



# Red Hat Advanced Cluster Management for Kubernetes 2.7

## ネットワーク

ネットワークの詳細について



ネットワークの詳細について

## 法律上の通知

Copyright © 2023 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

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

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

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

Node.js<sup>®</sup> 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<sup>®</sup> 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.

## 概要

ネットワークの詳細について

目次

第1章 ネットワーク .....	3
1.1. ハブクラスターのネットワーク設定	3
1.2. マネージドクラスターのネットワーク設定	5
1.3. 高度なネットワーク設定	7



## 第1章 ネットワーク

ここでは、ハブクラスターとマネージドクラスターの両方のネットワーク要件について説明します。

- [ハブクラスターのネットワーク設定](#)
- [マネージドクラスターのネットワーク設定](#)
- [高度なネットワーク設定](#)

### 1.1. ハブクラスターのネットワーク設定

**重要:** 信頼された CA バンドルは Red Hat Advanced Cluster Management の namespace で利用できませんが、その拡張にはネットワークへの変更が必要です。信頼できる CA バンドル ConfigMap は、**trusted-ca-bundle** のデフォルト名を使用します。この名前は、**TRUSTED\_CA\_BUNDLE** という名前の環境変数で Operator に提供すると、変更できます。詳細は、Red Hat OpenShift Container Platform の [ネットワーク](#) セクションで [クラスター全体のプロキシの設定](#) を参照してください。

ハブクラスターネットワークの設定を参照できます。

#### 1.1.1. ハブクラスターのネットワーク設定表

次の表でハブクラスターネットワーク要件を参照してください。

方向	プロトコル	接続	ポート (指定されている場合)	送信元アドレス	宛先アドレス
マネージドクラスターへのアウトバウンド	HTTPS	マネージドクラスターの Pod のログを Search コンソールから動的に取得し、マネージドクラスターで実行している <b>klusterlet-addon-workmgr</b> サービスを使用します。	443	なし	マネージドクラスタールートにアクセスするための IP アドレス
マネージドクラスターへのアウトバウンド	HTTPS	klusterlet をインストールするためにインストール時にプロビジョニングされるマネージドクラスターの Kubernetes API サーバー	6443	なし	Kubernetes マネージドクラスター API サーバーの IP

方向	プロトコル	接続	ポート (指定されている場合)	送信元アドレス	宛先アドレス
チャンネルソースへの送信	HTTPS	アプリケーションライフサイクル、OpenShift GitOps、または ArgoCD を使用して接続する場合にのみ必要となる、GitHub、Object Store、および Helm リポジトリを含むチャンネルソース	443	なし	チャンネルソースの IP
マネージドクラスターからの受信	HTTPS	メトリクスおよびアラートをプッシュするマネージドクラスターは、OpenShift Container Platform バージョン 4.8 以降を実行するマネージドクラスターに対してのみアラートが収集されます	443	なし	ハブクラスターアクセスルートへの IP アドレス
マネージドクラスターからの受信	HTTPS	マネージドクラスターからの変更を監視するハブクラスターの Kubernetes API サーバー	6443	なし	ハブクラスター Kubernetes API サーバーの IP アドレス
ObjectStore へのアウトバウンド	HTTPS	Cluster Backup Operator の実行時に、長期保存用の可観測性メトリクスデータを送信します	443	なし	ObjectStore の IP アドレス



方向	プロトコル	接続	ポート (指定されている場合)	送信元アドレス	宛先アドレス
イメージリポジトリへのアウトバウンド	HTTPS	OpenShift Container Platform および Red Hat Advanced Cluster Management のイメージにアクセスします	443	なし	イメージリポジトリの IP アドレス

## 1.2. マネージドクラスターのネットワーク設定

マネージドクラスターネットワークの設定を参照できます。

### 1.2.1. マネージドクラスターのネットワーク設定表

次の表でマネージドクラスターネットワーク要件を参照してください。

方向	プロトコル	接続	ポート (指定されている場合)	送信元アドレス	宛先アドレス
ハブクラスターからの受信	HTTPS	マネージドクラスターの Pod の Search コンソールからログを動的に送信するには、マネージドクラスターで実行している <b>klusterlet-addon-workmgr</b> サービスを使用します。	443	なし	マネージドクラスタールートにアクセスするための IP アドレス

方向	プロトコル	接続	ポート (指定されている場合)	送信元アドレス	宛先アドレス
ハブクラスターからの受信	HTTPS	klusterlet をインストールするためにインストール時にプロビジョニングされるマネージドクラスターの Kubernetes API サーバー	6443	なし	Kubernetes マネージドクラスター API サーバーの IP
イメージリポジトリへのアウトバウンド	HTTPS	OpenShift Container Platform および Red Hat Advanced Cluster Management のイメージにアクセスします	443	なし	イメージリポジトリの IP アドレス
ハブクラスターへの送信	HTTPS	メトリクスおよびアラートをプッシュするマネージドクラスターは、OpenShift Container Platform バージョン 4.8 以降を実行するマネージドクラスターに対してのみアラートが収集されます	443	なし	ハブクラスターアクセスルートへの IP アドレス
ハブクラスターへの送信	HTTPS	ハブクラスターの Kubernetes API サーバーで変更の有無を監視します	6443	なし	ハブクラスター Kubernetes API サーバーの IP アドレス

方向	プロトコル	接続	ポート (指定されている場合)	送信元アドレス	宛先アドレス
チャンネルソースへの送信	HTTPS	アプリケーションライフサイクル、OpenShift GitOps、または ArgoCD を使用して接続する場合にのみ必要となる、GitHub、Object Store、および Helm リポジトリを含むチャンネルソース	443	なし	チャンネルソースの IP

### 1.3. 高度なネットワーク設定

- [Infrastructure Operator の追加のネットワーク要件表](#)
- [Submariner のネットワーク要件表](#)
- [Hive テーブルの追加のネットワーク要件表](#)
- [ホストされたコントロールプレーンのネットワーク要件表 \(テクノロジープレビュー\)](#)
- [アプリケーションデプロイメントのネットワーク要件表](#)
- [namespace 接続のネットワーク要件表](#)

#### 1.3.1. Infrastructure Operator の追加のネットワーク要件表

Infrastructure Operator を使用してベアメタルマネージドクラスターをインストールする場合は、以下の表で追加のネットワーク要件を参照してください。

方向	プロトコル	接続	ポート (指定されている場合)
単一ノードの OpenShift Container Platform マネージドクラスターでの BMC インターフェイスへのハブクラスター送信	HTTPS (非接続環境では HTTP)	OpenShift Container Platform クラスターをブートします	443
OpenShift Container Platform マネージドクラスターからハブクラスターへの送信	HTTPS	<b>assistedService</b> ルートを使用してハードウェア情報を報告します	443

### 1.3.2. Submariner のネットワーク要件表

Submariner を使用するクラスターに対して、ポートを 3 つ開放する必要があります。以下の表は、どのポートを使用できるかを示しています。

方向	プロトコル	接続	ポート (指定されている場合)
送信および受信	UDP	各マネージドクラスター	4800
送信および受信	UDP	各マネージドクラスター	4500、500、およびゲートウェイノード上の IPsec トラフィックに使用されるその他のポート
受信	TCP	各マネージドクラスター	8080

### 1.3.3. Hive テーブルの追加のネットワーク要件表

Central Infrastructure Management の使用が含まれる Hive Operator を使用してベアメタルマネージドクラスターをインストールする場合は、ハブクラスターと **libvirt** プロビジョニングホスト間で、レイヤー 2 またはレイヤー 3 のポート接続を設定する必要があります。プロビジョニングホストへのこの接続は、Hive を使用したベースベアメタルクラスターの作成時に必要になります。詳細は、以下の表を参照してください。

方向	プロトコル	接続	ポート (指定されている場合)
<b>libvirt</b> プロビジョニングホストへのハブクラスターの送信および受信	IP	Hive Operator がインストールされているハブクラスターを、ベアメタルクラスターの作成時にブートストラップとして機能する <b>libvirt</b> プロビジョニングホストに接続します。	

**注記:**これらの要件はインストール時にのみ適用され、Infrastructure Operator でインストールされたクラスターのアップグレード時には必要ありません。

### 1.3.4. ホストされたコントロールプレーンのネットワーク要件表 (テクノロジープレビュー)

ホストされたコントロールプレーンを使用する場合、**HypershiftDeployment** リソースには、次の表に示すエンドポイントへの接続が必要です。

方向	接続	ポート (指定されている場合)
----	----	-----------------

方向	接続	ポート (指定されている場合)
Outbound	OpenShift Container Platform コントロールプレーンおよびワーカーノード	
Outbound	Amazon Web Services のホストされたクラスターのみ: AWS API および S3 API へのアウトバウンド接続	
Outbound	Microsoft Azure クラウドサービスのホストされたクラスターのみ: Azure API へのアウトバウンド接続	
Outbound	coreOS の ISO イメージと OpenShift Container Platform Pod のイメージレジストリーを格納する OpenShift Container Platform イメージリポジトリ	
Outbound	ホスティングクラスター上の klusterlet のローカル API クライアントは、HyperShift がホストするクラスターの API と通信します。	

### 1.3.5. アプリケーションデプロイメントのネットワーク要件表

一般的なアプリケーションのデプロイメント通信は、マネージドクラスターからハブクラスターへの一方向です。接続では、マネージドクラスターのエージェントによって設定される **kubeconfig** を使用します。マネージドクラスターでのアプリケーションデプロイメントは、ハブクラスターの以下の namespace にアクセスする必要があります。

- チャネルリソースの namespace
- マネージドクラスターの namespace

### 1.3.6. namespace 接続のネットワーク要件表

- アプリケーションライフサイクル接続:
  - namespace の **open-cluster-management** は、ポート 4000 のコンソール API にアクセスする必要があります。
  - namespace の **open-cluster-management** は、ポート 3001 でアプリケーション UI を公開する必要があります。
- アプリケーションライフサイクルバックエンドコンポーネント (Pod):  
ハブクラスターでは、す以下の Pod を含む **open-cluster-management** namespace にすべてのアプリケーションライフサイクル Pod がインストールされます。

- multicluster-operators-hub-subscription
- multicluster-operators-standalone-subscription
- multicluster-operators-channel
- multicluster-operators-application
- multicluster-integrations

これらの Pod が **open-cluster-management** namespace に作成されると、以下のようになります。

- namespace の **open-cluster-management** は、ポート 6443 で Kube API にアクセスする必要があります。

マネージドクラスターでは、**klusterlet-addon-appmgr** アプリケーションライフサイクル Pod のみが **open-cluster-management-agent-addon** namespace にインストールされます。

- namespace **open-cluster-management-agent-addon** は、ポート 6443 で Kube API にアクセスする必要があります。

- ガバナンスおよびリスク:

ハブクラスターでは、以下のアクセスが必要です。

- namespace **open-cluster-management** は、ポート 6443 で Kube API にアクセスする必要があります。
- namespace **open-cluster-management** は、ポート 5353 で OpenShift DNS にアクセスする必要があります。

マネージドクラスターでは、以下のアクセスが必要です。

- namespace **open-cluster-management-addon** は、ポート 6443 の Kube API にアクセスする必要があります。