



Red Hat Advanced Cluster Management for Kubernetes 2.7

Networking

[Read more to learn about networking.](#)

Red Hat Advanced Cluster Management for Kubernetes 2.7 Networking

[Read more to learn about networking.](#)

Legal Notice

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[®] 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

Read more to learn about networking.

Table of Contents

CHAPTER 1. NETWORKING	3
1.1. HUB CLUSTER NETWORK CONFIGURATION	3
1.1.1. Hub cluster network configuration table	3
1.2. MANAGED CLUSTER NETWORK CONFIGURATION	5
1.2.1. Managed cluster network configuration table	5
1.3. ADVANCED NETWORK CONFIGURATION	6
1.3.1. Additional networking requirements for infrastructure operator table	7
1.3.2. Submariner networking requirements table	7
1.3.3. Additional networking requirements for Hive table	7
1.3.4. Hosted control planes networking requirements table (Technology Preview)	8
1.3.5. Application deployment network requirements table	8
1.3.6. Namespace connection network requirements table	9

CHAPTER 1. NETWORKING

Learn about network requirements for both the hub cluster and the managed cluster.

- [Hub cluster network configuration](#)
- [Managed cluster network configuration](#)
- [Advanced network configuration](#)

1.1. HUB CLUSTER NETWORK CONFIGURATION

Important: The trusted CA bundle is available in the Red Hat Advanced Cluster Management namespace, but that enhancement requires changes to your network. The trusted CA bundle ConfigMap uses the default name of **trusted-ca-bundle**. You can change this name by providing it to the operator in an environment variable named **TRUSTED_CA_BUNDLE**. See [Configuring the cluster-wide proxy](#) in the *Networking* section of Red Hat OpenShift Container Platform for more information.

You can refer to the configuration for your hub cluster network.

1.1.1. Hub cluster network configuration table

See the hub cluster network requirements in the following table:

Direction	Protocol	Connection	Port (if specified)	Source address	Destination address
Outbound to the managed cluster	HTTPS	Retrieval of logs dynamically from Search console for the pods of the managed cluster, uses the klusterlet-addon-workmgr service that is running on the managed cluster	443	None	IP address to access managed cluster route
Outbound to the managed cluster	HTTPS	Kubernetes API server of the managed cluster that is provisioned during installation to install the klusterlet	6443	None	IP of Kubernetes managed cluster API server

Direction	Protocol	Connection	Port (if specified)	Source address	Destination address
Outbound to the channel source	HTTPS	The channel source, including GitHub, Object Store, and Helm repository, which is only required when you are using Application lifecycle, OpenShift GitOps, or ArgoCD to connect	443	None	IP of the channel source
Inbound from the managed cluster	HTTPS	Managed cluster to push metrics and alerts that are gathered only for managed clusters that are running OpenShift Container Platform version 4.8, or later	443	None	IP address to hub cluster access route
Inbound from the managed cluster	HTTPS	Kubernetes API Server of hub cluster that is watched for changes from the managed cluster	6443	None	IP address of hub cluster Kubernetes API Server
Outbound to the ObjectStore	HTTPS	Sends Observability metric data for long term storage when the Cluster Backup Operator is running	443	None	IP address of ObjectStore

Direction	Protocol	Connection	Port (if specified)	Source address	Destination address
Outbound to the image repository	HTTPS	Access images for OpenShift Container Platform and Red Hat Advanced Cluster Management	443	None	IP address of image repository

1.2. MANAGED CLUSTER NETWORK CONFIGURATION

You can refer to the configuration for your managed cluster network.

1.2.1. Managed cluster network configuration table

See the managed cluster network requirements in the following table:

Direction	Protocol	Connection	Port (if specified)	Source address	Destination address
Inbound from the hub cluster	HTTPS	Sending of logs dynamically from Search console for the pods of the managed cluster, uses the klusterlet-addon-workmgr service that is running on the managed cluster	443	None	IP address to access managed cluster route
Inbound from the hub cluster	HTTPS	Kubernetes API server of the managed cluster that is provisioned during installation to install the klusterlet	6443	None	IP of Kubernetes managed cluster API server

Direction	Protocol	Connection	Port (if specified)	Source address	Destination address
Outbound to the image repository	HTTPS	Access images for OpenShift Container Platform and Red Hat Advanced Cluster Management	443	None	IP address of image repository
Outbound to the hub cluster	HTTPS	Managed cluster to push metrics and alerts that are gathered only for managed clusters that are running OpenShift Container Platform version 4.8, or later	443	None	IP address to hub cluster access route
Outbound to the hub cluster	HTTPS	Watches the Kubernetes API server of the hub cluster for changes	6443	None	IP address of hub cluster Kubernetes API Server
Outbound to the channel source	HTTPS	The channel source, including GitHub, Object Store, and Helm repository, which is only required when you are using Application lifecycle, OpenShift GitOps, or ArgoCD to connect	443	None	IP of the channel source

1.3. ADVANCED NETWORK CONFIGURATION

- [Additional networking requirements for infrastructure operator table](#)
- [Submariner networking requirements table](#)
- [Additional networking requirements for Hive table](#)
- [Hosted control planes networking requirements table \(Technology Preview\)](#)
- [Application deployment network requirements table](#)
- [Namespace connection network requirements table](#)

1.3.1. Additional networking requirements for infrastructure operator table

When you are installing bare metal managed clusters with the Infrastructure Operator, see the following table for the additional networking requirements:

Direction	Protocol	Connection	Port (if specified)
Hub cluster outbound to BMC interface at single node OpenShift Container Platform managed cluster	HTTPS (HTTP in disconnected environment)	Boot the OpenShift Container Platform cluster	443
Outbound from the OpenShift Container Platform managed cluster to the hub cluster	HTTPS	Reports hardware information using the assistedService route	443

1.3.2. Submariner networking requirements table

Clusters that are using Submariner require three open ports. The following table shows which ports you might use:

Direction	Protocol	Connection	Port (if specified)
Outbound and inbound	UDP	Each of the managed clusters	4800
Outbound and inbound	UDP	Each of the managed clusters	4500, 500, and any other ports that are used for IPSec traffic on the gateway nodes
Inbound	TCP	Each of the managed clusters	8080

1.3.3. Additional networking requirements for Hive table

When you are installing bare metal managed clusters with the Hive Operator, which includes using Central Infrastructure Management, you must configure a layer 2 or layer 3 port connection between the hub cluster and the **libvirt** provisioning host. This connection to the provisioning host is required during the creation of a bare metal cluster with Hive. See the following table for more information:

Direction	Protocol	Connection	Port (if specified)
Hub cluster outbound and inbound to the libvirt provisioning host	IP	Connects the hub cluster, where the Hive operator is installed, to the libvirt provisioning host that serves as a bootstrap when creating the bare metal cluster	

Note: These requirements only apply when installing, and are not required when upgrading clusters that were installed with Infrastructure Operator.

1.3.4. Hosted control planes networking requirements table (Technology Preview)

When you use hosted control planes, the **HypershiftDeployment** resource must have connectivity to the endpoints listed in the following table:

Direction	Connection	Port (if specified)
Outbound	OpenShift Container Platform control-plane and worker nodes	
Outbound	For hosted clusters on Amazon Web Services only: Outbound connection to AWS API and S3 API	
Outbound	For hosted clusters on Microsoft Azure cloud services only: Outbound connection to Azure API	
Outbound	OpenShift Container Platform image repositories that store the ISO images of the coreOS and the image registry for OpenShift Container Platform pods	
Outbound	Local API client of the klusterlet on the hosting cluster communicates with the API of the HyperShift hosted cluster	

1.3.5. Application deployment network requirements table

In general, the application deployment communication is one way from a managed cluster to the hub cluster. The connection uses **kubeconfig**, which is configured by the agent on the managed cluster. The application deployment on the managed cluster needs to access the following namespaces on the hub cluster:

- The namespace of the channel resource
- The namespace of the managed cluster

1.3.6. Namespace connection network requirements table

- Application lifecycle connections:
 - The namespace **open-cluster-management** needs to access the console API on port 4000.
 - The namespace **open-cluster-management** needs to expose the Application UI on port 3001.

- Application lifecycle backend components (pods):
On the hub cluster, all of the application lifecycle pods are installed in the **open-cluster-management** namespace, including the following pods:

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

As a result of these pods being in the **open-cluster-management** namespace:

- The namespace **open-cluster-management** needs to access the Kube API on port 6443.

On the managed cluster, only the **klusterlet-addon-appmgr** application lifecycle pod is installed in the **open-cluster-management-agent-addon** namespace:

- The namespace **open-cluster-management-agent-addon** needs to access the Kube API on port 6443.

- Governance and risk:
On the hub cluster, the following access is required:

- The namespace **open-cluster-management** needs to access the Kube API on port 6443.
- The namespace **open-cluster-management** needs to access the OpenShift DNS on port 5353.

On the managed cluster, the following access is required:

- The namespace **open-cluster-management-addon** needs to access the Kube API on port 6443.

