Red Hat Advanced Cluster Management for Kubernetes 2.7

网络

了解更多信息以了解更多有关网络的信息。

Last Updated: 2024-09-05

Red Hat Advanced Cluster Management for Kubernetes 2.7 网络

了解更多信息以了解更多有关网络的信息。

法律通告

摘要

了解更多信息以了解更多有关网络的信息。

目录

第 1 章 网络

了解 hub 集群和受管集群的网络要求。

- hub 集群网络配置
- 受管集群网络配置
- 高级网络配置

1.1. HUB 集群网络配置

重要：可信 CA 捆绑包在 Red Hat Advanced Cluster Management 命名空间中可用，但该增强需要更改您的网络。可信 CA 捆绑包 ConfigMap 使用 **trusted-ca-bundle** 的默认名称。您可以通过在名为 **TRUSTED_CA_BUNDLE** 的环境变量中提供 Operator 来更改此名称。如需更多信息，请参阅 Red Hat OpenShift Container Platform 的*网络*部分中的配置集群范围代理。

您可以引用 hub 集群网络的配置。

1.1.1. hub 集群网络配置表

请参阅下表中的 hub 集群网络要求：

方向	协议	连接	端口（如果指定）	源地址	目标地址
出站到受管集群	HTTPS	从搜索控制台为受管集群的 pod 动态检索日志，使用受管集群中运行的 **klusterlet-addon-workmgr** 服务	443	无	用于访问受管集群路由的 IP 地址
出站到受管集群	HTTPS	安装过程中置备的受管集群的 Kubernetes API 服务器来安装 klusterlet	6443	无	Kubernetes 受管集群 API 服务器的 IP
到频道源的外向流量	HTTPS	频道源，包括 GitHub、Object Store 和 Helm 仓库，只有在您使用应用程序生命周期、OpenShift GitOps 或 ArgoCD 时才需要它	443	无	频道源的 IP

方向	协议	连接	端口（如果指定）	源地址	目标地址
来自受管集群的内向流量	HTTPS	用于推送只为运行 OpenShift Container Platform 版本 4.8 或更高版本的受管集群收集的指标和警报的受管集群	443	无	hub 集群访问路由的 IP 地址
来自受管集群的内向流量	HTTPS	监视受管集群的 Kubernetes API 服务器，用于监视受管集群的更改	6443	无	hub 集群 Kubernetes API 服务器的 IP 地址
出站到 ObjectStore	HTTPS	当 Cluster Backup Operator 运行时，为长期存储发送 Observability 指标数据	443	无	ObjectStore 的 IP 地址
出站到镜像存储库	HTTPS	访问 OpenShift Container Platform 和 Red Hat Advanced Cluster Management 的镜像	443	无	镜像存储库的 IP 地址

1.2. 受管集群网络配置

您可以引用受管集群网络的配置。

1.2.1. 受管集群网络配置表

下表中查看受管集群网络要求：

方向	协议	连接	端口（如果指定）	源地址	目标地址
来自 hub 集群的内向流量	HTTPS	从搜索控制台为受管集群的 pod 动态发送日志，使用受管集群中运行的 **klusterlet-addon-workmgr** 服务	443	无	用于访问受管集群路由的 IP 地址
来自 hub 集群的内向流量	HTTPS	安装过程中置备的受管集群的 Kubernetes API 服务器来安装 klusterlet	6443	无	Kubernetes 受管集群 API 服务器的 IP
出站到镜像存储库	HTTPS	访问 OpenShift Container Platform 和 Red Hat Advanced Cluster Management 的镜像	443	无	镜像存储库的 IP 地址
到 hub 集群的外向流量	HTTPS	用于推送只为运行 OpenShift Container Platform 版本 4.8 或更高版本的受管集群收集的指标和警报的受管集群	443	无	hub 集群访问路由的 IP 地址
到 hub 集群的外向流量	HTTPS	监视 hub 集群的 Kubernetes API 服务器的变化	6443	无	hub 集群 Kubernetes API 服务器的 IP 地址

方向	协议	连接	端口（如果指定）	源地址	目标地址
到频道源的外向流量	HTTPS	频道源，包括 GitHub、Object Store 和 Helm 仓库，只有在您使用应用程序生命周期、OpenShift GitOps 或 ArgoCD 时才需要它	443	无	频道源的 IP

1.3. 高级网络配置

- 基础架构 operator 表的额外网络要求
- Submariner 网络要求表
- Hive 表的额外网络要求
- 托管 control planes 网络要求表（技术预览）
- 应用程序部署网络要求表
- 命名空间连接网络要求表

1.3.1. 基础架构 operator 表的额外网络要求

当使用 Infrastructure Operator 安装裸机受管集群时，请参阅以下表以了解额外网络要求：

方向	协议	连接	端口（如果指定）
hub 集群在一个单一的节点 OpenShift Container Platform 受管集群中到 BMC 接口的外向流量	HTTPS（在断开连接的环境中的 HTTP）	引导 OpenShift Container Platform 集群	443
从 OpenShift Container Platform 受管集群到 hub 集群的外向流量	HTTPS	使用 **assistedService** 路由报告硬件信息	443

1.3.2. Submariner 网络要求表

使用 Submariner 的集群需要三个打开的端口。下表显示了您可以使用的端口：

方向	协议	连接	端口（如果指定）
出站和入站	UDP	每个受管集群	4800
出站和入站	UDP	每个受管集群	4500、500 以及网关节点上 IPSec 流量的任何其他端口
入站	TCP	每个受管集群	8080

1.3.3. Hive 表的额外网络要求

当使用 Hive Operator 安装裸机受管集群（包括使用中央基础架构管理）时，您必须在 hub 集群和 **libvirt** 置备主机间配置第 2 层或第 3 层端口连接。在使用 Hive 创建基本集群的过程中，需要它们来与置备主机进行连接。如需更多信息，请参阅下表：

方向	协议	连接	端口（如果指定）
到 **libvirt** 置备主机的 hub 集群的内向和外向流量	IP	将 hub 集群（Hive operator 安装的位置）连接到 **libvirt** 置备主机（在创建裸机集群时作为一个 bootstrap）	

注： 这些要求只适用于安装时，在升级使用 Infrastructure Operator 安装的集群时不需要。

1.3.4. 托管 control planes 网络要求表（技术预览）

使用托管的 control plane 时，**HypershiftDeployment** 资源必须具有与下表中列出的端点的连接：

方向	连接	端口（如果指定）
出站	OpenShift Container Platform control-plane 和 worker 节点	
出站	仅限 Amazon Web Services 上的托管集群：到 AWS API 和 S3 API 的出站连接	
出站	对于 Microsoft Azure 云服务上的托管集群：到 Azure API 的出站连接	
出站	OpenShift Container Platform 镜像存储库，用于存储 coreOS 的 ISO 镜像和 OpenShift Container Platform pod 的镜像 registry	

方向	连接	端口（如果指定）
出站	托管集群中 klusterlet 的本地 API 客户端与 HyperShift 托管集群的 API 通信	

1.3.5. 应用程序部署网络要求表

通常，应用程序部署通信是从受管集群到 hub 集群的一种方法。连接使用 **kubeconfig**，后者由受管集群上的代理配置。受管集群中的应用程序部署需要访问 hub 集群中的以下命名空间：

- 频道资源的命名空间
- 受管集群的命名空间

1.3.6. 命名空间连接网络要求表

- 应用程序生命周期连接：
  - 命名空间 **open-cluster-management** 需要访问端口 4000 上的控制台 API。
  - 命名空间 **open-cluster-management** 需要在端口 3001 上公开 Application UI。
- 应用程序生命周期后端组件(pod)：
  在 hub 集群中，所有应用程序生命周期 pod 都安装在 **open-cluster-management** 命名空间中，包括以下 pod：
  - multicluster-operators-hub-subscription
  - multicluster-operators-standalone-subscription
  - multicluster-operators-channel
  - multicluster-operators-application
  - multicluster-integrations
    由于这些 pod 位于 **open-cluster-management** 命名空间中：
  - 命名空间 **open-cluster-management** 需要通过端口 6443 访问 Kube API。

  在受管集群中，只有 **klusterlet-addon-appmgr** 应用程序生命周期 pod 安装在 **open-cluster-management-agent-addon** 命名空间中：
  - 命名空间 **open-cluster-management-agent-addon** 需要通过端口 6443 访问 Kube API。
- 监管和风险：
  在 hub 集群中，需要以下访问权限：
  - 命名空间 **open-cluster-management** 需要通过端口 6443 访问 Kube API。
  - 命名空间 **open-cluster-management** 需要访问端口 5353 上的 OpenShift DNS。

  在受管集群中，需要以下访问权限：

- 命名空间 **open-cluster-management-addon** 需要通过端口 6443 访问 Kube API。