credentials>","email": "you@example.com"}}}'
   ```

   <mirror_host_name> の場合、ミラーレジストリーの証明書で指定したレジストリードメイン名を指定し、**<credentials>** の場合は、ミラーレジストリーの base64 でエンコードされたユーザー名およびパスワードを指定します。

   b. **additionalTrustBundle** パラメーターおよび値を追加します。

   ```
   additionalTrustBundle: |
     -----BEGIN CERTIFICATE-----

   ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
     -----END CERTIFICATE-----
   ```

   この値は、ミラーレジストリーに使用した証明書ファイルの内容である必要があります。証明書ファイルは、既存の信頼できる認証局、またはミラーレジストリー用に生成した自己署名証明書のいずれかです。

   c. 次の YAML の抜粋のようなイメージコンテンツリソースを追加します。

   ```
   imageContentSources:
   - mirrors:
     - <mirror_host_name>:5000/<repo_name>/release
     source: quay.io/openshift-release-dev/ocp-release
   - mirrors:
     - <mirror_host_name>:5000/<repo_name>/release
     source: registry.redhat.io/ocp/release
   ```

   これらの値には、レジストリーをミラーリングしたときに作成された **imageContentSourcePolicy.yaml** ファイルを使用します。

4. オプション: **install.config.yaml** ファイル内の 1 つ以上のデフォルト設定パラメーターを更新して、インストールをカスタマイズします。
パラメーターの詳細については、インストール設定パラメーターを参照してください。

5. **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。

3.6.1. 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。

注記

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。

3.6.1.1. 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3.1 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。

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。	小文字いちぶハイフン (**-**) の文字列 (**dev** など)。
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**、**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。	`{ "auths":{ "cloud.openshift.com":{ "auth":"b3Blb=", "email":"you@example.com" }, "quay.io":{ "auth":"b3Blb=", "email":"you@example.com" } } }`

3.6.1.2. 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3.2 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。
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、全 Linux ネットワーク用の 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 以外のすべてのプラットフォームでは、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。	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。

3.6.1.3. 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3.3 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る際にも使用できます。	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
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
compute	コンピュートノードを設定するマシンの設定。	**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 **amd64** (デフォルト) です。	文字列

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**、**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設定するマシンの設定。	**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 **amd64** (デフォルト) です。	文字列
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**、**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。モードを指定しないと、CCO は指定された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 (**""**)。
fips	FIPS モードを有効または無効にします。デフォルトは **false** (無効) です。FIPS モードが有効にされている場合、OpenShift Container Platform が実行される Red Hat Enterprise Linux CoreOS (RHCOS) マシンがデフォルトの Kubernetes 暗号スイートをバイパスし、代わりに RHCOS で提供される暗号モジュールを使用します。	**false** または **true**

パラメーター	説明	値
	重要 クラスターで FIPS モードを有効にするには、FIPS モードで動作するように設定された Red Hat Enterprise Linux (RHEL) コンピューターからインストールプログラムを実行する必要があります。RHEL での FIPS モードの設定の詳細は、[FIPS モードでのシステムのインストール](#) を参照してください。FIPS 検証済み/Modules In Process 暗号ライブラリーの使用は、**x86_64**、**ppc64le**、および **s390x** アーキテクチャー上の OpenShift Container Platform デプロイメントでのみサポートされます。 **注記** Azure File ストレージを使用している場合、FIPS モードを有効にすることはできません。	
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**。デフォルト値は **External** です。 このパラメーターを **Internal** に設定することは、クラウド以外のプラットフォームではサポートされません。 **重要** フィールドの値が **Internal** に設定されている場合、クラスターは機能しなくなります。詳細は、BZ#1953035 を参照してください。
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。

3.6.1.4. 追加の Nutanix 設定パラメーター

追加の Nutanix 設定パラメーターは、次の表で説明します。

表3.4 追加の Nutanix クラスターパラメーター

パラメーター	説明	値
platform.nutanix.apiVIP	コントロールプレーン API のアクセス用に設定した仮想 IP (VIP) アドレス。	IP アドレス
platform.nutanix.ingressVIP	クラスター Ingress に設定した仮想 IP (VIP) アドレス。	IP アドレス

パラメーター	説明	値
platform.nutanix.prismCentral.endpoint.address	Prism Central ドメイン名または IP アドレス。	文字列
platform.nutanix.prismCentral.endpoint.port	Prism Central へのログインに使用されるポート。	文字列
platform.nutanix.prismCentral.password	Prism Central ユーザー名のパスワード。	文字列
platform.nutanix.prismCentral.username	Prism Central へのログインに使用されるユーザー名。	文字列
platform.nutanix.prismElments.endpoint.address	Prism Element ドメイン名または IP アドレス。[1]	文字列
platform.nutanix.prismElments.endpoint.port	Prism Element へのログインに使用されるポート。	文字列
platform.nutanix.prismElements.uuid	Prism Element の Universally Unique Identifier (UUID)。	文字列
platform.nutanix.subnetUUIDs	設定した仮想 IP アドレスと DNS レコードを含む Prism Element ネットワークの UUID。[2]	文字列
platform.nutanix.clusterOSImage	オプション: デフォルトでは、インストールプログラムは Red Hat Enterprise Linux CoreOS (RHCOS) イメージをダウンロードしてインストールします。Prism Central がインターネットにアクセスできない場合は、任意の HTTP サーバーで RHCOS イメージをホストし、インストールプログラムがそのイメージを指すようにすることで、デフォルトの動作をオーバーライドできます。	HTTP または HTTPS の URL (オプションで SHA-256 形式のチェックサムを使用)。例: http://example.com/images/rhcos-47.83.202103221318-0-nutanix.x86_64.qcow2

1. **prismElements** セクションには、Prism Elements (クラスター) のリストが含まれています。Prism Element は、OpenShift Container Platform クラスターをホストするために使用されるすべての Nutanix リソース (仮想マシンやサブネットなど) を包含します。サポートされている Prism Element は 1 つだけです。

2. OpenShift Container Platform クラスターごとに 1 つのサブネットのみがサポートされます。

3.6.2. Nutanix 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関する詳細を指定するか、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、これを変更する必要があります。

```
apiVersion: v1
baseDomain: example.com 1
compute: 2
- hyperthreading: Enabled 3
  name: worker
  replicas: 3
  platform:
    nutanix: 4
      cpus: 2
      coresPerSocket: 2
      memoryMiB: 8196
      osDisk:
        diskSizeGiB: 120
controlPlane: 5
  hyperthreading: Enabled 6
  name: master
  replicas: 3
  platform:
    nutanix: 7
      cpus: 4
      coresPerSocket: 2
      memoryMiB: 16384
      osDisk:
        diskSizeGiB: 120
metadata:
  creationTimestamp: null
  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:
  nutanix:
    apiVIP: 10.40.142.7 10
    ingressVIP: 10.40.142.8 11
    prismCentral:
      endpoint:
        address: your.prismcentral.domainname 12
```

```
      port: 9440 13
    password: <password> 14
    username: <username> 15
  prismElements:
  - endpoint:
      address: your.prismelement.domainname
      port: 9440
    uuid: 0005b0f1-8f43-a0f2-02b7-3cecef193712
  subnetUUIDs:
  - c7938dc6-7659-453e-a688-e26020c68e43
  clusterOSImage: http://example.com/images/rhcos-47.83.202103221318-0-nutanix.x86_64.qcow2
16
credentialsMode: Manual
publish: External
pullSecret: '{"auths":{"<local_registry>": {"auth": "<credentials>","email": "you@example.com"}}}' 17
fips: false 18
sshKey: ssh-ed25519 AAAA... 19
additionalTrustBundle: | 20
  -----BEGIN CERTIFICATE-----
  ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
  -----END CERTIFICATE-----
imageContentSources: 21
- mirrors:
  - <local_registry>/<local_repository_name>/release
  source: quay.io/openshift-release-dev/ocp-release
- mirrors:
  - <local_registry>/<local_repository_name>/release
  source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
```

1 8 10 11 12 13 14 15 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 **controlPlane** セクションは単一マッピングですが、コンピュート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。どちらのセクションも、現時点では単一のマシンプールを定義しますが、OpenShift Container Platform の今後のバージョンでは、インストール時の複数のコンピュートプールの定義をサポートする可能性があります。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。

3 6 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。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。

4 7 オプション: コンピュートおよびコントロールプレーンマシンのマシンプールパラメーターの追加設定を指定します。

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。

16 オプション: デフォルトでは、インストールプログラムは Red Hat Enterprise Linux CoreOS (RHCOS) イメージをダウンロードしてインストールします。Prism Central がインターネットにアクセスできない場合は、任意の HTTP サーバーまたは Nutanix オブジェクトで RHCOS イメージをホストし、インストールプログラムがそのイメージを指すようにすることで、デフォルトの動作をオーバーライドできます。

17 **<local_registry>** には、レジストリードメイン名と、ミラーレジストリーがコンテンツを提供するために使用するポートをオプションで指定します。例: **registry.example.com** または **registry.example.com:5000<credentials>** に、ミラーレジストリーの base64 でエンコードされたユーザー名およびパスワードを指定します。

18 FIPS モードを有効または無効にするかどうか。デフォルトでは、FIPS モードは有効にされません。FIPS モードが有効にされている場合、OpenShift Container Platform が実行される Red Hat Enterprise Linux CoreOS (RHCOS) マシンがデフォルトの Kubernetes 暗号スイートをバイパスし、代わりに RHCOS で提供される暗号モジュールを使用します。

重要

FIPS 検証済みまたは Modules in Process 暗号ライブラリーの使用は、**x86_64**、**ppc64le**、および **s390x** アーキテクチャー上の OpenShift Container Platform デプロイメントでのみサポートされます。

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。

20 ミラーレジストリーに使用した証明書ファイルの内容を指定します。

21 レジストリーをミラーリングしたときに作成された **imageContentSourcePolicy.yaml** ファイルの **metadata.name: release-0** セクションからこれらの値を指定します。

3.6.3. 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。

3.7. 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 4.12 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 v4.12 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 v4.12 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 v4.12 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 v4.12 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>
```

3.8. NUTANIX の IAM の設定

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が手動モード用に CCO を設定する間、ID およびアクセス管理シークレットを指定する必要があります。

前提条件

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

手順

1. 認証情報データを含む YAML ファイルを次の形式で作成します。

認証情報データの形式

```
credentials:
- type: basic_auth 1
  data:
    prismCentral: 2
      username: <username_for_prism_central>
      password: <password_for_prism_central>
    prismElements: 3
    - name: <name_of_prism_element>
      username: <username_for_prism_element>
      password: <password_for_prism_element>
```

1 認証タイプを指定します。Basic 認証のみがサポートされています。

2 Prism Central の認証情報を指定します。

3 オプション: Prism Element 認証情報を指定します。

2. 次のコマンドを実行して、インストールファイルのリリースイメージを **$RELEASE_IMAGE** 変数に設定します。

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

3. 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 **CredentialsRequest** カスタムリソース (CR) のリストを抽出します。

```
$ oc adm release extract \
  --from=$RELEASE_IMAGE \
  --credentials-requests \
  --cloud=nutanix \
  --to=<path_to_directory_with_list_of_credentials_requests>/credrequests 1
```

1 コンポーネント **CredentialsRequests** オブジェクトのファイルを含むディレクトリーへのパスを指定します。指定したディレクトリーが存在しない場合は、このコマンドによって作成されます。

サンプル CredentialsRequest オブジェクト

```
  apiVersion: cloudcredential.openshift.io/v1
  kind: CredentialsRequest
  metadata:
    annotations:
      include.release.openshift.io/self-managed-high-availability: "true"
    labels:
      controller-tools.k8s.io: "1.0"
    name: openshift-machine-api-nutanix
    namespace: openshift-cloud-credential-operator
  spec:
    providerSpec:
      apiVersion: cloudcredential.openshift.io/v1
      kind: NutanixProviderSpec
    secretRef:
      name: nutanix-credentials
      namespace: openshift-machine-api
```

4. 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。

Nutanix 上の OpenShift Container Platform 4.12 の credrequests ディレクトリーの内容の例

```
0000_30_machine-api-operator_00_credentials-request.yaml 1
```

1 Machine API Operator CR が必要です。

5. 次のコマンドを実行し、**ccoctl** ツールを使用して **credrequests** ディレクトリー内のすべての **CredentialsRequest** オブジェクトを処理します。

```
$ ccoctl nutanix create-shared-secrets \
```

```
--credentials-requests-dir=
<path_to_directory_with_list_of_credentials_requests>/credrequests \ 1
--output-dir=<ccoctl_output_dir> \ 2
--credentials-source-filepath=<path_to_credentials_file> 3
```

1. コンポーネント **CredentialsRequests** オブジェクトのファイルを含むディレクトリーへのパスを指定します。
2. **manifests** ディレクトリーの下に、コンポーネント認証情報シークレットのファイルを含むディレクトリーを指定します。デフォルトでは、**ccoctl** ツールは、コマンドが実行されるディレクトリーにオブジェクトを作成します。オブジェクトを別のディレクトリーに作成するには、**--output-dir** フラグを使用します。
3. オプション: 認証情報データ YAML ファイルを含むディレクトリーを指定します。デフォルトでは、**ccoctl** はこのファイルが **<home_directory>/.nutanix/credentials** にあると想定します。別のディレクトリーを指定するには、**--credentials-source-filepath** フラグを使用します。

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

サンプル install-config.yaml 設定ファイル

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Manual 1
...
```

1. この行を追加して、**credentialsMode** パラメーターを **Manual** に設定します。

7. 次のコマンドを実行して、インストールマニフェストを作成します。

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

1. クラスターの **install-config.yaml** ファイルを含むディレクトリーへのパスを指定します。

8. 次のコマンドを実行して、生成された認証情報ファイルをターゲットマニフェストディレクトリーにコピーします。

```
$ cp <ccoctl_output_dir>/manifests/*credentials.yaml ./<installation_directory>/manifests
```

検証

- **manifests** ディレクトリーに適切なシークレットが存在することを確認します。

```
$ ls ./<installation_directory>/manifests
```

出力例

```
total 64
```

```
-rw-r----- 1 <user> <user> 2335 Jul  8 12:22 cluster-config.yaml
-rw-r----- 1 <user> <user>  161 Jul  8 12:22 cluster-dns-02-config.yml
-rw-r----- 1 <user> <user>  864 Jul  8 12:22 cluster-infrastructure-02-config.yml
-rw-r----- 1 <user> <user>  191 Jul  8 12:22 cluster-ingress-02-config.yml
-rw-r----- 1 <user> <user> 9607 Jul  8 12:22 cluster-network-01-crd.yml
-rw-r----- 1 <user> <user>  272 Jul  8 12:22 cluster-network-02-config.yml
-rw-r----- 1 <user> <user>  142 Jul  8 12:22 cluster-proxy-01-config.yaml
-rw-r----- 1 <user> <user>  171 Jul  8 12:22 cluster-scheduler-02-config.yml
-rw-r----- 1 <user> <user>  200 Jul  8 12:22 cvo-overrides.yaml
-rw-r----- 1 <user> <user>  118 Jul  8 12:22 kube-cloud-config.yaml
-rw-r----- 1 <user> <user> 1304 Jul  8 12:22 kube-system-configmap-root-ca.yaml
-rw-r----- 1 <user> <user> 4090 Jul  8 12:22 machine-config-server-tls-secret.yaml
-rw-r----- 1 <user> <user> 3961 Jul  8 12:22 openshift-config-secret-pull-secret.yaml
-rw------- 1 <user> <user>  283 Jul  8 12:24 openshift-machine-api-nutanix-credentials-credentials.yaml
```

3.9. 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

- 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。

注記

ホストに設定した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十分なパーミッションがない場合、インストールプロセスは停止し、不足しているパーミッションが表示されます。

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。

3.10. インストール後の設定

以下の手順を実行して、クラスターの設定を完了します。

3.10.1. デフォルトの OperatorHub カタログソースの無効化

Red Hat によって提供されるコンテンツを調達する Operator カタログおよびコミュニティープロジェクトは、OpenShift Container Platform のインストール時にデフォルトで OperatorHub に設定されます。ネットワークが制限された環境では、クラスター管理者としてデフォルトのカタログを無効にする必要があります。

手順

- **disableAllDefaultSources: true** を **OperatorHub** オブジェクトに追加して、デフォルトカタログのソースを無効にします。

```
$ oc patch OperatorHub cluster --type json \
    -p '[{"op": "add", "path": "/spec/disableAllDefaultSources", "value": true}]'
```

ヒント

または、Web コンソールを使用してカタログソースを管理できます。**Administration → Cluster Settings → Configuration → OperatorHub** ページから、**Sources** タブをクリックして、個別のソースを作成、更新、削除、無効化、有効化できます。

3.10.2. クラスターへのポリシーリソースのインストール

oc-mirror OpenShift CLI (oc) プラグインを使用して OpenShift Container Platform コンテンツをミラーリングすると、**catalogSource-certified-operator-index.yaml** および **imageContentSourcePolicy.yaml** を含むリソースが作成されます。

- **ImageContentSourcePolicy** リソースは、ミラーレジストリーをソースレジストリーに関連付け、イメージプル要求をオンラインレジストリーからミラーレジストリーにリダイレクトします。
- **CatalogSource** リソースは、Operator Lifecycle Manager (OLM) によって使用され、ミラーレジストリーで使用可能な Operator に関する情報を取得します。これにより、ユーザーは Operator を検出してインストールできます。

クラスターをインストールしたら、これらのリソースをクラスターにインストールする必要があります。

前提条件

- 非接続環境で、イメージセットをレジストリーミラーにミラーリングしました。
- **cluster-admin** ロールを持つユーザーとしてクラスターにアクセスできる。

手順

1. **cluster-admin** ロールを持つユーザーとして OpenShift CLI にログインします。
2. results ディレクトリーからクラスターに YAML ファイルを適用します。

```
$ oc apply -f ./oc-mirror-workspace/results-<id>/
```

検証

1. **ImageContentSourcePolicy** リソースが正常にインストールされたことを確認します。

```
$ oc get imagecontentsourcepolicy
```

2. **CatalogSource** リソースが正常にインストールされたことを確認します。

```
$ oc get catalogsource --all-namespaces
```

3.10.3. デフォルトのストレージコンテナーの設定

クラスターをインストールしたら、Nutanix CSI Operator をインストールし、クラスターのデフォルトのストレージコンテナーを設定する必要があります。

詳細は、CSI Operator のインストール と レジストリーストレージの設定 に関する Nutanix のドキュメントを参照してください。

3.11. OPENSHIFT CONTAINER PLATFORM の TELEMETRY アクセス

OpenShift Container Platform 4.12 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。

3.12. 関連情報

- リモートヘルスモニタリングについて

3.13. 次のステップ

- 必要に応じて、リモートヘルスレポート を参照してください。
- 必要に応じて、非接続クラスターの登録 を参照してください。
- クラスターのカスタマイズ

第4章 NUTANIX でのクラスターのアンインストール

Nutanix にデプロイしたクラスターを削除できます。

4.1. INSTALLER-PROVISIONED INFRASTRUCTURE を使用するクラスターの削除

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、とくにユーザーによってプロビジョニングされるインフラストラクチャー (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。インストールプログラムが作成しなかったリソース、またはインストールプログラム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。

手順

1. クラスターのインストールに使用したコンピューターで、インストールプログラムを含むディレクトリーに移動し、次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。

2. 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。