



OpenShift Container Platform 4.6

网络

配置和管理集群网络

OpenShift Container Platform 4.6 网络

配置和管理集群网络

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律通告

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Networking.ent file |.

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.

摘要

本文档提供有关配置和管理 OpenShift Container Platform 集群网络的说明，其中包括 DNS、Ingress 和 Pod 网络。

目录

第 1 章 了解网络	10
1.1. OPENSIFT CONTAINER PLATFORM DNS	10
1.2. OPENSIFT CONTAINER PLATFORM INGRESS OPERATOR	10
1.2.1. 路由和 Ingress 的比较	10
第 2 章 访问主机	12
2.1. 访问安装程序置备的基础架构集群中 AMAZON WEB SERVICES 上的主机	12
第 3 章 网络 OPERATOR 概述	13
3.1. CLUSTER NETWORK OPERATOR	13
3.2. DNS OPERATOR	13
3.3. INGRESS OPERATOR	13
第 4 章 OPENSIFT CONTAINER PLATFORM 中的 CLUSTER NETWORK OPERATOR	14
4.1. CLUSTER NETWORK OPERATOR	14
4.2. 查看集群网络配置	14
4.3. 查看 CLUSTER NETWORK OPERATOR 状态	15
4.4. 查看 CLUSTER NETWORK OPERATOR 日志	15
4.5. CLUSTER NETWORK OPERATOR 配置	15
4.5.1. Cluster Network Operator 配置对象	16
defaultNetwork 对象配置	17
配置 OpenShift SDN CNI 集群网络供应商	17
配置 OVN-Kubernetes CNI 集群网络供应商	18
kubeProxyConfig 对象配置	18
4.5.2. Cluster Network Operator 配置示例	19
4.6. 其他资源	19
第 5 章 OPENSIFT CONTAINER PLATFORM 中的 DNS OPERATOR	20
5.1. DNS OPERATOR	20
5.2. 查看默认 DNS	20
5.3. 使用 DNS 转发	21
5.4. DNS OPERATOR 状态	23
5.5. DNS OPERATOR 日志	23
第 6 章 OPENSIFT CONTAINER PLATFORM 中的 INGRESS OPERATOR	24
6.1. OPENSIFT CONTAINER PLATFORM INGRESS OPERATOR	24
6.2. INGRESS 配置资产	24
6.3. INGRESS 控制器配置参数	24
6.3.1. Ingress Controller TLS 安全配置集	30
6.3.1.1. 了解 TLS 安全配置集	30
6.3.1.2. 为 Ingress Controller 配置 TLS 安全配置集	31
6.3.2. Ingress 控制器端点发布策略	33
6.4. 查看默认的 INGRESS CONTROLLER	35
6.5. 查看 INGRESS OPERATOR 状态	35
6.6. 查看 INGRESS CONTROLLER 日志	35
6.7. 查看 INGRESS CONTROLLER 状态	35
6.8. 配置 INGRESS CONTROLLER	36
6.8.1. 设置自定义默认证书	36
6.8.2. 删除自定义默认证书	37
6.8.3. 扩展 Ingress Controller	38
6.8.4. 配置 Ingress 访问日志	38
6.8.5. Ingress Controller 分片	41

6.8.5.1. 通过路由标签 (label) 配置 Ingress Controller 分片	41
6.8.5.2. 使用命名空间标签配置 Ingress Controller 分片	42
6.8.6. 配置 Ingress Controller 以使用内部负载均衡器	43
6.8.7. 将集群的默认 Ingress Controller 配置为内部	45
6.8.8. 配置路由准入策略	46
6.8.9. 使用通配符路由	46
6.8.10. 使用 X-Forwarded 标头	47
使用案例示例	47
6.8.11. 启用 HTTP/2 入口连接	48
6.9. 其他资源	49
第 7 章 配置节点端口服务范围	50
7.1. 先决条件	50
7.2. 扩展节点端口范围	50
7.3. 其他资源	50
第 8 章 在裸机集群中使用流控制传输协议 (SCTP)	52
8.1. 支持 OPENSIFT CONTAINER PLATFORM 上的流控制传输协议 (SCTP)	52
8.1.1. 使用 SCTP 协议的示例配置	52
8.2. 启用流控制传输协议 (SCTP)	53
8.3. 验证流控制传输协议 (SCTP) 已启用	54
第 9 章 配置 PTP 硬件	57
9.1. 关于 PTP 硬件	57
9.2. 自动发现 PTP 网络设备	57
9.3. 安装 PTP OPERATOR	58
9.3.1. CLI : 安装 PTP Operator	58
9.3.2. Web 控制台 : 安装 PTP Operator	59
9.4. 配置 LINUXPTP 服务	60
第 10 章 网络策略	63
10.1. 关于网络策略	63
10.1.1. 关于网络策略	63
10.1.2. 网络策略优化	65
10.1.3. 后续步骤	65
10.1.4. 其他资源	66
10.2. 创建网络策略	66
10.2.1. 创建网络策略	66
10.2.2. 示例 NetworkPolicy 对象	67
10.3. 查看网络策略	68
10.3.1. 查看网络策略	68
10.3.2. 示例 NetworkPolicy 对象	69
10.4. 编辑网络策略	69
10.4.1. 编辑网络策略	70
10.4.2. 示例 NetworkPolicy 对象	71
10.4.3. 其他资源	71
10.5. 删除网络策略	71
10.5.1. 删除网络策略	72
10.6. 为项目定义默认网络策略	72
10.6.1. 为新项目修改模板	72
10.6.2. 在新项目模板中添加网络策略	73
10.7. 使用网络策略配置多租户隔离	75
10.7.1. 使用网络策略配置多租户隔离	75
10.7.2. 后续步骤	77

10.7.3. 其他资源	77
第 11 章 多网络	78
11.1. 了解多网络	78
11.1.1. 额外网络使用场景	78
11.1.2. OpenShift Container Platform 中的额外网络	78
11.2. 配置额外网络	78
11.2.1. 管理额外网络的方法	79
11.2.2. 配置额外网络附加	79
11.2.2.1. 通过 Cluster Network Operator 配置额外网络	79
11.2.2.2. 从 YAML 清单配置额外网络	80
11.2.3. 额外网络类型的配置	80
11.2.3.1. 配置网桥额外网络	80
11.2.3.1.1. 网桥配置示例	81
11.2.3.2. 主机设备额外网络的配置	82
11.2.3.2.1. host-device 配置示例	82
11.2.3.3. 配置 IPVLAN 额外网络	82
11.2.3.3.1. ipvlan 配置示例	83
11.2.3.4. MACVLAN 额外网络的配置	83
11.2.3.4.1. macvlan 配置示例	84
11.2.4. 为额外网络配置 IP 地址分配	84
11.2.4.1. 静态 IP 地址分配配置	84
11.2.4.2. 动态 IP 地址(DHCP)分配配置	86
11.2.4.3. 使用 Whereabouts 进行动态 IP 地址分配配置	87
11.2.5. 使用 Cluster Network Operator 创建额外网络附加	87
11.2.6. 通过应用 YAML 清单来创建额外网络附加	89
11.3. 将 POD 附加到额外网络	89
11.3.1. 将 pod 添加到额外网络	89
11.3.1.1. 指定特定于 pod 的地址和路由选项	91
11.4. 从额外网络中删除 POD	94
11.4.1. 从额外网络中删除 pod	94
11.5. 编辑额外网络	95
11.5.1. 修改额外网络附加定义	95
11.6. 删除额外网络	95
11.6.1. 删除额外网络附加定义	96
第 12 章 硬件网络	97
12.1. 关于单根 I/O 虚拟化 (SR-IOV) 硬件网络	97
12.1.1. 负责管理 SR-IOV 网络设备的组件	97
12.1.1.1. 支持的平台	98
12.1.1.2. 支持的设备	98
12.1.1.3. 自动发现 SR-IOV 网络设备	98
12.1.1.3.1. SriovNetworkNodeState 对象示例	98
12.1.1.4. 在 pod 中使用虚拟功能的示例	100
12.1.2. 后续步骤	101
12.2. 安装 SR-IOV NETWORK OPERATOR	101
12.2.1. 安装 SR-IOV Network Operator	101
12.2.1.1. CLI : 安装 SR-IOV Network Operator	101
12.2.1.2. web 控制台 : 安装 SR-IOV Network Operator	103
12.2.2. 后续步骤	104
12.3. 配置 SR-IOV NETWORK OPERATOR	104
12.3.1. 配置 SR-IOV Network Operator	104
12.3.1.1. 关于 Network Resources Injector (网络资源注入器)。	104

12.3.1.2. 关于 SR-IOV Operator admission controller webhook	105
12.3.1.3. 关于自定义节点选择器	105
12.3.1.4. 禁用或启用网络资源注入器	105
12.3.1.5. 禁用或启用 SR-IOV Operator 准入控制器 Webhook	106
12.3.1.6. 为 SR-IOV 网络配置守护进程配置自定义 NodeSelector	106
12.3.2. 后续步骤	106
12.4. 配置 SR-IOV 网络设备	107
12.4.1. SR-IOV 网络节点配置对象	107
12.4.1.1. SR-IOV 网络节点配置示例	108
12.4.1.2. SR-IOV 设备的虚拟功能 (VF) 分区	109
12.4.2. 配置 SR-IOV 网络设备	110
12.4.3. SR-IOV 配置故障排除	111
12.4.4. 后续步骤	111
12.5. 配置 SR-IOV 以太网网络附加	111
12.5.1. 以太网设备配置对象	111
12.5.1.1. 为额外网络配置 IP 地址分配	112
12.5.1.1.1. 静态 IP 地址分配配置	113
12.5.1.1.2. 动态 IP 地址(DHCP)分配配置	114
12.5.1.1.3. 使用 Whereabouts 进行动态 IP 地址分配配置	115
12.5.2. 配置 SR-IOV 额外网络	116
12.5.3. 后续步骤	117
12.5.4. 其他资源	117
12.6. 配置 SR-IOV INFINIBAND 网络附加	117
12.6.1. Infiniband 设备配置对象	117
12.6.1.1. 为额外网络配置 IP 地址分配	118
12.6.1.1.1. 静态 IP 地址分配配置	118
12.6.1.1.2. 动态 IP 地址(DHCP)分配配置	119
12.6.1.1.3. 使用 Whereabouts 进行动态 IP 地址分配配置	120
12.6.2. 配置 SR-IOV 额外网络	121
12.6.3. 后续步骤	122
12.6.4. 其他资源	122
12.7. 将 POD 添加到额外网络	122
12.7.1. 网络附加的运行时配置	122
12.7.1.1. 基于以太网的 SR-IOV 附加的运行时配置	122
12.7.1.2. 基于 InfiniBand 的 SR-IOV 附加的运行时配置	123
12.7.2. 将 pod 添加到额外网络	124
12.7.3. 创建与 SR-IOV pod 兼容的非统一内存访问 (NUMA)	126
12.7.4. 其他资源	127
12.8. 配置高性能多播	127
12.8.1. 高性能多播	127
12.8.2. 为多播配置 SR-IOV 接口	128
12.9. 在 DPDK 和 RDMA 模式中使用虚拟功能 (VF) 的示例	129
12.9.1. 在 DPDK 和 RDMA 模式中使用虚拟功能 (VF) 的示例	129
12.9.2. 先决条件	130
12.9.3. 在 Intel NIC 的 DPDK 模式中使用虚拟功能 (VF) 示例	130
12.9.4. 使用带有 Mellanox NIC 的 DPDK 模式的虚拟功能 (VF) 示例	132
12.9.5. 带有 Mellanox NIC 的 RDMA 模式中的虚拟功能 (VF) 示例	135
12.10. 卸载 SR-IOV NETWORK OPERATOR	138
12.10.1. 卸载 SR-IOV Network Operator	138
第 13 章 OPENSIFT SDN 默认 CNI 网络供应商	140
13.1. 关于 OPENSIFT SDN 默认 CNI 网络供应商	140
13.1.1. OpenShift SDN 网络隔离模式	140

13.1.2. 支持的默认 CNI 网络供应商功能列表	140
13.2. 为项目配置出口 IP	140
13.2.1. 项目出口流量的出口 IP 地址分配	141
13.2.1.1. 使用自动分配的出口 IP 地址时的注意事项	141
13.2.1.2. 使用手动分配出口 IP 地址时的注意事项	142
13.2.2. 为一个命名空间启用自动分配出口 IP 地址	142
13.2.3. 为一个命名空间配置手动分配出口 IP 地址	143
13.3. 为项目配置出口防火墙	144
13.3.1. 出口防火墙在一个项目中的工作原理	144
13.3.1.1. 出口防火墙的限制	146
13.3.1.2. 出口防火墙策略规则的匹配顺序	146
13.3.1.3. 域名服务器 (DNS) 解析如何工作	146
13.3.2. EgressNetworkPolicy 自定义资源 (CR) 对象	147
13.3.2.1. EgressNetworkPolicy 规则	147
13.3.2.2. EgressNetworkPolicy CR 对象示例	147
13.3.3. 创建出口防火墙策略对象	148
13.4. 为项目编辑出口防火墙	149
13.4.1. 查看 EgressNetworkPolicy 对象	149
13.5. 为项目编辑出口防火墙	149
13.5.1. 编辑 EgressNetworkPolicy 对象	149
13.6. 从项目中删除出口防火墙	150
13.6.1. 删除 EgressNetworkPolicy 对象	150
13.7. 使用出口路由器 POD 的注意事项	150
13.7.1. 关于出口路由器 pod	150
13.7.1.1. 出口路由器模式	151
13.7.1.2. 出口路由器 pod 的实现	151
13.7.1.3. 部署注意事项	151
13.7.1.4. 故障切换配置	152
13.7.2. 其他资源	152
13.8. 以重定向模式部署出口路由器 POD	153
13.8.1. 重定向模式的出口路由器 pod 规格	153
13.8.2. 出口目的地配置格式	154
13.8.3. 以重定向模式部署出口路由器 pod	155
13.8.4. 其他资源	155
13.9. 以 HTTP 代理模式部署出口路由器 POD	155
13.9.1. HTTP 模式的出口路由器 pod 规格	155
13.9.2. 出口目的地配置格式	156
13.9.3. 以 HTTP 代理模式部署出口路由器 pod	157
13.9.4. 其他资源	158
13.10. 以 DNS 代理模式部署出口路由器 POD	158
13.10.1. DNS 模式的出口路由器 pod 规格	158
13.10.2. 出口目的地配置格式	159
13.10.3. 以 DNS 代理模式部署出口路由器 pod	160
13.10.4. 其他资源	161
13.11. 从配置映射配置出口路由器 POD 目的地列表	161
13.11.1. 使用配置映射配置出口路由器目的地映射	161
13.11.2. 其他资源	162
13.12. 为项目启用多播	162
13.12.1. 关于多播	162
13.12.2. 启用 pod 间多播	162
13.13. 为项目禁用多播	164
13.13.1. 禁用 pod 间多播	164
13.14. 使用 OPENSIFT SDN 配置网络隔离	165

13.14.1. 先决条件	165
13.14.2. 接合项目	165
13.14.3. 隔离项目	165
13.14.4. 对项目禁用网络隔离	166
13.15. 配置 KUBE-PROXY	166
13.15.1. 关于 iptables 规则同步	166
13.15.2. kube-proxy 配置参数	166
13.15.3. 修改 kube-proxy 配置	167
第 14 章 OVN-KUBERNETES 默认 CNI 网络供应商	169
14.1. 关于 OVN-KUBERNETES 默认 CONTAINER NETWORK INTERFACE (CNI) 网络供应商	169
14.1.1. OVN-Kubernetes 特性	169
14.1.2. 支持的默认 CNI 网络供应商功能列表	169
14.1.3. OVN-Kubernetes 限制	169
14.2. 从 OPENSIFT SDN 集群网络供应商迁移	170
14.2.1. 迁移到 OVN-Kubernetes 网络供应商	170
14.2.1.1. 迁移到 OVN-Kubernetes 网络供应商时的注意事项	170
命名空间隔离	170
出口 IP 地址	171
出口网络策略	171
出口路由器 pod	171
多播	171
网络策略	171
14.2.1.2. 迁移过程如何工作	172
14.2.2. 迁移至 OVN-Kubernetes 默认 CNI 网络供应商	172
14.2.3. 其他资源	176
14.3. 回滚到 OPENSIFT SDN 网络供应商	176
14.3.1. 将默认 CNI 网络供应商回滚到 OpenShift SDN	177
14.4. 为项目配置出口防火墙	180
14.4.1. 出口防火墙在一个项目中的工作原理	180
14.4.1.1. 出口防火墙的限制	182
14.4.1.2. 出口防火墙策略规则的匹配顺序	182
14.4.2. EgressFirewall 自定义资源 (CR) 对象	182
14.4.2.1. EgressFirewall 规则	182
14.4.2.2. EgressFirewall CR 对象示例	183
14.4.3. 创建出口防火墙策略对象	184
14.5. 查看项目的出口防火墙	184
14.5.1. 查看 EgressFirewall 对象	184
14.6. 为项目编辑出口防火墙	185
14.6.1. 编辑 EgressFirewall 对象	185
14.7. 从项目中删除出口防火墙	186
14.7.1. 删除 EgressFirewall 对象	186
14.8. 配置出口 IP 地址	186
14.8.1. 出口 IP 地址架构设计和实施	186
14.8.1.1. 平台支持	187
14.8.1.2. 将出口 IP 分配给 pod	187
14.8.1.3. 将出口 IP 分配给节点	187
14.8.1.4. 出口 IP 地址配置架构图	188
14.8.2. EgressIP 对象	189
14.8.3. 标记节点以托管出口 IP 地址	191
14.8.4. 后续步骤	191
14.8.5. 其他资源	191
14.9. 分配出口 IP 地址	191

14.9.1. 为一个命名空间分配出口 IP 地址	191
14.9.2. 其他资源	192
14.10. 为项目启用多播	192
14.10.1. 关于多播	193
14.10.2. 启用 pod 间多播	193
14.11. 为项目禁用多播	194
14.11.1. 禁用 pod 间多播	195
14.12. 配置混合联网	195
14.12.1. 使用 OVN-Kubernetes 配置混合网络	195
14.12.2. 其他资源	196
第 15 章 配置路由	198
15.1. 路由配置	198
15.1.1. 创建基于 HTTP 的路由	198
15.1.2. 配置路由超时	199
15.1.3. 启用 HTTP 严格传输安全性	199
15.1.4. 吞吐量问题错误排解	200
15.1.5. 使用 Cookie 来保持路由有状态性	200
15.1.5.1. 使用 Cookie 标注路由	201
15.1.6. 基于路径的路由	202
15.1.7. 特定于路由的注解	202
15.1.8. 配置路由准入策略	208
15.1.9. 通过 Ingress 对象创建路由	209
15.2. 安全路由	211
15.2.1. 使用自定义证书创建重新加密路由	211
15.2.2. 使用自定义证书创建边缘路由	212
15.2.3. 创建 passthrough 路由	214
第 16 章 配置集群入口流量	215
16.1. 集群入口流量配置概述	215
16.2. 为服务配置 EXTERNALIP	215
16.2.1. 先决条件	215
16.2.2. 关于 ExternalIP	215
16.2.2.1. 配置 ExternalIP	216
16.2.2.2. 对外部 IP 地址分配的限制	217
16.2.2.3. 策略对象示例	218
16.2.3. ExternalIP 地址块配置	219
外部 IP 配置示例	219
16.2.4. 为集群配置外部 IP 地址块	220
16.2.5. 后续步骤	221
16.3. 使用 INGRESS CONTROLLER 配置集群入口流量	221
16.3.1. 使用 Ingress Controller 和路由	221
16.3.2. 先决条件	221
16.3.3. 创建项目和服务	222
16.3.4. 通过创建路由公开服务	222
16.3.5. 通过路由标签 (label) 配置 Ingress Controller 分片	223
16.3.6. 使用命名空间标签配置 Ingress Controller 分片	224
16.3.7. 其他资源	225
16.4. 使用负载均衡器配置集群入口流量	225
16.4.1. 使用负载均衡器使流量进入集群	225
16.4.2. 先决条件	225
16.4.3. 创建项目和服务	226
16.4.4. 通过创建路由公开服务	226

16.4.5. 创建负载均衡器服务	227
16.5. 使用网络负载均衡器在 AWS 上配置集群入口流量	229
16.5.1. 使用网络负载均衡器替换 Ingress Controller Classic 负载均衡器	229
16.5.2. 在现有 AWS 集群上配置 Ingress Controller 网络负载均衡器	230
16.5.3. 在新 AWS 集群上配置 Ingress Controller 网络负载均衡	231
16.5.4. 其他资源	232
16.6. 为服务外部 IP 配置 INGRESS 集群流量	232
16.6.1. 先决条件	232
16.6.2. 将 ExternalIP 附加到服务	232
16.6.3. 其他资源	234
16.7. 使用 NODEPORT 配置集群入口流量	234
16.7.1. 使用 NodePort 使流量进入集群	234
16.7.2. 先决条件	234
16.7.3. 创建项目和服务	234
16.7.4. 通过创建路由公开服务	235
16.7.5. 其他资源	236
第 17 章 配置集群范围代理	237
17.1. 先决条件	237
17.2. 启用集群范围代理	237
17.3. 删除集群范围代理服务器	239
其他资源	239
第 18 章 配置自定义 PKI	240
18.1. 在安装过程中配置集群范围代理	240
18.2. 启用集群范围代理	241
18.3. 使用 OPERATOR 进行证书注入	243
第 19 章 RHOSP 负载均衡	245
19.1. 使用带有 KURYR SDN 的 OCTAVIA OVN 负载均衡器供应商驱动	245
19.2. 使用 OCTAVIA 为应用程序流量扩展集群	246
19.2.1. 使用 Octavia 扩展集群	246
19.2.2. 通过 Octavia 扩展使用 Kuryr 的集群	248
19.3. 使用 RHOSP OCTAVIA 为入站流量扩展	248
第 20 章 将二级接口指标与网络附加关联	251
20.1. 将二级接口指标与网络附加关联	251
20.1.1. 网络指标守护进程	251
20.1.2. 带有网络名称的指标	252

第 1 章 了解网络

集群管理员有几个选项可将集群中运行的应用程序公开给外部流量并保护网络连接安全：

- 服务类型，如节点端口或负载均衡器
- API 资源，如 **Ingress** 和 **Route**

默认情况下，Kubernetes 为 pod 内运行的应用分配内部 IP 地址。Pod 及其容器可以网络，但集群外的客户端无法访问网络。当您将应用公开给外部流量时，为每个容器集指定自己的 IP 地址意味着 pod 在端口分配、网络、命名、服务发现、负载均衡、应用配置和迁移方面可被视为物理主机或虚拟机。



注意

一些云平台提供侦听 169.254.169.254 IP 地址的元数据 API，它是 IPv4 **169.254.0.0/16** CIDR 块中的连接内部 IP 地址。

此 CIDR 块无法从 pod 网络访问。需要访问这些 IP 地址的 Pod 必须通过将 pod spec 中的 **spec.hostNetwork** 字段设置为 **true** 来获得主机网络访问。

如果允许 pod 主机网络访问，则将授予 pod 对底层网络基础架构的访问权限。

1.1. OPENSIFT CONTAINER PLATFORM DNS

如果您运行多个服务，比如使用多个 pod 的前端和后端服务，则要为用户名和服务 IP 等创建环境变量，使前端 pod 可以跟后端服务通信。如果删除并重新创建服务，可以为该服务分配一个新的 IP 地址，而且需要重新创建前端 pod 来获取服务 IP 环境变量的更新值。另外，必须在任何前端 pod 之前创建后端服务，以确保正确生成服务 IP，并将它作为环境变量提供给前端 pod。

因此，OpenShift Container Platform 具有一个内置 DNS，以便服务 DNS 以及服务 IP/端口能够访问这些服务。

1.2. OPENSIFT CONTAINER PLATFORM INGRESS OPERATOR

在创建 OpenShift Container Platform 集群时，在集群中运行的 Pod 和服务会各自分配自己的 IP 地址。IP 地址可供附近运行的其他容器集和服务访问，但外部客户端无法访问这些 IP 地址。Ingress Operator 实现 **IngressController** API，是负责启用对 OpenShift Container Platform 集群服务的外部访问的组件。

Ingress Operator 通过部署和管理一个或多个基于 HAProxy 的 **Ingress Controller** 来处理路由，使外部客户端可以访问您的服务。您可以通过指定 OpenShift Container Platform **Route** 和 Kubernetes **Ingress** 资源，来使用 Ingress Operator 路由流量。Ingress Controller 中的配置（如定义 **endpointPublishingStrategy** 类型和内部负载均衡）提供了发布 Ingress Controller 端点的方法。

1.2.1. 路由和 Ingress 的比较

OpenShift Container Platform 中的 Kubernetes Ingress 资源通过作为集群内 pod 运行的共享路由器服务来实现 Ingress Controller。管理 Ingress 流量的最常见方法是使用 Ingress Controller。您可以像任何其他常规 pod 一样扩展和复制此 pod。此路由器服务基于 **HAProxy**，后者是一个开源负载均衡器解决方案。

OpenShift Container Platform 路由为集群中的服务提供入口流量。路由提供了标准 Kubernetes Ingress Controller 可能不支持的高级功能，如 TLS 重新加密、TLS 直通和为蓝绿部署分割流量。

入口流量通过路由访问集群中的服务。路由和入口是处理入口流量的主要资源。Ingress 提供类似于路由的功能，如接受外部请求并根据路由委派它们。但是，对于 Ingress，您只能允许某些类型的连接：

HTTP/2、HTTPS 和服务器名称识别(SNI)，以及 TLS（证书）。在 OpenShift Container Platform 中，生成路由以满足 Ingress 资源指定的条件。

第 2 章 访问主机

了解如何创建堡垒主机来访问 OpenShift Container Platform 实例，以及使用安全 shell (SSH) 访问 control plane 节点（也称为 master 节点）。

2.1. 访问安装程序置备的基础架构集群中 AMAZON WEB SERVICES 上的主机

OpenShift Container Platform 安装程序不会为任何置备 OpenShift Container Platform 集群的 Amazon Elastic Compute Cloud (Amazon EC2) 实例创建公共 IP 地址。为了可以 SSH 到 OpenShift Container Platform 主机，您必须按照以下步骤操作。

流程

1. 创建一个安全组，允许 SSH 访问由 **openshift-install** 命令创建的虚拟私有云 (VPC)。
2. 在安装程序创建的某个公共子网中创建 Amazon EC2 实例。
3. 将公共 IP 地址与您创建的 Amazon EC2 实例相关联。
与 OpenShift Container Platform 安装不同，您应该将您创建的 Amazon EC2 实例与 SSH 密钥对关联。这与您为这个实例选择的操作系统无关，因为它只是一个 SSH 堡垒将互联网桥接到 OpenShift Container Platform 集群的 VPC。它与您使用的 Amazon Machine Image (AMI) 相关。例如，在 Red Hat Enterprise Linux CoreOS (RHCOS) 中，您可以像安装程序一样通过 Ignition 提供密钥。
4. 一旦置备了 Amazon EC2 实例并可以 SSH 到它，您必须添加与 OpenShift Container Platform 安装关联的 SSH 密钥。这个密钥可以与堡垒实例的密钥不同，也可以相同。



注意

直接通过 SSH 访问仅建议在灾难恢复时使用。当 Kubernetes API 正常工作时，应该使用特权 Pod。

5. 运行 **oc get nodes**，查看输出结果，然后选择一个 master 节点。主机名类似于 **ip-10-0-1-163.ec2.internal**。
6. 从您手动部署到 Amazon EC2 的堡垒 SSH 主机中，SSH 部署到那个 control plane 主机（也称为 master 主机）。确定您使用了在安装过程中指定的相同的 SSH 密钥：

```
$ ssh -i <ssh-key-path> core@<master-hostname>
```


第 3 章 网络 OPERATOR 概述

OpenShift Container Platform 支持多种类型的网络 Operator。您可以使用这些网络 Operator 管理集群网络。

3.1. CLUSTER NETWORK OPERATOR

Cluster Network Operator(CNO)在 OpenShift Container Platform 集群中部署和管理集群网络组件。这包括在安装过程中为集群选择的 Container Network Interface(CNI)默认网络供应商插件部署。如需更多信息，请参阅 [OpenShift Container Platform 中的 Cluster Network Operator](#)。

3.2. DNS OPERATOR

DNS Operator 部署并管理 CoreDNS，以便为 pod 提供名称解析服务。这会在 OpenShift Container Platform 中启用基于 DNS 的 Kubernetes 服务发现。如需更多信息，请参阅 [OpenShift Container Platform 中的 DNS Operator](#)。

3.3. INGRESS OPERATOR

创建 OpenShift Container Platform 集群时，集群中运行的 pod 和服务将为每个分配的 IP 地址。IP 地址可以被其他 pod 和服务访问，但外部客户端无法访问。Ingress Operator 实现 Ingress Controller API，并负责启用对 OpenShift Container Platform 集群服务的外部访问。如需更多信息，请参阅 [OpenShift Container Platform 中的 Ingress Operator](#)。

第 4 章 OPENSIFT CONTAINER PLATFORM 中的 CLUSTER NETWORK OPERATOR

Cluster Network Operator (CNO) 在 OpenShift Container Platform 集群上部署和管理集群网络组件，包括在安装过程中为集群选择的 Container Network Interface (CNI) 默认网络供应商插件。

4.1. CLUSTER NETWORK OPERATOR

Cluster Network Operator 从 **operator.openshift.io** API 组实现 **network** API。Operator 通过使用守护进程集，部署 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商插件，或部署您在集群安装过程中选择的默认网络供应商插件。

流程

Cluster Network Operator 在安装过程中被部署为一个 Kubernetes **部署**。

1. 运行以下命令，以查看部署状态：

```
$ oc get -n openshift-network-operator deployment/network-operator
```

输出示例

```
NAME          READY  UP-TO-DATE  AVAILABLE  AGE
network-operator  1/1    1           1          56m
```

2. 运行以下命令，以查看 Cluster Network Operator 的状态：

```
$ oc get clusteroperator/network
```

输出示例

```
NAME    VERSION  AVAILABLE  PROGRESSING  DEGRADED  SINCE
network 4.5.4    True       False        False     50m
```

以下字段提供有关 Operator 状态的信息：**AVAILABLE**、**Progressing** 和 **DEGRADED**。当 Cluster Network Operator 报告可用状态条件时，**AVAILABLE** 字段为 **True**。

4.2. 查看集群网络配置

每个 OpenShift Container Platform 新安装都有一个名为 **cluster** 的 **network.config** 对象。

流程

- 使用 **oc describe** 命令查看集群网络配置：

```
$ oc describe network.config/cluster
```

输出示例

```
Name:      cluster
Namespace:
```

```

Labels:    <none>
Annotations: <none>
API Version: config.openshift.io/v1
Kind:      Network
Metadata:
  Self Link:    /apis/config.openshift.io/v1/networks/cluster
Spec: ❶
  Cluster Network:
    Cidr:      10.128.0.0/14
    Host Prefix: 23
    Network Type: OpenShiftSDN
  Service Network:
    172.30.0.0/16
Status: ❷
  Cluster Network:
    Cidr:      10.128.0.0/14
    Host Prefix: 23
    Cluster Network MTU: 8951
    Network Type: OpenShiftSDN
  Service Network:
    172.30.0.0/16
Events: <none>

```

- ❶ **Spec** 字段显示集群网络的已配置状态。
- ❷ **Status** 字段显示集群网络配置当前状态。

4.3. 查看 CLUSTER NETWORK OPERATOR 状态

您可以使用 **oc describe** 命令来检查状态并查看 Cluster Network Operator 的详情。

流程

- 运行以下命令，以查看 Cluster Network Operator 的状态：

```
$ oc describe clusteroperators/network
```

4.4. 查看 CLUSTER NETWORK OPERATOR 日志

您可以使用 **oc logs** 命令来查看 Cluster Network Operator 日志。

流程

- 运行以下命令，以查看 Cluster Network Operator 的日志：

```
$ oc logs --namespace=openshift-network-operator deployment/network-operator
```

4.5. CLUSTER NETWORK OPERATOR 配置

集群网络的配置作为 Cluster Network Operator (CNO) 配置的一部分被指定，并存储在名为 **cluster** 的自定义资源 (CR) 对象中。CR 指定 **operator.openshift.io** API 组中的 **Network** API 的字段。

CNO 配置会在集群安装过程中从 **Network.config.openshift.io** API 组中的 **Network** API 继承以下字段，这些字段无法更改：

clusterNetwork

从中分配 pod IP 地址的 IP 地址池。

serviceNetwork

服务的 IP 地址池。

defaultNetwork.type

集群网络供应商，如 OpenShift SDN 或 OVN-Kubernetes。



注意

在集群安装后，您无法修改上一节中列出的字段。

您可以通过在名为 **cluster** 的 CNO 对象中设置 **defaultNetwork** 对象的字段来为集群指定集群网络供应商配置。

4.5.1. Cluster Network Operator 配置对象

Cluster Network Operator (CNO) 的字段在下表中描述：

表 4.1. Cluster Network Operator 配置对象


字段	类型	描述
metadata.name	字符串	CNO 对象的名称。这个名称始终是 cluster 。
spec.clusterNetwork	数组	<p>用于指定从哪些 IP 地址块分配 Pod IP 地址以及分配给集群中每个节点的子网前缀长度的列表。例如：</p> <pre>spec: clusterNetwork: - cidr: 10.128.0.0/19 hostPrefix: 23 - cidr: 10.128.32.0/19 hostPrefix: 23</pre> <p>此值是只读的，在集群安装过程中从名为 cluster 的 Network.config.openshift.io 对象继承。</p>
spec.serviceNetwork	数组	<p>服务的 IP 地址块。OpenShift SDN 和 OVN-Kubernetes Container Network Interface (CNI) 网络供应商只支持服务网络具有单个 IP 地址块。例如：</p> <pre>spec: serviceNetwork: - 172.30.0.0/14</pre> <p>此值是只读的，在集群安装过程中从名为 cluster 的 Network.config.openshift.io 对象继承。</p>

字段	类型	描述
spec.defaultNetwork	对象	为集群网络配置 Container Network Interface (CNI) 集群网络供应商。
spec.kubeProxyConfig	对象	此对象的字段指定 kube-proxy 配置。如果您使用 OVN-Kubernetes 集群网络供应商，则 kube-proxy 的配置不会起作用。

defaultNetwork 对象配置

defaultNetwork 对象的值在下表中定义：

表 4.2. defaultNetwork 对象

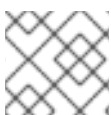
字段	类型	描述
type	字符串	<p>OpenShiftSDN 或 OVNKubernetes。在安装过程中选择了集群网络供应商。集群安装后无法更改这个值。</p> <div style="display: flex; align-items: center;">  <div> <p>注意</p> <p>OpenShift Container Platform 默认使用 OpenShift SDN Container Network Interface (CNI) 集群网络供应商。</p> </div> </div>
openshiftSDNConfig	对象	此对象仅对 OpenShift SDN 集群网络供应商有效。
ovnKubernetesConfig	对象	此对象仅对 OVN-Kubernetes 集群网络供应商有效。

配置 OpenShift SDN CNI 集群网络供应商

下表描述了 OpenShift SDN Container Network Interface (CNI) 集群网络供应商的配置字段。

表 4.3. openshiftSDNConfig 对象

字段	类型	描述
mode	字符串	OpenShift SDN 的网络隔离模式。
mtu	整数	VXLAN 覆盖网络的最大传输单元 (MTU)。这个值通常是自动配置的。
vxlanPort	整数	用于所有 VXLAN 数据包的端口。默认值为 4789 。



注意

您只能在集群安装过程中更改集群网络供应商的配置。

OpenShift SDN 配置示例

```
defaultNetwork:
  type: OpenShiftSDN
  openshiftSDNConfig:
    mode: NetworkPolicy
    mtu: 1450
    vxlanPort: 4789
```

配置 OVN-Kubernetes CNI 集群网络供应商

下表描述了 OVN-Kubernetes CNI 集群网络供应商的配置字段。

表 4.4. `ovnKubernetesConfig` 对象

字段	类型	描述
<code>mtu</code>	整数	Geneve (Generic Network Virtualization Encapsulation) 覆盖网络的最大传输单元 (MTU)。这个值通常是自动配置的。
<code>genevePort</code>	整数	Geneve 覆盖网络的 UDP 端口。



注意

您只能在集群安装过程中更改集群网络供应商的配置。

OVN-Kubernetes 配置示例

```
defaultNetwork:
  type: OVNKubernetes
  ovnKubernetesConfig:
    mtu: 1400
    genevePort: 6081
```

kubeProxyConfig 对象配置

`kubeProxyConfig` 对象的值在下表中定义：

表 4.5. `kubeProxyConfig` 对象

字段	类型	描述
<code>iptablesSyncPeriod</code>	字符串	<p><code>iptables</code> 规则的刷新周期。默认值为 30s。有效的后缀包括 s、m 和 h，具体参见 Go time 软件包文档。</p> <div style="display: flex; align-items: flex-start;"> <div style="flex: 1;"> </div> <div style="flex: 2;"> <p>注意</p> <p>由于 OpenShift Container Platform 4.3 及更高版本中引进了性能上的改进，现在不再需要调整 <code>iptablesSyncPeriod</code> 参数。</p> </div> </div>

字段	类型	描述
<code>proxyArguments.iptables-min-sync-period</code>	数组	刷新 <code>iptables</code> 规则前的最短时长。此字段确保刷新的频率不会过于频繁。有效的后缀包括 <code>s</code> 、 <code>m</code> 和 <code>h</code> ，具体参见 Go time 软件包 。默认值为： <pre>kubeProxyConfig: proxyArguments: iptables-min-sync-period: - 0s</pre>

4.5.2. Cluster Network Operator 配置示例

以下示例中指定了完整的 CNO 配置：

Cluster Network Operator 对象示例

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  clusterNetwork: 1
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  serviceNetwork: 2
  - 172.30.0.0/16
  defaultNetwork: 3
  type: OpenShiftSDN
  openshiftSDNConfig:
    mode: NetworkPolicy
    mtu: 1450
    vxlanPort: 4789
  kubeProxyConfig:
    iptablesSyncPeriod: 30s
    proxyArguments:
      iptables-min-sync-period:
        - 0s
```

1 2 3 仅在集群安装过程中配置。

4.6. 其他资源

- [operator .openshift.io](#) API 组中的 network API

第 5 章 OPENSIFT CONTAINER PLATFORM 中的 DNS OPERATOR

DNS Operator 部署并管理 CoreDNS，以便为 Pod 提供名称解析服务，从而在 OpenShift 中启用基于 DNS 的 Kubernetes 服务发现。

5.1. DNS OPERATOR

DNS Operator 从 **operator.openshift.io** API 组实现 **dns** API。Operator 使用守护进程集部署 CoreDNS，为守护进程集创建一个服务，并将 kubelet 配置为指示 pod 使用 CoreDNS 服务 IP 地址进行名称解析。

流程

在安装过程中使用 **Deployment** 对象部署 DNS Operator。

1. 使用 **oc get** 命令查看部署状态：

```
$ oc get -n openshift-dns-operator deployment/dns-operator
```

输出示例

```
NAME          READY   UP-TO-DATE   AVAILABLE   AGE
dns-operator  1/1     1             1           23h
```

2. 使用 **oc get** 命令来查看 DNS Operator 的状态：

```
$ oc get clusteroperator/dns
```

输出示例

```
NAME      VERSION   AVAILABLE   PROGRESSING   DEGRADED   SINCE
dns       4.1.0-0.11 True       False         False       92m
```

AVAILABLE、**PROGRESSING** 和 **DEGRADED** 提供了有关 Operator 状态的信息。当 CoreDNS 守护进程中至少有一个 pod 被设置为 **Available** 状态时，**AVAILABLE** 为 **True**。

5.2. 查看默认 DNS

每个 OpenShift Container Platform 新安装都有一个名为 **default** 的 **dns.operator**。

流程

1. 使用 **oc describe** 命令来查看默认 **dns**：

```
$ oc describe dns.operator/default
```

输出示例

```
Name:      default
Namespace:
```



```
Labels: <none>
Annotations: <none>
API Version: operator.openshift.io/v1
Kind: DNS
...
Status:
  Cluster Domain: cluster.local 1
  Cluster IP: 172.30.0.10 2
...
```

- 1** Cluster Domain 字段是用来构造完全限定的 pod 和服务域名的基本 DNS 域。
- 2** Cluster IP 是 Pod 为名称解析查询的地址。IP 由服务 CIDR 范围中的第 10 个地址定义。

2. 要查找集群的服务 CIDR，使用 **oc get** 命令：

```
$ oc get networks.config/cluster -o jsonpath='{$.status.serviceNetwork}'
```

输出示例

```
[172.30.0.0/16]
```

5.3. 使用 DNS 转发

您可以针对一个区（zone），使用 DNS 转发来覆盖 **/etc/resolv.conf** 中指定的转发配置，方法是指定这个区使用哪个名称解析服务器。如果转发区是 OpenShift Container Platform 管理的 Ingress 域，那么上游名称服务器必须为域授权。

流程

1. 修改名为 **default** 的 DNS Operator 对象：

```
$ oc edit dns.operator/default
```

这允许 Operator 使用基于 **Server** 的额外服务器配置块来创建和更新名为 **dns-default** 的 ConfigMap。如果没有服务器带有与查询匹配的区，则命名解析功能会返回到由 **/etc/resolv.conf** 中指定的名称服务器。

DNS 示例

```
apiVersion: operator.openshift.io/v1
kind: DNS
metadata:
  name: default
spec:
  servers:
  - name: foo-server 1
    zones: 2
    - example.com
  forwardPlugin:
    upstreams: 3
    - 1.1.1.1
```

```

- 2.2.2.2:5353
- name: bar-server
  zones:
  - bar.com
  - example.com
  forwardPlugin:
    upstreams:
    - 3.3.3.3
    - 4.4.4.4:5454

```

- 1 **name** 必须符合 **rfc6335** 服务名称的语法。
- 2 **zones** 必须符合 **rfc1123** 中的一个 **subdomain** 的定义。集群域 **cluster.local** 不是 **zones** 中的一个有效的 **subdomain**。
- 3 每个 **forwardPlugin** 最多允许 15 个 **upstreams**。



注意

如果 **servers** 未定义或无效，则 ConfigMap 只包括默认服务器。

2. 查看 ConfigMap :

```
$ oc get configmap/dns-default -n openshift-dns -o yaml
```

基于以上 DNS 示例的 DNS ConfigMap 示例

```

apiVersion: v1
data:
  Corefile: |
    example.com:5353 {
      forward . 1.1.1.1 2.2.2.2:5353
    }
    bar.com:5353 example.com:5353 {
      forward . 3.3.3.3 4.4.4.4:5454 1
    }
    .:5353 {
      errors
      health
      kubernetes cluster.local in-addr.arpa ip6.arpa {
        pods insecure
        upstream
        fallthrough in-addr.arpa ip6.arpa
      }
      prometheus :9153
      forward . /etc/resolv.conf {
        policy sequential
      }
      cache 30
      reload
    }
kind: ConfigMap
metadata:

```

```
labels:  
  dns.operator.openshift.io/owning-dns: default  
name: dns-default  
namespace: openshift-dns
```

- 1 对 **forwardPlugin** 的更改会触发 CoreDNS 守护进程集的滚动更新。

其他资源

- 有关 DNS 转发的详情，请查看 [CoreDNS 转发文档](#)。

5.4. DNS OPERATOR 状态

您可以使用 **oc describe** 命令来检查状态并查看 DNS Operator 的详情。

流程

查看 DNS Operator 的状态：

```
$ oc describe clusteroperators/dns
```

5.5. DNS OPERATOR 日志

您可以使用 **oc logs** 命令来查看 DNS Operator 日志。

流程

查看 DNS Operator 的日志：

```
$ oc logs -n openshift-dns-operator deployment/dns-operator -c dns-operator
```

第 6 章 OPENSIFT CONTAINER PLATFORM 中的 INGRESS OPERATOR

6.1. OPENSIFT CONTAINER PLATFORM INGRESS OPERATOR

在创建 OpenShift Container Platform 集群时，在集群中运行的 Pod 和服务会各自分配自己的 IP 地址。IP 地址可供附近运行的其他容器集和服务访问，但外部客户端无法访问这些 IP 地址。Ingress Operator 实现 **IngressController** API，是负责启用对 OpenShift Container Platform 集群服务的外部访问的组件。

Ingress Operator 通过部署和管理一个或多个基于 HAProxy 的 **Ingress Controller** 来处理路由，使外部客户端可以访问您的服务。您可以通过指定 OpenShift Container Platform **Route** 和 Kubernetes **Ingress** 资源，来使用 Ingress Operator 路由流量。Ingress Controller 中的配置（如定义 **endpointPublishingStrategy** 类型和内部负载均衡）提供了发布 Ingress Controller 端点的方法。

6.2. INGRESS 配置资产

安装程序在 **config.openshift.io** API 组中生成带有 **Ingress** 资源的资产，**cluster-ingress-02-config.yml**。

Ingress 资源的 YAML 定义

```
apiVersion: config.openshift.io/v1
kind: Ingress
metadata:
  name: cluster
spec:
  domain: apps.openshift demos.com
```

安装程序将这个资产保存在 **manifests/** 目录下的 **cluster-ingress-02-config.yml** 文件中。此 **Ingress** 资源定义 Ingress 的集群范围配置。此 Ingress 配置的用法如下所示：

- Ingress Operator 使用集群 Ingress 配置中的域，作为默认 Ingress Controller 的域。
- OpenShift API Server Operator 使用集群 Ingress 配置中的域。在为未指定显式主机的 **Route** 资源生成默认主机时，还会使用此域。

6.3. INGRESS 控制器配置参数

ingresscontrollers.operator.openshift.io 资源提供了以下配置参数。

参数	描述
----	----

参数	描述
domain	<p>domain 是 Ingress controller 服务的一个 DNS 名称，用于配置多个功能：</p> <ul style="list-style-type: none"> 对于 LoadBalancerService 端点发布策略，domain 被用来配置 DNS 记录。请参阅 endpointPublishingStrategy。 当使用生成的默认证书时，该证书对域及其子域有效。请参阅 defaultCertificate。 该值会发布到独立的 Route 状态，以便用户了解目标外部 DNS 记录的位置。 <p>一个 domain 值在所有 Ingress 控制器中需要是唯一的，且不能更新。</p> <p>如果为空，默认值为 ingress.config.openshift.io/cluster.spec.domain。</p>
replicas	<p>replicas 是 Ingress 控制器副本数量。如果没有设置，则默认值为 2。</p>
endpointPublishingStrategy	<p>endpointPublishingStrategy 用于向其他网络发布 Ingress Controller 端点，以启用负载均衡器集成，并提供对其他系统的访问。</p> <p>如果没有设置，则默认值基于 infrastructure.config.openshift.io/cluster.status.platform：</p> <ul style="list-style-type: none"> AWS: LoadBalancerService（具有外部范围） Azure: LoadBalancerService（具有外部范围） GCP: LoadBalancerService（具有外部范围） 裸机: NodePortService 其它: HostNetwork。 <p>endpointPublishingStrategy 的值不能被更新。</p>
defaultCertificate	<p>defaultCertificate 的值是一个到包括由 Ingress controller 提供的默认证书的 secret 的指代。当 Routes 没有指定其自身证书时，使用 defaultCertificate。</p> <p>secret 必须包含以下密钥和数据：*tls.crt：证书文件内容 *tls.key：密钥文件内容</p> <p>如果没有设置，则自动生成和使用通配符证书。该证书对 Ingress Controller 的域和子域有效，所生成的证书的 CA 会自动与集群的信任存储集成。</p> <p>内部证书（无论是生成的证书还是用户指定的证书）自动与 OpenShift Container Platform 内置的 OAuth 服务器集成。</p>
namespaceSelector	<p>namespaceSelector 用来过滤由 Ingress 控制器提供服务的一组命名空间。这对实现分片（shard）非常有用。</p>
routeSelector	<p>routeSelector 用于由 Ingress 控制器提供服务的一组 Route。这对实现分片（shard）非常有用。</p>

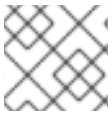
参数	描述
nodePlacement	<p>nodePlacement 启用对 Ingress 控制器调度的明确控制。</p> <p>如果没有设置，则使用默认值。</p>  <p>注意</p> <p>nodePlacement 参数包括两个部分：nodeSelector 和 tolerations。例如：</p> <pre>nodePlacement: nodeSelector: matchLabels: kubernetes.io/os: linux tolerations: - effect: NoSchedule operator: Exists</pre>

参数	描述
<p>tlsSecurityProfile</p>	<p>tlsSecurityProfile 指定 Ingress 控制器的 TLS 连接的设置。</p> <p>如果没有设置，则默认值基于 <code>apiservers.config.openshift.io/cluster</code> 资源。</p> <p>当使用 Old、Intermediate 和 Modern 配置集类型时，有效的配置集可能会在不同发行版本间有所改变。例如：在版本 X.Y.Z 中使用 Intermediate 进行了部署，当升级到版本 X.Y.Z+1 时可能会把一个新的配置集应用到 Ingress 控制器，从而导致一个 rollout 操作。</p> <p>Ingress 控制器的 TLS 的最低版本是 1.1，最高 TLS 版本为 1.2。</p> <div data-bbox="518 645 624 1173" style="background-color: black; width: 66px; height: 236px; margin-bottom: 10px;"></div> <p>重要</p> <p>HAProxy Ingress controller 镜像不支持 TLS 1.3。因为 Modern 配置集需要 TLS 1.3，所以这个配置集不被支持。Ingress Operator 会将 Modern 配置集转换为 Intermediate。</p> <p>Ingress Operator 还会将 Old 或 Custom 配置集的 TLS 1.0 转换为 1.1，将 Custom 配置集的 TLS 1.3 转换为 1.2。</p> <p>OpenShift Container Platform 路由器启用 Red Hat-distributed OpenSSL 默认集合 TLS 1.3 密码套件，它使用 TLS_AES_128_CCM_SHA256、TLS_CHACHA20_POLY1305_SHA256、TLS_AES_256_GCM_SHA384 和 TLS_AES_128_GCM_SHA256。您的集群可能会接受 TLS 1.3 连接和密码套件，即使 OpenShift Container Platform 4.6、4.7 和 4.8 不支持 TLS 1.3。</p> <div data-bbox="518 1223 624 1357" style="background-color: black; width: 66px; height: 60px;"></div> <p>注意</p> <p>加密器和配置的安全配置集的最小 TLS 版本反映在 TLSProfile 状态中。</p>

参数	描述
routeAdmission	<p>routeAdmission 定义了处理新路由声明的策略，如允许或拒绝命名空间间的声明。</p> <p>namespaceOwnership 描述了如何处理跨命名空间的主机名声明。默认为 Strict。</p> <ul style="list-style-type: none">● Strict : 不允许路由在命名空间间声明相同的主机名。● InterNamespaceAllowed : 允许路由在命名空间间声明相同主机名的不同路径。 <p>wildcardPolicy 描述了 Ingress Controller 如何处理采用通配符策略的路由。</p> <ul style="list-style-type: none">● WildcardsAllowed : 表示 Ingress Controller 允许采用任何通配符策略的路由。● WildcardsDisallowed : 表示 Ingress Controller 只接受采用 None 通配符策略的路由。将 wildcardPolicy 从 WildcardsAllowed 更新为 WildcardsDisallowed，会导致采用 Subdomain 通配符策略的已接受路由停止工作。这些路由必须重新创建为采用 None 通配符策略，让 Ingress Controller 重新接受。WildcardsDisallowed 是默认设置。

参数	描述
IngressControllerLogging	<p>logging 定义了有关在哪里记录什么内容的参数。如果此字段为空，则会启用运行日志，但禁用访问日志。</p> <ul style="list-style-type: none"> ● access 描述了客户端请求的日志记录方式。如果此字段为空，则禁用访问日志。 <ul style="list-style-type: none"> ○ destination 描述日志消息的目的地。 <ul style="list-style-type: none"> ■ type 是日志的目的地类型： <ul style="list-style-type: none"> ● Container 指定日志应该进入 sidecar 容器。Ingress Operator 在 Ingress Controller pod 上配置名为 logs 的容器，并配置 Ingress Controller 以将日志写入容器。管理员应该配置一个自定义日志记录解决方案，从该容器读取日志。使用容器日志意味着，如果日志速率超过容器运行时或自定义日志解决方案的容量，则可能会出现日志丢失的问题。 ● Syslog 指定日志发送到 Syslog 端点。管理员必须指定可以接收 Syslog 消息的端点。管理员应该已经配置了一个自定义 Syslog 实例。 ■ container 描述了 Container 日志记录目的地类型的参数。目前没有容器日志记录参数，因此此字段必须为空。 ■ syslog 描述了 Syslog 日志记录目的地类型的参数： <ul style="list-style-type: none"> ● address 是接收日志消息的 syslog 端点的 IP 地址。 ● port 是接收日志消息的 syslog 端点的 UDP 端口号。 ● facility 指定日志消息的 syslog 工具。如果该字段为空，则工具为 local1。否则，它必须指定一个有效的 syslog 工具：kern、user、mail、daemon、auth、syslog、lpr、news、uucp、cron、auth2、ftp、ntp、audit、alert、cron2、local0、local1、local2、local3、local4、local5、local6 或 local7。 ○ httpLogFormat 指定 HTTP 请求的日志消息格式。如果此字段为空，日志消息将使用实现中的默认 HTTP 日志格式。有关 HAProxy 的默认 HTTP 日志格式，请参阅 HAProxy 文档。

参数	描述
httpHeaders	<p>httpHeaders 为 HTTP 标头定义策略。</p> <p>通过为 IngressControllerHTTPHeaders 设置 forwardHeaderPolicy，您可以指定 Ingress 控制器何时和如何设置 Forwarded、X-Forwarded-For、X-Forwarded-Host、X-Forwarded-Port、X-Forwarded-Proto 和 X-Forwarded-Proto-Version HTTP 标头。</p> <p>默认情况下，策略设置为 Append。</p> <ul style="list-style-type: none"> ● Append 指定 Ingress Controller 会附加标头，并保留任何现有的标头。 ● Replace 指定 Ingress Controller 设置标头，删除任何现有的标头。 ● IfNone 指定 Ingress Controller 在尚未设置标头时设置它们。 ● Never 指定 Ingress Controller 不会设置标头，并保留任何现有的标头。



注意

所有参数都是可选的。

6.3.1. Ingress Controller TLS 安全配置集

TLS 安全配置文件为服务器提供了一种方式，以规范连接的客户端在连接服务器时可以使用哪些密码。

6.3.1.1. 了解 TLS 安全配置集

您可以使用 TLS（Transport Layer Security）安全配置集来定义各种 OpenShift Container Platform 组件需要哪些 TLS 密码。OpenShift Container Platform TLS 安全配置集基于 [Mozilla 推荐的配置](#)。

您可以为每个组件指定以下 TLS 安全配置集之一：

表 6.1. TLS 安全配置集

配置集	描述
Old	<p>此配置集用于旧的客户端或库。该配置集基于旧的向后兼容性建议配置。</p> <p>Old 配置集要求最低 TLS 版本 1.0。</p> <div style="display: flex; align-items: center;"> <div> <p>注意</p> <p>对于 Ingress Controller，最小 TLS 版本从 1.0 转换为 1.1。</p> </div> </div>

配置集	描述
Intermediate	<p>这个配置集是大多数客户端的建议配置。它是 Ingress Controller 和 control plane 的默认 TLS 安全配置集。该配置集基于 Intermediate 兼容性 推荐的配置。</p> <p>Intermediate 配置集需要最小 TLS 版本 1.2。</p>
Modern	<p>此配置集主要用于不需要向后兼容的现代客户端。这个配置集基于 Modern 兼容性 推荐的配置。</p> <p>Modern 配置集需要最低 TLS 版本 1.3。</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>注意</p> <p>在 OpenShift Container Platform 4.6、4.7 和 4.8 中，Modern 配置集不被支持。如果选择，Intermediate 配置集会被启用。</p> </div> </div> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 10px;"></div> <div> <p>重要</p> <p>Modern 配置集当前不受支持。</p> </div> </div>
Custom	<p>此配置集允许您定义要使用的 TLS 版本和密码。</p> <div style="background-color: #fff9c4; padding: 10px; margin: 10px 0;"> <div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"></div> <div> <p>警告</p> <p>使用 Custom 配置集时要谨慎，因为无效的配置可能会导致问题。</p> </div> </div> </div> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 10px;"></div> <div> <p>注意</p> <p>OpenShift Container Platform 路由器启用 Red Hat-istributed OpenSSL 默认 TLS 1.3 密码套件集。您的集群可能会接受 TLS 1.3 连接和密码套件，即使 OpenShift Container Platform 4.6、4.7 和 4.8 不支持 TLS 1.3。</p> </div> </div>



注意

当使用预定义的配置集类型时，有效的配置集配置可能会在发行版本之间有所改变。例如，使用在版本 X.Y.Z 中部署的 Intermediate 配置集指定了一个规格，升级到版本 X.Y.Z+1 可能会导致应用新的配置集配置，从而导致推出部署。

6.3.1.2. 为 Ingress Controller 配置 TLS 安全配置集

要为 Ingress Controller 配置 TLS 安全配置集，请编辑 **IngressController** 自定义资源（CR）来指定预定义或自定义 TLS 安全配置集。如果没有配置 TLS 安全配置集，则默认值基于为 API 服务器设置的 TLS 安全配置集。

配置 Old TLS 安全配置集的 IngressController CR 示例

```
apiVersion: operator.openshift.io/v1
kind: IngressController
...
spec:
  tlsSecurityProfile:
    old: {}
    type: Old
  ...
```

TLS 安全配置集定义 Ingress Controller 的 TLS 连接的最低 TLS 版本和 TLS 密码。

您可以在 **Status.Tls Profile** 和 **Spec.Tls Security Profile** 下看到 **IngressController** 自定义资源（CR）中配置的 TLS 安全配置集的密码和最小 TLS 版本。对于 **Custom** TLS 安全配置集，这两个参数下列出了特定的密码和最低 TLS 版本。



重要

HAProxy Ingress Controller 镜像不支持 TLS 1.3，因为 **Modern** 配置集需要 TLS 1.3，因此不支持它。Ingress Operator 会将 **Modern** 配置集转换为 **Intermediate**。Ingress Operator 还会将 **Old** 或 **Custom** 配置集的 TLS 1.0 转换为 1.1，将 **Custom** 配置集的 TLS 1.3 转换为 1.2。

先决条件

- 您可以使用具有 **cluster-admin** 角色的用户访问集群。

流程

1. 编辑 **openshift-ingress-operator** 项目中的 **IngressController** CR，以配置 TLS 安全配置集：

```
$ oc edit IngressController default -n openshift-ingress-operator
```

2. 添加 **spec.tlsSecurityProfile** 字段：

Custom 配置集的 IngressController CR 示例

```
apiVersion: operator.openshift.io/v1
kind: IngressController
...
spec:
  tlsSecurityProfile:
    type: Custom 1
    custom: 2
      ciphers: 3
        - ECDHE-ECDSA-CHACHA20-POLY1305
        - ECDHE-RSA-CHACHA20-POLY1305
        - ECDHE-RSA-AES128-GCM-SHA256
```

```
- ECDHE-ECDSA-AES128-GCM-SHA256
minTLSVersion: VersionTLS11
```

```
...
```

- 1 指定 TLS 安全配置集类型 (**Old**、**Intermediate** 或 **Custom**)。默认值为 **Intermediate**。
- 2 为所选类型指定适当的字段：
 - **old:** {}
 - **intermediate:** {}
 - **custom:**
- 3 对于 **custom** 类型，请指定 TLS 密码列表和最低接受的 TLS 版本。

3. 保存文件以使改变生效。

验证

- 验证 **IngressController** CR 中是否设置了配置集：

```
$ oc describe IngressController default -n openshift-ingress-operator
```

输出示例

```
Name:      default
Namespace: openshift-ingress-operator
Labels:    <none>
Annotations: <none>
API Version: operator.openshift.io/v1
Kind:      IngressController
...
Spec:
...
Tls Security Profile:
  Custom:
    Ciphers:
      ECDHE-ECDSA-CHACHA20-POLY1305
      ECDHE-RSA-CHACHA20-POLY1305
      ECDHE-RSA-AES128-GCM-SHA256
      ECDHE-ECDSA-AES128-GCM-SHA256
    Min TLS Version: VersionTLS11
  Type:      Custom
...

```

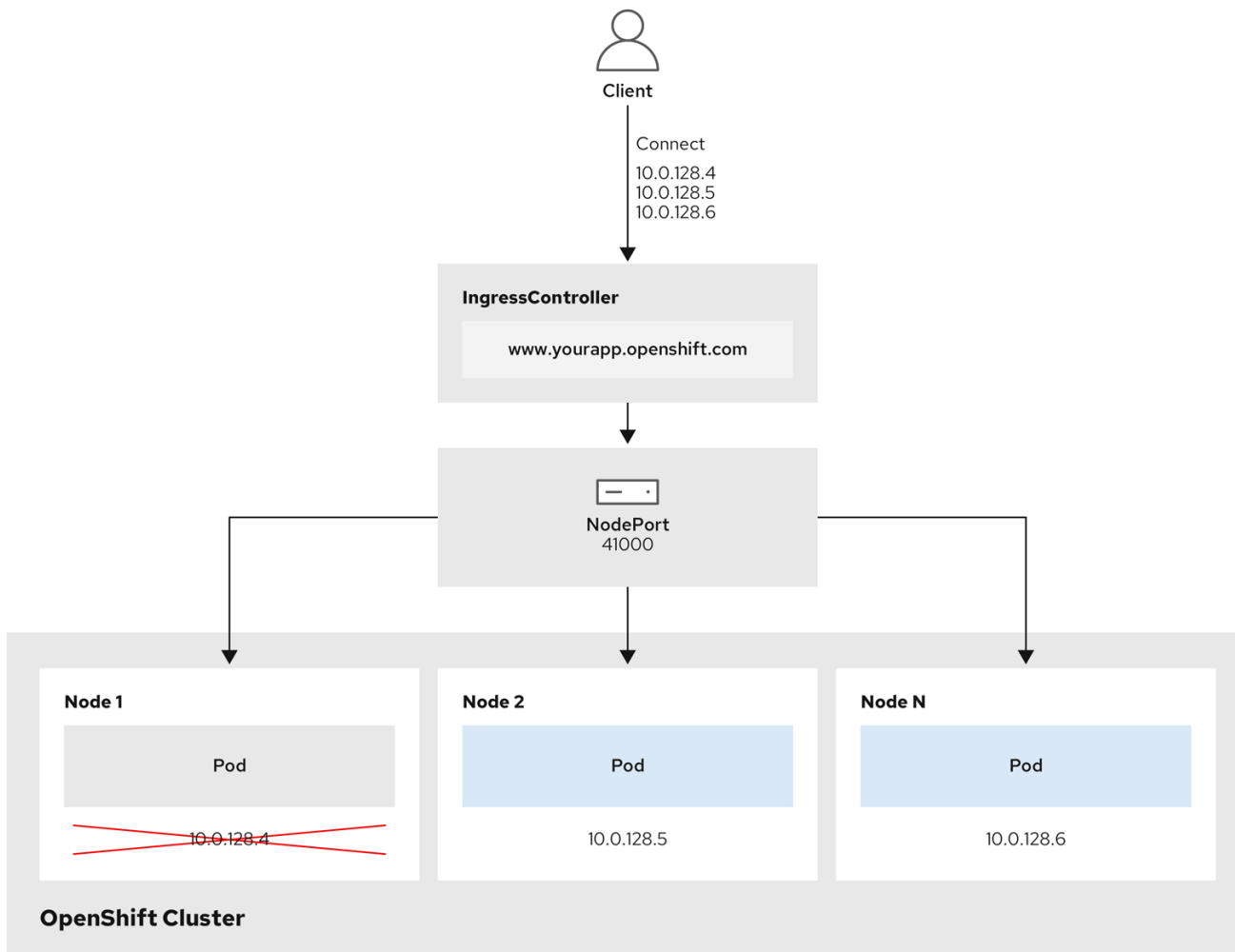
6.3.2. Ingress 控制器端点发布策略

NodePortService 端点发布策略

NodePortService 端点发布策略使用 Kubernetes NodePort 服务发布 Ingress Controller。

在这个配置中，Ingress Controller 部署使用容器网络。创建了一个 NodePortService 来发布部署。特定的节点端口由 OpenShift Container Platform 动态分配；但是，为了支持静态端口分配，您会保留对受管 NodePortService 的节点端口字段的更改。

图 6.1. NodePortService 图表



202_OpenShift_0222

上图显示了与 OpenShift Container Platform Ingress NodePort 端点发布策略相关的以下概念：

- 集群中的所有可用节点均有自己的外部可访问 IP 地址。集群中运行的服务绑定到所有节点的唯一 NodePort。
- 当客户端连接到停机的节点时，例如通过连接图形中的 **10.0.128.4** IP 地址，节点端口将客户端直接连接到运行该服务的可用节点。在这种情况下，不需要负载均衡。如图中所示，**10.0.128.4** 地址已停机，且必须改为使用另一个 IP 地址。



注意

Ingress Operator 忽略对服务的 `.spec.ports[].nodePort` 字段的任何更新。

默认情况下，端口会自动分配，您可以访问集成的端口分配。但是，有时需要静态分配端口来与现有基础架构集成，这些基础架构可能无法根据动态端口进行重新配置。要实现与静态节点端口的集成，您可以直接更新受管服务资源。

如需有关 daemonset 的更多信息，请参阅[关于 NodePort 的 Kubernetes 服务文档](#)。

HostNetwork 端点发布策略

HostNetwork 端点发布策略会在部署 Ingress Controller 的节点端口上发布 Ingress Controller。

带有 **HostNetwork** 端点发布策略的 Ingress 控制器每个节点只能有一个 pod 副本。如果您想要 n 个副本，则必须至少使用可调度这些副本的 n 个节点。因为每个 Pod 副本都会通过调度的节点主机上的端口 **80** 和 **443** 进行请求，所以如果同一节点上的其他 pod 使用这些端口，则无法将副本调度到该节点。

6.4. 查看默认的 INGRESS CONTROLLER

Ingress Operator 是 OpenShift Container Platform 的一个核心功能，开箱即用。

每个 OpenShift Container Platform 新安装都有一个名为 default 的 **ingresscontroller**。它可以通过额外的 Ingress Controller 来补充。如果删除了默认的 **ingresscontroller**，Ingress Operator 会在一分钟内自动重新创建。

流程

- 查看默认的 Ingress Controller :

```
$ oc describe --namespace=openshift-ingress-operator ingresscontroller/default
```

6.5. 查看 INGRESS OPERATOR 状态

您可以查看并检查 Ingress Operator 的状态。

流程

- 查看您的 Ingress Operator 状态 :

```
$ oc describe clusteroperators/ingress
```

6.6. 查看 INGRESS CONTROLLER 日志

您可以查看 Ingress Controller 日志。

流程

- 查看 Ingress Controller 日志 :

```
$ oc logs --namespace=openshift-ingress-operator deployments/ingress-operator
```

6.7. 查看 INGRESS CONTROLLER 状态

您可以查看特定 Ingress Controller 的状态。

流程

- 查看 Ingress Controller 的状态 :

```
$ oc describe --namespace=openshift-ingress-operator ingresscontroller/<name>
```

6.8. 配置 INGRESS CONTROLLER

6.8.1. 设置自定义默认证书

作为管理员，您可以通过创建 Secret 资源并编辑 **IngressController** 自定义资源 (CR)，将 Ingress Controller 配置为使用自定义证书。

先决条件

- 您必须在 PEM 编码文件中有一个证书/密钥对，其中该证书由可信证书认证机构签名，或者由您在一个自定义 PKI 中配置的私有可信证书认证机构签名。
- 您的证书满足以下要求：
 - 该证书对入口域有效。
 - 证书使用 **subjectAltName** 扩展来指定通配符域，如 ***.apps.ocp4.example.com**。
- 您必须有一个 **IngressController** CR。您可以使用默认值：

```
$ oc --namespace openshift-ingress-operator get ingresscontrollers
```

输出示例

```
NAME    AGE
default 10m
```



注意

如果您有中间证书，则必须将其包含在包含自定义默认证书的 secret 的 **tls.crt** 文件中。指定证书时指定的顺序是相关的；在任意服务器证书后列出您的中间证书。

流程

以下步骤假定自定义证书和密钥对位于当前工作目录下的 **tls.crt** 和 **tls.key** 文件中。替换 **tls.crt** 和 **tls.key** 的实际路径名。在创建 Secret 资源并在 IngressController CR 中引用它时，您也可以将 **custom-certs-default** 替换成另一名称。



注意

此操作会导致使用滚动部署策略重新部署 Ingress Controller。

1. 使用 **tls.crt** 和 **tls.key** 文件，创建在 **openshift-ingress** 命名空间中包含自定义证书的 Secret 资源。

```
$ oc --namespace openshift-ingress create secret tls custom-certs-default --cert=tls.crt --key=tls.key
```

2. 更新 IngressController CR，以引用新的证书 Secret：

```
$ oc patch --type=merge --namespace openshift-ingress-operator ingresscontrollers/default \
  --patch '{"spec":{"defaultCertificate":{"name":"custom-certs-default"}}}'
```


3. 验证更新是否已生效：

```
$ echo Q | \
  openssl s_client -connect console-openshift-console.apps.<domain>:443 -showcerts
2>/dev/null | \
  openssl x509 -noout -subject -issuer -enddate
```

其中：

<domain>

指定集群的基域名。

输出示例

```
subject=C = US, ST = NC, L = Raleigh, O = RH, OU = OCP4, CN = *.apps.example.com
issuer=C = US, ST = NC, L = Raleigh, O = RH, OU = OCP4, CN = example.com
notAfter=May 10 08:32:45 2022 GM
```

证书 Secret 名称应该与用来更新 CR 的值匹配。

修改了 IngressController CR 后，Ingress Operator 将更新 Ingress Controller 的部署以使用自定义证书。

6.8.2. 删除自定义默认证书

作为管理员，您可以删除配置了 Ingress Controller 的自定义证书。

先决条件

- 您可以使用具有 **cluster-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI (**oc**)。
- 您之前为 Ingress Controller 配置了自定义默认证书。

流程

- 要删除自定义证书并恢复 OpenShift Container Platform 附带的证书，请输入以下命令：

```
$ oc patch -n openshift-ingress-operator ingresscontrollers/default \
  --type json -p '$- op: remove\n path: /spec/defaultCertificate'
```

集群协调新证书配置时可能会有延迟。

验证

- 要确认原始集群证书已被恢复，请输入以下命令：

```
$ echo Q | \
  openssl s_client -connect console-openshift-console.apps.<domain>:443 -showcerts
2>/dev/null | \
  openssl x509 -noout -subject -issuer -enddate
```

其中：

<domain>

指定集群的基域名。

输出示例

```
subject=CN = *.apps.<domain>
issuer=CN = ingress-operator@1620633373
notAfter=May 10 10:44:36 2023 GMT
```

6.8.3. 扩展 Ingress Controller

手动扩展 Ingress Controller 以满足路由性能或可用性要求，如提高吞吐量的要求。**oc** 命令用于扩展 **IngressController** 资源。以下流程提供了扩展默认 **IngressController** 的示例。

流程

1. 查看默认 **IngressController** 的当前可用副本数：

```
$ oc get -n openshift-ingress-operator ingresscontrollers/default -o
jsonpath='{$.status.availableReplicas}'
```

输出示例

```
2
```

2. 使用 **oc patch** 命令，将默认 **IngressController** 扩展至所需的副本数。以下示例将默认 **IngressController** 扩展至 3 个副本：

```
$ oc patch -n openshift-ingress-operator ingresscontroller/default --patch '{"spec":{"replicas":
3}}' --type=merge
```

输出示例

```
ingresscontroller.operator.openshift.io/default patched
```

3. 验证默认 **IngressController** 是否已扩展至您指定的副本数：

```
$ oc get -n openshift-ingress-operator ingresscontrollers/default -o
jsonpath='{$.status.availableReplicas}'
```

输出示例

```
3
```

**注意**

扩展不是立刻就可以完成的操作，因为它需要时间来创建所需的副本数。

6.8.4. 配置 Ingress 访问日志

您可以配置 Ingress Controller 以启用访问日志。如果您的集群没有接收许多流量，那么您可以将日志记录到 sidecar。如果您的集群接收大量流量，为了避免超出日志记录堆栈的容量，或与 OpenShift Container Platform 之外的日志记录基础架构集成，您可以将日志转发到自定义 syslog 端点。您还可以指定访问日志的格式。

当不存在 Syslog 日志记录基础架构时，容器日志记录可用于在低流量集群中启用访问日志，或者在诊断 Ingress Controller 时进行简短使用。

对于访问日志可能会超过集群日志记录堆栈容量的高流量集群，或需要任何日志记录解决方案与现有 Syslog 日志记录基础架构集成的环境，则需要 syslog。Syslog 用例可能会相互重叠。

先决条件

- 以具有 **cluster-admin** 特权的用户身份登录。

流程

配置 Ingress 访问日志到 sidecar。

- 要配置 Ingress 访问日志记录，您必须使用 **spec.logging.access.destination** 指定一个目的地。要将日志记录指定到 sidecar 容器，您必须指定 **Container** **spec.logging.access.destination.type**。以下示例是将日志记录到 **Container** 目的地的 Ingress Controller 定义：

```
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  name: default
  namespace: openshift-ingress-operator
spec:
  replicas: 2
  endpointPublishingStrategy:
    type: NodePortService ❶
  logging:
    access:
      destination:
        type: Container
```

- ❶ 在将 Ingress 访问日志配置到 sidecar 时，不需要使用 **NodePortService**。Ingress 日志记录与任何 **endpointPublishingStrategy** 兼容。

- 当将 Ingress Controller 配置为日志记录到 sidecar 时，Operator 会在 Ingress Controller Pod 中创建一个名为 **logs** 的容器：

```
$ oc -n openshift-ingress logs deployment.apps/router-default -c logs
```

输出示例

```
2020-05-11T19:11:50.135710+00:00 router-default-57dfc6cd95-bpmk6 router-default-57dfc6cd95-bpmk6 haproxy[108]: 174.19.21.82:39654 [11/May/2020:19:11:50.133] public be_http:hello-openshift:hello-openshift/pod:hello-openshift:hello-openshift:10.128.2.12:8080 0/0/1/0/1 200 142 - - --NI 1/1/0/0/0 0/0 "GET / HTTP/1.1"
```

配置 Ingress 访问日志记录到 Syslog 端点。

- 要配置 Ingress 访问日志记录，您必须使用 **spec.logging.access.destination** 指定一个目的地。要将日志记录指定到 Syslog 端点目的地，您必须为 **spec.logging.access.destination.type** 指定 **Syslog**。如果目的地类型是 **Syslog**，则必须使用 **spec.logging.access.destination.syslog.endpoint** 指定一个目的地端点，并可使用 **spec.logging.access.destination.syslog.facility** 指定一个工具。以下示例是将日志记录到 **Syslog** 目的地的 Ingress Controller 定义：

```
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  name: default
  namespace: openshift-ingress-operator
spec:
  replicas: 2
  endpointPublishingStrategy:
    type: NodePortService
  logging:
    access:
      destination:
        type: Syslog
      syslog:
        address: 1.2.3.4
        port: 10514
```



注意

Syslog 目的地端口必须是 UDP。

使用特定的日志格式配置 Ingress 访问日志。

- 您可以指定 **spec.logging.access.httpLogFormat** 来自定义日志格式。以下示例是一个 Ingress Controller 定义，它将日志记录到 IP 地址为 1.2.3.4、端口为 10514 的 **syslog** 端点：

```
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  name: default
  namespace: openshift-ingress-operator
spec:
  replicas: 2
  endpointPublishingStrategy:
    type: NodePortService
  logging:
    access:
      destination:
        type: Syslog
      syslog:
        address: 1.2.3.4
        port: 10514
      httpLogFormat: '%ci:%cp [%t] %ft %b/%s %B %bq %HM %HU %HV'
```

禁用 Ingress 访问日志。

- 要禁用 Ingress 访问日志，请保留 **spec.logging** 或 **spec.logging.access** 为空：

■

```

apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  name: default
  namespace: openshift-ingress-operator
spec:
  replicas: 2
  endpointPublishingStrategy:
    type: NodePortService
  logging:
    access: null

```

6.8.5. Ingress Controller 分片

Ingress Controller 或路由器是网络流量进入集群的主要机制，因此对它们的需求可能非常大。作为集群管理员，您可以对路由进行分片，以达到以下目的：

- 在 Ingress Controller 或路由器与一些路由之间实现平衡，由此加快对变更的响应。
- 分配特定的路由，使其具有不同于其它路由的可靠性保证。
- 允许特定的 Ingress Controller 定义不同的策略。
- 只允许特定的路由使用其他功能。
- 在不同的地址上公开不同的路由，例如使内部和外部用户能够看到不同的路由。

Ingress Controller 可以使用路由标签或命名空间标签作为分片方法。

6.8.5.1. 通过路由标签 (label) 配置 Ingress Controller 分片

使用路由标签进行 Ingress Controller 分片，意味着 Ingress Controller 提供由路由选择器选择的任意命名空间中的所有路由。

在一组 Ingress Controller 之间平衡传入的流量负载时，以及在将流量隔离到特定 Ingress Controller 时，Ingress Controller 分片会很有用处。例如，A 公司的流量使用一个 Ingress Controller，B 公司的流量则使用另外一个 Ingress Controller。

流程

1. 编辑 **router-internal.yaml** 文件：

```

# cat router-internal.yaml
apiVersion: v1
items:
- apiVersion: operator.openshift.io/v1
  kind: IngressController
  metadata:
    name: sharded
    namespace: openshift-ingress-operator
  spec:
    domain: <apps-sharded.basedomain.example.net>
    nodePlacement:
      nodeSelector:
        matchLabels:

```

```

node-role.kubernetes.io/worker: ""
routeSelector:
  matchLabels:
    type: sharded
status: {}
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""

```

- 应用 Ingress Controller **router-internal.yaml** 文件：

```
# oc apply -f router-internal.yaml
```

Ingress Controller 选择具有 **type: sharded** 标签的任意命名空间中的路由。

6.8.5.2. 使用命名空间标签配置 Ingress Controller 分片

使用命名空间标签进行 Ingress Controller 分片，意味着 Ingress Controller 提供由命名空间选择器选择的任意命名空间中的所有路由。

在一组 Ingress Controller 之间平衡传入的流量负载时，以及在将流量隔离到特定 Ingress Controller 时，Ingress Controller 分片会很有用处。例如，A 公司的流量使用一个 Ingress Controller，B 公司的流量则使用另外一个 Ingress Controller。



警告

如果部署 Keepalived Ingress VIP，请不要为 **endpointPublishingStrategy** 参数部署一个值为 **HostNetwork** 的非默认 Ingress Controller。这样做可能会导致问题。将值 **NodePort** 而不是 **HostNetwork** 用于 **endpointPublishingStrategy**。

流程

- 编辑 **router-internal.yaml** 文件：

```
# cat router-internal.yaml
```

输出示例

```

apiVersion: v1
items:
- apiVersion: operator.openshift.io/v1
  kind: IngressController
  metadata:
    name: sharded
    namespace: openshift-ingress-operator
  spec:
    domain: <apps-sharded.basedomain.example.net>
    nodePlacement:
      nodeSelector:

```

```

matchLabels:
  node-role.kubernetes.io/worker: ""
namespaceSelector:
  matchLabels:
    type: sharded
status: {}
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""

```

- 应用 Ingress Controller **router-internal.yaml** 文件：

```
# oc apply -f router-internal.yaml
```

Ingress Controller 选择由命名空间选择器选择的具有 **type: sharded** 标签的任意命名空间中的路由。

6.8.6. 配置 Ingress Controller 以使用内部负载均衡器

当在云平台上创建 Ingress Controller 时，Ingress Controller 默认由一个公共云负载均衡器发布。作为管理员，您可以创建一个使用内部云负载均衡器的 Ingress Controller。



警告

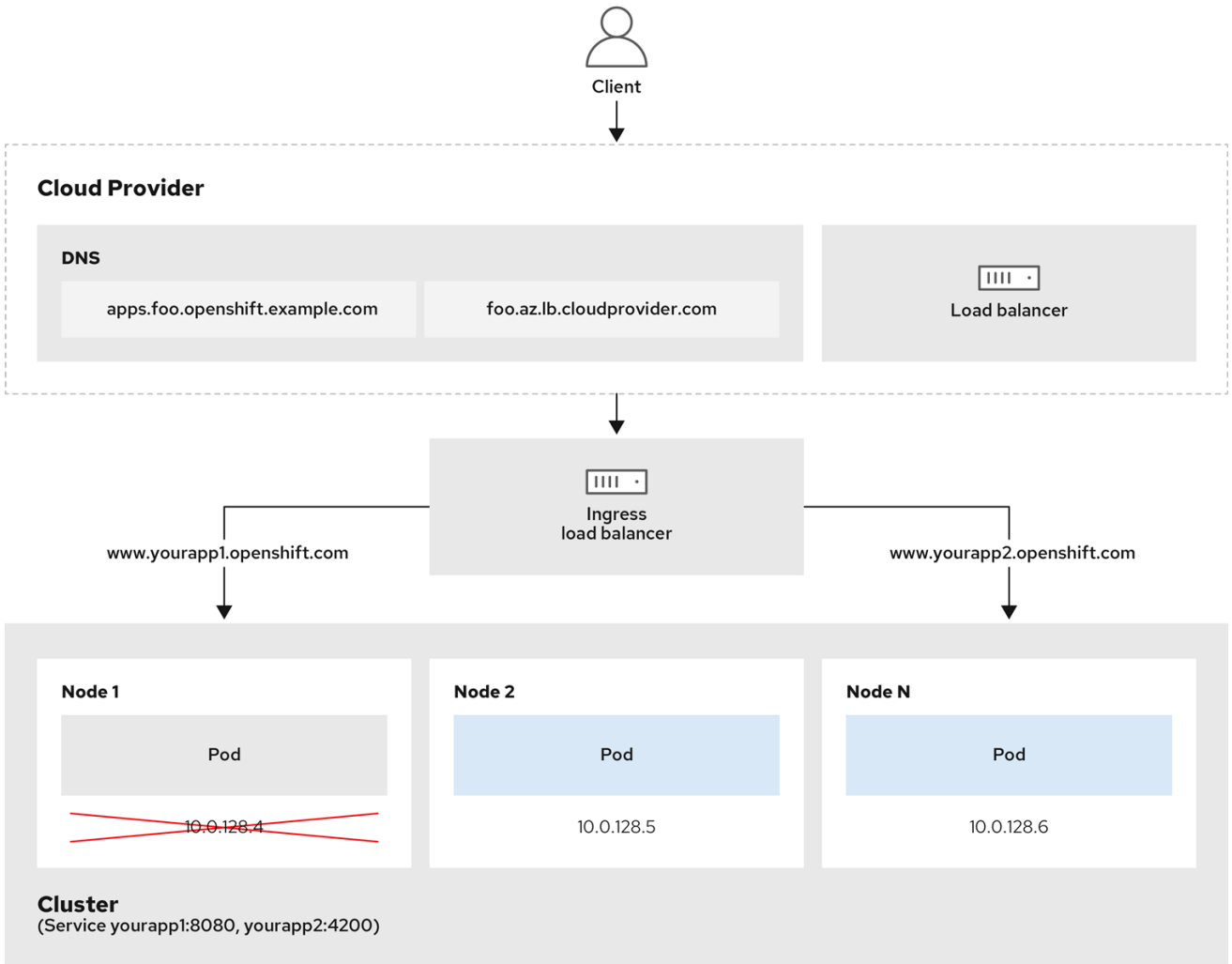
如果云供应商是 Microsoft Azure，则必须至少有一个指向节点的公共负载均衡器。如果不这样做，所有节点都将丢失到互联网的出站连接。



重要

如果要更改 **IngressController** 对象的 **scope**，您必须删除并重新创建 **IngressController** 对象。您无法在创建自定义资源 (CR) 后更改 **.spec.endpointPublishingStrategy.loadBalancer.scope** 参数。

图 6.2. LoadBalancer 图表



202_OpenShift_0222

上图显示了与 OpenShift Container Platform Ingress LoadBalancerService 端点发布策略相关的以下概念：

- 您可以使用 OpenShift Ingress Controller Load Balancer 在外部使用云供应商负载均衡器或内部加载负载。
- 您可以使用负载均衡器的单个 IP 地址以及更熟悉的端口，如 8080 和 4200，如图形中所述的集群所示。
- 来自外部负载均衡器的流量定向到 pod，并由负载均衡器管理，如下节点的实例中所述。有关实现详情请查看 [Kubernetes 服务文档](#)。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 在名为 `<name>-ingress-controller.yaml` 的文件中创建 **IngressController** 自定义资源 (CR)，如下例所示：

■


```

apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  namespace: openshift-ingress-operator
  name: <name> ❶
spec:
  domain: <domain> ❷
  endpointPublishingStrategy:
    type: LoadBalancerService
  loadBalancer:
    scope: Internal ❸

```

- ❶ 将 `<name>` 替换为 **IngressController** 对象的名称。
- ❷ 指定控制器发布的应用程序的 **domain**。
- ❸ 指定一个 **Internal** 值以使用内部负载均衡器。

2. 运行以下命令，创建上一步中定义的 Ingress Controller：

```
$ oc create -f <name>-ingress-controller.yaml ❶
```

- ❶ 将 `<name>` 替换为 **IngressController** 对象的名称。

3. 可选：通过运行以下命令确认创建了 Ingress Controller：

```
$ oc --all-namespaces=true get ingresscontrollers
```

6.8.7. 将集群的默认 Ingress Controller 配置为内部

您可以通过删除并重新它来将默认 Ingress Controller 配置为内部。



警告

如果云供应商是 Microsoft Azure，则必须至少有一个指向节点的公共负载均衡器。如果不这样做，所有节点都将丢失到互联网的出站连接。



重要

如果要更改 **IngressController** 对象的 **scope**，您必须删除并重新创建 **IngressController** 对象。您无法在创建自定义资源 (CR) 后更改 `.spec.endpointPublishingStrategy.loadBalancer.scope` 参数。

先决条件

- 安装 OpenShift CLI (**oc**)。

- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 通过删除并重新创建集群，将 **默认** Ingress Controller 配置为内部。

```
$ oc replace --force --wait --filename - <<EOF
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  namespace: openshift-ingress-operator
  name: default
spec:
  endpointPublishingStrategy:
    type: LoadBalancerService
  loadBalancer:
    scope: Internal
EOF
```

6.8.8. 配置路由准入策略

管理员和应用程序开发人员可在多个命名空间中运行具有相同域名的应用程序。这是针对多个团队开发的、在同一个主机名上公开的微服务的机构。



警告

只有在命名空间间有信任的集群才会启用跨命名空间之间的声明，否则恶意用户可能会接管主机名。因此，默认的准入策略不允许在命名空间间声明主机名。

先决条件

- 必须具有集群管理员权限。

流程

- 使用以下命令编辑 **ingresscontroller** 资源变量的 **spec**. **routeAdmission** 字段：

```
$ oc -n openshift-ingress-operator patch ingresscontroller/default --patch '{"spec": {"routeAdmission":{"namespaceOwnership":"InterNamespaceAllowed"}}}' --type=merge
```

Ingress 控制器配置参数

```
spec:
  routeAdmission:
    namespaceOwnership: InterNamespaceAllowed
  ...
```

6.8.9. 使用通配符路由

HAProxy Ingress Controller 支持通配符路由。Ingress Operator 使用 **wildcardPolicy** 来配置 Ingress Controller 的 **ROUTER_ALLOW_WILDCARD_ROUTES** 环境变量。

Ingress Controller 的默认行为是接受采用 **None** 通配符策略的路由，该策略与现有 **IngressController** 资源向后兼容。

流程

1. 配置通配符策略。
 - a. 使用以下命令来编辑 **IngressController** 资源：

```
$ oc edit IngressController
```

- b. 在 **spec** 下，将 **wildcardPolicy** 字段设置为 **WildcardsDisallowed** 或 **WildcardsAllowed**：

```
spec:
  routeAdmission:
    wildcardPolicy: WildcardsDisallowed # or WildcardsAllowed
```

6.8.10. 使用 X-Forwarded 标头

您可以将 HAProxy Ingress Controller 配置为指定如何处理 HTTP 标头的策略，其中包括 **Forwarded** 和 **X-Forwarded-For**。Ingress Operator 使用 **HTTPHeaders** 字段配置 Ingress Controller 的 **ROUTER_SET_FORWARDED_HEADERS** 环境变量。

流程

1. 为 Ingress Controller 配置 **HTTPHeaders** 字段。
 - a. 使用以下命令来编辑 **IngressController** 资源：
- b. 在 **spec** 下，将 **HTTPHeaders** 策略字段设置为 **Append**、**Replace**、**IfNone** 或 **Never**：

```
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  name: default
  namespace: openshift-ingress-operator
spec:
  httpHeaders:
    forwardedHeaderPolicy: Append
```

使用案例示例

作为集群管理员，您可以：

- 配置将 **X-Forwarded-For** 标头注入每个请求的外部代理，然后将其转发到 Ingress Controller。要将 Ingress Controller 配置为通过未修改的标头传递，您需要指定 **never** 策略。然后，Ingress Controller 不会设置标头，应用程序只接收外部代理提供的标头。

- 将 Ingress Controller 配置为通过未修改的外部代理在外部集群请求上设置 **X-Forwarded-For** 标头。
要将 Ingress Controller 配置为在不通过外部代理的内部集群请求上设置 **X-Forwarded-For** 标头，请指定 **if-none** 策略。如果 HTTP 请求已经通过外部代理设置了标头，则 Ingress Controller 会保留它。如果缺少标头，因为请求没有通过代理，Ingress Controller 会添加标头。

作为应用程序开发人员，您可以：

- 配置特定于应用程序的外部代理来注入 **X-Forwarded-For** 标头。
要配置 Ingress Controller，以便在不影响其他路由策略的情况下将标头传递到应用程序的路由，请在应用程序的路由上添加注解 **haproxy.router.openshift.io/set-forwarded-headers: if-none** 或 **haproxy.router.openshift.io/set-forwarded-headers: never**。



注意

您可以根据每个路由设置 **haproxy.router.openshift.io/set-forwarded-headers** 注解，独立于 Ingress Controller 的全局设置值。

6.8.11. 启用 HTTP/2 入口连接

您可以在 HAProxy 中启用透明端到端的 HTTP/2 连接。此功能使应用程序所有者利用 HTTP/2 协议功能，包括单一连接、标头压缩、二进制流等等。

您可以为单独的 Ingress Controller 或整个集群启用 HTTP/2 连接。

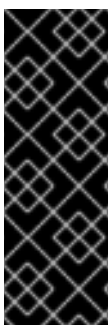
要在从客户端到 HAProxy 的连接中启用 HTTP/2，路由必须指定一个自定义证书。使用默认证书的路由无法使用 HTTP/2。这一限制是避免连接并发问题（如客户端为使用相同证书的不同路由重新使用连接）所必需的。

从 HAProxy 到应用程序 pod 的连接只能将 HTTP/2 用于 re-encrypt 路由，而不适用于 edge-terminated 或 insecure 路由。存在这个限制的原因是，在与后端协商使用 HTTP/2 时，HAProxy 要使用 ALPN (Application-Level Protocol Negotiation)，它是一个 TLS 的扩展。这意味着，端到端的 HTTP/2 适用于 passthrough 和 re-encrypt 路由，而不适用于 insecure 或 edge-terminated 路由。



警告

使用重新加密路由，在 Ingress Controller 上启用了 HTTP/2 的 WebSockets 需要通过 HTTP/2 支持 WebSocket。HTTP/2 的 websocket 是 HAProxy 2.4 的一个功能，目前在 OpenShift Container Platform 中不被支持。



重要

对于非 passthrough 路由，Ingress Controller 会独立于客户端的连接来协商它与应用程序的连接。这意味着，客户端可以连接到 Ingress Controller 并协商 HTTP/1.1，Ingress Controller 可连接到应用程序，协商 HTTP/2 并使用 HTTP/2 连接将客户端 HTTP/1.1 连接转发请求。如果客户端随后试图将其连接从 HTTP/1.1 升级到 WebSocket 协议，这会导致问题。因为 Ingress Controller 无法将 WebSocket 转发到 HTTP/2，也无法将其 HTTP/2 的连接升级到 WebSocket。因此，如果您有一个应用程序旨在接受 WebSocket 连接，则必须允许使用 HTTP/2 协议，或者其它客户端将无法升级到 WebSocket 协议。

流程

在单一 Ingress Controller 上启用 HTTP/2。

- 要在 Ingress Controller 上启用 HTTP/2，请输入 **oc annotate** 命令：

```
$ oc -n openshift-ingress-operator annotate ingresscontrollers/<ingresscontroller_name>  
ingress.operator.openshift.io/default-enable-http2=true
```

将 **<ingresscontroller_name>** 替换为要注解的 Ingress Controller 的名称。

在整个集群中启用 HTTP/2。

- 要为整个集群启用 HTTP/2，请输入 **oc annotate** 命令：

```
$ oc annotate ingresses.config/cluster ingress.operator.openshift.io/default-enable-http2=true
```

6.9. 其他资源

- [配置自定义 PKI](#)

第 7 章 配置节点端口服务范围

作为集群管理员，您可以扩展可用的节点端口范围。如果您的集群使用大量节点端口，可能需要增加可用端口的数量。

默认端口范围为 **30000-32767**。您永远不会缩小端口范围，即使您首先将其扩展超过默认范围。

7.1. 先决条件

- 集群基础架构必须允许访问您在扩展范围内指定的端口。例如，如果您将节点端口范围扩展到 **30000-32900**，防火墙或数据包过滤配置必须允许 **32768-32900** 端口范围。

7.2. 扩展节点端口范围

您可以扩展集群的节点端口范围。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 使用具有 **cluster-admin** 权限的用户登陆到集群。

流程

1. 要扩展节点端口范围，请输入以下命令。将 **<port>** 替换为新范围内的最大端口号码。

```
$ oc patch network.config.openshift.io cluster --type=merge -p \
  '{
    "spec":
      { "serviceNodePortRange": "30000-<port>" }
  }'
```

输出示例

```
network.config.openshift.io/cluster patched
```

2. 要确认配置是活跃的，请输入以下命令。应用更新可能需要几分钟。

```
$ oc get configmaps -n openshift-kube-apiserver config \
  -o jsonpath="{.data['config.yaml']}" | \
  grep -Eo '"service-node-port-range": "[[:digit:]]+-[[:digit:]]+"''
```

输出示例

```
"service-node-port-range":["30000-33000"]
```

7.3. 其他资源

- [使用 NodePort 配置集群入口流量](#)
- [Network \[config.openshift.io/v1\]](#)

- [Service \[core/v1\]](#)

第 8 章 在裸机集群中使用流控制传输协议 (SCTP)

作为集群管理员，您可以使用集群中的流控制传输协议 (SCTP)。

8.1. 支持 OPENSIFT CONTAINER PLATFORM 上的流控制传输协议 (SCTP)

作为集群管理员，您可以在集群中的主机上启用 SCTP。在 Red Hat Enterprise Linux CoreOS (RHCOS) 上，SCTP 模块被默认禁用。

SCTP 是基于信息的可靠协议，可在 IP 网络之上运行。

启用后，您可以使用 SCTP 作为带有 pod、服务和网络策略的协议。**Service** 对象必须通过将 **type** 参数设置为 **ClusterIP** 或 **NodePort** 值来定义。

8.1.1. 使用 SCTP 协议的示例配置

您可以通过将 pod 或服务对象中的 **protocol** 参数设置为 **SCTP** 来将 pod 或服务配置为使用 SCTP。

在以下示例中，pod 被配置为使用 SCTP：

```
apiVersion: v1
kind: Pod
metadata:
  namespace: project1
  name: example-pod
spec:
  containers:
  - name: example-pod
  ...
  ports:
  - containerPort: 30100
    name: sctpserver
    protocol: SCTP
```

在以下示例中，服务被配置为使用 SCTP：

```
apiVersion: v1
kind: Service
metadata:
  namespace: project1
  name: sctpserver
spec:
  ...
  ports:
  - name: sctpserver
    protocol: SCTP
    port: 30100
    targetPort: 30100
  type: ClusterIP
```

在以下示例中，**NetworkPolicy** 对象配置为对来自具有特定标签的任何 pod 的端口 **80** 应用 SCTP 网络流量：


```

kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-sctp-on-http
spec:
  podSelector:
    matchLabels:
      role: web
  ingress:
  - ports:
    - protocol: SCTP
      port: 80

```

8.2. 启用流控制传输协议 (SCTP)

作为集群管理员，您可以在集群中的 worker 节点上加载并启用列入黑名单的 SCTP 内核模块。

先决条件

- 安装 OpenShift CLI (**oc**) 。
- 使用具有 **cluster-admin** 角色的用户访问集群。

流程

1. 创建名为 **load-sctp-module.yaml** 的文件，其包含以下 YAML 定义：

```

apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: load-sctp-module
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.1.0
    storage:
      files:
      - path: /etc/modprobe.d/sctp-blacklist.conf
        mode: 0644
        overwrite: true
        contents:
          source: data:,
      - path: /etc/modules-load.d/sctp-load.conf
        mode: 0644
        overwrite: true
        contents:
          source: data:,sctp

```

2. 运行以下命令来创建 **MachineConfig** 对象：

```
$ oc create -f load-sctp-module.yaml
```

3. 可选：要在 MachineConfig Operator 应用配置更改时监测节点的状态，请使用以下命令。当节点状态变为 **Ready**时，则代表配置更新已被应用。

```
$ oc get nodes
```

8.3. 验证流控制传输协议 (SCTP) 已启用

您可以通过创建一个 pod 以及侦听 SCTP 流量的应用程序，将其与服务关联，然后连接到公开的服务，来验证 SCTP 是否在集群中工作。

先决条件

- 从集群访问互联网来安装 **nc** 软件包。
- 安装 OpenShift CLI (**oc**) 。
- 使用具有 **cluster-admin** 角色的用户访问集群。

流程

1. 创建 pod 启动 SCTP 侦听程序：
 - a. 创建名为 **sctp-server.yaml** 的文件，该文件使用以下 YAML 定义 pod:

```
apiVersion: v1
kind: Pod
metadata:
  name: sctpserver
  labels:
    app: sctpserver
spec:
  containers:
  - name: sctpserver
    image: registry.access.redhat.com/ubi8/ubi
    command: ["/bin/sh", "-c"]
    args:
      ["dnf install -y nc && sleep inf"]
    ports:
      - containerPort: 30102
        name: sctpserver
        protocol: SCTP
```

- b. 运行以下命令来创建 pod：

```
$ oc create -f sctp-server.yaml
```

2. 为 SCTP 侦听程序 pod 创建服务。
 - a. 创建名为 **sctp-service.yaml** 的文件，该文件使用以下 YAML 定义服务：

```
apiVersion: v1
kind: Service
metadata:
  name: sctpservice
```

```

labels:
  app: sctpserver
spec:
  type: NodePort
  selector:
    app: sctpserver
  ports:
    - name: sctpserver
      protocol: SCTP
      port: 30102
      targetPort: 30102

```

- b. 要创建服务，请输入以下命令：

```
$ oc create -f sctp-service.yaml
```

3. 为 SCTP 客户端创建 pod。

- a. 使用以下 YAML 创建名为 **sctp-client.yaml** 的文件：

```

apiVersion: v1
kind: Pod
metadata:
  name: sctpclient
  labels:
    app: sctpclient
spec:
  containers:
    - name: sctpclient
      image: registry.access.redhat.com/ubi8/ubi
      command: ["/bin/sh", "-c"]
      args:
        ["dnf install -y nc && sleep inf"]

```

- b. 运行以下命令来创建 **Pod** 对象：

```
$ oc apply -f sctp-client.yaml
```

4. 在服务器中运行 SCTP 侦听程序。

- a. 要连接到服务器 pod，请输入以下命令：

```
$ oc rsh sctpserver
```

- b. 要启动 SCTP 侦听程序，请输入以下命令：

```
$ nc -l 30102 --sctp
```

5. 连接到服务器上的 SCTP 侦听程序。

- a. 在终端程序里打开一个新的终端窗口或标签页。
- b. 获取 **sctpserver** 服务的 IP 地址。使用以下命令：

```
$ oc get services sctpsservice -o go-template='{{.spec.clusterIP}}{\n}'
```

- c. 要连接到客户端 pod，请输入以下命令：

```
$ oc rsh sctpclient
```

- d. 要启动 SCTP 客户端，请输入以下命令。将 **<cluster_IP>** 替换为 **sctpsservice** 服务的集群 IP 地址。

```
# nc <cluster_IP> 30102 --sctp
```

第 9 章 配置 PTP 硬件



重要

精确时钟协议 (PTP) 硬件只是技术预览功能。技术预览功能不被红帽产品服务等级协议 (SLA) 支持，且可能在功能方面有缺陷。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的详情，请参阅 <https://access.redhat.com/support/offerings/techpreview/>。

9.1. 关于 PTP 硬件

OpenShift Container Platform 包含在节点上使用 PTP (Precision Time Protocol) 硬件的能力。您可以在具有 PTP 功能硬件的集群中配置 linuxptp 服务。



注意

PTP Operator 只适用于仅在裸机基础架构上置备的集群上具有 PTP 功能的设备。

您可以通过部署 PTP Operator，使用 OpenShift Container Platform 控制台来安装 PTP。PTP Operator 会创建和管理 linuxptp 服务。Operator 提供以下功能：

- 在集群中发现具有 PTP 功能的设备。
- 管理 linuxptp 服务的配置。

9.2. 自动发现 PTP 网络设备

PTP Operator 将 **NodePtpDevice.ptp.openshift.io** 自定义资源定义 (CRD) 添加到 OpenShift Container Platform。PTP Operator 将搜索集群中每个节点上的具有 PTP 功能的网络设备。Operator 会为每个提供兼容 PTP 设备的节点创建和更新 **NodePtpDevice** 自定义资源 (CR) 对象。

为每个节点创建一个 CR，并共享与该节点相同的名称。**.status.devices** 列表提供有关节点上 PTP 设备的信息。

以下是由 PTP Operator 创建的 **NodePtpDevice** CR 示例：

```
apiVersion: ptp.openshift.io/v1
kind: NodePtpDevice
metadata:
  creationTimestamp: "2019-11-15T08:57:11Z"
  generation: 1
  name: dev-worker-0 1
  namespace: openshift-ptp 2
  resourceVersion: "487462"
  selfLink: /apis/ptp.openshift.io/v1/namespaces/openshift-ptp/nodeptpdevices/dev-worker-0
  uid: 08d133f7-aae2-403f-84ad-1fe624e5ab3f
spec: {}
status:
  devices: 3
  - name: eno1
  - name: eno2
```

```
- name: ens787f0
- name: ens787f1
- name: ens801f0
- name: ens801f1
- name: ens802f0
- name: ens802f1
- name: ens803
```

- 1 **name** 参数的值与节点的名称相同。
- 2 CR 由 PTP Operator 在 **openshift-ptp** 命名空间中创建。
- 3 **devices** 集合包含节点上 Operator 发现的所有 PTP 可用设备列表。

9.3. 安装 PTP OPERATOR

作为集群管理员，您可以使用 OpenShift Container Platform CLI 或 Web 控制台来安装 PTP Operator。

9.3.1. CLI : 安装 PTP Operator

作为集群管理员，您可以使用 CLI 安装 Operator。

先决条件

- 在裸机中安装有支持 PTP 硬件的节点的集群。
- 安装 OpenShift CLI (**oc**) 。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 要为 PTP Operator 创建命名空间，输入以下命令：

```
$ cat << EOF | oc create -f -
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-ptp
  labels:
    name: openshift-ptp
    openshift.io/cluster-monitoring: "true"
EOF
```

2. 要为 Operator 创建 Operator 组，输入以下命令：

```
$ cat << EOF | oc create -f -
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: ptp-operators
  namespace: openshift-ptp
spec:
```

```
targetNamespaces:
- openshift-ntp
EOF
```

3. 订阅 PTP Operator。

- a. 运行以下命令，将 OpenShift Container Platform 主版本和次版本设置为环境变量，该变量在下一步中作为 **channel** 的值。

```
$ OC_VERSION=$(oc version -o yaml | grep openshiftVersion | \
grep -o '[0-9]*[.][0-9]*' | head -1)
```

- b. 要为 PTP Operator 创建订阅，输入以下命令：

```
$ cat << EOF | oc create -f -
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: ptp-operator-subscription
  namespace: openshift-ntp
spec:
  channel: "${OC_VERSION}"
  name: ptp-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
EOF
```

4. 要验证是否已安装 Operator，请输入以下命令：

```
$ oc get csv -n openshift-ntp \
-o custom-columns=Name:.metadata.name,Phase:.status.phase
```

输出示例

Name	Phase
ptp-operator.4.4.0-202006160135	Succeeded

9.3.2. Web 控制台：安装 PTP Operator

作为集群管理员，您可以使用 Web 控制台安装 Operator。



注意

如上一节所述，您必须创建命名空间和 operator 组。

流程

1. 使用 OpenShift Container Platform Web 控制台安装 PTP Operator：
 - a. 在 OpenShift Container Platform Web 控制台中，点击 **Operators → OperatorHub**。
 - b. 从可用的 Operator 列表中选择 **PTP Operator**，然后点 **Install**。

- c. 在 **Install Operator** 页面中，在 **A specific namespace on the cluster** 下选择 **openshift-ntp**。然后点击 **Install**。
2. 可选：验证是否成功安装了 PTP Operator：
 - a. 切换到 **Operators → Installed Operators** 页面。
 - b. 确保 **openshift-ntp** 项目中列出的 PTP Operator 的 **Status** 为 **InstallSucceeded**。



注意

在安装过程中，Operator 可能会显示 **Failed** 状态。如果安装过程结束后有 **InstallSucceeded** 信息，您可以忽略这个 **Failed** 信息。

如果 Operator 没有被成功安装，请按照以下步骤进行故障排除：

- 进入 **Operators → Installed Operators** 页面，检查 **Operator Subscriptions** 和 **Install Plans** 选项卡中的 **Status** 项中是否有任何错误。
- 进入 **Workloads → Pods** 页面，检查 **openshift-ntp** 项目中 pod 的日志。

9.4. 配置 LINUXPTP 服务

PTP Operator 将 **PtpConfig.ptp.openshift.io** 自定义资源定义 (CRD) 添加至 OpenShift Container Platform。您可以通过创建 **PtpConfig** 自定义资源 (CR) 对象来配置 Linuxptp 服务 (ptp4l、phc2sys)。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。
- 已安装了 PTP Operator。

流程

1. 创建以下 **PtpConfig** CR，然后在 **<name>-ntp-config.yaml** 文件中保存 YAML。使用配置的实际名称替换 **<name>**。

```

apiVersion: ptp.openshift.io/v1
kind: PtpConfig
metadata:
  name: <name> 1
  namespace: openshift-ntp 2
spec:
  profile: 3
  - name: "profile1" 4
    interface: "ens787f1" 5
    ptp4lOpts: "-s -2" 6
    phc2sysOpts: "-a -r" 7
  recommend: 8
  - profile: "profile1" 9
    priority: 10 10

```



```
match: 11
- nodeLabel: "node-role.kubernetes.io/worker" 12
  nodeName: "dev-worker-0" 13
```

- 1 为 **PtpConfig** CR 指定名称。
- 2 指定安装 PTP Operator 的命名空间。
- 3 指定包括一个或多个 **profile** 的数组。
- 4 指定用于唯一标识配置集（profile）对象的配置集对象名称。
- 5 指定 **ptp4l** 服务要使用的网络接口名称，如 **ens787f1**。
- 6 为 **ptp4l** 服务指定系统配置选项，如 **-s -2**。这不应该包含接口名称 **-i <interface>** 和服务配置文件 **-f /etc/ptp4l.conf**，因为这些文件会被自动附加。
- 7 为 **phc2sys** 服务指定系统配置选项，如 **-a -r**。
- 8 指定包括一个或多个 **recommend** 对象的数组，该数组定义了如何将配置集应用到节点的规则。
- 9 指定 **profile** 部分中定义的 **profile** 对象名称。
- 10 使用 **0** 到 **99** 之间的一个整数值指定 **priority**。大数值的优先级较低，因此优先级 **99** 低于优先级 **10**。如果根据 **match** 项中定义的规则，节点可以与多个配置集相匹配，具有最高优先级的配置集将被应用到那个节点。
- 11 使用 **nodeLabel** 或 **nodeName** 指定 **match** 规则。
- 12 使用节点对象中的 **node.Labels** 的 **key** 指定 **nodeLabel**。
- 13 使用节点对象的 **node.Name** 指定 **nodeName**。

2. 运行以下命令来创建 CR：

```
$ oc create -f <filename> 1
```

- 1 将 **<filename>** 替换为您在上一步中创建的文件的名称。

3. 可选：检查 **PtpConfig** 配置集是否应用到与 **nodeLabel** 或 **nodeName** 匹配的节点。

```
$ oc get pods -n openshift-ptp -o wide
```

输出示例

```
NAME                                READY STATUS RESTARTS AGE IP           NODE
NOMINATED NODE READINESS GATES
linuxptp-daemon-4xkbb              1/1   Running 0      43m 192.168.111.15 dev-worker-0
<none>                             <none>
linuxptp-daemon-tdspf              1/1   Running 0      43m 192.168.111.11 dev-master-0
<none>                             <none>
ptp-operator-657bbb64c8-2f8sj      1/1   Running 0      43m 10.128.0.116   dev-master-0
<none>                             <none>
```

```

$ oc logs linuxptp-daemon-4xkbb -n openshift-ptp
l1115 09:41:17.117596 4143292 daemon.go:107] in applyNodePTPProfile
l1115 09:41:17.117604 4143292 daemon.go:109] updating NodePTPProfile to:
l1115 09:41:17.117607 4143292 daemon.go:110] -----
l1115 09:41:17.117612 4143292 daemon.go:102] Profile Name: profile1 1
l1115 09:41:17.117616 4143292 daemon.go:102] Interface: ens787f1 2
l1115 09:41:17.117620 4143292 daemon.go:102] Ptp4IOpts: -s -2 3
l1115 09:41:17.117623 4143292 daemon.go:102] Phc2sysOpts: -a -r 4
l1115 09:41:17.117626 4143292 daemon.go:116] -----
l1115 09:41:18.117934 4143292 daemon.go:186] Starting phc2sys...
l1115 09:41:18.117985 4143292 daemon.go:187] phc2sys cmd: &{Path:/usr/sbin/phc2sys
Args:[/usr/sbin/phc2sys -a -r] Env:[] Dir: Stdin:<nil> Stdout:<nil> Stderr:<nil> ExtraFiles:[]
SysProcAttr:<nil> Process:<nil> ProcessState:<nil> ctx:<nil> lookPathErr:<nil> finished:false
childFiles:[] closeAfterStart:[] closeAfterWait:[] goroutine:[] errch:<nil> waitDone:<nil>}
l1115 09:41:19.118175 4143292 daemon.go:186] Starting ptp4l...
l1115 09:41:19.118209 4143292 daemon.go:187] ptp4l cmd: &{Path:/usr/sbin/ptp4l Args:
[/usr/sbin/ptp4l -m -f /etc/ptp4l.conf -i ens787f1 -s -2] Env:[] Dir: Stdin:<nil> Stdout:<nil>
Stderr:<nil> ExtraFiles:[] SysProcAttr:<nil> Process:<nil> ProcessState:<nil> ctx:<nil>
lookPathErr:<nil> finished:false childFiles:[] closeAfterStart:[] closeAfterWait:[] goroutine:[]
errch:<nil> waitDone:<nil>}
ptp4l[102189.864]: selected /dev/ptp5 as PTP clock
ptp4l[102189.886]: port 1: INITIALIZING to LISTENING on INIT_COMPLETE
ptp4l[102189.886]: port 0: INITIALIZING to LISTENING on INIT_COMPLETE

```

- 1 **Profile Name** 是应用到 **dev-worker-0** 节点的名称。
- 2 **Interface** 是在 **profile1** 的 **interface** 项中指定的 PTP 设备。在这个接口中运行的 **ptp4l** 服务。
- 3 **ptp4IOpts** 是 **profile1** 中的 **ptp4IOpts** 项指定的 ptp4l sysconfig 选项。
- 4 **Phc2sysOpts** 是 **profile1** 中的 **Phc2sysOpts** 项指定的 phc2sys sysconfig 选项。

第 10 章 网络策略

10.1. 关于网络策略

作为集群管理员，您可以定义网络策略以限制到集群中的 pod 的网络通讯。

10.1.1. 关于网络策略

在使用支持 Kubernetes 网络策略的 Kubernetes Container Network Interface (CNI) 插件的集群中，网络隔离完全由 **NetworkPolicy** 对象控制。在 OpenShift Container Platform 4.6 中，OpenShift SDN 支持在默认的网络隔离模式中使用网络策略。



注意

在使用 OpenShift SDN 集群网络供应商时，网络策略会有以下限制：

- 不支持由 **egress** 字段指定的出口网络策略。
- 网络策略支持 IPBlock，但不支持 **except**。如果创建的策略带有一个有 **except** 的 IPBlock 项，SDN pod 的日志中会出现警告，策略中的整个 IPBlock 项都会被忽略。



警告

网络策略不适用于主机网络命名空间。启用主机网络的 Pod 不受网络策略规则的影响。

默认情况下，项目中的所有 pod 都可被其他 pod 和网络端点访问。要在一个项目中隔离一个或多个 Pod，您可以在该项目中创建 **NetworkPolicy** 对象来指示允许的入站连接。项目管理员可以在自己的项目中创建和删除 **NetworkPolicy** 对象。

如果一个 pod 由一个或多个 **NetworkPolicy** 对象中的选择器匹配，那么该 pod 将只接受至少被其中一个 **NetworkPolicy** 对象所允许的连接。未被任何 **NetworkPolicy** 对象选择的 pod 可以完全访问。

以下示例 **NetworkPolicy** 对象演示了支持不同的情景：

- 拒绝所有流量：
要使项目默认为拒绝流量，请添加一个匹配所有 pod 但不接受任何流量的 **NetworkPolicy** 对象：

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: deny-by-default
spec:
  podSelector: {}
  ingress: []
```

- 只允许 OpenShift Container Platform Ingress Controller 的连接：

要使项目只允许 OpenShift Container Platform Ingress Controller 的连接，请添加以下 **NetworkPolicy** 对象。

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-from-openshift-ingress
spec:
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          network.openshift.io/policy-group: ingress
  podSelector: {}
  policyTypes:
  - Ingress
```

- 只接受项目中 pod 的连接：
要使 pod 接受同一项目中其他 pod 的连接，但拒绝其他项目中所有 pod 的连接，请添加以下 **NetworkPolicy** 对象：

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-same-namespace
spec:
  podSelector: {}
  ingress:
  - from:
    - podSelector: {}
```

- 仅允许基于 pod 标签的 HTTP 和 HTTPS 流量：
要对带有特定标签（以下示例中的 **role=frontend**）的 pod 仅启用 HTTP 和 HTTPS 访问，请添加类似如下的 **NetworkPolicy** 对象：

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-http-and-https
spec:
  podSelector:
    matchLabels:
      role: frontend
  ingress:
  - ports:
    - protocol: TCP
      port: 80
    - protocol: TCP
      port: 443
```

- 使用命名空间和 pod 选择器接受连接：
要通过组合使用命名空间和 pod 选择器来匹配网络流量,您可以使用类似如下的 **NetworkPolicy** 对象：

```

kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-pod-and-namespace-both
spec:
  podSelector:
    matchLabels:
      name: test-pods
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            project: project_name
        podSelector:
          matchLabels:
            name: test-pods

```

NetworkPolicy 对象是可添加的；也就是说，您可以组合多个 **NetworkPolicy** 对象来满足复杂的网络要求。

例如，对于以上示例中定义的 **NetworkPolicy** 对象，您可以在同一个项目中定义 **allow-same-namespace** 和 **allow-http-and-https** 策略。因此，允许带有标签 **role=frontend** 的 pod 接受每一策略所允许的任何连接。即，任何端口上来自同一命名空间中的 pod 的连接，以及端口 **80** 和 **443** 上的来自任意命名空间中 pod 的连接。

10.1.2. 网络策略优化

使用一个网络策略来通过 pod 上的不同标签来在命名空间中将不同 pod 进行隔离。



注意

有效使用网络策略规则的指南只适用于 OpenShift SDN 集群网络供应商。

将 **NetworkPolicy** 对象应用到单一命名空间中的大量 pod 时，效率较低。因为 Pod 标签不存在于 IP 地址一级，因此网络策略会为使用 **podSelector** 选择的每个 pod 之间生成单独的 Open vSwitch (OVS) 流量规则。

例如，在一个 **NetworkPolicy** 对象中，如果 spec **podSelector** 和 ingress **podSelector** 每个都匹配 200 个 pod，则会产生 40,000 (200*200) OVS 流规则。这可能会减慢节点的速度。

在设计您的网络策略时，请参考以下指南：

- 使用命名空间使其包含需要隔离的 pod 组，可以减少 OVS 流规则数量。使用 **namespaceSelector** 或空 **podSelector** 选择整个命名空间的 **NetworkPolicy** 对象会只生成一个与命名空间的 VXLAN 虚拟网络 ID (VNID) 匹配的 OVS 流量规则。
- 保留不需要在原始命名空间中隔离的 pod，并将需要隔离的 pod 移到一个或多个不同的命名空间中。
- 创建额外的目标跨命名空间网络策略，以允许来自不同隔离的 pod 的特定流量。

10.1.3. 后续步骤

- [创建网络策略](#)

- 可选：[定义默认网络策略](#)

10.1.4. 其他资源

- [项目和命名空间](#)
- [配置多租户网络策略](#)
- [网络策略 API](#)

10.2. 创建网络策略

作为具有 **admin** 角色的用户，您可以为命名空间创建网络策略。

10.2.1. 创建网络策略

要定义细致的规则来描述集群中命名空间允许的入口或出口网络流量，您可以创建一个网络策略。



注意

如果使用具有 **cluster-admin** 角色的用户登录，则可以在集群中的任何命名空间中创建网络策略。

先决条件

- 集群使用支持 **NetworkPolicy** 对象的集群网络供应商，如 OVN-Kubernetes 网络供应商或设置了 **mode: NetworkPolicy** 的 OpenShift SDN 网络供应商。此模式是 OpenShift SDN 的默认模式。
- 已安装 OpenShift CLI (**oc**)。
- 您可以使用具有 **admin** 权限的用户登录到集群。
- 您在网络策略要应用到的命名空间中。

流程

1. 创建策略规则：

- a. 创建一个 **<policy_name>.yaml** 文件：

```
$ touch <policy_name>.yaml
```

其中：

<policy_name>

指定网络策略文件名。

- b. 在您刚才创建的文件中定义网络策略，如下例所示：

拒绝来自所有命名空间中的所有 pod 的入口流量

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
```

```

metadata:
  name: deny-by-default
spec:
  podSelector:
    ingress: []

```

允许来自所有命名空间中的所有 pod 的入口流量

```

kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-same-namespace
spec:
  podSelector:
    ingress:
      - from:
        - podSelector: {}

```

2. 运行以下命令来创建网络策略对象：

```
$ oc apply -f <policy_name>.yaml -n <namespace>
```

其中：

<policy_name>

指定网络策略文件名。

<namespace>

可选：如果对象在与当前命名空间不同的命名空间中定义，使用它来指定命名空间。

输出示例

```
networkpolicy "default-deny" created
```

10.2.2. 示例 NetworkPolicy 对象

下文解释了示例 NetworkPolicy 对象：

```

kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-27107 1
spec:
  podSelector: 2
    matchLabels:
      app: mongodb
  ingress:
    - from:
      - podSelector: 3
        matchLabels:
          app: app

```

```
ports: 4
- protocol: TCP
  port: 27017
```

- 1 NetworkPolicy 对象的名称。
- 2 描述策略应用到的 pod 的选择器。策略对象只能选择定义 NetworkPolicy 对象的项目中的 pod。
- 3 与策略对象允许入口流量的 pod 匹配的选择器。选择器与 NetworkPolicy 相同的命名空间中的 pod 匹配。
- 4 接受流量的一个或多个目标端口的列表。

10.3. 查看网络策略

以具有 **admin** 角色的用户，您可以查看命名空间的网络策略。

10.3.1. 查看网络策略

您可以检查命名空间中的网络策略。



注意

如果使用具有 **cluster-admin** 角色的用户登录，您可以查看集群中的任何网络策略。

先决条件

- 已安装 OpenShift CLI (**oc**)。
- 您可以使用具有 **admin** 权限的用户登陆到集群。
- 您在网络策略所在的命名空间中。

流程

- 列出命名空间中的网络策略：
 - 要查看命名空间中定义的 **NetworkPolicy** 对象，输入以下命令：

```
$ oc get networkpolicy
```

- 可选：要检查特定的网络策略，请输入以下命令：

```
$ oc describe networkpolicy <policy_name> -n <namespace>
```

其中：

<policy_name>

指定要检查的网络策略的名称。

<namespace>

可选：如果对象在与当前命名空间不同的命名空间中定义，使用它来指定命名空间。

例如：

```
$ oc describe networkpolicy allow-same-namespace
```

oc describe 命令的输出

```
Name:      allow-same-namespace
Namespace: ns1
Created on: 2021-05-24 22:28:56 -0400 EDT
Labels:    <none>
Annotations: <none>
Spec:
  PodSelector: <none> (Allowing the specific traffic to all pods in this namespace)
  Allowing ingress traffic:
    To Port: <any> (traffic allowed to all ports)
    From:
      PodSelector: <none>
  Not affecting egress traffic
  Policy Types: Ingress
```

10.3.2. 示例 NetworkPolicy 对象

下文解释了示例 NetworkPolicy 对象：

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-27107 1
spec:
  podSelector: 2
    matchLabels:
      app: mongodb
  ingress:
    - from:
      - podSelector: 3
        matchLabels:
          app: app
  ports: 4
    - protocol: TCP
      port: 27017
```

- 1** NetworkPolicy 对象的名称。
- 2** 描述策略应用到的 pod 的选择器。策略对象只能选择定义 NetworkPolicy 对象的项目中的 pod。
- 3** 与策略对象允许入口流量的 pod 匹配的选择器。选择器与 NetworkPolicy 相同的命名空间中的 pod 匹配。
- 4** 接受流量的一个或多个目标端口的列表。

10.4. 编辑网络策略

作为具有 **admin** 角色的用户，您可以编辑命名空间的现有网络策略。

10.4.1. 编辑网络策略

您可以编辑命名空间中的网络策略。



注意

如果使用具有 **cluster-admin** 角色的用户登录，则可以在集群中的任何命名空间中编辑网络策略。

先决条件

- 集群使用支持 **NetworkPolicy** 对象的集群网络供应商，如 OVN-Kubernetes 网络供应商或设置了 **mode: NetworkPolicy** 的 OpenShift SDN 网络供应商。此模式是 OpenShift SDN 的默认模式。
- 已安装 OpenShift CLI (**oc**)。
- 您可以使用具有 **admin** 权限的用户登陆到集群。
- 您在网络策略所在的命名空间中。

流程

1. 可选：要列出一个命名空间中的网络策略对象，请输入以下命令：

```
$ oc get networkpolicy -n <namespace>
```

其中：

<namespace>

可选：如果对象在与当前命名空间不同的命名空间中定义，使用它来指定命名空间。

2. 编辑 **NetworkPolicy** 对象。

- 如果您在文件中保存了网络策略定义，请编辑该文件并进行必要的更改，然后输入以下命令。

```
$ oc apply -n <namespace> -f <policy_file>.yaml
```

其中：

<namespace>

可选：如果对象在与当前命名空间不同的命名空间中定义，使用它来指定命名空间。

<policy_file>

指定包含网络策略的文件的名称。

- 如果您需要直接更新 **NetworkPolicy** 对象，请输入以下命令：

```
$ oc edit networkpolicy <policy_name> -n <namespace>
```

其中：

<policy_name>

指定网络策略的名称。

<namespace>

可选：如果对象在与当前命名空间不同的命名空间中定义，使用它来指定命名空间。

3. 确认 **NetworkPolicy** 对象已更新。

```
$ oc describe networkpolicy <policy_name> -n <namespace>
```

其中：

<policy_name>

指定网络策略的名称。

<namespace>

可选：如果对象在与当前命名空间不同的命名空间中定义，使用它来指定命名空间。

10.4.2. 示例 NetworkPolicy 对象

下文解释了示例 NetworkPolicy 对象：

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-27107 ①
spec:
  podSelector: ②
  matchLabels:
    app: mongodb
  ingress:
  - from:
    - podSelector: ③
      matchLabels:
        app: app
  ports: ④
  - protocol: TCP
    port: 27017
```

- ① NetworkPolicy 对象的名称。
- ② 描述策略应用到的 pod 的选择器。策略对象只能选择定义 NetworkPolicy 对象的项目中的 pod。
- ③ 与策略对象允许入口流量的 pod 匹配的选择器。选择器与 NetworkPolicy 相同的命名空间中的 pod 匹配。
- ④ 接受流量的一个或多个目标端口的列表。

10.4.3. 其他资源

- [创建网络策略](#)

10.5. 删除网络策略

以具有 **admin** 角色的用户，您可以从命名空间中删除网络策略。

10.5.1. 删除网络策略

您可以删除命名空间中的网络策略。



注意

如果使用具有 **cluster-admin** 角色的用户登录，您可以删除集群中的任何网络策略。

先决条件

- 集群使用支持 **NetworkPolicy** 对象的集群网络供应商，如 OVN-Kubernetes 网络供应商或设置了 **mode: NetworkPolicy** 的 OpenShift SDN 网络供应商。此模式是 OpenShift SDN 的默认模式。
- 已安装 OpenShift CLI (**oc**)。
- 您可以使用具有 **admin** 权限的用户登陆到集群。
- 您在网络策略所在的命名空间中。

流程

- 要删除 **NetworkPolicy** 对象，请输入以下命令：

```
$ oc delete networkpolicy <policy_name> -n <namespace>
```

其中：

<policy_name>

指定网络策略的名称。

<namespace>

可选：如果对象在与当前命名空间不同的命名空间中定义，使用它来指定命名空间。

输出示例

```
networkpolicy.networking.k8s.io/allow-same-namespace deleted
```

10.6. 为项目定义默认网络策略

作为集群管理员，您可以在创建新项目时修改新项目模板，使其自动包含网络策略。如果您还没有新项目的自定义模板，则需要首先创建一个。

10.6.1. 为新项目修改模板

作为集群管理员，您可以修改默认项目模板，以便使用自定义要求创建新项目。

创建自己的自定义项目模板：

流程

1. 以具有 **cluster-admin** 特权的用户身份登录。

2. 生成默认项目模板：

```
$ oc adm create-bootstrap-project-template -o yaml > template.yaml
```

3. 使用文本编辑器，通过添加对象或修改现有对象来修改生成的 **template.yaml** 文件。

4. 项目模板必须创建在 **openshift-config** 命名空间中。加载修改后的模板：

```
$ oc create -f template.yaml -n openshift-config
```

5. 使用 Web 控制台或 CLI 编辑项目配置资源。

- 使用 Web 控制台：

- i. 导航至 **Administration** → **Cluster Settings** 页面。

- ii. 点击 **Global Configuration**，查看所有配置资源。

- iii. 找到 **Project** 的条目，并点击 **Edit YAML**。

- 使用 CLI：

- i. 编辑 **project.config.openshift.io/cluster** 资源：

```
$ oc edit project.config.openshift.io/cluster
```

6. 更新 **spec** 部分，使其包含 **projectRequestTemplate** 和 **name** 参数，再设置您上传的项目模板的名称。默认名称为 **project-request**。

带有自定义项目模板的项目配置资源

```
apiVersion: config.openshift.io/v1
kind: Project
metadata:
  ...
spec:
  projectRequestTemplate:
    name: <template_name>
```

7. 保存更改后，创建一个新项目来验证是否成功应用了您的更改。

10.6.2. 在新项目模板中添加网络策略

作为集群管理员，您可以在新项目的默认模板中添加网络策略。OpenShift Container Platform 将自动创建项目中模板中指定的所有 **NetworkPolicy** 对象。

先决条件

- 集群使用支持 **NetworkPolicy** 对象的默认 CNI 网络供应商，如设置了 **mode: NetworkPolicy** 的 OpenShift SDN 网络供应商。此模式是 OpenShift SDN 的默认模式。
- 已安装 OpenShift CLI (**oc**)。

- 您需要使用具有 **cluster-admin** 权限的用户登陆到集群。
- 您必须已为新项目创建了自定义的默认项目模板。

流程

1. 运行以下命令来编辑新项目的默认模板：

```
$ oc edit template <project_template> -n openshift-config
```

将 **<project_template>** 替换为您为集群配置的缺省模板的名称。默认模板名称为 **project-request**。

2. 在模板中，将每个 **NetworkPolicy** 对象作为一个元素添加到 **objects** 参数中。**objects** 参数可以是一个或多个对象的集合。

在以下示例中，**objects** 参数集合包括几个 **NetworkPolicy** 对象：



重要

对于 OVN-Kubernetes 网络供应商插件，当 Ingress Controller 配置为使用 **HostNetwork** 端点发布策略时，不支持应用网络策略，以便允许入口流量，所有其他流量都会被拒绝。

```
objects:
- apiVersion: networking.k8s.io/v1
  kind: NetworkPolicy
  metadata:
    name: allow-from-same-namespace
  spec:
    podSelector: {}
    ingress:
    - from:
      - podSelector: {}
- apiVersion: networking.k8s.io/v1
  kind: NetworkPolicy
  metadata:
    name: allow-from-openshift-ingress
  spec:
    ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            network.openshift.io/policy-group: ingress
    podSelector: {}
    policyTypes:
    - Ingress
...
```

3. 可选：通过运行以下命令创建一个新项目，来确认您的网络策略对象已被成功创建：
 - a. 创建一个新项目

```
$ oc new-project <project> 1
```

1 将 **<project>** 替换为您要创建的项目的名称。

b. 确认新项目模板中的网络策略对象存在于新项目中：

```
$ oc get networkpolicy
NAME                POD-SELECTOR  AGE
allow-from-openshift-ingress <none>       7s
allow-from-same-namespace  <none>       7s
```

10.7. 使用网络策略配置多租户隔离

作为集群管理员，您可以配置网络策略以为多租户网络提供隔离功能。



注意

如果使用 OpenShift SDN 集群网络供应商，请按照本节所述配置网络策略，提供类似于多租户模式的网络隔离，但具有设置网络策略模式。

10.7.1. 使用网络策略配置多租户隔离

您可以配置项目，使其与其他项目命名空间中的 pod 和服务分离。

先决条件

- 集群使用支持 **NetworkPolicy** 对象的集群网络供应商，如 OVN-Kubernetes 网络供应商或设置了 **mode: NetworkPolicy** 的 OpenShift SDN 网络供应商。此模式是 OpenShift SDN 的默认模式。
- 已安装 OpenShift CLI (**oc**)。
- 您可以使用具有 **admin** 权限的用户登陆到集群。

流程

1. 创建以下 **NetworkPolicy** 对象：
 - a. 名为 **allow-from-openshift-ingress** 的策略。

```
$ cat << EOF | oc create -f -
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-from-openshift-ingress
spec:
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          policy-group.network.openshift.io/ingress: ""
  podSelector: {}
  policyTypes:
  - Ingress
EOF
```

- b. 名为 **allow-from-openshift-monitoring** 的策略：

```
$ cat << EOF | oc create -f -
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-from-openshift-monitoring
spec:
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          network.openshift.io/policy-group: monitoring
  podSelector: {}
  policyTypes:
  - Ingress
EOF
```

- c. 名为 **allow-same-namespace** 的策略：

```
$ cat << EOF | oc create -f -
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: allow-same-namespace
spec:
  podSelector:
  ingress:
  - from:
    - podSelector: {}
EOF
```

2. 可选：要确认当前项目中存在网络策略，请输入以下命令：

```
$ oc describe networkpolicy
```

输出示例

```
Name:      allow-from-openshift-ingress
Namespace: example1
Created on: 2020-06-09 00:28:17 -0400 EDT
Labels:    <none>
Annotations: <none>
Spec:
  PodSelector: <none> (Allowing the specific traffic to all pods in this namespace)
  Allowing ingress traffic:
    To Port: <any> (traffic allowed to all ports)
    From:
      NamespaceSelector: network.openshift.io/policy-group: ingress
  Not affecting egress traffic
  Policy Types: Ingress

Name:      allow-from-openshift-monitoring
```



```
Namespace: example1
Created on: 2020-06-09 00:29:57 -0400 EDT
Labels: <none>
Annotations: <none>
Spec:
  PodSelector: <none> (Allowing the specific traffic to all pods in this namespace)
  Allowing ingress traffic:
    To Port: <any> (traffic allowed to all ports)
    From:
      NamespaceSelector: network.openshift.io/policy-group: monitoring
  Not affecting egress traffic
  Policy Types: Ingress
```

10.7.2. 后续步骤

- [定义默认网络策略](#)

10.7.3. 其他资源

- [OpenShift SDN 网络隔离模式](#)

第 11 章 多网络

11.1. 了解多网络

在 Kubernetes 中，容器联网由实现了 Container Network Interface (CNI) 的网络插件负责。

OpenShift Container Platform 使用 Multus CNI 插件来实现对 CNI 插件的链接。在集群安装过程中，您要配置 *default* pod 网络。默认网络处理集群中的所有网络流量。您可以基于可用的 CNI 插件定义 *额外网络*，并将一个或多个这种网络附加到 pod。您可以根据需要为集群定义多个额外网络。这可让您灵活地配置提供交换或路由等网络功能的 pod。

11.1.1. 额外网络使用场景

您可以在需要网络隔离的情况下使用额外网络，包括分离数据平面与控制平面。隔离网络流量对以下性能和安全性原因很有用：

性能

您可以在两个不同的平面上发送流量，以管理每个平面上流量的多少。

安全性

您可以将敏感的数据发送到专为安全考虑而管理的网络平面，也可隔离不能在租户或客户间共享的私密数据。

集群中的所有 pod 仍然使用集群范围的默认网络，以维持整个集群中的连通性。每个 pod 都有一个 **eth0** 接口，附加到集群范围的 pod 网络。您可以使用 `oc exec -it <pod_name> -- ip a` 命令来查看 pod 的接口。如果您添加使用 Multus CNI 的额外网络接口，则名称为 **net1**、**net2**、...、**netN**。

要将额外网络接口附加到 pod，您必须创建配置来定义接口的附加方式。您可以使用 **NetworkAttachmentDefinition** 自定义资源 (CR) 来指定各个接口。各个 CR 中的 CNI 配置定义如何创建该接口。

11.1.2. OpenShift Container Platform 中的额外网络

OpenShift Container Platform 提供以下 CNI 插件，以便在集群中创建额外网络：

- **bridge**：配置基于网桥的额外网络，以允许同一主机上的容器集相互通信，并与主机通信。
- **host-device**：配置 *host-device* 额外网络，以允许 pod 访问主机系统上的物理以太网网络设备。
- **ipvlan**：配置基于 *ipvlan* 的额外网络，以允许主机上的 pod 与其他主机和那些主机上的 pod 通信，这类似于基于 *macvlan* 的额外网络。与基于 *macvlan* 的额外网络不同，每个 pod 共享与父级物理网络接口相同的 MAC 地址。
- **macvlan**：配置基于 *macvlan* 的额外网络，以允许主机上的 pod 通过使用物理网络接口与其他主机和那些主机上的 pod 通信。附加到基于 *macvlan* 的额外网络的每个 pod 都会获得一个唯一的 MAC 地址。
- **SR-IOV**：配置基于 *SR-IOV* 的额外网络，以允许 pod 附加到主机系统上支持 SR-IOV 的硬件的虚拟功能(VF)接口。

11.2. 配置额外网络

作为集群管理员，您可以为集群配置额外网络。支持以下网络类型：

- Bridge
- 主机设备
- IPVLAN
- MACVLAN

11.2.1. 管理额外网络的方法

您可以通过两种方法管理额外网络的生命周期：每种方法都是互斥的，您一次只能使用一种方法来管理额外网络。对于这两种方法，额外网络都由您配置的 Container Network Interface(CNI)插件管理。

对于额外网络，通过您配置为额外网络一部分的 IP 地址管理(IPAM)CNI 插件来置备 IP 地址。IPAM 插件支持各种 IP 地址分配方法，包括 DHCP 和静态分配。

- 修改 Cluster Network Operator(CNO)配置：CNO 会自动创建和管理 **NetworkAttachmentDefinition** 对象。除了管理对象生命周期外，CNO 还确保 DHCP 可用于使用 DHCP 分配的 IP 地址的额外网络。
- 应用 YAML 清单：您可以通过创建 **NetworkAttachmentDefinition** 对象直接管理额外网络。这种方法允许通过串联 CNI 插件。

11.2.2. 配置额外网络附加

通过 **k8s.cni.cncf.io** API 组中的 **NetworkAttachmentDefinition** API 配置额外网络。下表描述了 API 的配置：

表 11.1. NetworkAttachmentDefinition API 字段

字段	类型	描述
metadata.name	字符串	额外网络的名称。
metadata.namespace	字符串	与对象关联的命名空间。
spec.config	字符串	CNI 插件配置 JSON 格式。

11.2.2.1. 通过 Cluster Network Operator 配置额外网络

额外网络附加的配置作为 Cluster Network Operator(CNO)配置的一部分指定。

以下 YAML 描述了使用 CNO 管理额外网络的配置参数：

Cluster Network Operator 配置

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  # ...
  additionalNetworks: 1
```

```
- name: <name> 2
  namespace: <namespace> 3
  rawCNIConfig: |- 4
    {
      ...
    }
  type: Raw
```

- 1 包含一个或多个额外网络配置的数组。
- 2 正在创建的额外网络附加的名称。该名称在指定的 **namespace** 中需要是唯一的。
- 3 创建网络附加的命名空间。如果您未指定值，则使用 **default** 命名空间。
- 4 JSON 格式的 CNI 插件配置。

11.2.2.2. 从 YAML 清单配置额外网络

额外网络的配置是从 YAML 配置文件指定的，如下例所示：

```
apiVersion: k8s.cni.cncf.io/v1
kind: NetworkAttachmentDefinition
metadata:
  name: <name> 1
spec:
  config: |- 2
    {
      ...
    }
```

- 1 正在创建的额外网络附加的名称。
- 2 JSON 格式的 CNI 插件配置。

11.2.3. 额外网络类型的配置

以下部分介绍了额外网络的具体配置字段。

11.2.3.1. 配置网桥额外网络

以下对象描述了 bridge CNI 插件的配置参数：

表 11.2. bridge CNI 插件 JSON 配置对象

字段	类型	描述
cniVersion	字符串	CNI 规格版本。需要 0.3.1 值。
name	字符串	您之前为 CNO 配置提供的 name 参数的值。

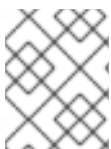
字段	类型	描述
type	字符串	
bridge	字符串	指定要使用的虚拟网桥名称。如果主机上不存在网桥接口，则进行创建。默认值为 cni0 。
ipam	对象	IPAM CNI 插件的配置对象。该插件管理网络附加定义的 IP 地址分配。
ipMasq	布尔值	设置为 true ，从而为离开虚拟网络的流量启用 IP 伪装。所有流量的源 IP 地址都会改写为网桥 IP 地址。如果网桥没有 IP 地址，此设置无效。默认值为 false 。
isGateway	布尔值	设置为 true ，从而为网桥分配 IP 地址。默认值为 false 。
isDefaultGateway	布尔值	设置为 true ，从而将网桥配置为虚拟网络的默认网关。默认值为 false 。如果 isDefaultGateway 设置为 true ，则 isGateway 也会自动设置为 true 。
forceAddress	布尔值	设置为 true ，从而允许将之前分配的 IP 地址分配给虚拟网桥。设置为 false 时，如果将来自于重叠子集的 IPv4 地址或者 IPv6 地址分配给虚拟网桥，则会发生错误。默认值为 false 。
hairpinMode	布尔值	设置为 true ，以允许虚拟网桥通过接收它的虚拟端口重新发送以太网帧。这个模式也被称为 <i>反射中继</i> 。默认值为 false 。
promiscMode	布尔值	设置为 true ，从而在网桥上启用混杂模式。默认值为 false 。
vlan	字符串	以整数值形式指定虚拟 LAN (VLAN) 标签。默认情况下不分配 VLAN 标签。
mtu	字符串	将最大传输单位 (MTU) 设置为指定的值。默认值由内核自动设置。

11.2.3.1.1. 网桥配置示例

以下示例配置了名为 **bridge-net** 的额外网络：

```
{
  "cniVersion": "0.3.1",
  "name": "work-network",
  "type": "bridge",
  "isGateway": true,
  "vlan": 2,
  "ipam": {
    "type": "dhcp"
  }
}
```

11.2.3.2. 主机设备额外网络的配置



注意

仅设置以下参数之一来指定您的网络设备：**device**、**HWaddr**、**kernelpath** 或 **pciBusID**。

以下对象描述了 host-device CNI 插件的配置参数：

表 11.3. 主机设备 CNI 插件 JSON 配置对象

字段	类型	描述
cniVersion	字符串	CNI 规格版本。需要 0.3.1 值。
name	字符串	您之前为 CNO 配置提供的 name 参数的值。
type	字符串	要配置的 CNI 插件的名称： host-device 。
device	字符串	可选：设备的名称，如 eth0 。
hwaddr	字符串	可选：设备硬件 MAC 地址。
kernelpath	字符串	可选：Linux 内核设备路径，如 /sys/devices/pci0000:00/0000:00:1f.6 。
pciBusID	字符串	可选：网络设备的 PCI 地址，如 0000:00:1f.6 。
ipam	对象	IPAM CNI 插件的配置对象。该插件管理网络附加定义的 IP 地址分配。

11.2.3.2.1. host-device 配置示例

以下示例配置了名为 **hostdev-net** 的额外网络：

```
{
  "cniVersion": "0.3.1",
  "name": "work-network",
  "type": "host-device",
  "device": "eth1",
  "ipam": {
    "type": "dhcp"
  }
}
```

11.2.3.3. 配置 IPVLAN 额外网络

以下对象描述了 IPVLAN CNI 插件的配置参数：

表 11.4. ipvlan CNI 插件 JSON 配置对象

字段	类型	描述
cniVersion	字符串	CNI 规格版本。需要 0.3.1 值。
name	字符串	您之前为 CNO 配置提供的 name 参数的值。
type	字符串	要配置的 CNI 插件的名称： ipvlan 。
mode	字符串	虚拟网络的操作模式。这个值必须是 I2 、 I3 或 I3s 。默认值为 I2 。
master	字符串	与网络附加关联的以太网接口。如果没有指定 master ，则使用默认网络路由的接口。
mtu	整数	将最大传输单位 (MTU) 设置为指定的值。默认值由内核自动设置。
ipam	对象	IPAM CNI 插件的配置对象。该插件管理网络附加定义的 IP 地址分配。 不要指定 dhcp 。不支持使用 DHCP 配置 IPVLAN，因为 IPVLAN 接口与主机接口共享 MAC 地址。

11.2.3.3.1. ipvlan 配置示例

以下示例配置了名为 **ipvlan -net** 的额外网络：

```
{
  "cniVersion": "0.3.1",
  "name": "work-network",
  "type": "ipvlan",
  "master": "eth1",
  "mode": "I3",
  "ipam": {
    "type": "static",
    "addresses": [
      {
        "address": "192.168.10.10/24"
      }
    ]
  }
}
```

11.2.3.4. MACVLAN 额外网络的配置

以下对象描述了 macvlan CNI 插件的配置参数：

表 11.5. MACVLAN CNI 插件 JSON 配置对象

字段	类型	描述
cniVersion	字符串	CNI 规格版本。需要 0.3.1 值。
name	字符串	您之前为 CNO 配置提供的 name 参数的值。
type	字符串	要配置的 CNI 插件的名称：mac vlan 。
mode	字符串	配置虚拟网络上的流量可见性。必须是 bridge 、 passthru 、 private 或 Vepa 。如果没有提供值，则默认值为 bridge 。
master	字符串	与虚拟接口关联的以太网、绑定或 VLAN 接口。如果未指定值，则使用主机系统的主以太网接口。
mtu	字符串	到指定值的最大传输单元(MTU)。默认值由内核自动设置。
ipam	对象	IPAM CNI 插件的配置对象。该插件管理网络附加定义的 IP 地址分配。

11.2.3.4.1. macvlan 配置示例

以下示例配置了名为 **macvlan-net** 的额外网络：

```
{
  "cniVersion": "0.3.1",
  "name": "macvlan-net",
  "type": "macvlan",
  "master": "eth1",
  "mode": "bridge",
  "ipam": {
    "type": "dhcp"
  }
}
```

11.2.4. 为额外网络配置 IP 地址分配

IP 地址管理(IPAM)Container Network Interface(CNI)插件为其他 CNI 插件提供 IP 地址。

您可以使用以下 IP 地址分配类型：

- 静态分配。
- 通过 DHCP 服务器进行动态分配。您指定的 DHCP 服务器必须可从额外网络访问。
- 通过 Whereabouts IPAM CNI 插件进行动态分配。

11.2.4.1. 静态 IP 地址分配配置

下表描述了静态 IP 地址分配的配置：

表 11.6. ipam 静态配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值是 静态 的。
地址	数组	指定分配给虚拟接口的 IP 地址的对象数组。支持 IPv4 和 IPv6 IP 地址。
Routes	数组	指定要在 pod 中配置的路由的对象数组。
dns	数组	可选：指定 DNS 配置的对象数组。

address 数组需要带有以下字段的对象：

表 11.7. ipam.addresses[] array

字段	类型	描述
地址	字符串	您指定的 IP 地址和网络前缀。例如：如果您指定 10.10.21.10/24 ，那么会为额外网络分配 IP 地址 10.10.21.10 ，网掩码为 255.255.255.0 。
gateway	字符串	出口网络流量要路由到的默认网关。

表 11.8. ipam.routes[] 数组

字段	类型	描述
dst	字符串	CIDR 格式的 IP 地址范围，如 192.168.17.0/24 或 0.0.0.0/0 （默认路由）。
gw	字符串	网络流量路由的网关。

表 11.9. ipam.dns 对象

字段	类型	描述
名称服务器	数组	用来发送 DNS 查询的一个或多个 IP 地址的数组。
domain	数组	要附加到主机名的默认域。例如，如果将域设置为 example.com ，对 example-host 的 DNS 查找查询将被改写为 example-host.example.com 。
search	数组	在 DNS 查找查询过程中，附加到非限定主机名（如 example-host ）的域名的数组。

静态 IP 地址分配配置示例

```

{
  "ipam": {
    "type": "static",
    "addresses": [
      {
        "address": "191.168.1.7/24"
      }
    ]
  }
}

```

11.2.4.2. 动态 IP 地址(DHCP)分配配置

以下 JSON 描述了使用 DHCP 进行动态 IP 地址地址分配的配置：

DHCP 租期续订

pod 在创建时获取其原始 DHCP 租期。该租期必须由集群中运行的一个小型的 DHCP 服务器部署定期续订。

要触发 DHCP 服务器的部署，您必须编辑 Cluster Network Operator 配置来创建 shim 网络附加，如下例所示：

shim 网络附加定义示例

```

apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  additionalNetworks:
  - name: dhcp-shim
    namespace: default
    type: Raw
    rawCNConfig: |-
      {
        "name": "dhcp-shim",
        "cniVersion": "0.3.1",
        "type": "bridge",
        "ipam": {
          "type": "dhcp"
        }
      }
    # ...

```

表 11.10. ipam DHCP 配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值 dhcp 是必需的。

动态 IP 地址(DHCP)分配配置示例

```
{
  "ipam": {
    "type": "dhcp"
  }
}
```

11.2.4.3. 使用 Whereabouts 进行动态 IP 地址分配配置

Whereabouts CNI 插件允许在不使用 DHCP 服务器的情况下动态地将 IP 地址分配给额外网络。

下表描述了使用 Whereabouts 进行动态 IP 地址分配的配置：

表 11.11. ipam 观察配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值是 必填 的。
范围	字符串	CIDR 表示法中的 IP 地址和范围。IP 地址是通过这个地址范围来分配的。
exclude	数组	可选：CIDR 表示法中存在零或多个 IP 地址和范围的列表。包含在排除地址范围中的 IP 地址。

使用 Whereabouts 的动态 IP 地址分配配置示例

```
{
  "ipam": {
    "type": "whereabouts",
    "range": "192.0.2.192/27",
    "exclude": [
      "192.0.2.192/30",
      "192.0.2.196/32"
    ]
  }
}
```

11.2.5. 使用 Cluster Network Operator 创建额外网络附加

Cluster Network Operator (CNO) 管理额外网络定义。当您指定要创建的额外网络时，CNO 会自动创建 **NetworkAttachmentDefinition** 对象。



重要

不要编辑 Cluster Network Operator 所管理的 **NetworkAttachmentDefinition** 对象。这样做可能会破坏额外网络上的网络流量。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 要编辑 CNO 配置，请输入以下命令：

```
$ oc edit networks.operator.openshift.io cluster
```

2. 通过为您要创建的额外网络添加配置来修改您要创建的 CR，如下例所示。

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  # ...
  additionalNetworks:
  - name: tertiary-net
    namespace: project2
    type: Raw
    rawCNICofig: |-
      {
        "cniVersion": "0.3.1",
        "name": "tertiary-net",
        "type": "ipvlan",
        "master": "eth1",
        "mode": "l2",
        "ipam": {
          "type": "static",
          "addresses": [
            {
              "address": "192.168.1.23/24"
            }
          ]
        }
      }
    }
```

3. 保存您的更改，再退出文本编辑器以提交更改。

验证

- 运行以下命令确认 CNO 创建了 NetworkAttachmentDefinition 对象。CNO 创建对象之前可能会有延迟。

```
$ oc get network-attachment-definitions -n <namespace>
```

其中：

<namespace>

指定添加到 CNO 配置的网络附加的命名空间。

输出示例

```
NAME           AGE
test-network-1 14m
```

11.2.6. 通过应用 YAML 清单来创建额外网络附加

先决条件

- 安装 OpenShift CLI (**oc**) 。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 使用额外网络配置创建 YAML 文件，如下例所示：

```
apiVersion: k8s.cni.cncf.io/v1
kind: NetworkAttachmentDefinition
metadata:
  name: next-net
spec:
  config: |-
    {
      "cniVersion": "0.3.1",
      "name": "work-network",
      "type": "host-device",
      "device": "eth1",
      "ipam": {
        "type": "dhcp"
      }
    }
  }
```

2. 运行以下命令来创建额外网络：

```
$ oc apply -f <file>.yaml
```

其中：

<file>

指定包含 YAML 清单的文件名称。

11.3. 将 POD 附加到额外网络

作为集群用户，您可以将 pod 附加到额外网络。

11.3.1. 将 pod 添加到额外网络

您可以将 pod 添加到额外网络。pod 继续通过默认网络发送与集群相关的普通网络流量。

创建 pod 时会附加额外网络。但是，如果 pod 已存在，您无法为其附加额外网络。

pod 必须与额外网络处于相同的命名空间。

先决条件

- 安装 OpenShift CLI (**oc**) 。
- 登录到集群。

流程

1. 为 **Pod** 对象添加注解。只能使用以下注解格式之一：

- a. 要在没有自定义的情况下附加额外网络，请使用以下格式添加注解。将 **<network>** 替换为要与 pod 关联的额外网络的名称：

```
metadata:
  annotations:
    k8s.v1.cni.cncf.io/networks: <network>[,<network>,...] 1
```

- 1 要指定多个额外网络，请使用逗号分隔各个网络。逗号之间不可包括空格。如果您多次指定同一额外网络，则该 pod 会将多个网络接口附加到该网络。

b. 要通过自定义来附加额外网络，请添加具有以下格式的注解：

```
metadata:
  annotations:
    k8s.v1.cni.cncf.io/networks: |-
      [
        {
          "name": "<network>", 1
          "namespace": "<namespace>", 2
          "default-route": ["<default-route>"] 3
        }
      ]
```

- 1 指定 **NetworkAttachmentDefinition** 对象定义的额外网络的名称。
- 2 指定定义 **NetworkAttachmentDefinition** 对象的命名空间。
- 3 可选：为默认路由指定覆盖，如 **192.168.17.1**。

2. 运行以下命令来创建 pod。将 **<name>** 替换为 pod 的名称。

```
$ oc create -f <name>.yaml
```

3. 可选：要确认 **Pod** CR 中是否存在注解，请输入以下命令将 **<name>** 替换为 pod 的名称。

```
$ oc get pod <name> -o yaml
```

在以下示例中，**example-pod** pod 附加到 **net1** 额外网络：

```
$ oc get pod example-pod -o yaml
apiVersion: v1
kind: Pod
metadata:
  annotations:
    k8s.v1.cni.cncf.io/networks: macvlan-bridge
    k8s.v1.cni.cncf.io/networks-status: |- 1
      [{
        "name": "openshift-sdn",
        "interface": "eth0",
```

```

      "ips": [
        "10.128.2.14"
      ],
      "default": true,
      "dns": {}
    },{
      "name": "macvlan-bridge",
      "interface": "net1",
      "ips": [
        "20.2.2.100"
      ],
      "mac": "22:2f:60:a5:f8:00",
      "dns": {}
    }
  ]
  name: example-pod
  namespace: default
  spec:
  ...
  status:
  ...

```

- 1 **k8s.v1.cni.cncf.io/networks-status** 参数是对象的 JSON 数组。每个对象描述附加到 pod 的额外网络的状态。注解值保存为纯文本值。

11.3.1.1. 指定特定于 pod 的地址和路由选项

将 pod 附加到额外网络时，您可能需要在特定 pod 中指定有关该网络的其他属性。这可让您更改路由的某些方面，并指定静态 IP 地址和 MAC 地址。要达到此目的，您可以使用 JSON 格式的注解。

先决条件

- pod 必须与额外网络处于相同的命名空间。
- 安装 OpenShift 命令行界面 (oc)。
- 您必须登录集群。

流程

要在指定地址和/或路由选项的同时将 pod 添加到额外网络，请完成以下步骤：

1. 编辑 **Pod** 资源定义。如果要编辑现有 **Pod** 资源，请运行以下命令在默认编辑器中编辑其定义。将 **<name>** 替换为要编辑的 **Pod** 资源的名称。

```
$ oc edit pod <name>
```

2. 在 **Pod** 资源定义中，将 **k8s.v1.cni.cncf.io/networks** 参数添加到 pod **metadata** 映射中。**k8s.v1.cni.cncf.io/networks** 接受 JSON 字符串，该字符串除指定附加属性外，还引用 **NetworkAttachmentDefinition** 自定义资源 (CR) 名称的对象。

```

metadata:
  annotations:
    k8s.v1.cni.cncf.io/networks: ' [<network>[,<network>,...]' 1

```

1 将 `<network>` 替换为 JSON 对象，如下例所示。单引号是必需的。

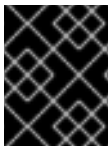
3. 在以下示例中，通过 `default-route` 参数，注解指定了哪个网络附加将使用默认路由。

```
apiVersion: v1
kind: Pod
metadata:
  name: example-pod
  annotations:
    k8s.v1.cni.cncf.io/networks: '
    {
      "name": "net1"
    },
    {
      "name": "net2", 1
      "default-route": ["192.0.2.1"] 2
    }
  '
spec:
  containers:
  - name: example-pod
    command: ["/bin/bash", "-c", "sleep 200000000000000"]
    image: centos/tools
```

1 **name** 是与 pod 关联的额外网络的名称。

2 **default-route** 指定了一个网关，当在路由表中没有其它路由条目时使用这个网关。如果指定了多个 **default-route** 键，这将导致 pod 无法成为活跃状态。

默认路由将导致任何没有在其路由中指定的流量被路由到网关。



重要

将 OpenShift Container Platform 的默认路由设置为默认网络接口以外的接口时，可能会导致应该是 pod 和 pod 间的网络流量被路由到其他接口。

要验证 pod 的路由属性，可使用 `oc` 命令在 pod 中执行 `ip` 命令。

```
$ oc exec -it <pod_name> -- ip route
```



注意

您还可以引用 pod 的 `k8s.v1.cni.cncf.io/networks-status` 来查看哪个额外网络已经分配了默认路由，这可以通过 JSON 格式的对象列表中的 `default-route` 键实现。

要为 pod 设置静态 IP 地址或 MAC 地址，您可以使用 JSON 格式的注解。这要求您创建允许此功能的网络。这可以在 CNO 的 `rawCNICConfig` 中指定。

1. 运行以下命令来编辑 CNO CR :

```
$ oc edit networks.operator.openshift.io cluster
```


以下 YAML 描述了 CNO 的配置参数：

Cluster Network Operator YAML 配置

```
name: <name> ❶
namespace: <namespace> ❷
rawCNConfig: '{ ❸
  ...
}'
type: Raw
```

- ❶ 为您要创建的额外网络附加指定名称。该名称在指定的 **namespace** 中需要是唯一的。
- ❷ 指定要在其中创建网络附加的命名空间。如果您未指定值，则使用 **default** 命名空间。
- ❸ 基于以下模板，以 JSON 格式指定 CNI 插件配置。

以下对象描述了使用 macvlan CNI 插件的静态 MAC 地址和 IP 地址的配置参数：

使用静态 IP 和 MAC 地址的 macvlan CNI 插件 JSON 配置对象

```
{
  "cniVersion": "0.3.1",
  "name": "<name>", ❶
  "plugins": [{ ❷
    "type": "macvlan",
    "capabilities": { "ips": true }, ❸
    "master": "eth0", ❹
    "mode": "bridge",
    "ipam": {
      "type": "static"
    }
  }, {
    "capabilities": { "mac": true }, ❺
    "type": "tuning"
  }
]}
```

- ❶ 指定要创建的额外网络附加的名称。该名称在指定的 **namespace** 中需要是唯一的。
- ❷ 指定 CNI 插件配置的数组。第一个对象指定 macvlan 插件配置，第二个对象指定 tuning 插件配置。
- ❸ 指定一个请求启用 CNI 插件运行时配置功能的静态 IP 地址功能。
- ❹ 指定 macvlan 插件使用的接口。
- ❺ 指定一个请求启用 CNI 插件的静态 MAC 地址功能。

以上网络附加可能会以 JSON 格式的注解引用，同时使用相关的键来指定将哪些静态 IP 和 MAC 地址分配给指定 pod。

使用以下内容编辑 pod：

```
$ oc edit pod <name>
```

使用静态 IP 和 MAC 地址的 macvlan CNI 插件 JSON 配置对象

```
apiVersion: v1
kind: Pod
metadata:
  name: example-pod
  annotations:
    k8s.v1.cni.cncf.io/networks: '[
  {
    "name": "<name>", ①
    "ips": [ "192.0.2.205/24" ], ②
    "mac": "CA:FE:C0:FF:EE:00" ③
  }
]'
```

- ① 使用在创建 **rawCNICConfig** 时提供的 **<name>** 。
- ② 提供包括子网掩码的 IP 地址。
- ③ 提供 MAC 地址。



注意

静态 IP 地址和 MAC 地址不需要同时使用，您可以单独使用，也可以一起使用。

要验证一个带有额外网络的 pod 的 IP 地址和 MAC 属性，请使用 **oc** 命令在 pod 中执行 **ip** 命令。

```
$ oc exec -it <pod_name> -- ip a
```

11.4. 从额外网络中删除 POD

作为集群用户，您可以从额外网络中删除 pod。

11.4.1. 从额外网络中删除 pod

您只能通过删除 pod 来从额外网络中删除 pod。

先决条件

- 一个额外网络被附加到 pod。
- 安装 OpenShift CLI (**oc**) 。
- 登录到集群。

流程

- 要删除 pod，输入以下命令：

```
$ oc delete pod <name> -n <namespace>
```

- **<name>** 是 pod 的名称。
- **<namespace>** 是包含 pod 的命名空间。

11.5. 编辑额外网络

作为集群管理员，您可以修改现有额外网络的配置。

11.5.1. 修改额外网络附加定义

作为集群管理员，您可以对现有额外网络进行更改。任何附加到额外网络的现有 pod 都不会被更新。

先决条件

- 已为集群配置了额外网络。
- 安装 OpenShift CLI (**oc**) 。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

要为集群编辑额外网络，请完成以下步骤：

1. 运行以下命令，在默认文本编辑器中编辑 Cluster Network Operator (CNO) CR：

```
$ oc edit networks.operator.openshift.io cluster
```

2. 在 **additionalNetworks** 集合中，用您的更改更新额外网络。
3. 保存您的更改，再退出文本编辑器以提交更改。
4. 可选：运行以下命令确认 CNO 更新了 **NetworkAttachmentDefinition** 对象。将 **<network-name>** 替换为要显示的额外网络名称。CNO 根据您的更改更新 **NetworkAttachmentDefinition** 对象前可能会有延迟。

```
$ oc get network-attachment-definitions <network-name> -o yaml
```

例如，以下控制台输出显示名为 **net1** 的 **NetworkAttachmentDefinition** 对象：

```
$ oc get network-attachment-definitions net1 -o go-template='{{printf "%s\n" .spec.config}}'
{ "cniVersion": "0.3.1", "type": "macvlan",
  "master": "ens5",
  "mode": "bridge",
  "ipam": { "type": "static", "routes": [{"dst": "0.0.0.0/0", "gw": "10.128.2.1"}], "addresses":
  [{"address": "10.128.2.100/23", "gateway": "10.128.2.1"}], "dns": {"nameservers":
  ["172.30.0.10"], "domain": "us-west-2.compute.internal", "search": ["us-west-
  2.compute.internal"]}} }
```

11.6. 删除额外网络

作为集群管理员，您可以删除额外网络附加。

11.6.1. 删除额外网络附加定义

作为集群管理员，您可以从 OpenShift Container Platform 集群中删除额外网络。额外网络不会从它所附加的任何 pod 中删除。

先决条件

- 安装 OpenShift CLI (**oc**) 。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

要从集群中删除额外网络，请完成以下步骤：

1. 运行以下命令，在默认文本编辑器中编辑 Cluster Network Operator (CNO)：

```
$ oc edit networks.operator.openshift.io cluster
```

2. 从您要删除的网络附加定义的 **additionalNetworks** 集合中删除配置，以此修改 CR。

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  additionalNetworks: [] 1
```

- 1** 如果要删除 **additionalNetworks** 集合中唯一额外网络附加定义的配置映射，您必须指定一个空集合。

3. 保存您的更改，再退出文本编辑器以提交更改。
4. 可选：通过运行以下命令确认删除了额外网络 CR：

```
$ oc get network-attachment-definition --all-namespaces
```

第 12 章 硬件网络

12.1. 关于单根 I/O 虚拟化 (SR-IOV) 硬件网络

Single Root I/O 虚拟化 (SR-IOV) 规范是针对一类 PCI 设备分配的标准，可与多个 pod 共享单个设备。

通过 SR-IOV，您可以将主机节点上识别为物理功能 (PF) 的兼容网络设备分段为多个虚拟功能 (VF)。VF 和其它网络设备一样使用。该设备的 SR-IOV 设备驱动程序决定了如何公开容器中的 VF：

- **netdevice** 驱动程序：容器 **netns** 中的常规内核网络设备
- **vfio-pci** 驱动程序：挂载到容器中的字符设备

您可以将 SR-IOV 网络设备与 OpenShift Container Platform 集群上安装在裸机或 Red Hat OpenStack Platform(RHOSP)基础架构上安装的额外网络一起使用，用于需要高带宽或低延迟的应用程序。

您可以使用以下命令在节点上启用 SR-IOV：

```
$ oc label node <node_name> feature.node.kubernetes.io/network-sriov.capable="true"
```

12.1.1. 负责管理 SR-IOV 网络设备的组件

SR-IOV Network Operator 会创建和管理 SR-IOV 堆栈的组件。它执行以下功能：

- 编配 SR-IOV 网络设备的发现和管理
- 为 SR-IOV Container Network Interface (CNI) 生成 **NetworkAttachmentDefinition** 自定义资源
- 创建和更新 SR-IOV 网络设备插件的配置
- 创建节点特定的 **SriovNetworkNodeState** 自定义资源
- 更新每个 **SriovNetworkNodeState** 自定义资源中的 **spec.interfaces** 字段

Operator 置备以下组件：

SR-IOV 网络配置守护进程

SR-IOV Operator 启动时在 worker 节点上部署的 DaemonSet。守护进程负责在集群中发现和初始化 SR-IOV 网络设备。

SR-IOV Operator Webhook

这是动态准入控制器 Webhook，用于验证 Operator 自定义资源，并为未设置的字段设置适当的默认值。

SR-IOV Network Resources Injector (网络资源注入器)。

这是一个动态准入控制器 Webhook，它提供通过请求和限制为自定义网络资源（如 SR-IOV VF）应用 Kubernetes pod 规格的功能。SR-IOV 网络资源注入程序仅将 **resource** 字段添加到 pod 中的第一个容器。

SR-IOV 网络设备插件

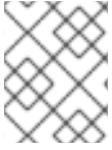
这个设备插件用于发现、公告并分配 SR-IOV 网络虚拟功能 (VF) 资源。在 Kubernetes 中使用设备插件能够利用有限的资源，这些资源通常为物理设备中。设备插件可以使 Kubernetes 调度程序了解资源可用性，因此调度程序可以在具有足够资源的节点上调度 pod。

SR-IOV CNI 插件

SR-IOV CNI 插件会附加从 SR-IOV 设备插件中直接分配给 pod 的 VF 接口。

SR-IOV InfiniBand CNI 插件

附加从 SR-IOV 设备插件中直接分配给 pod 的 InfiniBand (IB) VF 接口的 CNI 插件。



注意

SR-IOV Network resources injector 和 SR-IOV Operator Webhook 会被默认启用，可通过编辑 **default SriovOperatorConfig** CR 来禁用。

12.1.1.1. 支持的平台

SR-IOV Network Operator 在以下平台上受支持：

- 裸机
- Red Hat OpenStack Platform (RHOSP)

12.1.1.2. 支持的设备

OpenShift Container Platform 支持以下网络接口控制器：

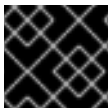
表 12.1. 支持的网络接口控制器

制造商	Model	供应商 ID	设备 ID
Intel	X710	8086	1572
Intel	XXV710	8086	158b
Mellanox	MT27700 系列 [ConnectX-4]	15b3	1013
Mellanox	MT27710 系列 [ConnectX-4 Lx]	15b3	1015
Mellanox	MT27800 系列 [ConnectX-5]	15b3	1017
Mellanox	MT28908 系列 [ConnectX-6]	15b3	101b

12.1.1.3. 自动发现 SR-IOV 网络设备

SR-IOV Network Operator 将搜索集群以获取 worker 节点上的 SR-IOV 功能网络设备。Operator 会为每个提供兼容 SR-IOV 网络设备的 worker 节点创建并更新一个 SriovNetworkNodeState 自定义资源 (CR)。

为 CR 分配了与 worker 节点相同的名称。**status.interfaces** 列表提供有关节点上网络设备的信息。



重要

不要修改 **SriovNetworkNodeState** 对象。Operator 会自动创建和管理这些资源。

12.1.1.3.1. SriovNetworkNodeState 对象示例

以下 YAML 是由 SR-IOV Network Operator 创建的 **SriovNetworkNodeState** 对象的示例：

一个 SriovNetworkNodeState 对象

```

apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodeState
metadata:
  name: node-25 1
  namespace: openshift-sriov-network-operator
  ownerReferences:
  - apiVersion: sriovnetwork.openshift.io/v1
    blockOwnerDeletion: true
    controller: true
    kind: SriovNetworkNodePolicy
    name: default
spec:
  dpConfigVersion: "39824"
status:
  interfaces: 2
  - deviceID: "1017"
    driver: mlx5_core
    mtu: 1500
    name: ens785f0
    pciAddress: "0000:18:00.0"
    totalvfs: 8
    vendor: 15b3
  - deviceID: "1017"
    driver: mlx5_core
    mtu: 1500
    name: ens785f1
    pciAddress: "0000:18:00.1"
    totalvfs: 8
    vendor: 15b3
  - deviceID: 158b
    driver: i40e
    mtu: 1500
    name: ens817f0
    pciAddress: 0000:81:00.0
    totalvfs: 64
    vendor: "8086"
  - deviceID: 158b
    driver: i40e
    mtu: 1500
    name: ens817f1
    pciAddress: 0000:81:00.1
    totalvfs: 64
    vendor: "8086"
  - deviceID: 158b
    driver: i40e
    mtu: 1500
    name: ens803f0
    pciAddress: 0000:86:00.0
    totalvfs: 64
    vendor: "8086"
  syncStatus: Succeeded

```

- 1 **name** 字段的值与 worker 节点的名称相同。
- 2 **interfaces** 小节包括 Operator 在 worker 节点上发现的所有 SR-IOV 设备列表。

12.1.1.4. 在 pod 中使用虚拟功能的示例

您可以在附加了 SR-IOV VF 的 pod 中运行远程直接内存访问 (RDMA) 或 Data Plane Development Kit (DPDK) 应用程序。

本示例演示了在 RDMA 模式中使用虚拟功能 (VF) 的 pod :

使用 RDMA 模式的 Pod 规格

```
apiVersion: v1
kind: Pod
metadata:
  name: rdma-app
  annotations:
    k8s.v1.cni.cncf.io/networks: sriov-rdma-mlnx
spec:
  containers:
  - name: testpmd
    image: <RDMA_image>
    imagePullPolicy: IfNotPresent
    securityContext:
      runAsUser: 0
    capabilities:
      add: ["IPC_LOCK","SYS_RESOURCE","NET_RAW"]
    command: ["sleep", "infinity"]
```

以下示例演示了在 DPDK 模式中使用 VF 的 pod:

使用 DPDK 模式的 Pod 规格

```
apiVersion: v1
kind: Pod
metadata:
  name: dpdk-app
  annotations:
    k8s.v1.cni.cncf.io/networks: sriov-dpdk-net
spec:
  containers:
  - name: testpmd
    image: <DPDK_image>
    securityContext:
      runAsUser: 0
    capabilities:
      add: ["IPC_LOCK","SYS_RESOURCE","NET_RAW"]
  volumeMounts:
  - mountPath: /dev/hugepages
    name: hugepage
  resources:
    limits:
      memory: "1Gi"
```



```

cpu: "2"
hugepages-1Gi: "4Gi"
requests:
  memory: "1Gi"
cpu: "2"
hugepages-1Gi: "4Gi"
command: ["sleep", "infinity"]
volumes:
- name: hugepage
  emptyDir:
    medium: HugePages

```

可以使用一个可选的库来协助容器中运行的应用程序收集与 pod 关联的网络信息。这个程序库名为 'app-netutil'。这个库的源代码包括在 [app-netutil GitHub repo](#) 中。

这个库的目的是简化将 SR-IOV VF 整合到 DPDK 模式中的操作。该程序库提供 GO API 和 C API，并包括了使用这两种语言的示例。

还有一个 Docker 镜像示例 'dpdk-app-centos'，它可以根据 pod-spec: l2fwd、l3wd 或 testpmd 中的环境变量运行以下 DPDK 示例应用程序之一。这个 Docker 镜像提供了将 'app-netutil' 整合到容器镜像本身的示例。这个库也可以整合到初始容器（init-container）中，该容器收集所需数据并将数据传递给现有的 DPDK 工作负载。

12.1.2. 后续步骤

- [安装 SR-IOV Network Operator](#)
- 可选：[配置 SR-IOV Network Operator](#)
- [配置 SR-IOV 网络设备](#)
- 如果使用 OpenShift Virtualization: [为虚拟机配置 SR-IOV 网络设备](#)
- [配置 SR-IOV 网络附加](#)
- [将 pod 添加到额外网络](#)

12.2. 安装 SR-IOV NETWORK OPERATOR

您可以在集群上安装单根 I/O 虚拟化（SR-IOV）网络 Operator，以管理 SR-IOV 网络设备和网络附加。

12.2.1. 安装 SR-IOV Network Operator

作为集群管理员，您可以使用 OpenShift Container Platform CLI 或 web 控制台安装 SR-IOV Network Operator。

12.2.1.1. CLI : 安装 SR-IOV Network Operator

作为集群管理员，您可以使用 CLI 安装 Operator。

先决条件

- 在裸机环境中安装的集群，其中的节点带有支持 SR-IOV 的硬件。
- 安装 OpenShift CLI (**oc**)。

- 具有 **cluster-admin** 特权的帐户

流程

1. 要创建 **openshift-sriov-network-operator** 命名空间，输入以下命令：

```
$ cat << EOF | oc create -f -
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-sriov-network-operator
EOF
```

2. 运行以下命令来创建 OperatorGroup CR：

```
$ cat << EOF | oc create -f -
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: sriov-network-operators
  namespace: openshift-sriov-network-operator
spec:
  targetNamespaces:
    - openshift-sriov-network-operator
EOF
```

3. 订阅 SR-IOV Network Operator。

- a. 运行以下命令以获取 OpenShift Container Platform 的主版本和次版本。下一步中需要 **channel** 值。

```
$ OC_VERSION=$(oc version -o yaml | grep openshiftVersion | \
grep -o '[0-9]*[.][0-9]*' | head -1)
```

- b. 要为 SR-IOV Network Operator 创建 Subscription CR，输入以下命令：

```
$ cat << EOF | oc create -f -
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: sriov-network-operator-subscription
  namespace: openshift-sriov-network-operator
spec:
  channel: "${OC_VERSION}"
  name: sriov-network-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
EOF
```

4. 要验证是否已安装 Operator，请输入以下命令：

```
$ oc get csv -n openshift-sriov-network-operator \
-o custom-columns=Name:.metadata.name,Phase:.status.phase
```

插图示例

Name	Phase
sriov-network-operator.4.4.0-202006160135	Succeeded

12.2.1.2. web 控制台：安装 SR-IOV Network Operator

作为集群管理员，您可以使用 Web 控制台安装 Operator。



注意

您必须使用 CLI 创建 operator 组。

先决条件

- 在裸机环境中安装的集群，其中的节点带有支持 SR-IOV 的硬件。
- 安装 OpenShift CLI (**oc**)。
- 具有 **cluster-admin** 特权的帐户

流程

1. 为 SR-IOV Network Operator 创建一个命名空间：
 - a. 在 OpenShift Container Platform web 控制台中，点 **Administration** → **Namespaces**。
 - b. 点 **Create Namespace**。
 - c. 在 **Name** 字段中输入 **openshift-sriov-network-operator**，然后点击 **Create**。
2. 安装 SR-IOV Network Operator：
 - a. 在 OpenShift Container Platform Web 控制台中，点击 **Operators** → **OperatorHub**。
 - b. 从可用的 Operators 列表中选择 **SR-IOV Network Operator**，然后点击 **Install**。
 - c. 在 **Install Operator** 页面中，在 **A specific namespace on the cluster** 中选择 **openshift-sriov-network-operator**。
 - d. 点击 **Install**。
3. 验证 SR-IOV Network Operator 是否已成功安装：
 - a. 导航到 **Operators** → **Installed Operators** 页面。
 - b. 确保 **SR-IOV Network Operator** 在 **openshift-sriov-network-operator** 项目中列出，状态为 **InstallSucceeded**。



注意

在安装过程中，Operator 可能会显示 **Failed** 状态。如果安装过程结束后有 **InstallSucceeded** 信息，您可以忽略这个 **Failed** 信息。

如果 Operator 没有被成功安装，请按照以下步骤进行故障排除：

- 检查 **Operator Subscriptions** 和 **Install Plans** 选项卡中的 **Status** 项中是否有任何错误。
- 进入 **Workloads** → **Pods** 页面，在 **openshift-sriov-network-operator** 项目中检查 pod 的日志。

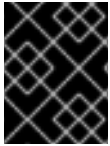
12.2.2. 后续步骤

- 可选：配置 [SR-IOV Network Operator](#)

12.3. 配置 SR-IOV NETWORK OPERATOR

Single Root I/O Virtualization (SR-IOV) Network Operator 管理集群中的 SR-IOV 网络设备和网络附加。

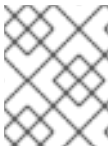
12.3.1. 配置 SR-IOV Network Operator



重要

通常不需要修改 SR-IOV Network Operator 配置。我们推荐在大多数用例中使用默认配置。只有 Operator 的默认行为与您的用例不兼容时，才需要按照以下步骤修改相关配置。

SR-IOV Network Operator 添加了 **SriovOperatorConfig.sriovnetwork.openshift.io** 自定义资源定义 (CRD)。Operator 会在 **openshift-sriov-network-operator** 命名空间中自动创建一个名为 **default** 的 SriovOperatorConfig 自定义资源 (CR)。



注意

default CR 包含集群的 SR-IOV Network Operator 配置。要更改 Operator 配置，您必须修改这个 CR。

SriovOperatorConfig 对象为配置 Operator 提供以下几个字段：

- **enableInjector** 允许项目管理员启用或禁用 Network Resources Injector 守护进程集。
- **enableOperatorWebhook** 允许项目管理员启用或禁用 Operator Admission Controller webhook 守护进程集。
- **configDaemonNodeSelector** 允许项目管理员在所选节点上调度 SR-IOV 网络配置守护进程。

12.3.1.1. 关于 Network Resources Injector（网络资源注入器）。

Network Resources Injector 是一个 Kubernetes Dynamic Admission Controller 应用。它提供以下功能：

- 根据 SR-IOV 网络附加定义注解，对 **Pod** 规格中的资源请求和限值进行修改，以添加 SR-IOV 资源名称。
- 使用下游 API 卷修改 **Pod** 规格，将 pod 注解和标签作为 **/etc/podnetinfo** 路径下的文件提供给正在运行的容器。

默认情况下，Network Resources Injector 由 SR-IOV 操作器启用，并作为守护进程集在所有 control plane 节点上运行（也称为 master 节点）。以下是在具有三个 control plane 节点的集群中运行的 Network Resources Injector pod 示例：

```
$ oc get pods -n openshift-sriov-network-operator
```

输出示例

NAME	READY	STATUS	RESTARTS	AGE
network-resources-injector-5cz5p	1/1	Running	0	10m
network-resources-injector-dwqpx	1/1	Running	0	10m
network-resources-injector-lktz5	1/1	Running	0	10m

12.3.1.2. 关于 SR-IOV Operator admission controller webhook

SR-IOV Operator Admission Controller Webhook 是一个 Kubernetes Dynamic Admission Controller 应用程序。它提供以下功能：

- 在创建或更新时，验证 **SriovNetworkNodePolicy** CR。
- 修改 **SriovNetworkNodePolicy** CR，在创建或更新 CR 时为 **priority** 和 **deviceType** 项设置默认值。

默认情况下，SR-IOV Operator Admission Controller Webhook 由 Operator 启用，并作为守护进程集在所有 control plane 节点上运行。以下是在具有三个 control plane 节点的集群中运行的 Operator Admission Controller webhook pod 的示例：

```
$ oc get pods -n openshift-sriov-network-operator
```

输出示例

NAME	READY	STATUS	RESTARTS	AGE
operator-webhook-9jkw6	1/1	Running	0	16m
operator-webhook-kbr5p	1/1	Running	0	16m
operator-webhook-rpfrl	1/1	Running	0	16m

12.3.1.3. 关于自定义节点选择器

SR-IOV 网络配置守护进程在集群节点上发现并配置 SR-IOV 网络设备。默认情况下，它将部署到集群中的所有 **worker** 节点。您可以使用节点标签指定 SR-IOV 网络配置守护进程在哪些节点上运行。

12.3.1.4. 禁用或启用网络资源注入器

要禁用或启用默认启用的网络资源注入器，请完成以下步骤。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。
- 您必须已安装了 SR-IOV Operator。

流程

- 设置 **enableInjector** 字段。将 **<value>** 替换为 **false** 来禁用这个功能；或替换为 **true** 来启用这个功能。

```
$ oc patch sriovoperatorconfig default \
  --type=merge -n openshift-sriov-network-operator \
  --patch '{"spec": {"enableInjector": <value> } }'
```

12.3.1.5. 禁用或启用 SR-IOV Operator 准入控制器 Webhook

要禁用或启用默认启用的准入控制器 Webhook，请完成以下步骤。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。
- 您必须已安装了 SR-IOV Operator。

流程

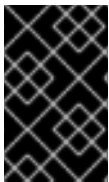
- 设置 **enableOperatorWebhook** 字段。将 **<value>** 替换为 **false** 来禁用这个功能；或替换为 **true** 来启用这个功能：

```
$ oc patch sriovoperatorconfig default --type=merge \
  -n openshift-sriov-network-operator \
  --patch '{"spec": {"enableOperatorWebhook": <value> } }'
```

12.3.1.6. 为 SR-IOV 网络配置守护进程配置自定义 NodeSelector

SR-IOV 网络配置守护进程在集群节点上发现并配置 SR-IOV 网络设备。默认情况下，它将部署到集群中的所有 **worker** 节点。您可以使用节点标签指定 SR-IOV 网络配置守护进程在哪些节点上运行。

要指定部署了 SR-IOV 网络配置守护进程的节点，请完成以下步骤。



重要

当您更新 **configDaemonNodeSelector** 字段时，SR-IOV 网络配置守护进程会在所选节点中重新创建。在重新创建守护进程时，集群用户无法应用任何新的 SR-IOV 网络节点策略或创建新的 SR-IOV Pod。

流程

- 要为 Operator 更新节点选择器，请输入以下命令：

```
$ oc patch sriovoperatorconfig default --type=json \
  -n openshift-sriov-network-operator \
  --patch '{
    "op": "replace",
    "path": "/spec/configDaemonNodeSelector",
    "value": {<node-label>}
  }'
```

将 **<node-label>** 替换为一个标签以应用它，例如：**"node-role.kubernetes.io/worker": ""**。

12.3.2. 后续步骤

- 配置 SR-IOV 网络设备

12.4. 配置 SR-IOV 网络设备

您可以在集群中配置单一根 I/O 虚拟化（SR-IOV）设备。

12.4.1. SR-IOV 网络节点配置对象

您可以通过定义 **SriovNetworkNodePolicy** 对象来指定节点的 SR-IOV 网络设备配置。该对象是 **sriovnetwork.openshift.io** API 组的一部分。

以下 YAML 描述了 **SriovNetworkNodePolicy** 对象：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: <name> 1
  namespace: openshift-sriov-network-operator 2
spec:
  resourceName: <sriov_resource_name> 3
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true" 4
  priority: <priority> 5
  mtu: <mtu> 6
  numVfs: <num> 7
  nicSelector: 8
    vendor: "<vendor_code>" 9
    deviceID: "<device_id>" 10
    pfNames: ["<pf_name>", ...] 11
    rootDevices: ["<pci_bus_id>", "..."] 12
  deviceType: <device_type> 13
  isRdma: false 14
  linkType: <link_type> 15
```

- 1 CR 对象的名称。
- 2 安装 SR-IOV Operator 的命名空间。
- 3 SR-IOV 设备插件的资源名称。您可以为一个资源名称创建多个 **SriovNetworkNodePolicy** 对象。
- 4 选择要配置哪些节点的节点选择器。只有所选节点上的 SR-IOV 网络设备才会被配置。SR-IOV Container Network Interface (CNI) 插件和设备插件仅在所选节点上部署。
- 5 可选：0 到 99 之间的整数。较小的数值具有较高的优先权，优先级 10 高于优先级 99。默认值为 99。
- 6 可选：虚拟功能的最大传输单元（MTU）。最大 MTU 值可能因不同的 NIC 型号而有所不同。
- 7 为 SR-IOV 物理网络设备创建的虚拟功能（VF）的数量。对于 Intel 网络接口卡（NIC），VF 的数量不能超过该设备支持的 VF 总数。对于 Mellanox NIC，VF 的数量不能超过 128。
- 8

nicSelector 映射为 Operator 选择要配置的设备。您不必为所有参数指定值。建议您足够精确地识别网络设备以避免意外选择设备。如果指定了 **rootDevices**，则必须同时为 **vendor**、**deviceID** 或

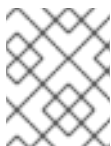
- 9 可选：SR-IOV 网络设备的厂商十六进制代码。允许的值只能是 **8086** 和 **15b3**。
- 10 可选：SR-IOV 网络设备的设备十六进制代码。允许的值只能是 **158b**、**1015** 和 **1017**。
- 11 可选：该设备的一个或多个物理功能（PF）名称的数组。
- 12 用于该设备的 PF 的一个或多个 PCI 总线地址的数组。使用以下格式提供地址：**0000:02:00.1**。
- 13 可选：虚拟功能的驱动程序类型。允许的值只能是 **netdevice** 和 **vfio-pci**。默认值为 **netdevice**。



注意

对于裸机节点上的 Data Plane Development Kit (DPDK) 模式中的 Mellanox 卡，请使用 **netdevice** 驱动程序类型，并将 **isRdma** 设为 **true**。

- 14 可选：是否启用远程直接访问（RDMA）模式。默认值为 **false**。



注意

如果将 **isRDMA** 参数设定为 **true**，您可以继续使用启用了 RDMA 的 VF 作为普通网络设备。设备可在其中的一个模式中使用。

- 15 可选：VF 的链接类型。您可以指定以下值之一：**eth** 或 **ib**。**eth** 是 ethernet，**ib** 是 InfiniBand。如果没有显式设置，则默认值为 **eth**。当将 **linkType** 设置为 **ib** 时，SR-IOV Network Operator Webhook 会自动将 **isRdma** 设置为 **true**。当将 **linkType** 设定为 **ib** 时，**deviceType** 不应该被设置为 **vfio-pci**。

12.4.1.1. SR-IOV 网络节点配置示例

以下示例论述了如何配置 IB 设备：

IB 设备配置示例

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: policy-ib-net-1
  namespace: openshift-sriov-network-operator
spec:
  resourceName: ibnic1
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true"
  numVfs: 4
  nicSelector:
    vendor: "15b3"
    deviceID: "101b"
    rootDevices:
      - "0000:19:00.0"
  linkType: ib
  isRdma: true
```


12.4.1.2. SR-IOV 设备的虚拟功能 (VF) 分区

在某些情况下，您可能想要将同一个物理功能 (PF) 的虚拟功能 (VF) 分成多个资源池。例如：您可能想要某些 VF 使用默认驱动程序载入，而其他的 VF 负载使用 **vfio-pci** 驱动程序。在这样的部署中，您可以使用 `SriovNetworkNodePolicy` 自定义资源 (CR) 中的 **pfNames** 选项器 (selector) 来为池指定 VF 的范围，其格式为：`<pfname>#<first_vf>-<last_vf>`。

例如，以下 YAML 显示名为 **netpf0** 的、带有 VF 2 到 7 的接口的选择器：

```
pfNames: ["netpf0#2-7"]
```

- **netpf0** 是 PF 接口名称。
- **2** 是包含在范围内的第一个 VF 索引（基于 0）。
- **7** 是包含在范围内的最后一个 VF 索引（基于 0）。

如果满足以下要求，您可以使用不同的策略 CR 从同一 PF 中选择 VF：

- 选择相同 PF 的不同策略的 **numVfs** 值必须相同。
- VF 索引范围是从 0 到 `<numVfs>-1` 之间。例如，如果您有一个策略，它的 **numVfs** 被设置为 8，则 `<first_vf>` 的值不能小于 0，`<last_vf>` 的值不能大于 7。
- 不同策略中的 VF 范围不得互相重叠。
- `<first_vf>` 不能大于 `<last_vf>`。

以下示例演示了 SR-IOV 设备的 NIC 分区。

策略 **policy-net-1** 定义了一个资源池 **net-1**，其中包含带有默认 VF 驱动的 PF **netpf0** 的 VF 0。策略 **policy-net-1-dpdk** 定义了一个资源池 **net-1-dpdk**，其中包含带有 **vfio** VF 驱动程序的 PF **netpf0** 的 VF 8 到 15。

策略 **policy-net-1**：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: policy-net-1
  namespace: openshift-sriov-network-operator
spec:
  resourceName: net1
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true"
  numVfs: 16
  nicSelector:
    pfNames: ["netpf0#0-0"]
  deviceType: netdevice
```

策略 **policy-net-1-dpdk**：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: policy-net-1-dpdk
```

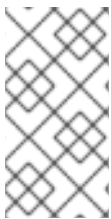
```

namespace: openshift-sriov-network-operator
spec:
  resourceName: net1dpdk
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true"
  numVfs: 16
  nicSelector:
    pfNames: ["netpf0#8-15"]
  deviceType: vfio-pci

```

12.4.2. 配置 SR-IOV 网络设备

SR-IOV Network Operator 把 **SriovNetworkNodePolicy.sriovnetwork.openshift.io** CRD 添加到 OpenShift Container Platform。您可以通过创建一个 **SriovNetworkNodePolicy** 自定义资源 (CR) 来配置 SR-IOV 网络设备。



注意

在应用由 **SriovNetworkNodePolicy** 对象中指定的配置时，SR-IOV Operator 可能会排空节点，并在某些情况下会重启节点。

它可能需要几分钟时间来应用配置更改。

先决条件

- 已安装 OpenShift CLI (**oc**)。
- 您可以使用具有 **cluster-admin** 角色的用户访问集群。
- 已安装 SR-IOV Network Operator。
- 集群中有足够的可用节点，用于处理从排空节点中驱除的工作负载。
- 您还没有为 SR-IOV 网络设备配置选择任何 control plane 节点。

流程

1. 创建一个 **SriovNetworkNodePolicy** 对象，然后在 **<name>-sriov-node-network.yaml** 文件中保存 YAML。使用配置的实际名称替换 **<name>**。
2. 可选：将 SR-IOV 功能的集群节点标记为 **SriovNetworkNodePolicy.Spec.NodeSelector**（如果它们还没有标记）。有关标记节点的更多信息，请参阅“了解如何更新节点上的标签”。
2. 创建 **SriovNetworkNodePolicy** 对象：

```
$ oc create -f <name>-sriov-node-network.yaml
```

其中 **<name>** 指定这个配置的名称。

在应用配置更新后，**sriov-network-operator** 命名空间中的所有 Pod 都会变为 **Running** 状态。

3. 要验证是否已配置了 SR-IOV 网络设备，请输入以下命令。将 **<node_name>** 替换为带有您刚才配置的 SR-IOV 网络设备的节点名称。

```
$ oc get sriovnetworknodestates -n openshift-sriov-network-operator <node_name> -o
jsonpath='{.status.syncStatus}'
```

其他资源

- [了解如何更新节点上的标签。](#)

12.4.3. SR-IOV 配置故障排除

在进行了配置 SR-IOV 网络设备的步骤后，以下部分会处理一些错误条件。

要显示节点状态，请运行以下命令：

```
$ oc get sriovnetworknodestates -n openshift-sriov-network-operator <node_name>
```

其中：**<node_name>** 指定带有 SR-IOV 网络设备的节点名称。

错误输出：无法分配内存

```
"lastSyncError": "write /sys/bus/pci/devices/0000:3b:00.1/sriov_numvfs: cannot allocate memory"
```

当节点表示无法分配内存时，检查以下项目：

- 确认在 BIOS 中为节点启用了全局 SR-IOV 设置。
- 确认在 BIOS 中为该节点启用了 VT-d。

12.4.4. 后续步骤

- [配置 SR-IOV 网络附加](#)

12.5. 配置 SR-IOV 以太网网络附加

您可以为集群中的单根 I/O 虚拟化（SR-IOV）设备配置以太网网络附加。

12.5.1. 以太网设备配置对象

您可以通过定义 **SriovNetwork** 对象来配置以太网网络设备。

以下 YAML 描述了 **SriovNetwork** 对象：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetwork
metadata:
  name: <name> 1
  namespace: openshift-sriov-network-operator 2
spec:
  resourceName: <sriov_resource_name> 3
  networkNamespace: <target_namespace> 4
  vlan: <vlan> 5
  spoofChk: "<spooof_check>" 6
  ipam: |- 7
```

```

{}
linkState: <link_state> 8
maxTxRate: <max_tx_rate> 9
minTxRate: <min_tx_rate> 10
vlanQoS: <vlan_qos> 11
trust: "<trust_vf>" 12
capabilities: <capabilities> 13

```

- 1 对象的名称。SR-IOV Network Operator 创建一个名称相同的 **NetworkAttachmentDefinition** 对象。
- 2 安装 SR-IOV Network Operator 的命名空间。
- 3 用于为这个额外网络定义 SR-IOV 硬件的 **SriovNetworkNodePolicy** 对象中的 **spec.resourceName** 参数的值。
- 4 **SriovNetwork** 对象的目标命名空间。只有目标命名空间中的 pod 可以附加到额外网络。
- 5 可选：额外网络的虚拟 LAN (VLAN) ID。它需要是一个从 0 到 4095 范围内的一个整数值。默认值为 0。
- 6 可选：VF 的 spoof 检查模式。允许的值是字符串 "on" 和 "off"。



重要

指定的值必须由引号包括，否则 SR-IOV Network Operator 将拒绝对象。

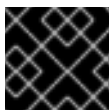
- 7 为 IPAM CNI 插件指定一个配置对象作为一个 YAML 块 scalar。该插件管理网络附加定义的 IP 地址分配。
- 8 可选：虚拟功能 (VF) 的连接状态。允许的值是 **enable**、**disable** 和 **auto**。
- 9 可选：VF 的最大传输率（以 Mbps 为单位）。
- 10 可选：VF 的最低传输率（以 Mbps 为单位）。这个值必须小于或等于最大传输率。



注意

Intel NIC 不支持 **minTxRate** 参数。如需更多信息，请参阅 [BZ#1772847](#)。

- 11 可选：VF 的 IEEE 802.1p 优先级级别。默认值为 0。
- 12 可选：VF 的信任模式。允许的值是字符串 "on" 和 "off"。



重要

您必须在引号中包含指定的值，或者 SR-IOV Network Operator 拒绝对象。

- 13 可选：为这个额外网络配置功能。您可以指定 "{ **ips**: true }" 来启用 IP 地址支持，或指定 "{ **mac**: true }" 来启用 MAC 地址支持。

12.5.1.1. 为额外网络配置 IP 地址分配

IP 地址管理(IPAM)Container Network Interface(CNI)插件为其他 CNI 插件提供 IP 地址。

您可以使用以下 IP 地址分配类型：

- 静态分配。
- 通过 DHCP 服务器进行动态分配。您指定的 DHCP 服务器必须可从额外网络访问。
- 通过 Whereabouts IPAM CNI 插件进行动态分配。

12.5.1.1.1. 静态 IP 地址分配配置

下表描述了静态 IP 地址分配的配置：

表 12.2. ipam 静态配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值是 静态 的。
地址	数组	指定分配给虚拟接口的 IP 地址的对象数组。支持 IPv4 和 IPv6 IP 地址。
Routes	数组	指定要在 pod 中配置的路由的对象数组。
dns	数组	可选：指定 DNS 配置的对象数组。

address 数组需要带有以下字段的对象：

表 12.3. ipam.addresses[] array

字段	类型	描述
地址	字符串	您指定的 IP 地址和网络前缀。例如：如果您指定 10.10.21.10/24 ，那么会为额外网络分配 IP 地址 10.10.21.10 ，网掩码为 255.255.255.0 。
gateway	字符串	出口网络流量要路由到的默认网关。

表 12.4. ipam.routes[] 数组

字段	类型	描述
dst	字符串	CIDR 格式的 IP 地址范围，如 192.168.17.0/24 或 0.0.0.0/0 （默认路由）。
gw	字符串	网络流量路由的网关。

表 12.5. ipam.dns 对象

字段	类型	描述
名称服务器	数组	用来发送 DNS 查询的一个或多个 IP 地址的数组。
domain	数组	要附加到主机名的默认域。例如，如果将域设置为 example.com ，对 example-host 的 DNS 查找查询将被改写为 example-host.example.com 。
search	数组	在 DNS 查找查询过程中，附加到非限定主机名（如 example-host ）的域名的数组。

静态 IP 地址分配配置示例

```
{
  "ipam": {
    "type": "static",
    "addresses": [
      {
        "address": "191.168.1.7/24"
      }
    ]
  }
}
```

12.5.1.1.2. 动态 IP 地址(DHCP)分配配置

以下 JSON 描述了使用 DHCP 进行动态 IP 地址地址分配的配置：

DHCP 租期续订

pod 在创建时获取其原始 DHCP 租期。该租期必须由集群中运行的一个小型的 DHCP 服务器部署定期续订。

SR-IOV Network Operator 不创建 DHCP 服务器部署。Cluster Network Operator 负责创建小型的 DHCP 服务器部署。

要触发 DHCP 服务器的部署，您必须编辑 Cluster Network Operator 配置来创建 shim 网络附加，如下例所示：

shim 网络附加定义示例

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  additionalNetworks:
  - name: dhcp-shim
    namespace: default
    type: Raw
    rawCNIConfig: |-
      {
        "name": "dhcp-shim",
        "cniVersion": "0.3.1",
        "type": "bridge",
        "ipam": {
          "type": "dhcp"
        }
      }
# ...
```

表 12.6. ipam DHCP 配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值 dhcp 是必需的。

动态 IP 地址(DHCP)分配配置示例

```
{
  "ipam": {
    "type": "dhcp"
  }
}
```

12.5.1.1.3. 使用 Whereabouts 进行动态 IP 地址分配配置

Whereabouts CNI 插件允许在不使用 DHCP 服务器的情况下动态地将 IP 地址分配给额外网络。

下表描述了使用 Whereabouts 进行动态 IP 地址分配的配置：

表 12.7. ipam 观察配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值是 必填 的。
范围	字符串	CIDR 表示法中的 IP 地址和范围。IP 地址是通过这个地址范围来分配的。
exclude	数组	可选：CIDR 表示法中存在零或多个 IP 地址和范围的列表。包含在排除地址范围中的 IP 地址。

使用 Whereabouts 的动态 IP 地址分配配置示例

```
{
  "ipam": {
    "type": "whereabouts",
    "range": "192.0.2.192/27",
    "exclude": [
      "192.0.2.192/30",
      "192.0.2.196/32"
    ]
  }
}
```

12.5.2. 配置 SR-IOV 额外网络

您可以通过创建一个 **SriovNetwork** 对象来配置使用 SR-IOV 硬件的额外网络。创建 **SriovNetwork** 对象时，SR-IOV Operator 会自动创建一个 **NetworkAttachmentDefinition** 对象。



注意

如果一个 **SriovNetwork** 对象已被附加到状态为 **running** 的 pod，则不要修改或删除它。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 创建一个 **SriovNetwork** 对象，然后在 **<name>.yaml** 文件中保存 YAML，其中 **<name>** 是这个额外网络的名称。对象规格可能类似以下示例：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetwork
metadata:
  name: attach1
  namespace: openshift-sriov-network-operator
spec:
  resourceName: net1
```



```
networkNamespace: project2
ipam: |-
  {
    "type": "host-local",
    "subnet": "10.56.217.0/24",
    "rangeStart": "10.56.217.171",
    "rangeEnd": "10.56.217.181",
    "gateway": "10.56.217.1"
  }
```

2. 运行以下命令来创建对象：

```
$ oc create -f <name>.yaml
```

这里的 **<name>** 指定额外网络的名称。

3. 可选：要确认与您在上一步中创建的 **SriovNetwork** 对象关联的 **NetworkAttachmentDefinition** 对象是否存在，请输入以下命令。将 **<namespace>** 替换为您在 **SriovNetwork** 对象中指定的 **networkNamespace**。

```
$ oc get net-attach-def -n <namespace>
```

12.5.3. 后续步骤

- [将 pod 添加到额外网络](#)

12.5.4. 其他资源

- [配置 SR-IOV 网络设备](#)

12.6. 配置 SR-IOV INFINIBAND 网络附加

您可以为集群中的单根 I/O 虚拟化（SR-IOV）设备配置 InfiniBand（IB）网络附加。

12.6.1. Infiniband 设备配置对象

您可以通过定义 **SriovIBNetwork** 对象来配置 InfiniBand（IB）网络设备。

以下 YAML 描述了 **SriovIBNetwork** 对象：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovIBNetwork
metadata:
  name: <name> ①
  namespace: openshift-sriov-network-operator ②
spec:
  resourceName: <sriov_resource_name> ③
  networkNamespace: <target_namespace> ④
  ipam: |- ⑤
    {}
  linkState: <link_state> ⑥
  capabilities: <capabilities> ⑦
```

- 1 对象的名称。SR-IOV Network Operator 创建一个名称相同的 **NetworkAttachmentDefinition** 对象。
- 2 安装 SR-IOV Operator 的命名空间。
- 3 用于为这个额外网络定义 SR-IOV 硬件的 **SriovNetworkNodePolicy** 对象中的 **spec.resourceName** 参数的值。
- 4 **SriovIBNetwork** 对象的目标命名空间。只有目标命名空间中的 pod 可以附加到网络设备。
- 5 可选：将 IPAM CNI 插件配置为 YAML 块 scalar。该插件管理网络附加定义的 IP 地址分配。
- 6 可选：虚拟功能（VF）的连接状态。允许的值是 **enable**、**disable** 和 **auto**。
- 7 可选：为此网络配置功能。您可以指定 **"{ "ips": true }"** 来启用 IP 地址支持，或者 **"{ "infinibandGUID": true }"** 启用 IB Global Unique Identifier（GUID）支持。

12.6.1.1. 为额外网络配置 IP 地址分配

IP 地址管理(IPAM)Container Network Interface(CNI)插件为其他 CNI 插件提供 IP 地址。

您可以使用以下 IP 地址分配类型：

- 静态分配。
- 通过 DHCP 服务器进行动态分配。您指定的 DHCP 服务器必须可从额外网络访问。
- 通过 Whereabouts IPAM CNI 插件进行动态分配。

12.6.1.1.1. 静态 IP 地址分配配置

下表描述了静态 IP 地址分配的配置：

表 12.8. ipam 静态配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值是 静态 的。
地址	数组	指定分配给虚拟接口的 IP 地址的对象数组。支持 IPv4 和 IPv6 IP 地址。
Routes	数组	指定要在 pod 中配置的路由的对象数组。
dns	数组	可选：指定 DNS 配置的对象数组。

address 数组需要带有以下字段的对象：

表 12.9. ipam.addresses[] array

字段	类型	描述
地址	字符串	您指定的 IP 地址和网络前缀。例如：如果您指定 10.10.21.10/24 ，那么会为额外网络分配 IP 地址 10.10.21.10 ，网掩码为 255.255.255.0 。
gateway	字符串	出口网络流量要路由到的默认网关。

表 12.10. ipam.routes[] 数组

字段	类型	描述
dst	字符串	CIDR 格式的 IP 地址范围，如 192.168.17.0/24 或 0.0.0.0/0 （默认路由）。
gw	字符串	网络流量路由的网关。

表 12.11. ipam.dns 对象

字段	类型	描述
名称服务器	数组	用来发送 DNS 查询的一个或多个 IP 地址的数组。
domain	数组	要附加到主机名的默认域。例如，如果将域设置为 example.com ，对 example-host 的 DNS 查找查询将被改写为 example-host.example.com 。
search	数组	在 DNS 查找查询过程中，附加到非限定主机名（如 example-host ）的域名的数组。

静态 IP 地址分配配置示例

```
{
  "ipam": {
    "type": "static",
    "addresses": [
      {
        "address": "191.168.1.7/24"
      }
    ]
  }
}
```

12.6.1.1.2. 动态 IP 地址(DHCP)分配配置

以下 JSON 描述了使用 DHCP 进行动态 IP 地址地址分配的配置：

DHCP 租期续订

pod 在创建时获取其原始 DHCP 租期。该租期必须由集群中运行的一个小型的 DHCP 服务器部署定期续订。

要触发 DHCP 服务器的部署，您必须编辑 Cluster Network Operator 配置来创建 shim 网络附加，如下例所示：

shim 网络附加定义示例

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  additionalNetworks:
  - name: dhcp-shim
    namespace: default
    type: Raw
    rawCNIConfig: |-
      {
        "name": "dhcp-shim",
        "cniVersion": "0.3.1",
        "type": "bridge",
        "ipam": {
          "type": "dhcp"
        }
      }
# ...
```

表 12.12. ipam DHCP 配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值 dhcp 是必需的。

动态 IP 地址(DHCP)分配配置示例

```
{
  "ipam": {
    "type": "dhcp"
  }
}
```

12.6.1.1.3. 使用 Whereabouts 进行动态 IP 地址分配配置

Whereabouts CNI 插件允许在不使用 DHCP 服务器的情况下动态地将 IP 地址分配给额外网络。

下表描述了使用 Whereabouts 进行动态 IP 地址分配的配置：

表 12.13. ipam 观察配置对象

字段	类型	描述
type	字符串	IPAM 地址类型。值是 必填 的。
范围	字符串	CIDR 表示法中的 IP 地址和范围。IP 地址是通过这个地址范围来分配的。
exclude	数组	可选：CIDR 表示法中存在零或多个 IP 地址和范围的列表。包含在排除地址范围中的 IP 地址。

使用 Whereabouts 的动态 IP 地址分配配置示例

```
{
  "ipam": {
    "type": "whereabouts",
    "range": "192.0.2.192/27",
    "exclude": [
      "192.0.2.192/30",
      "192.0.2.196/32"
    ]
  }
}
```

12.6.2. 配置 SR-IOV 额外网络

您可以通过创建一个 **SriovIBNetwork** 对象来配置使用 SR-IOV 硬件的额外网络。创建 **SriovIBNetwork** 对象时，SR-IOV Operator 会自动创建一个 **NetworkAttachmentDefinition** 对象。



注意

如果一个 **SriovIBNetwork** 对象已被附加到状态为 **running** 的 pod，则不要修改或删除它。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 创建一个 **SriovIBNetwork** 对象，然后在 **<name>.yaml** 文件中保存 YAML，其中 **<name>** 是这个额外网络的名称。对象规格可能类似以下示例：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovIBNetwork
metadata:
  name: attach1
  namespace: openshift-sriov-network-operator
spec:
  resourceName: net1
  networkNamespace: project2
```

```
ipam: |-
  {
    "type": "host-local",
    "subnet": "10.56.217.0/24",
    "rangeStart": "10.56.217.171",
    "rangeEnd": "10.56.217.181",
    "gateway": "10.56.217.1"
  }
```

2. 运行以下命令来创建对象：

```
$ oc create -f <name>.yaml
```

这里的 **<name>** 指定额外网络的名称。

3. 可选：要确认与您在上一步中创建的 **SriovNetwork** 对象关联的 **NetworkAttachmentDefinition** 对象是否存在，请输入以下命令。将 **<namespace>** 替换为您在 **SriovNetwork** 对象中指定的 `networkNamespace`。

```
$ oc get net-attach-def -n <namespace>
```

12.6.3. 后续步骤

- [将 pod 添加到额外网络](#)

12.6.4. 其他资源

- [配置 SR-IOV 网络设备](#)

12.7. 将 POD 添加到额外网络

您可以将 pod 添加到现有的单根 I/O 虚拟化（SR-IOV）网络。

12.7.1. 网络附加的运行时配置

将 pod 附加到额外网络时，您可以指定运行时配置来为 pod 进行特定的自定义。例如，您可以请求特定的 MAC 硬件地址。

您可以通过在 pod 规格中设置注解来指定运行时配置。注解键是 **k8s.v1.cni.cncf.io/network**，它接受一个 JSON 对象来描述运行时配置。

12.7.1.1. 基于以太网的 SR-IOV 附加的运行时配置

以下 JSON 描述了基于以太网的 SR-IOV 网络附加的运行时配置选项。

```
[
  {
    "name": "<name>", ①
    "mac": "<mac_address>", ②
    "ips": ["<cidr_range>"] ③
  }
]
```

- ❶ SR-IOV 网络附加定义 CR 的名称。
- ❷ 可选：从 SR-IOV 网络附加定义 CR 中定义的资源类型分配的 SR-IOV 设备的 MAC 地址。要使用这个功能，还必须在 **SriovNetwork** 对象中指定 { "mac": true }。
- ❸ 可选：从 SR-IOV 网络附加定义 CR 中定义的资源类型分配的 SR-IOV 设备的 IP 地址。支持 IPv4 和 IPv6 IP 地址。要使用这个功能，还必须在 **SriovNetwork** 对象中指定 { "ips": true }。

运行时配置示例

```
apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
  annotations:
    k8s.v1.cni.cncf.io/networks: |-
      [
        {
          "name": "net1",
          "mac": "20:04:0f:f1:88:01",
          "ips": ["192.168.10.1/24", "2001::1/64"]
        }
      ]
spec:
  containers:
  - name: sample-container
    image: <image>
    imagePullPolicy: IfNotPresent
    command: ["sleep", "infinity"]
```

12.7.1.2. 基于 InfiniBand 的 SR-IOV 附加的运行时配置

以下 JSON 描述了基于 InfiniBand 的 SR-IOV 网络附加的运行时配置选项。

```
[
  {
    "name": "<network_attachment>", ❶
    "infiniband-guid": "<guid>", ❷
    "ips": ["<cidr_range>"] ❸
  }
]
```

- ❶ SR-IOV 网络附加定义 CR 的名称。
- ❷ SR-IOV 设备的 InfiniBand GUID。要使用这个功能，还必须在 **SriovIBNetwork** 对象中指定 { "infinibandGUID": true }。
- ❸ 从 SR-IOV 网络附加定义 CR 中定义的资源类型分配的 SR-IOV 设备的 IP 地址。支持 IPv4 和 IPv6 IP 地址。要使用这个功能,你还必须在 **SriovIBNetwork** 对象中指定 { "ips": true }。

运行时配置示例

```

apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
  annotations:
    k8s.v1.cni.cncf.io/networks: |-
      [
        {
          "name": "ib1",
          "infiniband-guid": "c2:11:22:33:44:55:66:77",
          "ips": ["192.168.10.1/24", "2001::1/64"]
        }
      ]
spec:
  containers:
  - name: sample-container
    image: <image>
    imagePullPolicy: IfNotPresent
    command: ["sleep", "infinity"]

```

12.7.2. 将 pod 添加到额外网络

您可以将 pod 添加到额外网络。pod 继续通过默认网络发送与集群相关的普通网络流量。

创建 pod 时会附加额外网络。但是，如果 pod 已存在，您无法为其附加额外网络。

pod 必须与额外网络处于相同的命名空间。



注意

SR-IOV 网络资源注入器会自动将 **resource** 字段添加到 pod 中的第一个容器中。

如果您在 Data Plane Development Kit (DPDK) 模式中使用 Intel 网络接口控制器 (NIC)，则只有 pod 中的第一个容器被配置为访问 NIC。如果在 **SriovNetworkNodePolicy** 对象中的 **deviceType** 设置为 **vfio-pci**，则会为 DPDK 模式配置 SR-IOV 额外网络。

您可以解决此问题，方法是确保需要访问 NIC 的容器是 **Pod** 对象中定义的第一个容器，或者禁用 Network Resource Injector。如需更多信息，请参阅 [BZ# 953](#)。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 登录到集群。
- 安装 SR-IOV Operator。
- 创建 **SriovNetwork** 对象或 **SriovIBNetwork** 对象以将 pod 附加到。

流程

1. 为 **Pod** 对象添加注解。只能使用以下注解格式之一：
 - a. 要在没有自定义的情况下附加额外网络，请使用以下格式添加注解。将 **<network>** 替换为要与 pod 关联的额外网络的名称：


```

metadata:
  annotations:
    k8s.v1.cni.cncf.io/networks: <network>[,<network>,...] ❶

```

- ❶ 要指定多个额外网络，请使用逗号分隔各个网络。逗号之间不可包括空格。如果您多次指定同一额外网络，则该 pod 会将多个网络接口附加到该网络。

b. 要通过自定义来附加额外网络，请添加具有以下格式的注解：

```

metadata:
  annotations:
    k8s.v1.cni.cncf.io/networks: |-
      [
        {
          "name": "<network>", ❶
          "namespace": "<namespace>", ❷
          "default-route": ["<default-route>"] ❸
        }
      ]

```

- ❶ 指定 **NetworkAttachmentDefinition** 对象定义的额外网络的名称。
- ❷ 指定定义 **NetworkAttachmentDefinition** 对象的命名空间。
- ❸ 可选：为默认路由指定覆盖，如 **192.168.17.1**。

2. 运行以下命令来创建 pod。将 **<name>** 替换为 pod 的名称。

```
$ oc create -f <name>.yaml
```

3. 可选：要确认 **Pod** CR 中是否存在注解，请输入以下命令将 **<name>** 替换为 pod 的名称。

```
$ oc get pod <name> -o yaml
```

在以下示例中，**example-pod** pod 附加到 **net1** 额外网络：

```

$ oc get pod example-pod -o yaml
apiVersion: v1
kind: Pod
metadata:
  annotations:
    k8s.v1.cni.cncf.io/networks: macvlan-bridge
    k8s.v1.cni.cncf.io/networks-status: |- ❶
      [{
        "name": "openshift-sdn",
        "interface": "eth0",
        "ips": [
          "10.128.2.14"
        ],
        "default": true,
        "dns": {}
      }],{

```

```

      "name": "macvlan-bridge",
      "interface": "net1",
      "ips": [
        "20.2.2.100"
      ],
      "mac": "22:2f:60:a5:f8:00",
      "dns": {}
    }]
  name: example-pod
  namespace: default
spec:
  ...
status:
  ...

```

- 1** `k8s.v1.cni.cncf.io/networks-status` 参数是对象的 JSON 数组。每个对象描述附加到 pod 的额外网络的状态。注解值保存为纯文本值。

12.7.3. 创建与 SR-IOV pod 兼容的非统一内存访问 (NUMA)

您可以通过限制 SR-IOV 和从相同 NUMA 节点分配的 CPU 资源，使用 **restricted** 或 **single-numa-node** Topology Manager 来创建与 SR-IOV pod 兼容的 NUMA。

先决条件

- 已安装 OpenShift CLI (**oc**)。
- 您已将 CPU Manager 策略配置为 **static**。有关 CPU Manager 的详情请参考 "Additional resources" 部分。
- 您已将 Topology Manager 策略配置为 **single-numa-node**。



注意

当 **single-numa-node** 无法满足请求时，您可以将拓扑管理器策略配置为 **restricted**。

流程

1. 创建以下 SR-IOV pod 规格，然后在 `<name>-sriov-pod.yaml` 文件中保存 YAML。将 `<name>` 替换为这个 pod 的名称。

以下示例显示了 SR-IOV pod 规格：

```

apiVersion: v1
kind: Pod
metadata:
  name: sample-pod
  annotations:
    k8s.v1.cni.cncf.io/networks: <name> 1
spec:
  containers:
  - name: sample-container
    image: <image> 2

```

```

command: ["sleep", "infinity"]
resources:
  limits:
    memory: "1Gi" ③
    cpu: "2" ④
  requests:
    memory: "1Gi"
    cpu: "2"

```

- ① 将 **<name>** 替换为 SR-IOV 网络附加定义 CR 的名称。
- ② 将 **<image>** 替换为 **sample-pod** 镜像的名称。
- ③ 要创建带有保证 QoS 的 SR-IOV pod，将 **memory limits** 设置为与 **memory requests** 相同的值。
- ④ 要创建带有保证 QoS 的 SR-IOV pod，将 **cpu limits** 设置为与 **cpu requests** 相同。

2. 运行以下命令来创建 SR-IOV pod 示例：

```
$ oc create -f <filename> ①
```

- ① 将 **<filename>** 替换为您在上一步中创建的文件名称。

3. 确认 **sample-pod** 配置为带有保证 QoS。

```
$ oc describe pod sample-pod
```

4. 确认 **sample-pod** 被分配了独有的 CPU。

```
$ oc exec sample-pod -- cat /sys/fs/cgroup/cpuset/cpuset.cpus
```

5. 确认为 **sample-pod** 分配的 SR-IOV 设备和 CPU 位于相同的 NUMA 节点上。

```
$ oc exec sample-pod -- cat /sys/fs/cgroup/cpuset/cpuset.cpus
```

12.7.4. 其他资源

- [配置 SR-IOV 以太网网络附加](#)
- [配置 SR-IOV InfiniBand 网络附加](#)
- [使用 CPU Manager](#)

12.8. 配置高性能多播

您可以在您的单根 I/O 虚拟化（SR-IOV）硬件网络中使用多播。

12.8.1. 高性能多播

OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商支持默认网络上的 pod 间的多播。

目前，多播最适用于低带宽协调或服务发现。它不适用于高带宽的应用程序。对于流传输介质应用程序，如 IPTV 和多方视频会议，可以使用 Single Root I/O Virtualization (SR-IOV) 硬件来提供接近原生的性能。

使用额外的 SR-IOV 接口进行多播时：

- pod 必须通过额外的 SR-IOV 接口发送或接收多播软件包。
- 连接 SR-IOV 接口的物理网络决定了多播路由和拓扑结构，不受 OpenShift Container Platform 的控制。

12.8.2. 为多播配置 SR-IOV 接口

以下步骤为多播创建一个 SR-IOV 接口示例。

先决条件

- 安装 OpenShift CLI (**oc**) 。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

1. 创建一个 **SriovNetworkNodePolicy** 对象：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: policy-example
  namespace: openshift-sriov-network-operator
spec:
  resourceName: example
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true"
  numVfs: 4
  nicSelector:
    vendor: "8086"
    pfNames: ["ens803f0"]
    rootDevices: ["0000:86:00.0"]
```

2. 创建一个 **SriovNetwork** 对象：

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetwork
metadata:
  name: net-example
  namespace: openshift-sriov-network-operator
spec:
  networkNamespace: default
  ipam: | 1
    {
      "type": "host-local", 2
      "subnet": "10.56.217.0/24",
      "rangeStart": "10.56.217.171",
      "rangeEnd": "10.56.217.181",
```

```

"routes": [
  {"dst": "224.0.0.0/5"},
  {"dst": "232.0.0.0/5"}
],
"gateway": "10.56.217.1"
}
resourceName: example

```

- 1 2** 如果选择将 DHCP 配置为 IPAM，请确保通过 DHCP 服务器提供了以下默认路由：**224.0.0.0/5** 和 **232.0.0.0/5**。这会覆盖由默认网络供应商设置的静态多播路由。

3. 创建带有多播应用程序的 pod:

```

apiVersion: v1
kind: Pod
metadata:
  name: testpmd
  namespace: default
  annotations:
    k8s.v1.cni.cncf.io/networks: nic1
spec:
  containers:
  - name: example
    image: rhel7:latest
    securityContext:
      capabilities:
        add: ["NET_ADMIN"] 1
    command: ["sleep", "infinity"]

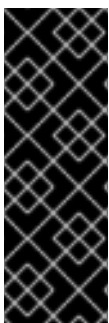
```

- 1** 只有在应用程序需要为 SR-IOV 接口分配多播 IP 地址时，才需要 **NET_ADMIN** 功能。否则，可以省略它。

12.9. 在 DPDK 和 RDMA 模式中使用虚拟功能（VF）的示例

您可以使用单一根 I/O 虚拟化（SR-IOV）网络硬件和 Data Plane Development Kit (DPDK) 以及远程直接内存访问 (RDMA)。

12.9.1. 在 DPDK 和 RDMA 模式中使用虚拟功能（VF）的示例



重要

Data Plane Development Kit (DPDK) 只是一个技术预览功能。技术预览功能不被红帽产品服务等级协议 (SLA) 支持，且可能在功能方面有缺陷。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的详情，请参阅 <https://access.redhat.com/support/offerings/techpreview/>。



重要

远程直接内存访问 (RDMA) 只是一个技术预览功能。技术预览功能不被红帽产品服务等级协议 (SLA) 支持，且可能在功能方面有缺陷。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的详情，请参阅 <https://access.redhat.com/support/offerings/techpreview/>。

12.9.2. 先决条件

- 安装 OpenShift CLI (**oc**) 。
- 以具有 **cluster-admin** 特权的用户身份登录。
- 您必须已安装了 SR-IOV Network Operator。

12.9.3. 在 Intel NIC 的 DPDK 模式中使用虚拟功能 (VF) 示例

流程

1. 创建以下 **SriovNetworkNodePolicy** 对象，然后在 **intel-dpdk-node-policy.yaml** 文件中保存 YAML。

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: intel-dpdk-node-policy
  namespace: openshift-sriov-network-operator
spec:
  resourceName: intelnic
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true"
  priority: <priority>
  numVfs: <num>
  nicSelector:
    vendor: "8086"
    deviceID: "158b"
    pfNames: ["<pf_name>", ...]
    rootDevices: ["<pci_bus_id>", "..."]
  deviceType: vfio-pci ❶
```

- ❶ 将虚拟功能 (VF) 的驱动器类型指定为 **vfio-pci**。



注意

请参阅 **Configuring SR-IOV network devices** 一节以了解 **SriovNetworkNodePolicy** 中的每个选项的信息。

当应用由 **SriovNetworkNodePolicy** 对象中指定的配置时，SR-IOV Operator 可能会排空节点，并在某些情况下会重启节点。它可能需要几分钟时间来应用配置更改。确保集群中有足够的可用节点，用以预先处理被驱除的工作负载。

应用配置更新后，**openshift-sriov-network-operator** 命名空间中的所有 pod 将变为 **Running** 状态。

- 运行以下命令来创建 **SriovNetworkNodePolicy** 对象：

```
$ oc create -f intel-dpdk-node-policy.yaml
```

- 创建以下 **SriovNetwork** 对象，然后在 **intel-dpdk-network.yaml** 文件中保存 YAML。

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetwork
metadata:
  name: intel-dpdk-network
  namespace: openshift-sriov-network-operator
spec:
  networkNamespace: <target_namespace>
  ipam: "{}" ①
  vlan: <vlan>
  resourceName: intelnic
```

- 为 ipam CNI 插件指定一个空对象 "{}"。DPDK 在用户空间模式下工作，不需要 IP 地址。



注意

如需 **SriovNetwork** 中的每个选项的详细说明，请参阅“Configuring SR-IOV additional network”部分。

- 运行以下命令来创建 **SriovNetwork** 对象：

```
$ oc create -f intel-dpdk-network.yaml
```

- 创建以下 **Pod** spec，然后在 **intel-dpdk-pod.yaml** 文件中保存 YAML。

```
apiVersion: v1
kind: Pod
metadata:
  name: dpdk-app
  namespace: <target_namespace> ①
  annotations:
    k8s.v1.cni.cncf.io/networks: intel-dpdk-network
spec:
  containers:
    - name: testpmd
      image: <DPDK_image> ②
```

```

securityContext:
  runAsUser: 0
  capabilities:
    add: ["IPC_LOCK","SYS_RESOURCE","NET_RAW"] ③
volumeMounts:
- mountPath: /dev/hugepages ④
  name: hugepage
resources:
  limits:
    openshift.io/intelnic: "1" ⑤
    memory: "1Gi"
    cpu: "4" ⑥
    hugepages-1Gi: "4Gi" ⑦
  requests:
    openshift.io/intelnic: "1"
    memory: "1Gi"
    cpu: "4"
    hugepages-1Gi: "4Gi"
  command: ["sleep", "infinity"]
volumes:
- name: hugepage
  emptyDir:
    medium: HugePages

```

- ① 指定 `target_namespace`，它与 `SriovNetwork` 对象 `intel-dpdk-network` 创建于的命令空间相同。如果要在其他命名空间中创建 pod，在 `Pod spec` 和 `SriovNetwork` 对象中更改 `target_namespace`。
- ② 指定包含应用程序和应用程序使用的 DPDK 库的 DPDK 镜像。
- ③ 指定容器内的应用程序进行大页分配、系统资源分配和网络接口访问所需的额外功能。
- ④ 在 `/dev/hugepages` 下将巨页卷挂载到 DPDK pod。巨页卷由 `emptyDir` 卷类型支持，`medium` 为 `Hugepages`。
- ⑤ 可选：指定分配给 DPDK pod 的 DPDK 设备数。如果未明确指定，则此资源请求和限制将被 SR-IOV 网络资源注入程序自动添加。SR-IOV 网络资源注入程序是由 SR-IOV Operator 管理的准入控制器组件。它默认是启用的，可以通过把默认的 `SriovOperatorConfig` CR 中的 `enableInjector` 选项设置为 `false` 来禁用它。
- ⑥ 指定 CPU 数量。DPDK pod 通常需要从 kubelet 分配专用 CPU。这可以通过将 CPU Manager 策略设置为 `static`，并创建带有有保障的 QoS 的 pod 来实现。
- ⑦ 指定巨页大小 `hugepages-1Gi` 或 `hugepages-2Mi` 以及分配给 DPDK pod 的巨页数量。单独配置 `2Mi` 和 `1Gi` 巨页。配置 `1Gi` 巨页需要在节点中添加内核参数。例如：添加内核参数 `default_hugepagesz=1GB`，`hugepagesz=1G` 和 `hugepages=16` 将在系统引导时分配 `16*1Gi` 巨页。

6. 运行以下命令来创建 DPDK pod:

```
$ oc create -f intel-dpdk-pod.yaml
```

12.9.4. 使用带有 Mellanox NIC 的 DPDK 模式的虚拟功能（VF）示例

流程

1. 创建以下 **SriovNetworkNodePolicy** 对象，然后在 **mlx-dpdk-node-policy.yaml** 文件中保存 YAML。

```

apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: mlx-dpdk-node-policy
  namespace: openshift-sriov-network-operator
spec:
  resourceName: mlxnic
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true"
  priority: <priority>
  numVfs: <num>
  nicSelector:
    vendor: "15b3"
    deviceID: "1015" ❶
    pfNames: ["<pf_name>", ...]
    rootDevices: ["<pci_bus_id>", "..."]
  deviceType: netdevice ❷
  isRdma: true ❸

```

- ❶ 指定 SR-IOV 网络设备的设备十六进制代码。Mellanox 卡允许的值是 **1015**，**1017**。
- ❷ 指定到 **netdevice** 的虚拟功能（VF）的驱动器类型。Mellanox SR-IOV VF 可以在 DPDK 模式下工作，而无需使用 **vfio-pci** 设备类型。VF 设备作为容器内的内核网络接口出现。
- ❸ 启用 RDMA 模式。Mellanox 卡需要在 DPDK 模式下工作。



注意

请参阅 **Configuring SR-IOV network devices** 一节以了解 **SriovNetworkNodePolicy** 中的每个选项的信息。

当应用由 **SriovNetworkNodePolicy** 对象中指定的配置时，SR-IOV Operator 可能会排空节点，并在某些情况下会重启节点。它可能需要几分钟时间来应用配置更改。确保集群中有足够的可用节点，用以预先处理被驱除的工作负载。

应用配置更新后，**openshift-sriov-network-operator** 命名空间中的所有 pod 将变为 **Running** 状态。

2. 运行以下命令来创建 **SriovNetworkNodePolicy** 对象：

```
$ oc create -f mlx-dpdk-node-policy.yaml
```

3. 创建以下 **SriovNetwork** 对象，然后在 **mlx-dpdk-network.yaml** 文件中保存 YAML。

```

apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetwork
metadata:
  name: mlx-dpdk-network
  namespace: openshift-sriov-network-operator

```

```
spec:
  networkNamespace: <target_namespace>
  ipam: |- ❶
    ...
  vlan: <vlan>
  resourceName: mlxnic
```

- ❶ 为 ipam CNI 插件指定一个配置对象作为一个 YAML 块 scalar。该插件管理网络附加定义的 IP 地址分配。



注意

如需 **SriovNetwork** 中的每个选项的详细说明，请参阅“Configuring SR-IOV additional network”部分。

4. 运行以下命令来创建 **SriovNetworkNodePolicy** 对象：

```
$ oc create -f mlx-dpdk-network.yaml
```

5. 创建以下 **Pod** spec，然后在 **mlx-dpdk-pod.yaml** 文件中保存 YAML。

```
apiVersion: v1
kind: Pod
metadata:
  name: dpdk-app
  namespace: <target_namespace> ❶
  annotations:
    k8s.v1.cni.cncf.io/networks: mlx-dpdk-network
spec:
  containers:
  - name: testpmd
    image: <DPDK_image> ❷
    securityContext:
      runAsUser: 0
      capabilities:
        add: ["IPC_LOCK", "SYS_RESOURCE", "NET_RAW"] ❸
    volumeMounts:
  - mountPath: /dev/hugepages ❹
    name: hugepage
  resources:
    limits:
      openshift.io/mlxnics: "1" ❺
      memory: "1Gi"
      cpu: "4" ❻
      hugepages-1Gi: "4Gi" ❼
    requests:
      openshift.io/mlxnics: "1"
      memory: "1Gi"
      cpu: "4"
      hugepages-1Gi: "4Gi"
    command: ["sleep", "infinity"]
  volumes:
```

```
- name: hugepage
  emptyDir:
    medium: HugePages
```

- 1 指定 **target_namespace**，它与 **SriovNetwork** 对象 **mlx-dpdk-network** 创建于的命令空间相同。如果要在其他命名空间中创建 pod，在 **Pod spec** 和 **SriovNetwork** 对象中更改 **target_namespace**。
- 2 指定包含应用程序和应用程序使用的 DPDK 库的 DPDK 镜像。
- 3 指定容器内的应用程序进行大页分配、系统资源分配和网络接口访问所需的额外功能。
- 4 在 **/dev/hugepages** 下将巨页卷挂载到 DPDK pod。巨页卷由 **emptyDir** 卷类型支持，**medium** 为 **Hugepages**。
- 5 可选：指定分配给 DPDK pod 的 DPDK 设备数。如果未明确指定，则此资源请求和限制将被 SR-IOV 网络资源注入程序自动添加。SR-IOV 网络资源注入程序是由 SR-IOV Operator 管理的准入控制器组件。它默认是启用的，可以通过把默认的 **SriovOperatorConfig** CR 中的 **enableInjector** 选项设置为 **false** 来禁用它。
- 6 指定 CPU 数量。DPDK pod 通常需要从 kubelet 分配专用 CPU。这可以通过将 CPU Manager 策略设置为 **static**，并创建带有有保障的 QoS 的 pod 来实现。
- 7 指定巨页大小 **hugepages-1Gi** 或 **hugepages-2Mi** 以及分配给 DPDK pod 的巨页数量。单独配置 **2Mi** 和 **1Gi** 巨页。配置 **1Gi** 巨页需要在节点中添加内核参数。

6. 运行以下命令来创建 DPDK pod:

```
$ oc create -f mlx-dpdk-pod.yaml
```

12.9.5. 带有 Mellanox NIC 的 RDMA 模式中的虚拟功能（VF）示例

在 OpenShift Container Platform 上使用 RDMA 时，RDMA over Converged Ethernet (RoCE) 是唯一支持的模式。

流程

1. 创建以下 **SriovNetworkNodePolicy** 对象，然后在 **mlx-rdma-node-policy.yaml** 文件中保存 YAML。

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: mlx-rdma-node-policy
  namespace: openshift-sriov-network-operator
spec:
  resourceName: mlxnic
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable: "true"
  priority: <priority>
  numVfs: <num>
  nicSelector:
    vendor: "15b3"
    deviceId: "1015" 1
```

```

pfNames: ["<pf_name>", ...]
rootDevices: ["<pci_bus_id>", "..."]
deviceType: netdevice ❷
isRdma: true ❸

```

- ❶ 指定 SR-IOV 网络设备的设备十六进制代码。Mellanox 卡允许的值是 **1015**, **1017**。
- ❷ 指定到 **netdevice** 的虚拟功能 (VF) 的驱动器类型。
- ❸ 启用 RDMA 模式。



注意

请参阅 **Configuring SR-IOV network devices** 一节以了解 **SriovNetworkNodePolicy** 中的每个选项的信息。

当应用由 **SriovNetworkNodePolicy** 对象中指定的配置时，SR-IOV Operator 可能会排空节点，并在某些情况下会重启节点。它可能需要几分钟时间来应用配置更改。确保集群中有足够的可用节点，用以预先处理被驱除的工作负载。

应用配置更新后，**openshift-sriov-network-operator** 命名空间中的所有 pod 将变为 **Running** 状态。

2. 运行以下命令来创建 **SriovNetworkNodePolicy** 对象：

```
$ oc create -f mlx-rdma-node-policy.yaml
```

3. 创建以下 **SriovNetwork** 对象，然后在 **mlx-rdma-network.yaml** 文件中保存 YAML。

```

apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetwork
metadata:
  name: mlx-rdma-network
  namespace: openshift-sriov-network-operator
spec:
  networkNamespace: <target_namespace>
  ipam: |- ❶
    ...
  vlan: <vlan>
  resourceName: mlxnic

```

- ❶ 为 ipam CNI 插件指定一个配置对象作为一个 YAML 块 scalar。该插件管理网络附加定义的 IP 地址分配。



注意

如需 **SriovNetwork** 中的每个选项的详细说明，请参阅“Configuring SR-IOV additional network”部分。

4. 运行以下命令来创建 **SriovNetworkNodePolicy** 对象：

```
$ oc create -f mlx-rdma-network.yaml
```

5. 创建以下 **Pod spec**，然后在 **mlx-rdma-pod.yaml** 文件中保存 YAML。

```

apiVersion: v1
kind: Pod
metadata:
  name: rdma-app
  namespace: <target_namespace> ❶
  annotations:
    k8s.v1.cni.cncf.io/networks: mlx-rdma-network
spec:
  containers:
  - name: testpmd
    image: <RDMA_image> ❷
    securityContext:
      runAsUser: 0
      capabilities:
        add: ["IPC_LOCK","SYS_RESOURCE","NET_RAW"] ❸
    volumeMounts:
    - mountPath: /dev/hugepages ❹
      name: hugepage
  resources:
    limits:
      memory: "1Gi"
      cpu: "4" ❺
      hugepages-1Gi: "4Gi" ❻
    requests:
      memory: "1Gi"
      cpu: "4"
      hugepages-1Gi: "4Gi"
    command: ["sleep", "infinity"]
  volumes:
  - name: hugepage
    emptyDir:
      medium: HugePages

```

- ❶ 指定 **target_namespace**，它与 **SriovNetwork** 对象 **mlx-rdma-network** 创建于的命令空间相同。如果要在其他命名空间中创建 pod，在 **Pod spec** 和 **SriovNetwork** 对象中更改 **target_namespace**。
- ❷ 指定包含应用程序和应用程序使用的 RDMA 库的 RDMA 镜像。
- ❸ 指定容器内的应用程序进行大页分配、系统资源分配和网络接口访问所需的额外功能。
- ❹ 在 **/dev/hugepages** 下将巨页卷挂载到 RDMA pod。巨页卷由 **emptyDir** 卷类型支持，**medium** 为 **Hugepages**。
- ❺ 指定 CPU 数量。RDMA pod 通常需要从 kubelet 分配专用 CPU。这可以通过将 CPU Manager 策略设置为 **static**，并创建带有有保障的 QoS 的 pod 来实现。
- ❻ 指定巨页大小 **hugepages-1Gi** 或 **hugepages-2Mi** 以及分配给 RDMA pod 的巨页数量。单独配置 **2Mi** 和 **1Gi** 巨页。配置 **1Gi** 巨页需要在节点中添加内核参数。

6. 运行以下命令来创建 RDMA pod:

```
$ oc create -f mlx-rdma-pod.yaml
```

12.10. 卸载 SR-IOV NETWORK OPERATOR

要卸载 SR-IOV Network Operator，您必须删除任何正在运行的 SR-IOV 工作负载，卸载 Operator，并删除 Operator 使用的 webhook。

12.10.1. 卸载 SR-IOV Network Operator

作为集群管理员，您可以卸载 SR-IOV Network Operator。

先决条件

- 可以使用具有 **cluster-admin** 权限的账户访问 OpenShift Container Platform 集群。
- 已安装 SR-IOV Network Operator。

流程

1. 删除所有 SR-IOV 自定义资源(CR)：

```
$ oc delete sriovnetwork -n openshift-sriov-network-operator --all
```

```
$ oc delete sriovnetworknodepolicy -n openshift-sriov-network-operator --all
```

```
$ oc delete sriovibnetwork -n openshift-sriov-network-operator --all
```

2. 按照 "Deleting Operators from a cluster" 部分的内容进行操作，从集群中删除 SR-IOV Network Operator。
3. 删除在卸载 SR-IOV Network Operator 后保留的 SR-IOV 自定义资源定义：

```
$ oc delete crd sriovibnetworks.sriovnetwork.openshift.io
```

```
$ oc delete crd sriovnetworknodepolicies.sriovnetwork.openshift.io
```

```
$ oc delete crd sriovnetworknodestates.sriovnetwork.openshift.io
```

```
$ oc delete crd sriovnetworkpoolconfigs.sriovnetwork.openshift.io
```

```
$ oc delete crd sriovnetworks.sriovnetwork.openshift.io
```

```
$ oc delete crd sriovoperatorconfigs.sriovnetwork.openshift.io
```

4. 删除 SR-IOV Webhook：

```
$ oc delete mutatingwebhookconfigurations network-resources-injector-config
```

```
$ oc delete MutatingWebhookConfiguration sriov-operator-webhook-config
```

```
$ oc delete ValidatingWebhookConfiguration sriov-operator-webhook-config
```

5. 删除 SR-IOV Network Operator 命名空间：

```
$ oc delete namespace openshift-sriov-network-operator
```

其他资源

- [从集群中删除 Operator](#)

第 13 章 OPENSIFT SDN 默认 CNI 网络供应商

13.1. 关于 OPENSIFT SDN 默认 CNI 网络供应商

OpenShift Container Platform 使用软件定义网络 (SDN) 方法来提供一个统一的集群网络，它允许 OpenShift Container Platform 集群中的不同 pod 相互间进行通信。此 pod 网络是由 OpenShift SDN 建立和维护的，它使用 Open vSwitch (OVS) 配置覆盖网络。

13.1.1. OpenShift SDN 网络隔离模式

OpenShift SDN 提供三种 SDN 模式来配置 pod 网络：

- **网络策略模式**允许项目管理员使用 **NetworkPolicy** 对象配置自己的隔离策略。Network policy 是 OpenShift Container Platform 4.6 的默认模式。
- **多租户模式**为 Pod 和服务提供项目级别的隔离。来自不同项目的 Pod 不能与不同项目的 Pod 和服务互相发送或接收数据包。您可以针对项目禁用隔离，允许它将网络流量发送到整个集群中的所有 pod 和服务，并从那些 pod 和服务接收网络流量。
- **子网模式**提供一个扁平 pod 网络，每个 pod 都可以与所有其他 pod 和服务通信。网络策略模式提供与子网模式相同的功能。

13.1.2. 支持的默认 CNI 网络供应商功能列表

OpenShift Container Platform 为默认的 Container Network Interface (CNI) 网络供应商提供两个支持的选择：OpenShift SDN 和 OVN-Kubernetes。下表总结了这两个网络供应商当前支持的功能：

表 13.1. 默认 CNI 网络供应商功能比较

功能	OpenShift SDN	OVN-Kubernetes
出口 IP	支持	支持
Egress 防火墙 ^[1]	支持	支持
出口路由器	支持	不支持
Kubernetes 网络策略	部分支持 ^[2]	支持
多播	支持	支持

1. 在 OpenShift SDN 中，出口防火墙也称为出口网络策略。这和网络策略出口不同。
2. 不支持出口规则和一些 **ipBlock** 规则。

13.2. 为项目配置出口 IP

作为集群管理员，您可以配置 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商，为项目分配一个或多个出口 IP 地址。

13.2.1. 项目出口流量的出口 IP 地址分配

通过为项目配置出口 IP 地址，来自指定项目的所有出站外部连接将共享相同的固定源 IP 地址。外部资源可以根据出口 IP 地址识别来自特定项目的流量。分配给项目的出口 IP 地址与用来向特定目的地发送流量的出口路由器不同。

出口 IP 地址是作为额外 IP 地址在节点的主网络接口中实现的，且必须与节点的主 IP 地址处于同一个子网中。



重要

不能在任何 Linux 网络配置文件中配置出口 IP 地址，比如 `ifcfg-eth0`。

Amazon Web Services(AWS)、Google Cloud Platform(GCP)和 Azure 上的出口 IP 仅在 OpenShift Container Platform 版本 4.10 及更新的版本中支持。

在使用一些虚拟机解决方案时，在主网络接口上允许额外的 IP 地址可能需要额外的配置。

您可以通过设置 **NetNamespace** 对象的 **egressIPs** 参数,将出口 IP 地址分配给命名空间。在出口 IP 与项目关联后，OpenShift SDN 允许您以两种方式为主机分配出口 IP：

- 在 *自动分配* 方法中，给节点分配一个出口 IP 地址范围。
- 在 *手动分配* 方法中，给节点分配包含一个或多个出口 IP 地址的列表。

请求出口 IP 地址的命名空间与可以托管那些出口 IP 地址的节点匹配，然后为那些节点分配出口 IP 地址。如果在 **NetNamespace** 对象中设置了 **egressIPs** 参数，但没有节点托管该出口 IP 地址，则会丢弃来自该命名空间的出口流量。

节点高可用性是自动的。如果托管出口 IP 地址的节点不可访问，并且有可以托管那些出口 IP 地址的节点，那么出口 IP 地址将会移到新节点。当无法访问的托管原始出口 IP 地址的节点恢复正常后，出口 IP 地址会自动转移，以在不同节点之间均衡出口 IP 地址。



重要

将出口 IP 地址与 OpenShift SDN 集群网络供应商搭配使用时会有以下限制：

- 您不能在同一节点上同时使用手动分配和自动分配的出口 IP 地址。
- 如果手动从 IP 地址范围分配出口 IP 地址，则不得将该范围用于自动 IP 分配。
- 您不能使用 OpenShift SDN 出口 IP 地址在多个命名空间间共享出口 IP 地址。如果您需要在命名空间间共享 IP 地址，则 OVN-Kubernetes 集群网络供应商出口 IP 地址可以在多个命名空间中分散 IP 地址。



注意

如果您以多租户模式使用 OpenShift SDN，则无法将出口 IP 地址与与其关联的项目附加到另一个命名空间的任何命名空间一起使用。例如，如果 **project1** 和 **project2** 通过运行 **oc adm pod-network join-projects --to=project1 project2** 命令被连接，则这两个项目都不能使用出口 IP 地址。如需更多信息，请参阅 [BZ#1645577](#)。

13.2.1.1. 使用自动分配的出口 IP 地址时的注意事项

当对出口 IP 地址使用自动分配方法时，请注意以下事项：

- 您可以设置每个节点的 **HostSubnet** 资源的 **egressCIDRs** 参数，以指明节点可以托管的出口 IP 地址范围。OpenShift Container Platform 根据您指定的 IP 地址范围设置 **HostSubnet** 资源的 **egressIPs** 参数。
- 使用自动分配模式时，支持每个命名空间具有一个出口 IP 地址。

如果托管命名空间的出口 IP 地址的节点不可访问，OpenShift Container Platform 会将出口 IP 地址重新分配给具有兼容出口 IP 地址范围的另外一个节点。自动分配方法最适合在把额外的 IP 地址与节点进行关联时具有灵活性的环境中安装的集群。

13.2.1.2. 使用手动分配出口 IP 地址时的注意事项

此方法用于集群，在公共云环境中将其他 IP 地址与节点（如公共云环境中）关联可能存在限制。

当手动分配出口 IP 地址时，请考虑以下事项：

- 您可以设置每个节点的 **HostSubnet** 资源的 **egressIPs** 参数，以指明节点可以托管的 IP 地址。
- 支持一个命名空间带有多个出口 IP 地址。

当命名空间有多个出口 IP 地址时，如果托管第一个出口 IP 地址的节点不可访问，OpenShift Container Platform 将自动切换到使用下一个可用的出口 IP 地址，直到可以再次访问第一个出口 IP 地址。

13.2.2. 为一个命名空间启用自动分配出口 IP 地址

在 OpenShift Container Platform 中，可以为一个或多个节点上的特定命名空间启用自动分配出口 IP 地址。

先决条件

- 您可以使用具有 **cluster-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI (**oc**)。

流程

1. 使用以下 JSON，用出口 IP 地址更新 **NetNamespace** 资源：

```
$ oc patch netnamespace <project_name> --type=merge -p \ 1
{
  "egressIPs": [
    "<ip_address>" 2
  ]
}
```

- 1** 指定项目的名称。
- 2** 指定单个出口 IP 地址。不支持使用多 IP 地址。

例如，将 **project1** 分配给 IP 地址 192.168.1.100，将 **project2** 分配给 IP 地址 192.168.1.101：

```
$ oc patch netnamespace project1 --type=merge -p \
  '{"egressIPs": ["192.168.1.100"]}'
$ oc patch netnamespace project2 --type=merge -p \
```

```
'{"egressIPs": ["192.168.1.101"]}'
```



注意

由于 OpenShift SDN 管理 **NetNamespace** 对象，因此只能通过修改现有的 **NetNamespace** 对象来进行更改。不要创建新的 **NetNamespace** 对象。

2. 使用以下 JSON 设置每一主机的 **egressCIDRs** 参数，以指明哪些节点可以托管出口 IP 地址：

```
$ oc patch hostsubnet <node_name> --type=merge -p \ 1
{
  "egressCIDRs": [
    "<ip_address_range_1>", "<ip_address_range_2>" 2
  ]
}
```

- 1** 指定节点名称。
- 2** 以 CIDR 格式指定一个或多个 IP 地址范围。

例如，将 **node1** 和 **node2** 设置为托管范围为 192.168.1.0 到 192.168.1.255 的出口 IP 地址：

```
$ oc patch hostsubnet node1 --type=merge -p \
  '{"egressCIDRs": ["192.168.1.0/24"]}'
$ oc patch hostsubnet node2 --type=merge -p \
  '{"egressCIDRs": ["192.168.1.0/24"]}'
```

OpenShift Container Platform 会自动以均衡的方式将特定的出口 IP 地址分配给可用的节点。在本例中，它会将出口 IP 地址 192.168.1.100 分配给 **node1**，并将出口 IP 地址 192.168.1.101 分配给 **node2**，或反之。

13.2.3. 为一个命名空间配置手动分配出口 IP 地址

在 OpenShift Container Platform 中，您可以将一个或多个出口 IP 与一个项目关联。

先决条件

- 您可以使用具有 **cluster-admin** 角色的用户访问集群。
- 已安装 OpenShift CLI (**oc**)。

流程

1. 通过使用所需 IP 地址指定以下 JSON 对象来更新 **NetNamespace** 对象：

```
$ oc patch netnamespace <project> --type=merge -p \ 1
{
  "egressIPs": [ 2
    "<ip_address>"
  ]
}
```

- 1 指定项目的名称。
- 2 指定一个或多个出口 IP 地址。**egressIPs** 参数是一个数组。

例如，将 **project1** 项目分配给 IP 地址 **192.168.1.100**：

```
$ oc patch netnamespace project1 --type=merge \
-p '{"egressIPs": ["192.168.1.100"]}'
```

您可以将 **egressIPs** 设置为位于不同节点上的两个或多个 IP 地址，以提高可用性。如果设置了多个出口 IP 地址，Pod 会将列表中的第一个 IP 用于出口，但如果托管该 IP 地址的节点失败，Pod 会在短暂的延迟后切换到使用列表中的下一个 IP。



注意

由于 OpenShift SDN 管理 **NetNamespace** 对象，因此只能通过修改现有的 **NetNamespace** 对象来进行更改。不要创建新的 **NetNamespace** 对象。

2. 手动将出口 IP 分配给节点主机。在节点主机上的 **HostSubnet** 对象中设置 **egressIPs** 参数。使用以下 JSON，尽可能纳入您要分配给该节点主机的所有 IP：

```
$ oc patch hostsubnet <node_name> --type=merge -p \ 1
{
  "egressIPs": [ 2
    "<ip_address_1>",
    "<ip_address_N>"
  ]
}
```

- 1 指定节点的名称。
- 2 指定一个或多个出口 IP 地址。**egressIPs** 字段是一个数组。

例如，指定 **node1** 应具有出口 IP **192.168.1.100**、**192.168.1.101** 和 **192.168.1.102**：

```
$ oc patch hostsubnet node1 --type=merge -p \
 '{"egressIPs": ["192.168.1.100", "192.168.1.101", "192.168.1.102"]}'
```

在上例中，**project1** 的所有出口流量都会被路由到托管指定出口 IP 地址的节点，然后（使用 NAT）连接到那个 IP 地址。

13.3. 为项目配置出口防火墙

作为集群管理员，您可以为项目创建一个出口防火墙，用于限制离开 OpenShift Container Platform 集群的出口流量。

13.3.1. 出口防火墙在一个项目中的工作原理

作为集群管理员，您可以使用一个 **出口防火墙** 来限制集群内的一些 pod 或所有 pod 可以访问的外部主机。出口防火墙适用于以下情况：

- pod 只能连接到内部主机，且无法启动到公共互联网的连接。

- pod 只能连接到公共互联网，且无法启动到 OpenShift Container Platform 集群以外的内部主机的连接。
- pod 无法访问 OpenShift Container Platform 集群外的特定内部子网或主机。
- pod 只能连接到特定的外部主机。

例如，您可以允许某一个项目访问指定的 IP 范围，但拒绝其他项目对同一 IP 范围的访问。或者您可以限制应用程序开发人员从 Python pip 的镜像点进行更新，并强制要求更新只能来自于批准的源。

您可以通过创建一个 EgressNetworkPolicy 自定义资源（CR）对象来配置出口防火墙策略。出口防火墙与满足以下任一条件的网络流量匹配：

- CIDR 格式的 IP 地址范围
- 解析为 IP 地址的 DNS 名称

重要

如果您的出口防火墙包含 **0.0.0.0/0** 的拒绝规则，则阻止访问 OpenShift Container Platform API 服务器。为确保 pod 能够继续访问 OpenShift Container Platform API 服务器，您必须在出口防火墙规则中包含 API 服务器侦听的 IP 地址范围，如下例所示：

```
apiVersion: network.openshift.io/v1
kind: EgressNetworkPolicy
metadata:
  name: default
  namespace: <namespace> ❶
spec:
  egress:
    - to:
      cidrSelector: <api_server_address_range> ❷
      type: Allow
  # ...
  - to:
    cidrSelector: 0.0.0.0/0 ❸
    type: Deny
```

- ❶ 出口防火墙的命名空间。
- ❷ 包含 OpenShift Container Platform API 服务器的 IP 地址范围。
- ❸ 一个全局拒绝规则会阻止访问 OpenShift Container Platform API 服务器。

要查找 API 服务器的 IP 地址，请运行 **oc get ep kubernetes -n default**。

如需更多信息，请参阅 [BZ#1988324](#)。

重要

您必须将 OpenShift SDN 配置为使用网络策略或多租户模式来配置出口防火墙。

如果您使用网络策略模式，则出口防火墙只与每个命名空间的一个策略兼容，且无法用于共享网络的项目，如全局项目。



警告

出口防火墙规则不适用于通过路由器的网络流量。任何有权创建 Route CR 对象的用户，都可以通过创建指向禁止的目的地的路由来绕过出口防火墙策略规则。

13.3.1.1. 出口防火墙的限制

出口防火墙有以下限制：

- 项目不能有多个 EgressNetworkPolicy 对象。
- **default** 项目无法使用出口防火墙。
- 当在多租户模式下使用 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商时，会有以下限制：
 - 全局项目无法使用出口防火墙。您可以使用 **oc adm pod-network make-projects-global** 把一个项目设置为全局项目。
 - 通过 **oc adm pod-network join-projects** 命令合并的项目，无法在任何合并的项目中使用出口防火墙。

违反这些限制会导致项目的出口防火墙出现问题，并可能导致所有外部网络流量被丢弃。

13.3.1.2. 出口防火墙策略规则的匹配顺序

出口防火墙策略规则按照它们定义的顺序来评估，从第一个到最后一个的顺序。第一个与 pod 的出口连接匹配的规则会被应用。该连接会忽略后续的所有规则。

13.3.1.3. 域名服务器 (DNS) 解析如何工作

如果您在 egress 防火墙策略规则中使用 DNS 名称，则正确解析域名会受到以下限制：

- 域名更新根据本地非授权服务器返回的域的 TTL (time to live) 值进行轮询。
- 在需要时，pod 必须通过相同的本地名称服务器解析域名。否则，egress 防火墙控制器和 pod 已知的域的 IP 地址可能会有所不同。如果主机名的 IP 地址不同，则出口防火墙的强制实施可能不一致。
- 因为出口防火墙控制器和 pod 异步轮询相同的本地名称服务器，所以 pod 可能会在出口控制器执行前获取更新的 IP 地址，从而导致竞争条件。由于这个限制，仅建议在 EgressNetworkPolicy 对象中使用域名来更改 IP 地址的域。



注意

出口防火墙始终允许 pod 访问 pod 所在的用于 DNS 解析的节点的外部接口。

如果您在出口防火墙策略中使用域名，且您的 DNS 解析不是由本地节点上的 DNS 服务器处理，那么您必须添加出口防火墙规则，允许访问您的 DNS 服务器的 IP 地址。如果您在 pod 中使用域名。

13.3.2. EgressNetworkPolicy 自定义资源 (CR) 对象

您可以为出口防火墙定义一个或多个规则。规则是一个 **Allow** 规则，也可以是一个 **Deny** 规则，它包括规则适用的流量规格。

以下 YAML 描述了一个 EgressNetworkPolicy CR 对象：

EgressNetworkPolicy 对象

```
apiVersion: network.openshift.io/v1
kind: EgressNetworkPolicy
metadata:
  name: <name> ❶
spec:
  egress: ❷
  ...
```

- ❶ 出口防火墙的名称。
- ❷ 以下部分所述，一个或多个出口网络策略规则的集合。

13.3.2.1. EgressNetworkPolicy 规则

以下 YAML 描述了一个出口防火墙规则对象。**egress** 小节需要一个包括一个或多个对象的数组。

出口策略规则小节

```
egress:
- type: <type> ❶
  to: ❷
    cidrSelector: <cidr> ❸
    dnsName: <dns_name> ❹
```

- ❶ 规则类型。该值必须是 **Allow** 或 **Deny**。
- ❷ 描述出口流量匹配规则的小节。规则的 **cidrSelector** 字段或 **dnsName** 字段的值。您不能在同一规则中使用这两个字段。
- ❸ CIDR 格式的 IP 地址范围。
- ❹ 一个域名。

13.3.2.2. EgressNetworkPolicy CR 对象示例

以下示例定义了几个出口防火墙策略规则：

```
apiVersion: network.openshift.io/v1
kind: EgressNetworkPolicy
metadata:
  name: default
spec:
  egress: ❶
```



```

- type: Allow
  to:
    cidrSelector: 1.2.3.0/24
- type: Allow
  to:
    dnsName: www.example.com
- type: Deny
  to:
    cidrSelector: 0.0.0.0/0

```

- 1 出口防火墙策略规则对象的集合。

13.3.3. 创建出口防火墙策略对象

作为集群管理员，您可以为项目创建一个出口防火墙策略对象。



重要

如果项目已经定义了一个 EgressNetworkPolicy 对象，您必须编辑现有的策略来更改出口防火墙规则。

先决条件

- 使用 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift CLI (**oc**)。
- 您需要使用集群管理员身份登陆到集群。

流程

1. 创建策略规则：
 - a. 创建一个 **<policy_name>.yaml** 文件，其中 **<policy_name>** 描述出口策略规则。
 - b. 在您创建的文件中，定义出口策略对象。
2. 运行以下命令来创建策略对象。将 **<policy_name>** 替换为策略的名称，**<project>** 替换为规则应用到的项目。

```
$ oc create -f <policy_name>.yaml -n <project>
```

在以下示例中，在名为 **project1** 的项目中创建一个新的 EgressNetworkPolicy 对象：

```
$ oc create -f default.yaml -n project1
```

输出示例

```
egressnetworkpolicy.network.openshift.io/v1 created
```

3. 可选：保存 **<policy_name>.yaml** 文件，以便在以后进行修改。

13.4. 为项目编辑出口防火墙

作为集群管理员，您可以修改现有出口防火墙的网络流量规则。

13.4.1. 查看 EgressNetworkPolicy 对象

您可以查看集群中的 EgressNetworkPolicy 对象。

先决条件

- 使用 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift 命令行界面 (CLI)，通常称为 **oc**。
- 您必须登录集群。

流程

1. 可选：要查看集群中定义的 EgressNetworkPolicy 对象的名称，请输入以下命令：

```
$ oc get egressnetworkpolicy --all-namespaces
```

2. 要检查策略，请输入以下命令。将 **<policy_name>** 替换为要检查的策略名称。

```
$ oc describe egressnetworkpolicy <policy_name>
```

输出示例

```
Name: default
Namespace: project1
Created: 20 minutes ago
Labels: <none>
Annotations: <none>
Rule: Allow to 1.2.3.0/24
Rule: Allow to www.example.com
Rule: Deny to 0.0.0.0/0
```

13.5. 为项目编辑出口防火墙

作为集群管理员，您可以修改现有出口防火墙的网络流量规则。

13.5.1. 编辑 EgressNetworkPolicy 对象

作为集群管理员，您可以更新一个项目的出口防火墙。

先决条件

- 使用 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift CLI (**oc**)。
- 您需要使用集群管理员身份登录到集群。

流程

1. 查找项目的 EgressNetworkPolicy 对象的名称。将 **<project>** 替换为项目的名称。

```
$ oc get -n <project> egressnetworkpolicy
```

2. 可选，如果您在创建出口网络防火墙时没有保存 EgressNetworkPolicy 对象的副本，请输入以下命令来创建副本。

```
$ oc get -n <project> egressnetworkpolicy <name> -o yaml > <filename>.yaml
```

将 **<project>** 替换为项目的名称。将 **<name>** 替换为 Pod 的名称。将 **<filename>** 替换为要将 YAML 保存到的文件的名称。

3. 更改了策略规则后，请输入以下命令替换 EgressNetworkPolicy 对象。将 **<filename>** 替换为包含更新的 EgressNetworkPolicy 对象的文件名称。

```
$ oc replace -f <filename>.yaml
```

13.6. 从项目中删除出口防火墙

作为集群管理员，您可以从项目中删除出口防火墙，从而删除对项目的离开 OpenShift Container Platform 集群的网络流量的限制。

13.6.1. 删除 EgressNetworkPolicy 对象

作为集群管理员，您可以从项目中删除出口防火墙。

先决条件

- 使用 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift CLI (**oc**) 。
- 您需要使用集群管理员身份登陆到集群。

流程

1. 查找项目的 EgressNetworkPolicy 对象的名称。将 **<project>** 替换为项目的名称。

```
$ oc get -n <project> egressnetworkpolicy
```

2. 输入以下命令删除 EgressNetworkPolicy 对象。将 **<project>** 替换为项目名称，**<name>** 替换为对象名称。

```
$ oc delete -n <project> egressnetworkpolicy <name>
```

13.7. 使用出口路由器 POD 的注意事项

13.7.1. 关于出口路由器 pod

OpenShift Container Platform 出口路由器 (egress router) pod 使用一个专用的私有源 IP 地址，将网络流量重定向到指定的远程服务器。这可让您将网络流量发送到设定仅允许从特定 IP 地址访问的服务器。



注意

出口路由器 pod 并不适用于所有外向的连接。创建大量出口路由器 pod 可能会超过您的网络硬件的限制。例如，为每个项目或应用程序创建出口路由器 pod 可能会导致，在转换为使用软件来进行 MAC 地址过滤前超过了网络接口可以处理的本地 MAC 地址的数量。



重要

出口路由器镜像与 Amazon AWS、Azure Cloud 或其他不支持第 2 层操作的云平台不兼容，因为它们与 macvlan 流量不兼容。

13.7.1.1. 出口路由器模式

在 *重定向模式* 中，出口路由器 pod 会设置 iptables 规则将流量从其自身 IP 地址重定向到一个或多个目标 IP 地址。需要使用保留源 IP 地址的客户端 pod 必须修改来连接到出口路由器，而不是直接连接到目标 IP。

在 *HTTP 代理模式* 中，出口路由器 pod 作为一个 HTTP 代理在端口 **8080** 上运行。这个模式只适用于连接到基于 HTTP 或基于 HTTPS 服务的客户端，但通常需要较少的更改就可以使客户端 pod 正常工作。很多程序可以通过设置环境变量来使用 HTTP 代理服务器。

在 *DNS 代理模式* 中，出口路由器 pod 作为基于 TCP 服务的 DNS 代理运行，将其自身的 IP 地址转换到一个或多个目标 IP 地址。要使用保留的源 IP 地址，客户端 pod 必须进行修改来连接到出口路由器 pod，而不是直接连接到目标 IP 地址。此修改确保了外部的目的地将流量视为来自一个已知源的流量。

重定向模式可用于除 HTTP 和 HTTPS 以外的所有服务。对于 HTTP 和 HTTPS 服务，请使用 HTTP 代理模式。对于使用 IP 地址或域名的基于 TCP 的服务，请使用 DNS 代理模式。

13.7.1.2. 出口路由器 pod 的实现

出口路由器 pod 的设置由一个初始化容器执行。该容器在特权环境中运行，以便可以配置 macvlan 接口并设置 iptables 规则。在初始化容器完成设置 iptables 规则后会退出。接下来，出口路由器 pod 会执行容器来处理出口路由器流量。取决于出口路由器的模式，所使用的镜像会有所不同。

环境变量决定 egress-router 镜像使用的地址。镜像将 macvlan 接口配置为使用 **EGRESS_SOURCE** 作为其 IP 地址，并将 **EGRESS_GATEWAY** 作为网关的 IP 地址。

网络地址转换 (NAT) 规则被设置，使任何到 TCP 或 UDP 端口上的 pod 的集群 IP 地址的连接被重新指向由 **EGRESS_DESTINATION** 变量指定的 IP 地址的同一端口。

如果集群中只有部分节点能够声明指定的源 IP 地址并使用指定的网关，您可以指定一个 **nodeName** 或 **nodeSelector** 来表示哪些节点可以接受。

13.7.1.3. 部署注意事项

出口路由器 pod 会为节点的主网络接口添加额外的 IP 地址和 MAC 地址。因此，您可能需要配置虚拟机监控程序或云供应商来允许额外的地址。

Red Hat OpenStack Platform (RHOSP)

如果要在 RHOSP 上部署 OpenShift Container Platform，则必须将 OpenStack 环境中的 IP 和 MAC 地址列入白名单，否则 [通信将失败](#)：

```
$ openstack port set --allowed-address \
  ip_address=<ip_address>,mac_address=<mac_address> <neutron_port_uuid>
```

Red Hat Virtualization (RHV)

如果使用 [RHV](#)，必须为虚拟网络接口控制器(vNIC)选择 **No Network Filter**。

VMware vSphere

如果使用 VMware vSphere，请参阅 [VMware 文档](#) 以了解 [vSphere 标准交换机的安全](#)。通过从 vSphere Web 客户端中选择主机虚拟交换机来查看并更改 VMware vSphere 默认设置。

具体来说，请确保启用了以下功能：

- [MAC 地址更改](#)
- [Forged Transits](#)
- [Promiscuous Mode Operation](#)

13.7.1.4. 故障切换配置

为了避免停机，可以使用 **Deployment** 资源部署出口路由器 pod，如下例所示。要为示例部署创建新 **Service** 对象，使用 `oc expose deployment/egress-demo-controller` 命令。

```
apiVersion: v1
kind: Deployment
metadata:
  name: egress-demo-controller
spec:
  replicas: 1 1
  selector:
    name: egress-router
  template:
    metadata:
      name: egress-router
      labels:
        name: egress-router
      annotations:
        pod.network.openshift.io/assign-macvlan: "true"
    spec: 2
      initContainers:
        ...
      containers:
        ...
```

1 确保副本数被设置为 **1**，因为在任何同一个时间点上，只有一个 pod 可以使用给定的出口源 IP 地址。这意味着，在一个节点上运行的路由器只有一个副本。

2 为出口路由器 pod 指定 **Pod** 对象模板。

13.7.2. 其他资源

- [在重定向模式中部署出口路由器](#)

- 以 HTTP 代理模式部署出口路由器
- 以 DNS 代理模式部署出口路由器

13.8. 以重定向模式部署出口路由器 POD

作为集群管理员，您可以部署一个出口路由器 pod，该 pod 被配置为将流量重新定向到指定的目的地 IP 地址。

13.8.1. 重定向模式的出口路由器 pod 规格

为 **Pod** 对象中的一个出口路由器 pod 定义其配置。以下 YAML 描述了以重定向模式配置出口路由器 pod 的字段：

```
apiVersion: v1
kind: Pod
metadata:
  name: egress-1
  labels:
    name: egress-1
  annotations:
    pod.network.openshift.io/assign-macvlan: "true" 1
spec:
  initContainers:
  - name: egress-router
    image: registry.redhat.io/openshift4/ose-egress-router
    securityContext:
      privileged: true
    env:
  - name: EGRESS_SOURCE 2
    value: <egress_router>
  - name: EGRESS_GATEWAY 3
    value: <egress_gateway>
  - name: EGRESS_DESTINATION 4
    value: <egress_destination>
  - name: EGRESS_ROUTER_MODE
    value: init
  containers:
  - name: egress-router-wait
    image: registry.redhat.io/openshift4/ose-pod
```

1 该注解告知 OpenShift Container Platform 在主网络接口控制器(NIC)上创建一个 macvlan 网络接口，并将 macvlan 接口移到 pod 的网络命名空间中。您必须把 **"true"** 值包括在引号中。要在不同的 NIC 接口上让 OpenShift Container Platform 创建 macvlan 接口，请将注解值设置为该接口的名称。例如：**eth1**。

2 保留给出口路由器 pod 使用的物理网络的 IP 地址。可选：您可以包括子网长度（/24 后缀），以便正确路由到本地子网。如果没有指定子网长度，则出口路由器只能访问使用 **EGRESS_GATEWAY** 变量指定的主机，且子网上没有其他主机。

3 值与节点使用的默认网关相同。

4 将流量定向到的外部服务器。使用这个示例，连接到 pod 流量被重新定向到 **203.0.113.25**，源 IP 地址为 **192.168.12.99**。

出口路由器 pod 规格示例

```

apiVersion: v1
kind: Pod
metadata:
  name: egress-multi
  labels:
    name: egress-multi
  annotations:
    pod.network.openshift.io/assign-macvlan: "true"
spec:
  initContainers:
  - name: egress-router
    image: registry.redhat.io/openshift4/ose-egress-router
    securityContext:
      privileged: true
    env:
  - name: EGRESS_SOURCE
    value: 192.168.12.99/24
  - name: EGRESS_GATEWAY
    value: 192.168.12.1
  - name: EGRESS_DESTINATION
    value: |
      80 tcp 203.0.113.25
      8080 tcp 203.0.113.26 80
      8443 tcp 203.0.113.26 443
      203.0.113.27
  - name: EGRESS_ROUTER_MODE
    value: init
  containers:
  - name: egress-router-wait
    image: registry.redhat.io/openshift4/ose-pod

```

13.8.2. 出口目的地配置格式

当出口路由器 pod 被部署为重定向模式时，您可以使用以下一种或多种格式指定重定向规则：

- **<port> <protocol> <ip_address>** - 到给定 **<port>** 的内向连接应该被重新定向到给定 **<ip_address>** 上的同一端口。**<protocol>** 可以是 **tcp** 或 **udp**。
- **<port> <protocol> <ip_address> <remote_port>** - 和以上一样，除了连接被重新定向到 **<ip_address>** 上的一个不同的 **<remote_port>** 中。
- **<ip_address>** - 如果最后一行是一个 IP 地址，那么其它端口上的所有连接都会被重新指向那个 IP 地址的对应端口。如果没有故障切换 IP 地址，则其它端口上的连接将被拒绝。

在示例中定义了几个规则：

- 第一行将流量从本地端口 **80** 重定向到 **203.0.113.25** 的端口 **80**。
- 第二行和第三行将本地端口 **8080** 和 **8443** 重定向到 **203.0.113.26** 的远程端口 **80** 和 **443**。
- 最后一行与之前规则中没有指定的端口的流量匹配。

配置示例

-

```
80 tcp 203.0.113.25
8080 tcp 203.0.113.26 80
8443 tcp 203.0.113.26 443
203.0.113.27
```

13.8.3. 以重定向模式部署出口路由器 pod

在*重定向模式*中，出口路由器 pod 会设置 iptables 规则将流量从其自身 IP 地址重定向到一个或多个目标 IP 地址。需要使用保留源 IP 地址的客户端 pod 必须修改来连接到出口路由器，而不是直接连接到目标 IP。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 创建出口路由器 pod。
2. 为确保其他 pod 可以查找出口路由器 pod 的 IP 地址，请创建一个服务指向出口路由器 pod，如下例所示：

```
apiVersion: v1
kind: Service
metadata:
  name: egress-1
spec:
  ports:
    - name: http
      port: 80
    - name: https
      port: 443
  type: ClusterIP
  selector:
    name: egress-1
```

您的 pod 现在可以连接到此服务。使用保留的出口 IP 地址将其连接重新指向外部服务器的对应端口。

13.8.4. 其他资源

- [使用 ConfigMap 配置出口路由器目的地映射](#)

13.9. 以 HTTP 代理模式部署出口路由器 POD

作为集群管理员，您可以将出口路由器 pod 配置为代理流量到指定的 HTTP 和基于 HTTPS 的服务。

13.9.1. HTTP 模式的出口路由器 pod 规格

为 **Pod** 对象中的一个出口路由器 pod 定义其配置。以下 YAML 描述了以 HTTP 模式配置出口路由器 pod 的字段：

```

apiVersion: v1
kind: Pod
metadata:
  name: egress-1
  labels:
    name: egress-1
  annotations:
    pod.network.openshift.io/assign-macvlan: "true" ❶
spec:
  initContainers:
  - name: egress-router
    image: registry.redhat.io/openshift4/ose-egress-router
    securityContext:
      privileged: true
    env:
      - name: EGRESS_SOURCE ❷
        value: <egress-router>
      - name: EGRESS_GATEWAY ❸
        value: <egress-gateway>
      - name: EGRESS_ROUTER_MODE
        value: http-proxy
  containers:
  - name: egress-router-pod
    image: registry.redhat.io/openshift4/ose-egress-http-proxy
    env:
      - name: EGRESS_HTTP_PROXY_DESTINATION ❹
        value: |-
          ...
          ...

```

- ❶ 该注解告知 OpenShift Container Platform 在主网络接口控制器(NIC)上创建一个 macvlan 网络接口，并将 macvlan 接口移到 pod 的网络命名空间中。您必须把 "true" 值包括在引号中。要在不同的 NIC 接口上让 OpenShift Container Platform 创建 macvlan 接口，请将注解值设置为该接口的名称。例如：**eth1**。
- ❷ 保留给出口路由器 pod 使用的物理网络的 IP 地址。可选：您可以包括子网长度 (/24 后缀)，以便正确路由到本地子网。如果没有指定子网长度，则出口路由器只能访问使用 **EGRESS_GATEWAY** 变量指定的主机，且子网上没有其他主机。
- ❸ 值与节点使用的默认网关相同。
- ❹ 一个字符串或 YAML 多行字符串指定如何配置代理。请注意，这作为 HTTP 代理容器中的环境变量指定，而不是与 init 容器中的其他环境变量指定。

13.9.2. 出口目的地配置格式

当出口路由器 pod 以 HTTP 代理模式部署时，您可以使用以下一个或多个格式指定重定向规则。配置中的每行都指定允许或者拒绝的连接组：

- IP 地址允许连接到那个 IP 地址，如 **192.168.1.1**。
- CIDR 范围允许连接到那个 CIDR 范围，如 **192.168.1.0/24**。
- 主机名允许代理该主机，如 **www.example.com**。

- 前面带有 * 的域名允许代理到那个域及其所有子域，如 *.example.com。
- ! 再加上以前匹配的表达式会拒绝连接。
- 如果最后一行是 *，则任何没有被显式拒绝的都会被允许。否则，任何没有被允许的都会被拒绝。

您还可以使用 * 允许到所有远程目的地的连接。

配置示例

```
!*example.com
!192.168.1.0/24
192.168.2.1
*
```

13.9.3. 以 HTTP 代理模式部署出口路由器 pod

在 HTTP 代理模式中，出口路由器 pod 作为一个 HTTP 代理在端口 **8080** 上运行。这个模式只适用于连接到基于 HTTP 或基于 HTTPS 服务的客户端，但通常需要较少的更改就可以使客户端 pod 正常工作。很多程序可以通过设置环境变量来使用 HTTP 代理服务器。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 创建出口路由器 pod。
2. 为确保其他 pod 可以查找出口路由器 pod 的 IP 地址，请创建一个服务指向出口路由器 pod，如下例所示：

```
apiVersion: v1
kind: Service
metadata:
  name: egress-1
spec:
  ports:
    - name: http-proxy
      port: 8080 ①
  type: ClusterIP
selector:
  name: egress-1
```

- ① 确定 http 端口被设置为 **8080**。

3. 要将客户端 pod（不是出口代理 Pod）配置为使用 HTTP 代理，设置 **http_proxy** 或 **https_proxy** 变量：

```
apiVersion: v1
kind: Pod
metadata:
```

```

name: app-1
labels:
  name: app-1
spec:
  containers:
    env:
      - name: http_proxy
        value: http://egress-1:8080/ ❶
      - name: https_proxy
        value: http://egress-1:8080/
      ...

```

❶ 上一步中创建的服务。



注意

不需要在所有设置中使用 **http_proxy** 和 **https_proxy** 环境变量。如果以上内容没有创建可以正常工作设置，请查阅 pod 中运行的工具或软件的文档。

13.9.4. 其他资源

- [使用 ConfigMap 配置出口路由器目的地映射](#)

13.10. 以 DNS 代理模式部署出口路由器 POD

作为集群管理员，您可以将配置为代理流量的出口路由器 pod 部署到指定的 DNS 名称和 IP 地址。

13.10.1. DNS 模式的出口路由器 pod 规格

为 **Pod** 对象中的一个出口路由器 pod 定义其配置。以下 YAML 描述了在 DNS 模式中配置出口路由器 pod 的字段：

```

apiVersion: v1
kind: Pod
metadata:
  name: egress-1
  labels:
    name: egress-1
  annotations:
    pod.network.openshift.io/assign-macvlan: "true" ❶
spec:
  initContainers:
    - name: egress-router
      image: registry.redhat.io/openshift4/ose-egress-router
      securityContext:
        privileged: true
      env:
        - name: EGRESS_SOURCE ❷
          value: <egress-router>
        - name: EGRESS_GATEWAY ❸
          value: <egress-gateway>
        - name: EGRESS_ROUTER_MODE
          value: dns-proxy

```

```

containers:
- name: egress-router-pod
  image: registry.redhat.io/openshift4/ose-egress-dns-proxy
  securityContext:
    privileged: true
  env:
  - name: EGRESS_DNS_PROXY_DESTINATION 4
    value: |-
      ...
  - name: EGRESS_DNS_PROXY_DEBUG 5
    value: "1"
  ...

```

- 1 该注解告知 OpenShift Container Platform 在主网络接口控制器(NIC)上创建一个 macvlan 网络接口，并将 macvlan 接口移到 pod 的网络命名空间中。您必须把 **"true"** 值包括在引号中。要在不同的 NIC 接口上让 OpenShift Container Platform 创建 macvlan 接口，请将注解值设置为该接口的名称。例如：**eth1**。
- 2 保留给出口路由器 pod 使用的物理网络的 IP 地址。可选：您可以包括子网长度（/24 后缀），以便正确路由到本地子网。如果没有指定子网长度，则出口路由器只能访问使用 **EGRESS_GATEWAY** 变量指定的主机，且子网上没有其他主机。
- 3 值与节点使用的默认网关相同。
- 4 指定一个或多个代理目的地列表。
- 5 可选：指定输出 DNS 代理日志输出到 **stdout**。

13.10.2. 出口目的地配置格式

当路由器以 DNS 代理模式部署时，您会指定一个端口和目标映射列表。目的地可以是 IP 地址，也可以是 DNS 名称。

出口路由器 pod 支持以下格式来指定端口和目的地映射：

端口和远程地址

您可以使用两个字段格式来指定源端口和目标主机：**<port> <remote_address>**。

主机可以是 IP 地址或 DNS 名称。如果提供了 DNS 名称，DNS 解析会在运行时进行。对于给定主机，代理在连接到目标主机的 IP 地址时连接到目标主机上指定的源端口。

端口和远程地址对示例

```

80 172.16.12.11
100 example.com

```

端口、远程地址和远程端口

您可以使用三字段格式 **<port> <remote_address> <remote_port>** 指定源端口、目标主机和目的地端口。

三字段格式的行为与两字段版本相同，但目的地端口可能与源端口不同。

端口、远程地址和远程端口示例

■

```
8080 192.168.60.252 80
8443 web.example.com 443
```

13.10.3. 以 DNS 代理模式部署出口路由器 pod

在 *DNS 代理模式* 中，出口路由器 pod 作为基于 TCP 服务的 DNS 代理运行，将其自身的 IP 地址转换到一个或多个目标 IP 地址。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 创建出口路由器 pod。
2. 为出口路由器 pod 创建服务：
 - a. 创建名为 **egress-router-service.yaml** 的文件，其包含以下 YAML。将 **spec.ports** 设置为您之前为 **EGRESS_DNS_PROXY_DESTINATION** 环境变量定义的端口列表。

```
apiVersion: v1
kind: Service
metadata:
  name: egress-dns-svc
spec:
  ports:
    ...
  type: ClusterIP
  selector:
    name: egress-dns-proxy
```

例如：

```
apiVersion: v1
kind: Service
metadata:
  name: egress-dns-svc
spec:
  ports:
    - name: con1
      protocol: TCP
      port: 80
      targetPort: 80
    - name: con2
      protocol: TCP
      port: 100
      targetPort: 100
  type: ClusterIP
  selector:
    name: egress-dns-proxy
```

- b. 要创建服务，请输入以下命令：

```
$ oc create -f egress-router-service.yaml
```

Pod 现在可以连接至此服务。使用保留的出口 IP 地址将其代理到外部服务器的对应端口。

13.10.4. 其他资源

- [使用 ConfigMap 配置出口路由器目的地映射](#)

13.11. 从配置映射配置出口路由器 POD 目的地列表

作为集群管理员，您可以定义一个 **ConfigMap** 对象来指定出口路由器 pod 的目标映射。配置的特定格式取决于出口路由器 pod 的类型。有关格式的详情，请参阅特定出口路由器 pod 的文档。

13.11.1. 使用配置映射配置出口路由器目的地映射

对于大量或经常更换的目标映射集合，您可以使用配置映射来外部维护列表。这种方法的优点是可将编辑配置映射的权限委派给没有 **cluster-admin** 特权的用户。因为出口路由器 pod 需要特权容器，没有 **cluster-admin** 特权的用户无法直接编辑 pod 定义。



注意

配置映射更改时，出口路由器 pod 不会自动更新。您必须重启出口路由器 pod 来获得更新。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以具有 **cluster-admin** 特权的用户身份登录。

流程

1. 创建包含出口路由器 pod 映射数据的文件，如下例所示：

```
# Egress routes for Project "Test", version 3

80 tcp 203.0.113.25

8080 tcp 203.0.113.26 80
8443 tcp 203.0.113.26 443

# Fallback
203.0.113.27
```

您可以在这个文件中放入空白行和评论。

2. 从文件创建 **ConfigMap** 对象：

```
$ oc delete configmap egress-routes --ignore-not-found

$ oc create configmap egress-routes \
  --from-file=destination=my-egress-destination.txt
```

在以前的版本中，**egress-routes** 值是要创建的 **ConfigMap** 对象的名称，**my-egress-destination.txt** 是数据从中读取的文件的名称。

3. 创建出口路由器 pod 定义，并为环境片段中的 **EGRESS_DESTINATION** 字段指定 **configMapKeyRef** 小节：

```
...
env:
- name: EGRESS_DESTINATION
  valueFrom:
    configMapKeyRef:
      name: egress-routes
      key: destination
...
```

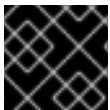
13.11.2. 其他资源

- [重定向模式](#)
- [HTTP 代理模式](#)
- [DNS 代理模式](#)

13.12. 为项目启用多播

13.12.1. 关于多播

通过使用 IP 多播，数据可同时广播到许多 IP 地址。



重要

目前，多播最适用于低带宽协调或服务发现。它不是一个高带宽解决方案。

默认情况下，OpenShift Container Platform pod 之间多播流量被禁用。如果使用 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商，可以根据每个项目启用多播。

以 **networkpolicy** 隔离模式使用 OpenShift SDN 网络插件时：

- pod 发送的多播数据包将传送到项目中的所有其他 pod，而无需考虑 **NetworkPolicy** 对象。即使在无法通过单播通信时，Pod 也能通过多播进行通信。
- 一个项目中的 pod 发送的多播数据包不会传送到任何其他项目中的 pod，即使存在允许项目间通信的 **NetworkPolicy** 对象。

以 **multitenant** 隔离模式使用 OpenShift SDN 网络插件时：

- pod 发送的多播数据包将传送到项目中的所有其他 pod。
- 只有在各个项目接合在一起并且每个接合的项目上都启用了多播时，一个项目中的 pod 发送的多播数据包才会传送到其他项目中的 pod。

13.12.2. 启用 pod 间多播

您可以为项目启用 pod 间多播。

先决条件

- 安装 OpenShift CLI (**oc**) 。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

- 运行以下命令，为项目启用多播。使用您要启用多播的项目的名称替换 **<namespace>**。

```
$ oc annotate netnamespace <namespace> \
  netnamespace.network.openshift.io/multicast-enabled=true
```

验证

要验证项目是否启用了多播，请完成以下步骤：

1. 将您的当前项目更改为启用多播的项目。使用项目名替换 **<project>**。

```
$ oc project <project>
```

2. 创建 pod 以作为多播接收器：

```
$ cat <<EOF | oc create -f -
apiVersion: v1
kind: Pod
metadata:
  name: mlistener
  labels:
    app: multicast-verify
spec:
  containers:
  - name: mlistener
    image: registry.access.redhat.com/ubi8
    command: ["/bin/sh", "-c"]
    args:
      ["dnf -y install socat hostname && sleep inf"]
    ports:
    - containerPort: 30102
      name: mlistener
      protocol: UDP
EOF
```

3. 创建 pod 以作为多播发送器：

```
$ cat <<EOF | oc create -f -
apiVersion: v1
kind: Pod
metadata:
  name: msender
  labels:
    app: multicast-verify
spec:
  containers:
  - name: msender
```

```

image: registry.access.redhat.com/ubi8
command: ["/bin/sh", "-c"]
args:
  ["dnf -y install socat && sleep inf"]
EOF

```

4. 在新的终端窗口中或选项卡中，启动多播侦听器。

a. 获得 Pod 的 IP 地址：

```
$ POD_IP=$(oc get pods mlistener -o jsonpath='{.status.podIP}')
```

b. 输入以下命令启动多播监听程序：

```
$ oc exec mlistener -i -t -- \
  socat UDP4-RECVFROM:30102,ip-add-membership=224.1.0.1:$POD_IP,fork
  EXEC:hostname
```

5. 启动多播传输。

a. 获取 pod 网络 IP 地址范围：

```
$ CIDR=$(oc get Network.config.openshift.io cluster \
  -o jsonpath='{.status.clusterNetwork[0].cidr}')
```

b. 要发送多播信息，请输入以下命令：

```
$ oc exec msender -i -t -- \
  /bin/bash -c "echo | socat STDIO UDP4-
  DATAGRAM:224.1.0.1:30102,range=$CIDR,ip-multicast-ttl=64"
```

如果多播正在工作，则上一个命令会返回以下输出：

```
mlistener
```

13.13. 为项目禁用多播

13.13.1. 禁用 pod 间多播

您可以为项目禁用 pod 间多播。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

- 运行以下命令来禁用多播：


```
$ oc annotate netnamespace <namespace> \ 1
netnamespace.network.openshift.io/multicast-enabled-
```

- 1 您要禁用多播的项目的 **namespace**。

13.14. 使用 OPENSIFT SDN 配置网络隔离

将集群配置为使用 OpenShift SDN CNI 插件的多租户隔离模式时，每个项目会被默认隔离。在多租户隔离模式下，不同项目中的 pod 或服务间不允许网络流量。

您可以通过两种方式更改项目的多租户隔离行为：

- 您可以接合一个或多个项目，允许不同项目中的 pod 和服务间的网络流量。
- 您可以对项目禁用网络隔离。它可全局访问，接受所有其他项目中的 pod 和服务的网络流量。可全局访问的项目可以访问所有其他项目中的 pod 和服务。

13.14.1. 先决条件

- 您必须将集群配置为以多租户隔离模式使用 OpenShift SDN Container Network Interface (CNI) 插件。

13.14.2. 接合项目

您可以接合两个或多个项目，以允许不同项目中的 Pod 和服务间的网络流量。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

1. 使用以下命令，将项目接合到现有项目网络中：

```
$ oc adm pod-network join-projects --to=<project1> <project2> <project3>
```

另外，除了指定具体的项目名称，也可以使用 **--selector=<project_selector>** 选项来基于关联标签指定项目。

2. 可选：运行以下命令来查看您接合在一起的 Pod 网络：

```
$ oc get netnamespaces
```

在 **NETID** 列中，同一 Pod 网络中的项目具有相同的网络 ID。

13.14.3. 隔离项目

您可以隔离项目，使其他项目中的 pod 和服务无法访问这个项目中的 pod 和服务。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

- 要隔离集群中的项目，请运行以下命令：

```
$ oc adm pod-network isolate-projects <project1> <project2>
```

另外，除了指定具体的项目名称，也可以使用 **--selector=<project_selector>** 选项来基于关联标签指定项目。

13.14.4. 对项目禁用网络隔离

您可以对项目禁用网络隔离。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

- 对项目运行以下命令：

```
$ oc adm pod-network make-projects-global <project1> <project2>
```

另外，除了指定具体的项目名称，也可以使用 **--selector=<project_selector>** 选项来基于关联标签指定项目。

13.15. 配置 KUBE-PROXY

Kubernetes 网络代理 (kube-proxy) 在每个节点上运行，并由 Cluster Network Operator (CNO) 管理。kube-proxy 维护网络规则，以转发与服务关联的端点的连接。

13.15.1. 关于 iptables 规则同步

同步周期决定 Kubernetes 网络代理 (kube-proxy) 在节点上同步 iptables 规则的频率。

同步在发生以下事件之一时开始：

- 发生某一事件，例如服务或端点添加到集群中或从集群中删除。
- 距最后一次同步的时间已超过为 kube-proxy 定义的同步周期。

13.15.2. kube-proxy 配置参数

您可以修改以下 **kubeProxyConfig** 参数。



注意

由于 OpenShift Container Platform 4.3 及更高版本中引进了性能上的改进，现在不再需要调整 **iptablesSyncPeriod** 参数。

表 13.2. 参数

参数	描述	值	默认值
iptablesSyncPeriod	iptables 规则的刷新周期。	一个时间间隔，如 30s 或 2m 。有效的后缀包括 s 、 m 和 h ，具体参见 Go 时间包文档 。	30s
proxyArguments.iptables-min-sync-period	刷新 iptables 规则前的最短时长。此参数确保刷新的频率不会过于频繁。默认情况下，当发生影响 iptables 规则的更改时就会立即进行刷新。	一个时间间隔，如 30s 或 2m 。有效的后缀包括 s 、 m 和 h ，具体参见 Go 时间包 。	0s

13.15.3. 修改 kube-proxy 配置

您可以为集群修改 Kubernetes 网络代理配置。

先决条件

- 安装 OpenShift CLI (**oc**) 。
- 使用 **cluster-admin** 角色登录正在运行的集群。

流程

1. 运行以下命令来编辑 **Network.operator.openshift.io** 自定义资源 (CR) ：

```
$ oc edit network.operator.openshift.io cluster
```

2. 利用您对 kube-proxy 配置的更改修改 CR 中的 **kubeProxyConfig** 参数，如以下示例 CR 中所示：

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  kubeProxyConfig:
    iptablesSyncPeriod: 30s
    proxyArguments:
      iptables-min-sync-period: ["30s"]
```

3. 保存文件并退出文本编辑器。
保存文件并退出编辑器时，**oc** 命令会验证其语法。如果您的修改含有语法错误，编辑器会打开该文件并显示错误消息。
4. 运行以下命令来确认配置更新：

```
$ oc get networks.operator.openshift.io -o yaml
```

输出示例

```
apiVersion: v1
items:
- apiVersion: operator.openshift.io/v1
  kind: Network
  metadata:
    name: cluster
  spec:
    clusterNetwork:
    - cidr: 10.128.0.0/14
      hostPrefix: 23
    defaultNetwork:
      type: OpenShiftSDN
    kubeProxyConfig:
      iptablesSyncPeriod: 30s
      proxyArguments:
        iptables-min-sync-period:
        - 30s
    serviceNetwork:
    - 172.30.0.0/16
  status: {}
kind: List
```

5. 可选：运行以下命令，确认 Cluster Network Operator 已接受配置更改：

```
$ oc get clusteroperator network
```

输出示例

NAME	VERSION	AVAILABLE	PROGRESSING	DEGRADED	SINCE
network	4.1.0-0.9	True	False	False	1m

成功应用配置更新后，**AVAILABLE** 字段为 **True**。

第 14 章 OVN-KUBERNETES 默认 CNI 网络供应商

14.1. 关于 OVN-KUBERNETES 默认 CONTAINER NETWORK INTERFACE (CNI) 网络供应商

OpenShift Container Platform 集群在 pod 和服务网络中使用虚拟网络。OVN-Kubernetes Container Network Interface (CNI) 插件是默认集群网络的一个网络供应商。OVN-Kubernetes 基于 Open Virtual Network (OVN)，它提供了一个基于 overlay 的网络实现。使用 OVN-Kubernetes 网络供应商的集群还在每个节点上运行 Open vSwitch (OVS)。OVN 在每个节点上配置 OVS 来实现声明的网络配置。

14.1.1. OVN-Kubernetes 特性

OVN-Kubernetes Container Network Interface (CNI) 集群网络供应商实现以下功能：

- 使用 OVN（开源虚拟网络）管理网络流量。OVN 是一个社区开发、与供应商无关的网络虚拟化解决方案。
- 实现 Kubernetes 网络策略支持，包括入口和出口规则。
- 使用 Geneve（通用网络虚拟化封装）协议而不是 VXLAN 在节点间创建覆盖网络。

14.1.2. 支持的默认 CNI 网络供应商功能列表

OpenShift Container Platform 为默认的 Container Network Interface (CNI) 网络供应商提供两个支持的选择：OpenShift SDN 和 OVN-Kubernetes。下表总结了这两个网络供应商当前支持的功能：

表 14.1. 默认 CNI 网络供应商功能比较

功能	OVN-Kubernetes	OpenShift SDN
出口 IP	支持	支持
Egress 防火墙 ^[1]	支持	支持
出口路由器	不支持	支持
Kubernetes 网络策略	支持	部分支持 ^[2]
多播	支持	支持

1. 在 OpenShift SDN 中，出口防火墙也称为出口网络策略。这和网络策略出口不同。
2. 不支持出口规则和一些 **ipBlock** 规则。

14.1.3. OVN-Kubernetes 限制

OVN-Kubernetes Container Network Interface (CNI) 集群网络供应商有一个与流量策略相关的限制。网络供应商不支持将 Kubernetes 服务的外部流量策略或内部流量策略设置为 **local**。两个参数都支持默认值 **cluster**。当您添加类型为 **LoadBalancer**、**NodePort** 的服务或使用外部 IP 添加服务时，这个限制可能会影响您。

其他资源

- [为项目配置出口防火墙](#)
- [关于网络策略](#)
- [为项目启用多播](#)
- [Network \[operator.openshift.io/v1\]](#)

14.2. 从 OPENSIFT SDN 集群网络供应商迁移

作为集群管理员，您可以从 OpenShift SDN CNI 集群网络供应商迁移到 OVN-Kubernetes Container Network Interface (CNI) 集群网络供应商。

要了解更多有关 OVN-Kubernetes 的信息，请参阅[关于 OVN-Kubernetes 网络供应商](#)。

14.2.1. 迁移到 OVN-Kubernetes 网络供应商

迁移到 OVN-Kubernetes Container Network Interface (CNI) 默认网络供应商是一个手动过程，其中会包括一些停机时间使集群无法访问。虽然提供了一个回滚过程，但迁移通常被认为是一个单向过程。



注意

迁移至 OVN-Kubernetes 网络供应商仅在裸机硬件的安装程序置备的集群中支持。

不支持在裸机硬件的用户置备的集群上执行迁移。

14.2.1.1. 迁移到 OVN-Kubernetes 网络供应商时的注意事项

迁移过程中不会保留分配给节点的子网以及分配给各个 pod 的 IP 地址。

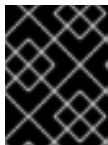
虽然 OVN-Kubernetes 网络供应商实现了 OpenShift SDN 网络供应商中的许多功能，但配置并不相同。

- 如果您的集群使用以下 OpenShift SDN 功能，则必须在 OVN-Kubernetes 中手动配置相同的功能：
 - 命名空间隔离
 - 出口 IP 地址
 - 出口网络策略
 - 出口路由器 pod
 - 多播
- 如果您的集群使用 **100.64.0.0/16** IP 地址范围中的任何部分，则无法迁移到 OVN-Kubernetes，因为它在内部使用这个 IP 地址范围。

以下小节重点介绍了上述功能在 OVN-Kubernetes 和 OpenShift SDN 中的配置的不同。

命名空间隔离

OVN-Kubernetes 仅支持网络策略隔离模式。



重要

如果您的集群使用在多租户或子网隔离模式中配置的 OpenShift SDN，则无法迁移到 OVN-Kubernetes 网络供应商。

出口 IP 地址

下表中描述了在 OVN-Kubernetes 和 OpenShift SDN 配置出口 IP 地址的不同：

表 14.2. 出口 IP 地址配置的不同

OVN-Kubernetes	OpenShift SDN
<ul style="list-style-type: none"> ● 创建 EgressIPs 对象 ● 在一个 Node 对象上添加注解 	<ul style="list-style-type: none"> ● 对 NetNamespace 对象进行补丁 ● 对 HostSubnet 对象进行补丁

有关在 OVN-Kubernetes 中使用出口 IP 地址的更多信息，请参阅“配置出口 IP 地址”。

出口网络策略

下表中描述在 OVN-Kubernetes 和 OpenShift SDN 间配置出口网络策略（也称为出口防火墙）的不同之处：

表 14.3. 出口网络策略配置的不同

OVN-Kubernetes	OpenShift SDN
<ul style="list-style-type: none"> ● 在命名空间中创建 EgressFirewall 对象 	<ul style="list-style-type: none"> ● 在命名空间中创建一个 EgressNetworkPolicy 对象

有关在 OVN-Kubernetes 中使用出口防火墙的更多信息，请参阅“配置项目出口防火墙”。

出口路由器 pod

OVN-Kubernetes 不支持在 OpenShift Container Platform 4.6 中使用出口路由器 Pod。

多播

下表中描述了在 OVN-Kubernetes 和 OpenShift SDN 上启用多播流量的区别：

表 14.4. 多播配置的不同

OVN-Kubernetes	OpenShift SDN
<ul style="list-style-type: none"> ● 在 Namespace 对象上添加注解 	<ul style="list-style-type: none"> ● 在 NetNamespace 对象中添加注解

有关在 OVN-Kubernetes 中使用多播的更多信息，请参阅“启用项目多播”。

网络策略

OVN-Kubernetes 在 **networking.k8s.io/v1** API 组中完全支持 Kubernetes **NetworkPolicy** API。从 OpenShift SDN 进行迁移时，网络策略不需要更改。

14.2.1.2. 迁移过程如何工作

迁移过程按如下方式工作：

1. 在 Cluster Network Operator (CNO) 配置对象上设置一个临时注解。此注解会触发 CNO 来监视 **defaultNetwork** 字段的变化。
2. 挂起 Machine Config Operator (MCO) 以确保它不会中断迁移。
3. 更新 **defaultNetwork** 字段。更新会导致 CNO 销毁 OpenShift SDN control plane pod 并部署 OVN-Kubernetes control plane pod。另外，它会更新 Multus 对象以反映新的集群网络供应商。
4. 重新引导集群中的每个节点。由于集群中的现有 pod 不知道集群网络供应商的更改，因此重新引导每个节点可确保每个节点排空 pod。新的 pod 附加到 OVN-Kubernetes 提供的新集群网络中。
5. 在集群重启中的所有节点后启用 MCO。MCO 向完成迁移所需的 systemd 配置推出更新。MCO 默认更新每个池的单个机器，因此迁移总时间随着集群的大小增加而增加。

14.2.2. 迁移至 OVN-Kubernetes 默认 CNI 网络供应商

作为集群管理员，您可以将集群的默认 Container Network Interface (CNI) 网络供应商更改为 OVN-Kubernetes。在迁移过程中，您必须重新引导集群中的每个节点。



重要

在进行迁移时，集群不可用，工作负载可能会中断。仅在服务中断可以接受时才执行迁移。

先决条件

- 在裸机安装程序置备的基础架构上安装的集群，以及在网络策略隔离模式下使用 OpenShift SDN 默认 CNI 网络供应商进行配置。
- 安装 OpenShift CLI (**oc**)。
- 使用具有 **cluster-admin** 角色的用户访问集群。
- etcd 数据库的最新备份可用。
- 集群处于已知良好状态，没有任何错误。

流程

1. 要备份集群网络的配置，请输入以下命令：

```
$ oc get Network.config.openshift.io cluster -o yaml > cluster-openshift-sdn.yaml
```

2. 要启用迁移，请输入以下命令在 Cluster Network Operator 配置对象上设置注解：

```
$ oc annotate Network.operator.openshift.io cluster \
  'networkoperator.openshift.io/network-migration'=""
```

3. 停止由 Machine Config Operator (MCO) 管理的所有机器配置池：

- 停止 master 配置池：


```
$ oc patch MachineConfigPool master --type='merge' --patch \
  '{ "spec": { "paused": true } }'
```

- 停止 worker 配置池：

```
$ oc patch MachineConfigPool worker --type='merge' --patch \
  '{ "spec": { "paused": true } }'
```

4. 要配置 OVN-Kubernetes 集群网络供应商，请输入以下命令：

```
$ oc patch Network.config.openshift.io cluster \
  --type='merge' --patch '{ "spec": { "networkType": "OVNKubernetes" } }'
```

5. 可选：您可以自定义 OVN-Kubernetes 的以下设置，以满足您的网络基础架构要求：

- 最大传输单元（MTU）
- Geneve（Generic Network Virtualization Encapsulation）覆盖网络端口

要自定义之前记录的设置之一，请输入以下命令。如果您不需要更改默认值，请从补丁中省略该键。

```
$ oc patch Network.operator.openshift.io cluster --type=merge \
  --patch '{
  "spec":{
    "defaultNetwork":{
      "ovnKubernetesConfig":{
        "mtu":<mtu>,
        "genevePort":<port>
      }
    }
  }
}'
```

mtu

Geneve 覆盖网络的 MTU。这个值通常是自动配置的；但是，如果集群中的节点没有都使用相同的 MTU，那么您必须将此值明确设置为比最小节点 MTU 的值小 **100**。

port

Geneve 覆盖网络的 UDP 端口。

更新 mtu 字段的 patch 命令示例

```
$ oc patch Network.operator.openshift.io cluster --type=merge \
  --patch '{
  "spec":{
    "defaultNetwork":{
      "ovnKubernetesConfig":{
        "mtu":1200
      }
    }
  }
}'
```

6. 等待 Multus 守护进程集的 rollout 完成。

```
$ oc -n openshift-multus rollout status daemonset/multus
```

Multus pod 的名称格式为 **multus-`<xxxxxx>`**，其中 **`<xxxxxxx>`** 是字母的随机序列。pod 可能需要一些时间才能重启。

输出示例

```
Waiting for daemon set "multus" rollout to finish: 1 out of 6 new pods have been updated...
...
Waiting for daemon set "multus" rollout to finish: 5 of 6 updated pods are available...
daemon set "multus" successfully rolled out
```

7. 要完成迁移，请重新引导集群中的每个节点。例如，您可以使用类似以下示例的 bash 脚本。这个脚本假定您可以使用 **ssh** 连接到每个主机，并将 **sudo** 配置为不提示输入密码。

```
#!/bin/bash

for ip in $(oc get nodes -o jsonpath='{.items[*].status.addresses[?(@.type=="InternalIP")].address}')
do
  echo "reboot node $ip"
  ssh -o StrictHostKeyChecking=no core@$ip sudo shutdown -r -t 3
done
```

如果无法使用 ssh 访问，您可能无法通过基础架构供应商的管理门户重新引导每个节点。

8. 重新引导集群中的节点后，启动所有机器配置池：

- 启动 master 配置池：

```
$ oc patch MachineConfigPool master --type='merge' --patch \
  '{"spec": {"paused": false }}'
```

- 启动 worker 配置池：

```
$ oc patch MachineConfigPool worker --type='merge' --patch \
  '{"spec": {"paused": false }}'
```

当 MCO 更新每个配置池中的机器时，它会重新引导每个节点。

默认情况下，MCO 会在一个时间段内为每个池更新一台机器，因此迁移完成所需要的时间会随集群大小的增加而增加。

9. 确认主机上新机器配置的状态：

- a. 要列出机器配置状态和应用的机器配置名称，请输入以下命令：

```
$ oc describe node | egrep "hostname|machineconfig"
```

输出示例

```
kubernetes.io/hostname=master-0
machineconfiguration.openshift.io/currentConfig: rendered-master-
c53e221d9d24e1c8bb6ee89dd3d8ad7b
machineconfiguration.openshift.io/desiredConfig: rendered-master-
c53e221d9d24e1c8bb6ee89dd3d8ad7b
machineconfiguration.openshift.io/reason:
machineconfiguration.openshift.io/state: Done
```

验证以下语句是否正确：

- `machineconfiguration.openshift.io/state` 字段的值为 **Done**。
- `machineconfiguration.openshift.io/currentConfig` 字段的值等于 `machineconfiguration.openshift.io/desiredConfig` 字段的值。

b. 要确认机器配置正确，请输入以下命令：

```
$ oc get machineconfig <config_name> -o yaml | grep ExecStart
```

这里的 `<config_name>` 是 `machineconfiguration.openshift.io/currentConfig` 字段中机器配置的名称。

机器配置必须包括以下对 `systemd` 配置的更新：

```
ExecStart=/usr/local/bin/configure-ovs.sh OVNKubernetes
```

10. 确认迁移成功完成：

a. 要确认默认 CNI 网络供应商是 OVN-Kubernetes，请输入以下命令。`status.networkType` 的值必须是 **OVNKubernetes**。

```
$ oc get network.config/cluster -o jsonpath='{.status.networkType}'
```

b. 要确认集群节点处于 **Ready** 状态，请输入以下命令：

```
$ oc get nodes
```

c. 如果节点一直处于 **NotReady** 状态，检查机器配置守护进程 pod 日志并解决所有错误。

i. 运行以下命令列出 pod：

```
$ oc get pod -n openshift-machine-config-operator
```

输出示例

```
NAME                                READY STATUS RESTARTS AGE
machine-config-controller-75f756f89d-sjp8b 1/1 Running 0 37m
machine-config-daemon-5cf4b             2/2 Running 0 43h
machine-config-daemon-7wzcd             2/2 Running 0 43h
machine-config-daemon-fc946             2/2 Running 0 43h
machine-config-daemon-g2v28             2/2 Running 0 43h
machine-config-daemon-gcl4f             2/2 Running 0 43h
machine-config-daemon-l5tnv             2/2 Running 0 43h
machine-config-operator-79d9c55d5-hth92 1/1 Running 0 37m
machine-config-server-bsc8h             1/1 Running 0 43h
machine-config-server-hklrm             1/1 Running 0 43h
machine-config-server-k9rtx             1/1 Running 0 43h
```

配置守护进程 pod 的名称使用以下格式：`machine-config-daemon-<seq>`。`<seq>` 值是一个随机的 5 个字符的字母数字序列。

ii. 使用以下命令，输出在上一个输出中显示的第一个机器配置守护进程 pod 的 pod 日志：

```
$ oc logs <pod> -n openshift-machine-config-operator
```

其中 **pod** 是机器配置守护进程 pod 的名称。

iii. 解决上一命令输出中显示的日志中的任何错误。

d. 要确认您的 pod 不在错误状态，请输入以下命令：

```
$ oc get pods --all-namespaces -o wide --sort-by='{.spec.nodeName}'
```

如果节点上的 pod 处于错误状态，请重新引导该节点。

11. 只有在迁移成功且集群处于良好状态时完成以下步骤：

a. 要从 Cluster Network Operator 配置对象中删除迁移注解，请输入以下命令：

```
$ oc annotate Network.operator.openshift.io cluster \
networkoperator.openshift.io/network-migration-
```

b. 要删除 OpenShift SDN 网络供应商命名空间，请输入以下命令：

```
$ oc delete namespace openshift-sdn
```

14.2.3. 其他资源

- [OVN-Kubernetes 网络供应商的配置参数](#)
- [备份 etcd](#)
- [关于网络策略](#)
- OVN-Kubernetes 功能
 - [配置出口 IP 地址](#)
 - [为项目配置出口防火墙](#)
 - [为项目启用多播](#)
- OpenShift SDN 功能
 - [为项目配置出口 IP](#)
 - [为项目配置出口防火墙](#)
 - [为项目启用多播](#)
- [Network \[operator.openshift.io/v1\]](#)

14.3. 回滚到 OPENSIFT SDN 网络供应商

作为集群管理员，如果迁移到 OVN-Kubernetes-Kubernetes 失败，您可以回滚到 OVN-Kubernetes CNI 集群网络供应商的 OpenShift SDN Container Network Interface (CNI) 集群网络供应商。

14.3.1. 将默认 CNI 网络供应商回滚到 OpenShift SDN

作为集群管理员，您可以将集群回滚到 OpenShift SDN 默认 Container Network Interface (CNI) 网络供应商。在回滚过程中，您必须重新引导集群中的每个节点。



重要

只有迁移到 OVN-Kubernetes 失败时才会回滚到 OpenShift SDN。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 使用具有 **cluster-admin** 角色的用户访问集群。
- 在裸机基础架构上安装的集群，使用 OVN-Kubernetes 默认 CNI 网络供应商进行了配置。

流程

1. 要启用迁移，请输入以下命令在 Cluster Network Operator 配置对象上设置注解：

```
$ oc annotate Network.operator.openshift.io cluster \
'networkoperator.openshift.io/network-migration=""
```

2. 停止由 Machine Config Operator (MCO) 管理的所有机器配置池：

- 停止 master 配置池：

```
$ oc patch MachineConfigPool master --type='merge' --patch \
'{"spec":{"paused": true}}'
```

- 停止 worker 配置池：

```
$ oc patch MachineConfigPool worker --type='merge' --patch \
'{"spec":{"paused": true}}'
```

3. 要配置 OpenShift SDN 集群网络供应商，输入以下命令：

```
$ oc patch Network.config.openshift.io cluster \
--type='merge' --patch '{"spec":{"networkType": "OpenShiftSDN"}}'
```

4. 可选：您可以自定义 OpenShift SDN 的以下设置，以满足您的网络基础架构的要求：

- 最大传输单元 (MTU)
- VXLAN 端口

要自定义之前记录的设置或其中的一个设置，进行自定义并输入以下命令。如果您不需要更改默认值，请从补丁中省略该键。

```
$ oc patch Network.operator.openshift.io cluster --type=merge \
--patch '{
  "spec":{
    "defaultNetwork":{
```

```
"openshiftSDNConfig":{
  "mtu":<mtu>,
  "vxlanPort":<port>
}}}'
```

mtu

Geneve 覆盖网络的 MTU。这个值通常是自动配置的；但是，如果集群中的节点没有都使用相同的 MTU，那么您必须将此值明确设置为比最小节点 MTU 的值小 **100**。

port

Geneve 覆盖网络的 UDP 端口。

patch 命令示例

```
$ oc patch Network.operator.openshift.io cluster --type=merge \
--patch '{
  "spec":{
    "defaultNetwork":{
      "openshiftSDNConfig":{
        "mtu":1200
      }
    }
  }
}'
```

5. 等待 Multus 守护进程集的 rollout 完成。

```
$ oc -n openshift-multus rollout status daemonset/multus
```

Multus pod 的名称格式为 **multus-`<xxxxxx>`**，其中 `<xxxxxxx>` 是字母的随机序列。pod 可能需要一些时间才能重启。

输出示例

```
Waiting for daemon set "multus" rollout to finish: 1 out of 6 new pods have been updated...
...
Waiting for daemon set "multus" rollout to finish: 5 of 6 updated pods are available...
daemon set "multus" successfully rolled out
```

6. 要完成回滚，请重新引导集群中的每个节点。例如，您可以使用类似如下的 bash 脚本。这个脚本假定您可以使用 **ssh** 连接到每个主机，并将 **sudo** 配置为不提示输入密码。

```
#!/bin/bash

for ip in $(oc get nodes -o jsonpath='{.items[*].status.addresses[?(@.type=="InternalIP")].address}')
do
  echo "reboot node $ip"
  ssh -o StrictHostKeyChecking=no core@$ip sudo shutdown -r -t 3
done
```

7. 重新引导集群中的节点后，启动所有机器配置池：

- 启动 master 配置池：

```
$ oc patch MachineConfigPool master --type='merge' --patch \
'{ "spec": { "paused": false } }
```

- 启动 worker 配置池：

```
$ oc patch MachineConfigPool worker --type='merge' --patch \
  '{"spec": {"paused": false }}'
```

当 MCO 更新每个配置池中的机器时，它会重新引导每个节点。

默认情况下，MCO 会在一个时间段内为每个池更新一台机器，因此迁移完成所需要的时间会随集群大小的增加而增加。

8. 确认主机上新机器配置的状态：

- a. 要列出机器配置状态和应用的机器配置名称，请输入以下命令：

```
$ oc describe node | egrep "hostname|machineconfig"
```

输出示例

```
kubernetes.io/hostname=master-0
machineconfiguration.openshift.io/currentConfig: rendered-master-
c53e221d9d24e1c8bb6ee89dd3d8ad7b
machineconfiguration.openshift.io/desiredConfig: rendered-master-
c53e221d9d24e1c8bb6ee89dd3d8ad7b
machineconfiguration.openshift.io/reason:
machineconfiguration.openshift.io/state: Done
```

验证以下语句是否正确：

- **machineconfiguration.openshift.io/state** 字段的值为 **Done**。
- **machineconfiguration.openshift.io/currentConfig** 字段的值等于 **machineconfiguration.openshift.io/desiredConfig** 字段的值。

- b. 要确认机器配置正确，请输入以下命令：

```
$ oc get machineconfig <config_name> -o yaml
```

这里的 **<config_name>** 是 **machineconfiguration.openshift.io/currentConfig** 字段中机器配置的名称。

9. 确认迁移成功完成：

- a. 要确认默认 CNI 网络供应商是 OVN-Kubernetes，请输入以下命令。**status.networkType** 的值必须是 **OpenShiftSDN**。

```
$ oc get network.config/cluster -o jsonpath='{.status.networkType}'
```

- b. 要确认集群节点处于 **Ready** 状态，请输入以下命令：

```
$ oc get nodes
```

- c. 如果节点一直处于 **NotReady** 状态，检查机器配置守护进程 pod 日志并解决所有错误。

- i. 运行以下命令列出 pod：

■

```
$ oc get pod -n openshift-machine-config-operator
```

输出示例

NAME	READY	STATUS	RESTARTS	AGE
machine-config-controller-75f756f89d-sjp8b	1/1	Running	0	37m
machine-config-daemon-5cf4b	2/2	Running	0	43h
machine-config-daemon-7wzcd	2/2	Running	0	43h
machine-config-daemon-fc946	2/2	Running	0	43h
machine-config-daemon-g2v28	2/2	Running	0	43h
machine-config-daemon-gcl4f	2/2	Running	0	43h
machine-config-daemon-l5tnv	2/2	Running	0	43h
machine-config-operator-79d9c55d5-hth92	1/1	Running	0	37m
machine-config-server-bsc8h	1/1	Running	0	43h
machine-config-server-hklrm	1/1	Running	0	43h
machine-config-server-k9rtx	1/1	Running	0	43h

配置守护进程 pod 的名称使用以下格式：**machine-config-daemon-`<seq>`**。`<seq>` 值是一个随机的 5 个字符的字母数字序列。

- ii. 要显示上一输出中显示的每个机器配置守护进程 pod 的 pod 日志，请输入以下命令：

```
$ oc logs <pod> -n openshift-machine-config-operator
```

其中 **pod** 是机器配置守护进程 pod 的名称。

- iii. 解决上一命令输出中显示的日志中的任何错误。

- d. 要确认您的 pod 不在错误状态，请输入以下命令：

```
$ oc get pods --all-namespaces -o wide --sort-by='{.spec.nodeName}'
```

如果节点上的 pod 处于错误状态，请重新引导该节点。

10. 只有在迁移成功且集群处于良好状态时完成以下步骤：

- a. 要从 Cluster Network Operator 配置对象中删除迁移注解，请输入以下命令：

```
$ oc annotate Network.operator.openshift.io cluster \
networkoperator.openshift.io/network-migration-
```

- b. 要删除 OVN-Kubernetes 网络供应商命名空间，请输入以下命令：

```
$ oc delete namespace openshift-ovn-kubernetes
```

14.4. 为项目配置出口防火墙

作为集群管理员，您可以为项目创建一个出口防火墙，用于限制离开 OpenShift Container Platform 集群的出口流量。

14.4.1. 出口防火墙在一个项目中的工作原理

作为集群管理员，您可以使用一个 **出口防火墙** 来限制集群内的一些 pod 或所有 pod 可以访问的外部主机。出口防火墙适用于以下情况：

- pod 只能连接到内部主机，且无法启动到公共互联网的连接。
- pod 只能连接到公共互联网，且无法启动到 OpenShift Container Platform 集群以外的内部主机的连接。
- pod 无法访问 OpenShift Container Platform 集群外的特定内部子网或主机。
- pod 只能连接到特定的外部主机。

例如，您可以允许某一个项目访问指定的 IP 范围，但拒绝其他项目对同一 IP 范围的访问。或者您可以限制应用程序开发人员从 Python pip 的镜像点进行更新，并强制要求更新只能来自于批准的源。

您可以通过创建一个 EgressFirewall 自定义资源（CR）对象来配置出口防火墙策略。出口防火墙与满足以下任一条件的网络流量匹配：

- CIDR 格式的 IP 地址范围
- 端口号
- 协议是以下协议之一：TCP、UDP 和 SCTP

重要

如果您的出口防火墙包含 **0.0.0.0/0** 的拒绝规则，则阻止访问 OpenShift Container Platform API 服务器。为确保 pod 能够继续访问 OpenShift Container Platform API 服务器，您必须在出口防火墙规则中包含 API 服务器侦听的 IP 地址范围，如下例所示：

```
apiVersion: k8s.ovn.org/v1
kind: EgressFirewall
metadata:
  name: default
  namespace: <namespace> ①
spec:
  egress:
  - to:
    cidrSelector: <api_server_address_range> ②
    type: Allow
  # ...
  - to:
    cidrSelector: 0.0.0.0/0 ③
    type: Deny
```

- ① 出口防火墙的命名空间。
- ② 包含 OpenShift Container Platform API 服务器的 IP 地址范围。
- ③ 一个全局拒绝规则会阻止访问 OpenShift Container Platform API 服务器。

要查找 API 服务器的 IP 地址，请运行 **oc get ep kubernetes -n default**。

如需更多信息，请参阅 [BZ#1988324](#)。



警告

出口防火墙规则不适用于通过路由器的网络流量。任何有权创建 Route CR 对象的用户，都可以通过创建指向禁止的目的地的路由来绕过出口防火墙策略规则。

14.4.1.1. 出口防火墙的限制

出口防火墙有以下限制：

- 项目不能有一个以上的 EgressFirewall 对象。
- 每个项目最多可定义一个具有最多 8,000 个规则的 EgressFirewall 对象。

违反这些限制会导致项目的出口防火墙出现问题，并可能导致所有外部网络流量被丢弃。

14.4.1.2. 出口防火墙策略规则的匹配顺序

出口防火墙策略规则按照它们定义的顺序来评估，从第一个到最后一个的顺序。第一个与 pod 的出口连接匹配的规则会被应用。该连接会忽略后续的所有规则。

14.4.2. EgressFirewall 自定义资源（CR）对象

您可以为出口防火墙定义一个或多个规则。规则是一个 **Allow** 规则，也可以是一个 **Deny** 规则，它包括规则适用的流量规格。

以下 YAML 描述了 EgressFirewall CR 对象：

EgressFirewall 对象

```
apiVersion: k8s.ovn.org/v1
kind: EgressFirewall
metadata:
  name: <name> ①
spec:
  egress: ②
  ...
```

- ① 对象的名称必须是 **default**。
- ② 以下部分所述，一个或多个出口网络策略规则的集合。

14.4.2.1. EgressFirewall 规则

以下 YAML 描述了一个出口防火墙规则对象。**egress** 小节需要一个包括一个或多个对象的数组。

出口策略规则小节

```
egress:
- type: <type> ①
```

```
to: 2
  cidrSelector: <cidr> 3
ports: 4
  ...
```

- 1 规则类型。该值必须是 **Allow** 或 **Deny**。
- 2 描述出口流量匹配规则的小节。
- 3 CIDR 格式的 IP 地址范围。
- 4 可选：描述该规则的网络端口和协议集合的小节。

端口小节

```
ports:
- port: <port> 1
  protocol: <protocol> 2
```

- 1 网络端口，比如 **80** 或 **443**。如果为这个字段指定值，还必须为 **protocol** 指定一个值。
- 2 网络协议。该值必须是 **TCP**、**UDP** 或 **SCTP**。

14.4.2.2. EgressFirewall CR 对象示例

以下示例定义了几个出口防火墙策略规则：

```
apiVersion: k8s.ovn.org/v1
kind: EgressFirewall
metadata:
  name: default
spec:
  egress: 1
  - type: Allow
    to:
      cidrSelector: 1.2.3.0/24
  - type: Deny
    to:
      cidrSelector: 0.0.0.0/0
```

- 1 出口防火墙策略规则对象的集合。

以下示例定义了一个策略规则，即如果流量使用 TCP 协议和目标端口 **80**，或任何协议和目标端口 **443**，则拒绝通过 **172.16.1.1** IP 地址到主机的流量。

```
apiVersion: k8s.ovn.org/v1
kind: EgressFirewall
metadata:
  name: default
spec:
  egress:
```

```
- type: Deny
  to:
    cidrSelector: 172.16.1.1
  ports:
  - port: 80
    protocol: TCP
  - port: 443
```

14.4.3. 创建出口防火墙策略对象

作为集群管理员，您可以为项目创建一个出口防火墙策略对象。



重要

如果项目已经定义了 EgressFirewall 对象，您必须编辑现有策略来更改出口防火墙规则。

先决条件

- 使用 OVN-Kubernetes 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift CLI (**oc**)。
- 您需要使用集群管理员身份登陆到集群。

流程

1. 创建策略规则：
 - a. 创建一个 **<policy_name>.yaml** 文件，其中 **<policy_name>** 描述出口策略规则。
 - b. 在您创建的文件中，定义出口策略对象。
2. 运行以下命令来创建策略对象。将 **<policy_name>** 替换为策略的名称，**<project>** 替换为规则应用到的项目。

```
$ oc create -f <policy_name>.yaml -n <project>
```

在以下示例中，在名为 **project1** 的项目中创建一个新的 EgressFirewall 对象：

```
$ oc create -f default.yaml -n project1
```

输出示例

```
egressfirewall.k8s.ovn.org/v1 created
```

3. 可选：保存 **<policy_name>.yaml** 文件，以便在以后进行修改。

14.5. 查看项目的出口防火墙

作为集群管理员，您可以列出任何现有出口防火墙的名称，并查看特定出口防火墙的流量规则。

14.5.1. 查看 EgressFirewall 对象

您可以查看集群中的 EgressFirewall 对象。

先决条件

- 使用 OVN-Kubernetes 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift 命令行界面 (CLI)，通常称为 **oc**。
- 您必须登录集群。

流程

1. 可选：要查看集群中定义的 EgressFirewall 对象的名称，请输入以下命令：

```
$ oc get egressfirewall --all-namespaces
```

2. 要检查策略，请输入以下命令。将 **<policy_name>** 替换为要检查的策略名称。

```
$ oc describe egressfirewall <policy_name>
```

输出示例

```
Name: default
Namespace: project1
Created: 20 minutes ago
Labels: <none>
Annotations: <none>
Rule: Allow to 1.2.3.0/24
Rule: Allow to www.example.com
Rule: Deny to 0.0.0.0/0
```

14.6. 为项目编辑出口防火墙

作为集群管理员，您可以修改现有出口防火墙的网络流量规则。

14.6.1. 编辑 EgressFirewall 对象

作为集群管理员，您可以更新一个项目的出口防火墙。

先决条件

- 使用 OVN-Kubernetes 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift CLI (**oc**)。
- 您需要使用集群管理员身份登录到集群。

流程

1. 查找项目的 EgressFirewall 对象的名称。将 **<project>** 替换为项目的名称。

```
$ oc get -n <project> egressfirewall
```

2. 可选：如果您在创建出口网络防火墙时没有保存 EgressFirewall 对象的副本，请输入以下命令来创建副本。

```
$ oc get -n <project> egressfirewall <name> -o yaml > <filename>.yaml
```

将 **<project>** 替换为项目的名称。将 **<name>** 替换为 Pod 的名称。将 **<filename>** 替换为要将 YAML 保存到的文件的名称。

3. 修改策略规则后，请输入以下命令替换 EgressFirewall 对象。将 **<filename>** 替换为包含更新的 EgressFirewall 对象的文件名称。

```
$ oc replace -f <filename>.yaml
```

14.7. 从项目中删除出口防火墙

作为集群管理员，您可以从项目中删除出口防火墙，从而删除对项目的离开 OpenShift Container Platform 集群的网络流量的限制。

14.7.1. 删除 EgressFirewall 对象

作为集群管理员，您可以从项目中删除出口防火墙。

先决条件

- 使用 OVN-Kubernetes 默认 Container Network Interface (CNI) 网络供应商插件的集群。
- 安装 OpenShift CLI (**oc**)。
- 您需要使用集群管理员身份登陆到集群。

流程

1. 查找项目的 EgressFirewall 对象的名称。将 **<project>** 替换为项目的名称。

```
$ oc get -n <project> egressfirewall
```

2. 输入以下命令删除 EgressFirewall 对象。将 **<project>** 替换为项目名称，**<name>** 替换为对象名称。

```
$ oc delete -n <project> egressfirewall <name>
```

14.8. 配置出口 IP 地址

作为集群管理员，您可以配置 OVN-Kubernetes 默认 Container Network Interface (CNI) 网络供应商，为命名空间分配一个或多个出口 IP 地址，或分配给命名空间中的特定 pod。

14.8.1. 出口 IP 地址架构设计和实施

OpenShift Container Platform 出口 IP 地址功能可确保来自一个或多个命名空间中的一个或多个 pod 的流量具有集群网络之外的服务具有一致的源 IP 地址。

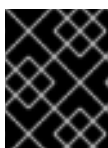
例如，您可能有一个 pod 定期查询托管在集群外服务器上的数据库。要强制对服务器进行访问要求，将数据包过滤设备配置为只允许来自特定 IP 地址的流量。为确保您可以可靠地允许从该特定 pod 访问服务器，您可以为向服务器发出请求的 pod 配置特定的出口 IP 地址。

出口 IP 地址作为额外 IP 地址在节点的主网络接口中使用，且必须与节点的主 IP 地址位于同一个子网中。不能为集群中的任何其他节点分配额外的 IP 地址。

在一些集群配置中，应用程序 pod 和入口路由器 pod 在同一个节点上运行。如果在这种情况下为应用程序项目配置出口 IP，则在从应用程序项目向路由发送请求时不会使用 IP。

14.8.1.1. 平台支持

下表概述了对不同平台中的出口 IP 地址功能的支持：



重要

出口 IP 地址的实现与 Amazon Web Services(AWS)、Azure Cloud 或任何其它与自动第 2 层网络操作不兼容的公共云平台。

平台	支持
裸机	是
vSphere	是
Red Hat OpenStack Platform (RHOSP)	否
公有云	否

14.8.1.2. 将出口 IP 分配给 pod

要将一个或多个出口 IP 分配给命名空间中的命名空间或特定 pod,必须满足以下条件：

- 集群中至少有一个节点必须具有 `k8s.ovn.org/egress-assignable: ""` 标签。
- 存在一个 **EgressIP** 对象定义一个或多个出口 IP 地址，用作从命名空间中离开集群的流量的源 IP 地址。



重要

如果您在为出口 IP 分配标记集群中的任何节点之前创建 **EgressIP** 对象，OpenShift Container Platform 可能会将每个出口 IP 地址分配给第一个节点，并使用 `k8s.ovn.org/egress-assignable: ""` 标签。

要确保出口 IP 地址在集群中的不同节点广泛分发，请在创建任何 **EgressIP** 对象前，始终将标签应用到您想托管出口 IP 地址的节点。

14.8.1.3. 将出口 IP 分配给节点

在创建 **EgressIP** 对象时，以下条件适用于标记为 `k8s.ovn.org/egress-assignable: ""` 标签的节点：

- 每次不会将出口 IP 地址分配给多个节点。

- 出口 IP 地址可在可以托管出口 IP 地址的可用节点之间平衡。
- 如果 **EgressIP** 对象中的 **spec.EgressIPs** 数组指定了多个 IP 地址，则不会有超过一个指定地址的节点托管。
- 如果节点不可用，则会自动重新分配给它的所有出口 IP 地址，但符合前面描述的条件。

当 Pod 与多个 **EgressIP** 对象的选择器匹配时，无法保证在 **EgressIP** 对象中指定的出口 IP 地址被分配为 pod 的出口 IP 地址。

另外，如果 **EgressIP** 对象指定了多个出口 IP 地址，则无法保证可以使用哪些出口 IP 地址。例如，如果 pod 与具有两个出口 IP 地址 **10.10.20.1** 和 **10.10.20.2** 的 **EgressIP** 对象的选择器匹配，则可能用于每个 TCP 连接或 UDP 对话。

14.8.1.4. 出口 IP 地址配置架构图

下图显示了出口 IP 地址配置。图中描述了，在一个集群的三个节点上运行的两个不同命名空间中的四个 pod。节点从主机网络上的 **192.168.126.0/18** CIDR 块中分配 IP 地址。



Node 1 和 Node 3 都标记为 **k8s.ovn.org/egress-assignable: ""**，因此可用于分配出口 IP 地址。

图中的横线描述了 pod1、pod2 和 pod 3 的流量流，通过 pod 网络来从 Node 1 和 Node 3 出口集群。当外部服务从示例 **EgressIP** 对象选择的任何 pod 接收流量时，源 IP 地址为 **192.168.126.10** 或 **192.168.126.102**。

图中的以下资源被详细描述：

命名空间对象

命名空间在以下清单中定义：

命名空间对象

```

apiVersion: v1
kind: Namespace
metadata:
  name: namespace1
  labels:
    env: prod
---
apiVersion: v1
kind: Namespace
metadata:
  
```



```
name: namespace2
labels:
  env: prod
```

EgressIP 对象

以下 **EgressIP** 对象描述了一个配置，该配置选择将 **env** 标签设置为 **prod** 的任意命名空间中的所有 pod。所选 pod 的出口 IP 地址为 **192.168.126.10** 和 **192.168.126.102**。

EgressIP 对象

```
apiVersion: k8s.ovn.org/v1
kind: EgressIP
metadata:
  name: egressips-prod
spec:
  egressIPs:
    - 192.168.126.10
    - 192.168.126.102
  namespaceSelector:
    matchLabels:
      env: prod
status:
  assignments:
    - node: node1
      egressIP: 192.168.126.10
    - node: node3
      egressIP: 192.168.126.102
```

对于上例中的配置，OpenShift Container Platform 会为可用节点分配两个出口 IP 地址。**status** 字段显示是否以及在哪里分配了出口 IP 地址。

14.8.2. EgressIP 对象

以下 YAML 描述了 **EgressIP** 对象的 API。对象有效的范围为集群，它不是在命名空间中创建的。

```
apiVersion: k8s.ovn.org/v1
kind: EgressIP
metadata:
  name: <name> ①
spec:
  egressIPs: ②
  - <ip_address>
  namespaceSelector: ③
  ...
  podSelector: ④
  ...
```

- ① **EgressIPs** 对象的名称。
- ② 包括一个或多个 IP 地址的数组。
- ③ 出口 IP 地址与其关联的一个或多个命名空间选择器将。

- 4 可选：指定命名空间中的 pod 的一个或多个选择器，以将出口 IP 地址与其关联。通过使用这些选择器，可以选择命名空间中的 pod 子集。

以下 YAML 描述了命名空间选择器的小节：

命名空间选择器小节

```
namespaceSelector: 1
  matchLabels:
    <label_name>: <label_value>
```

- 1 命名空间的一个或多个匹配规则。如果提供多个匹配规则，则会选择所有匹配的命名空间。

以下 YAML 描述了 pod 选择器的可选小节：

Pod 选择器片段

```
podSelector: 1
  matchLabels:
    <label_name>: <label_value>
```

- 1 可选：与指定 **namespaceSelector** 规则匹配的命名空间中 pod 的一个或多个匹配规则。如果指定，则仅选择匹配的 pod。命名空间中的其他 Pod 不会被选择。

在以下示例中，**EgressIP** 对象将 **192.168.126.11** 和 **192.168.126.102** 出口 IP 地址与将 **app** 标签设置为 **web** 的 pod 关联，并位于将 **env** 标签设置为 **prod** 的命名空间中：

EgressIP 对象示例

```
apiVersion: k8s.ovn.org/v1
kind: EgressIP
metadata:
  name: egress-group1
spec:
  egressIPs:
    - 192.168.126.11
    - 192.168.126.102
  podSelector:
    matchLabels:
      app: web
  namespaceSelector:
    matchLabels:
      env: prod
```

在以下示例中，**EgressIP** 对象将 **192.168.127.30** 和 **192.168.127.40** 出口 IP 地址与任何没有将 **environment** 标签设置为 **development** 的 pod 相关联：

EgressIP 对象示例

```
apiVersion: k8s.ovn.org/v1
kind: EgressIP
metadata:
```

```

name: egress-group2
spec:
  egressIPs:
  - 192.168.127.30
  - 192.168.127.40
  namespaceSelector:
    matchExpressions:
    - key: environment
      operator: NotIn
      values:
      - development

```

14.8.3. 标记节点以托管出口 IP 地址

您可以将 `k8s.ovn.org/egress-assignable=""` 标签应用到集群中的节点，以便 OpenShift Container Platform 可以为该节点分配一个或多个出口 IP 地址。

先决条件

- 安装 OpenShift CLI (`oc`)。
- 以集群管理员身份登录集群。

流程

- 要标记节点，使其可以托管一个或多个出口 IP 地址，请输入以下命令：

```
$ oc label nodes <node_name> k8s.ovn.org/egress-assignable="" 1
```

- 1 要标记的节点的名称。

14.8.4. 后续步骤

- [分配出口 IP](#)

14.8.5. 其他资源

- [labelSelector meta/v1](#)
- [LabelSelectorRequirement meta/v1](#)

14.9. 分配出口 IP 地址

作为集群管理员，您可以为从一个命名空间中，或从一个命名空间内的特定 pod 中离开集群的网络流量分配一个出口 IP 地址。

14.9.1. 为一个命名空间分配出口 IP 地址

您可以将一个或多个出口 IP 地址分配给一个命名空间，或分配给命名空间中的特定 pod。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 以集群管理员身份登录集群。
- 至少配置一个节点来托管出口 IP 地址。

流程

1. 创建 **EgressIP** 对象：

- a. 创建一个 `<egressips_name>.yaml` 文件，其中 `<egressips_name>` 是对象的名称。
- b. 在您创建的文件中，定义一个 **EgressIP** 对象，如下例所示：

```
apiVersion: k8s.ovn.org/v1
kind: EgressIP
metadata:
  name: egress-project1
spec:
  egressIPs:
    - 192.168.127.10
    - 192.168.127.11
  namespaceSelector:
    matchLabels:
      env: qa
```

2. 运行以下命令来创建对象。

```
$ oc apply -f <egressips_name>.yaml 1
```

- 1** 将 `<egressips_name>` 替换为对象的名称。

输出示例

```
egressips.k8s.ovn.org/<egressips_name> created
```

3. 可选：保存 `<egressips_name>.yaml` 文件，以便在以后进行修改。
4. 向命名空间添加需要出口 IP 地址的标签。要在第 1 步中定义的 **EgressIP** 对象的命名空间中添加标签，请运行以下命令：

```
$ oc label ns <namespace> env=qa 1
```

- 1** 将 `<namespace>` 替换为需要出口 IP 地址的命名空间。

14.9.2. 其他资源

- [配置出口 IP 地址](#)

14.10. 为项目启用多播

14.10.1. 关于多播

通过使用 IP 多播，数据可同时广播到许多 IP 地址。



重要

目前，多播最适用于低带宽协调或服务发现。它不是一个高带宽解决方案。

默认情况下，OpenShift Container Platform pod 之间多播流量被禁用。如果使用 OVN-Kubernetes 默认 Container Network Interface (CNI) 网络供应商，则可以根据每个项目启用多播。

14.10.2. 启用 pod 间多播

您可以为项目启用 pod 间多播。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

- 运行以下命令，为项目启用多播。使用您要启用多播的项目的名称替换 **<namespace>**。

```
$ oc annotate namespace <namespace> \
k8s.ovn.org/multicast-enabled=true
```

验证

要验证项目是否启用了多播，请完成以下步骤：

1. 将您的当前项目更改为启用多播的项目。使用项目名替换 **<project>**。

```
$ oc project <project>
```

2. 创建 pod 以作为多播接收器：

```
$ cat <<EOF | oc create -f -
apiVersion: v1
kind: Pod
metadata:
  name: mlistener
  labels:
    app: multicast-verify
spec:
  containers:
  - name: mlistener
    image: registry.access.redhat.com/ubi8
    command: ["/bin/sh", "-c"]
    args:
      ["dnf -y install socat hostname && sleep inf"]
    ports:
      - containerPort: 30102
```

```

name: mlistener
protocol: UDP
EOF

```

3. 创建 pod 以作为多播发送器：

```

$ cat <<EOF | oc create -f -
apiVersion: v1
kind: Pod
metadata:
  name: msender
  labels:
    app: multicast-verify
spec:
  containers:
  - name: msender
    image: registry.access.redhat.com/ubi8
    command: ["/bin/sh", "-c"]
    args:
      ["dnf -y install socat && sleep inf"]
EOF

```

4. 在新的终端窗口中或选项卡中，启动多播侦听器。

- a. 获得 Pod 的 IP 地址：

```
$ POD_IP=$(oc get pods mlistener -o jsonpath='{.status.podIP}')
```

- b. 输入以下命令启动多播监听程序：

```
$ oc exec mlistener -i -t -- \
  socat UDP4-RECVFROM:30102,ip-add-membership=224.1.0.1:$POD_IP,fork
  EXEC:hostname

```

5. 启动多播传输。

- a. 获取 pod 网络 IP 地址范围：

```
$ CIDR=$(oc get Network.config.openshift.io cluster \
  -o jsonpath='{.status.clusterNetwork[0].cidr}')
```

- b. 要发送多播信息，请输入以下命令：

```
$ oc exec msender -i -t -- \
  /bin/bash -c "echo | socat STDIO UDP4-
  DATAGRAM:224.1.0.1:30102,range=$CIDR,ip-multicast-ttl=64"

```

如果多播正在工作，则上一个命令会返回以下输出：

```
mlistener
```

14.11. 为项目禁用多播

14.11.1. 禁用 pod 间多播

您可以为项目禁用 pod 间多播。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 您必须作为 **cluster-admin** 角色用户登录集群。

流程

- 运行以下命令来禁用多播：

```
$ oc annotate namespace <namespace> \ 1
k8s.ovn.org/multicast-enabled-
```

- 1 您要禁用多播的项目的 **namespace**。

14.12. 配置混合联网

作为集群管理员，您可以配置 OVN-Kubernetes Container Network Interface(CNI)集群网络供应商，允许 Linux 和 Windows 节点分别托管 Linux 和 Windows 工作负载。

14.12.1. 使用 OVN-Kubernetes 配置混合网络

您可以将集群配置为使用 OVN-Kubernetes 的混合网络。这允许支持不同节点网络配置的混合集群。例如：集群中运行 Linux 和 Windows 节点时需要这样做。



重要

您必须在安装集群过程中使用 OVN-Kubernetes 配置混合网络。您不能在安装过程中切换到混合网络。

先决条件

- 您在 **install-config.yaml** 文件中为 **networking.networkType** 参数定义了 **OVNKubernetes**。如需更多信息，请参阅有关在所选云供应商上配置 OpenShift Container Platform 网络自定义的安装文档。

流程

1. 进入包含安装程序的目录并创建清单：

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

其中：

<installation_directory>

指定包含集群的 **install-config.yaml** 文件的目录名称。

- 在 `<installation_directory>/manifests/` 目录下，为高级网络配置创建一个名为 `cluster-network-03-config.yml` 的 stub 清单文件：

```
$ cat <<EOF > <installation_directory>/manifests/cluster-network-03-config.yml
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
EOF
```

其中：

`<installation_directory>`

指定包含集群的 `manifests/` 目录的目录名称。

- 在编辑器中打开 `cluster-network-03-config.yml` 文件，并使用混合网络配置 OVN-Kubernetes，如下例所示：

指定混合网络配置

```
apiVersion: operator.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  defaultNetwork:
    ovnKubernetesConfig:
      hybridOverlayConfig:
        hybridClusterNetwork: ❶
        - cidr: 10.132.0.0/14
          hostPrefix: 23
        hybridOverlayVXLANPort: 9898 ❷
```

- ❶ 指定用于额外覆盖网络上节点的 CIDR 配置。`hybridClusterNetwork` CIDR 无法与 `clusterNetwork` CIDR 重叠。
- ❷ 为额外覆盖网络指定自定义 VXLAN 端口。这是在 vSphere 上安装的集群中运行 Windows 节点所需要的，且不得为任何其他云供应商配置。自定义端口可以是除默认 4789 端口外的任何打开的端口。有关此要求的更多信息，请参阅 Microsoft 文档中的 [Pod 到主机间的 pod 连接性](#)。

- 保存 `cluster-network-03-config.yml` 文件，再退出文本编辑器。
- 可选：备份 `manifests/cluster-network-03-config.yml` 文件。创建集群时，安装程序会删除 `manifests/` 目录。

完成所有进一步的安装配置，然后创建集群。安装过程完成后会启用 Hybrid 网络。

14.12.2. 其他资源

- 了解 Windows 容器工作负载
- 启用 Windows 容器工作负载

- [使用自定义网络在 AWS 上安装集群](#)
- [使用网络自定义在 Azure 上安装集群](#)

第 15 章 配置路由

15.1. 路由配置

15.1.1. 创建基于 HTTP 的路由

路由允许您通过公共 URL 托管您的应用。根据应用的网络安全配置，它可以安全或不受保护。基于 HTTP 的路由是一种不安全的路由，使用基本的 HTTP 路由协议，并在不安全的应用端口上公开服务。

以下流程描述了如何使用 **hello-openshift** 应用创建到 Web 应用的简单基于 HTTP 的路由。

先决条件

- 已安装 OpenShift CLI (**oc**)。
- 以管理员身份登录。
- 您有一个 Web 应用，它公开了侦听端口上流量的端口和 TCP 端点。

流程

1. 运行以下命令，创建名为 **hello-openshift** 的项目：

```
$ oc new-project hello-openshift
```

2. 运行以下命令在项目中创建 pod：

```
$ oc create -f https://raw.githubusercontent.com/openshift/origin/master/examples/hello-openshift/hello-pod.json
```

3. 运行以下命令，创建一个名为 **hello-openshift** 的服务：

```
$ oc expose pod/hello-openshift
```

4. 运行以下命令，创建到 **hello-openshift** 应用的不安全路由：

```
$ oc expose svc hello-openshift
```

如果您检查生成的 **Route** 资源，它应该类似于如下：

创建的不安全路由的 YAML 定义：

```
apiVersion: route.openshift.io/v1
kind: Route
metadata:
  name: hello-openshift
spec:
  host: hello-openshift-hello-openshift.<Ingress_Domain> 1
  port:
    targetPort: 8080
```

```
to:
  kind: Service
  name: hello-openshift
```

- 1 **<Ingress_Domain>** 是默认的入口域名。



注意

要显示默认入口域，请运行以下命令：

```
$ oc get ingresses.config/cluster -o jsonpath={.spec.domain}
```

15.1.2. 配置路由超时

如果您的服务需要低超时（满足服务级别可用性 (SLA) 目的）或高超时（具有慢速后端的情况），您可以为现有路由配置默认超时。

先决条件

- 您需要在运行的集群中部署了 Ingress Controller。

流程

1. 使用 **oc annotate** 命令，为路由添加超时：

```
$ oc annotate route <route_name> \
  --overwrite haproxy.router.openshift.io/timeout=<timeout><time_unit> 1
```

- 1 支持的时间单位是微秒 (us)、毫秒 (ms)、秒钟 (s)、分钟 (m)、小时 (h)、或天 (d)。

以下示例在名为 **myroute** 的路由上设置两秒的超时：

```
$ oc annotate route myroute --overwrite haproxy.router.openshift.io/timeout=2s
```

15.1.3. 启用 HTTP 严格传输安全性

HTTP 严格传输安全性 (HSTS) 策略是一种安全增强，可确保主机上只允许 HTTPS 流量。所有 HTTP 请求都会默认丢弃。这可用于确保与网站安全交互，或提供安全应用程序让用户受益。

当 HSTS 启用时，HSTS 会添加一个 Strict Transport Security 标头到站点的 HTTPS 响应。您可以在要重定向的路由中使用 **insecureEdgeTerminationPolicy** 值，以将 HTTP 发送到 HTTPS。但是，当启用 HSTS 时，客户端会在发送请求前将所有来自 HTTP URL 的请求更改为 HTTPS，从而消除对重定向的需求。客户端不需要支持此功能，而且也可通过设置 **max-age=0** 来禁用。



重要

HSTS 仅适用于安全路由（边缘终止或重新加密）。其配置在 HTTP 或传递路由上无效。

流程

- 要在路由上启用 HSTS，请将 `haproxy.router.openshift.io/hsts_header` 值添加到边缘终止或重新加密路由：

```
apiVersion: v1
kind: Route
metadata:
  annotations:
    haproxy.router.openshift.io/hsts_header: max-age=31536000;includeSubDomains;preload
```

1 2 3

- 1 **max-age** 是唯一的必要参数。它会测量 HSTS 策略生效的时间长度，以秒为单位。每当从主机收到含有 HSTS 标头的响应时，客户端会更新 **max-age**。如果 **max-age** 超时，客户端会丢弃该策略。
- 2 **includeSubDomains** 是可选的。含有此参数时，它会告知客户端应像主机一样对待主机上的所有子域。
- 3 **preload** 是可选的。当 **max-age** 大于 0 时，在 `haproxy.router.openshift.io/hsts_header` 中包含 **preload** 会使外部服务将这个站点包括在 HSTS 预加载列表中。例如，Google 等站点可以构造设有 **preload** 的站点的列表。浏览器可以使用这些列表来决定哪些站点可通过 HTTPS 进行通信，然后再与站点交互。如果没有设置 **preload**，浏览器必须通过 HTTPS 与站点交互才能获取该标头。

15.1.4. 吞吐量问题错误排解

有时，通过 OpenShift Container Platform 部署的应用程序可能会导致网络吞吐量问题，如特定服务间的延迟异常高。

如果 pod 日志未能揭示造成问题的原因，请使用以下方法分析性能问题：

- 使用 ping 或 `tcpdump` 等数据包分析器，分析 pod 与其节点之间的流量。例如，在每个 pod 上运行 `tcpdump` 工具，同时重现导致问题的行为。检查两端的捕获信息，以便比较发送和接收时间戳来分析与 pod 往来的流量的延迟。如果节点接口被其他 pod、存储设备或者数据平面的流量过载，则 OpenShift Container Platform 中可能会出现延迟。

```
$ tcpdump -s 0 -i any -w /tmp/dump.pcap host <podip 1> && host <podip 2> 1
```

- 1 **podip** 是 pod 的 IP 地址。运行 `oc get pod <pod_name> -o wide` 命令来获取 pod 的 IP 地址。

`tcpdump` 在 `/tmp/dump.pcap` 中生成一个包含这两个 pod 间所有流量的文件。最好在运行分析器后立即重现问题，并在问题重现完成后马上停止分析器，从而尽量减小文件的大小。您还可以通过以下命令，在节点之间运行数据包分析器（从考量范围中剔除 SDN）：

```
$ tcpdump -s 0 -i any -w /tmp/dump.pcap port 4789
```

- 使用 `iperf` 等带宽测量工具来测量数据流吞吐量和 UDP 吞吐量。先从 pod 运行该工具，再从节点运行，以此来查找瓶颈。
 - 如需有关安装和使用 `iperf` 的信息，请参阅此[红帽解决方案](#)。

15.1.5. 使用 Cookie 来保持路由有状态性

OpenShift Container Platform 提供粘性会话，通过确保所有流量都到达同一端点来实现有状态应用程序流量。但是，如果端点 pod 以重启、扩展或更改配置的方式被终止，这种有状态性可能会消失。

OpenShift Container Platform 可以使用 Cookie 来配置会话持久性。Ingress Controller 选择一个端点来处理任何用户请求，并为会话创建一个 Cookie。Cookie 在响应请求时返回，用户则通过会话中的下一请求发回 Cookie。Cookie 告知 Ingress Controller 哪个端点正在处理会话，确保客户端请求使用这个 Cookie 使请求路由到同一个 pod。



注意

Cookie 无法在直通路由上设置，因为无法看到 HTTP 流量。相反，数字根据源 IP 地址计算，后者决定了后端。

如果后端有变化，流量可以定向到错误的服务器，使其更少粘性。如果您使用隐藏源 IP 的负载均衡器，则会为所有连接设置相同的数字，并将流量发送到同一 pod。

15.1.5.1. 使用 Cookie 标注路由

您可以设置 Cookie 名称来覆盖为路由自动生成的默认名称。这样，接收路由流量的应用程序就能知道 Cookie 名称。通过删除 Cookie，它可以强制下一请求重新选择端点。因此，如果服务器过载，它会尝试从客户端中删除请求并重新分发它们。

流程

1. 使用指定的 Cookie 名称标注路由：

```
$ oc annotate route <route_name> router.openshift.io/cookie_name="<cookie_name>"
```

其中：

<route_name>

指定路由的名称。

<cookie_name>

指定 Cookie 的名称。

例如，使用 cookie 名称 **my_cookie** 标注路由 **my_route**：

```
$ oc annotate route my_route router.openshift.io/cookie_name="my_cookie"
```

2. 在变量中捕获路由主机名：

```
$ ROUTE_NAME=$(oc get route <route_name> -o jsonpath='{.spec.host}')
```

其中：

<route_name>

指定路由的名称。

3. 保存 cookie，然后访问路由：

```
$ curl $ROUTE_NAME -k -c /tmp/cookie_jar
```

使用上一个命令在连接到路由时保存的 cookie：

```
$ curl $ROUTE_NAME -k -b /tmp/cookie_jar
```

15.1.6. 基于路径的路由

基于路径的路由指定了一个路径组件，可以与 URL 进行比较，该 URL 需要基于 HTTP 的路由流量。因此，可以使用同一主机名提供多个路由，每个主机名都有不同的路径。路由器应该匹配基于最具体路径的路由。不过，这还取决于路由器的实现。

下表显示了路由及其可访问性示例：

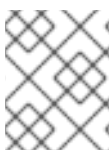
表 15.1. 路由可用性

Route	当比较到	可访问
<i>www.example.com/test</i>	<i>www.example.com/test</i>	是
	<i>www.example.com</i>	否
<i>www.example.com/test</i> 和 <i>www.example.com</i>	<i>www.example.com/test</i>	是
	<i>www.example.com</i>	是
<i>www.example.com</i>	<i>www.example.com/text</i>	yes（由主机匹配，而不是路由）
	<i>www.example.com</i>	是

带有路径的未安全路由

```
apiVersion: v1
kind: Route
metadata:
  name: route-unsecured
spec:
  host: www.example.com
  path: "/test" ❶
  to:
    kind: Service
    name: service-name
```

❶ 该路径是基于路径的路由的唯一添加属性。



注意

使用 passthrough TLS 时，基于路径的路由不可用，因为路由器不会在这种情况下终止 TLS，且无法读取请求的内容。

15.1.7. 特定于路由的注解

Ingress Controller 可以为它公开的所有路由设置默认选项。单个路由可以通过在其注解中提供特定配置来覆盖这些默认设置。红帽不支持在 Operator 管理的路由中添加路由注解。



重要

要创建带有多个源 IP 或子网的白名单，请使用以空格分隔的列表。任何其他限定类型会导致忽略列表，而不发出警告或错误消息。

表 15.2. 路由注解

变量	描述	默认的环境变量
<code>haproxy.router.openshift.io/balance</code>	设置负载均衡算法。可用选项包括 source 、 roundrobin 和 leastconn 。	passthrough 路由 使用 ROUTER_TCP_BALANCE_SCHEME 。否则，使用 ROUTER_LOAD_BALANCE_algorithm 。
<code>haproxy.router.openshift.io/disable_cookies</code>	禁用使用 cookie 来跟踪相关连接。如果设置为 true 或 TRUE ，则使用均衡算法来选择每个传入 HTTP 请求的后端服务连接。	
<code>router.openshift.io/cookie_name</code>	指定一个可选的、用于此路由的 cookie。名称只能包含大写字母和小写字母、数字、“_”和“-”。默认为路由的内部密钥进行哈希处理。	
<code>haproxy.router.openshift.io/pod-concurrent-connections</code>	设置路由器支持的 pod 允许的最大连接数。 注：如果有多个 pod，每个 pod 都有这些数量的连接。如果有多个路由器，它们之间没有协调关系，每个路由器都可能会多次连接。如果没有设置，或者将其设定为 0，则没有限制。	
<code>haproxy.router.openshift.io/rate-limit-connections</code>	设置 true 或 TRUE 可启用通过每个路由特定后端上的粘滞位来实现的速率限制功能。 注：使用此注解可提供基本保护，防止分布式拒绝服务 (DDoS) 攻击。	
<code>haproxy.router.openshift.io/rate-limit-connections.concurrent-tcp</code>	限制通过同一源 IP 地址进行的并发 TCP 连接数。它接受一个数字值。 注：使用此注解可提供基本保护，防止分布式拒绝服务 (DDoS) 攻击。	

变量	描述	默认的环境变量
haproxy.router.openshift.io/rate-limit-connections.rate-http	限制具有相同源 IP 地址的客户端可以发出 HTTP 请求的速率。它接受一个数字值。 注：使用此注解可提供基本保护，防止分布式拒绝服务 (DDoS) 攻击。	
haproxy.router.openshift.io/rate-limit-connections.rate-tcp	限制具有相同源 IP 地址的客户端可以进行 TCP 连接的速率。它接受一个数字值。 注：使用此注解可提供基本保护，防止分布式拒绝服务 (DDoS) 攻击。	
haproxy.router.openshift.io/timeout	为路由设定服务器端超时。 (TimeUnits)	ROUTER_DEFAULT_SERVER_TIMEOUT
haproxy.router.openshift.io/timeout-tunnel	这个超时适用于隧道连接，如 WebSocket over cleartext、edge、reencrypt 或 passthrough 路由。使用 cleartext、边缘或 reencrypt 路由类型时，此注解会作为带有现有超时值的超时隧道应用。对于 passthrough 路由类型，注解优先于任何设定的现有超时值。	ROUTER_DEFAULT_TUNNEL_TIMEOUT
ingresses.config/cluster ingress.operator.openshift.io/hard-stop-after	您可以设置 IngressController 或 ingress 配置。此注释重新部署路由器并将 HA 代理配置为发出 haproxy hard-stop-after global 选项，该选项定义执行清洁软停止的最长时间。	ROUTER_HARD_STOP_AFTER
router.openshift.io/haproxy.health.check.interval	为后端健康检查设定间隔。 (TimeUnits)	ROUTER_BACKEND_CHECK_INTERVAL
haproxy.router.openshift.io/ip_whitelist	为路由设置白名单。白名单是以空格分开的 IP 地址和 CIDR 范围列表，用来代表批准的源地址。来自白名单以外的 IP 地址的请求会被丢弃。 白名单中允许的最大 IP 地址和 CIDR 范围数为 61。	

变量	描述	默认的环境变量
<code>haproxy.router.openshift.io/https_header</code>	为 edge terminated 或 re-encrypt 路由设置 Strict-Transport-Security 标头。	
<code>haproxy.router.openshift.io/log-send-hostname</code>	在 Syslog 标头中设置 hostname 字段。使用系统的主机名。如果路由器启用了任何 Ingress API 日志记录方法（如 sidecar 或 Syslog 工具），则默认启用 log-send-hostname 。	
<code>haproxy.router.openshift.io/rewrite-target</code>	在后端中设置请求的重写路径。	
<code>router.openshift.io/cookie-same-site</code>	<p>设置一个值来限制 cookies。数值是：</p> <p>Lax : cookies 在访问的站点和第三方站点间进行传输。</p> <p>Strict : cookies 仅限于访问的站点。</p> <p>None : cookies 仅限于指定的站点。</p> <p>这个值仅适用于重新加密和边缘路由。如需更多信息，请参阅 SameSite cookies 文档。</p>	
<code>haproxy.router.openshift.io/set-forwarded-headers</code>	<p>设置用于处理每个路由的 Forwarded 和 X-Forwarded-For HTTP 标头的策略。数值是：</p> <p>Append 附加标头，保留任何现有的标头。这是默认值。</p> <p>replace : 设置标头，删除任何现有的标头。</p> <p>Never : 不设置标头，而是保留任何现有的标头。</p> <p>if-none : 如果没有设置标头，则设置它。</p>	ROUTER_SET_FORWARDED_HEADERS



注意

环境变量不能编辑。

路由器超时变量

TimeUnits 由一个数字及一个时间单位表示：**us** *(microseconds), **ms** (毫秒, 默认)、**s** (秒)、**m** (分钟)、**h** *(小时)、**d** (天)。

正则表达式是：`[1-9][0-9]*(us|ms|s|m|h|d)`。

变量	默认	描述
ROUTER_BACKEND_CHECK_INTERVAL	5000ms	后端上后续存活度检查之间的时长。
ROUTER_CLIENT_FIN_TIMEOUT	1s	控制连接到路由的客户端的 TCP FIN 超时周期。如果发送到关闭连接的 FIN 在给定时间内没有回答，HAProxy 会关闭连接。如果设置为较低值，并且在路由器上使用较少的资源，则这不会产生任何损害。
ROUTER_DEFAULT_CLIENT_TIMEOUT	30s	客户端必须确认或发送数据的时长。
ROUTER_DEFAULT_CONNECT_TIMEOUT	5s	最长连接时间。
ROUTER_DEFAULT_SERVER_FIN_TIMEOUT	1s	控制路由器到支持路由的 pod 的 TCP FIN 超时。
ROUTER_DEFAULT_SERVER_TIMEOUT	30s	服务器必须确认或发送数据的时长。
ROUTER_DEFAULT_TUNNEL_TIMEOUT	1h	TCP 或 WebSocket 连接保持打开的时长。每当 HAProxy 重新加载时，这个超时期限都会重置。
ROUTER_SLOWLORIS_HTTP_KEEPALIVE	300s	<p>设置等待出现新 HTTP 请求的最长时间。如果设置得太低，可能会导致浏览器和应用程序无法期望较小的 keepalive 值。</p> <p>某些有效的超时值可以是某些变量的总和，而不是特定的预期超时。例如：ROUTER_SLOWLORIS_HTTP_KEEPALIVE 调整 timeout http-keep-alive。默认情况下，它设置为 300s，但 HAProxy 也会在 tcp-request inspect-delay 上等待，它被设置为 5s。在这种情况下，整个超时时间将是 300s 加 5s。</p>
ROUTER_SLOWLORIS_TIMEOUT	10s	HTTP 请求传输可以花费的时间长度。
RELOAD_INTERVAL	5s	允许路由器至少执行重新加载和接受新更改的频率。

变量	默认	描述
ROUTER_METRICS_HAPROXY_TIMEOUT	5s	收集 HAProxy 指标的超时时间。

设置自定义超时的路由

```
apiVersion: v1
kind: Route
metadata:
  annotations:
    haproxy.router.openshift.io/timeout: 5500ms ❶
...
```

- ❶ 使用 HAProxy 支持的时间单位 (**us, ms, s, m, h, d**) 指定新的超时时间。如果没有提供时间单位, **ms** 会被默认使用。



注意

如果为 passthrough 路由设置的服务器端的超时值太低, 则会导致 WebSocket 连接在那个路由上经常出现超时的情况。

只允许一个特定 IP 地址的路由

```
metadata:
  annotations:
    haproxy.router.openshift.io/ip_whitelist: 192.168.1.10
```

允许多个 IP 地址的路由

```
metadata:
  annotations:
    haproxy.router.openshift.io/ip_whitelist: 192.168.1.10 192.168.1.11 192.168.1.12
```

允许 IP 地址 CIDR 网络的路由

```
metadata:
  annotations:
    haproxy.router.openshift.io/ip_whitelist: 192.168.1.0/24
```

允许 IP 地址和 IP 地址 CIDR 网络的路由

```
metadata:
  annotations:
    haproxy.router.openshift.io/ip_whitelist: 180.5.61.153 192.168.1.0/24 10.0.0.0/8
```

指定重写对象的路由

```
apiVersion: v1
```

```

kind: Route
metadata:
  annotations:
    haproxy.router.openshift.io/rewrite-target: / ❶
...

```

❶ 将 / 设为后端请求的重写路径。

在路由上设置 `haproxy.router.openshift.io/rewrite-target` 注解，指定 Ingress Controller 在将请求转发到后端应用程序之前，应该使用此路由在 HTTP 请求中重写路径。与 `spec.path` 中指定的路径匹配的请求路径部分将替换为注解中指定的重写对象。

下表提供了在 `spec.path`、请求路径和重写对象的各种组合中重写行为的路径示例。

表 15.3. rewrite-target 示例：

Route.spec.path	请求路径	重写目标	转发请求路径
/foo	/foo	/	/
/foo	/foo/	/	/
/foo	/foo/bar	/	/bar
/foo	/foo/bar/	/	/bar/
/foo	/foo	/bar	/bar
/foo	/foo/	/bar	/bar/
/foo	/foo/bar	/baz	/baz/bar
/foo	/foo/bar/	/baz	/baz/bar/
/foo/	/foo	/	不适用（请求路径不匹配路由路径）
/foo/	/foo/	/	/
/foo/	/foo/bar	/	/bar

15.1.8. 配置路由准入策略

管理员和应用程序开发人员可在多个命名空间中运行具有相同域名的应用程序。这是针对多个团队开发的、在同一个主机名上公开的微服务的机构。



警告

只有在命名空间有信任的集群才会启用跨命名空间之间的声明，否则恶意用户可能会接管主机名。因此，默认的准入策略不允许在命名空间声明主机名。

先决条件

- 必须具有集群管理员权限。

流程

- 使用以下命令编辑 **ingresscontroller** 资源变量的 **spec**. `routeAdmission` 字段：

```
$ oc -n openshift-ingress-operator patch ingresscontroller/default --patch '{"spec": {"routeAdmission":{"namespaceOwnership":"InterNamespaceAllowed"}}}' --type=merge
```

Ingress 控制器配置参数

```
spec:
  routeAdmission:
    namespaceOwnership: InterNamespaceAllowed
  ...
```

15.1.9. 通过 Ingress 对象创建路由

一些生态系统组件与 Ingress 资源集成，但与路由资源不集成。要涵盖此问题单，OpenShift Container Platform 会在创建 Ingress 对象时自动创建受管路由对象。当相应 Ingress 对象被删除时，这些路由对象会被删除。

流程

1. 在 OpenShift Container Platform 控制台中或通过 **oc create** 命令来定义 Ingress 对象：

Ingress 的 YAML 定义

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: frontend
  annotations:
    route.openshift.io/termination: "reencrypt" 1
spec:
  rules:
  - host: www.example.com
    http:
      paths:
      - backend:
          service:
            name: frontend
```

```

    port:
      number: 443
    path: /
    pathType: Prefix
  tls:
  - hosts:
    - www.example.com
    secretName: example-com-tls-certificate

```

1 `route.openshift.io/termination` 注解可用于配置 `Route` 的 `spec.tls.termination` 字段，因为 `Ingress` 没有此字段。可接受的值为 `edge`、`passthrough` 和 `reencrypt`。所有其他值都会被静默忽略。当注解值未设置时，`edge` 是默认路由。模板文件中必须定义 TLS 证书详细信息，才能实现默认的边缘路由。

- a. 如果您在 `route.openshift.io/termination` 注解中指定 `passthrough` 值，在 `spec` 中将 `path` 设置为 `"`，将 `pathType` 设置为 `ImplementationSpecific`：

```

spec:
  rules:
  - host: www.example.com
    http:
      paths:
      - path: ""
        pathType: ImplementationSpecific
      backend:
        service:
          name: frontend
          port:
            number: 443

```

```
$ oc apply -f ingress.yaml
```

2. 列出您的路由：

```
$ oc get routes
```

结果包括一个自动生成的路由，其名称以 `frontend-` 开头：

NAME	HOST/PORT	PATH	SERVICES	PORT	TERMINATION
WILDCARD					
frontend-gnztq	www.example.com		frontend	443	reencrypt/Redirect None

如果您检查这个路由，它会类似于：

自动生成的路由的 YAML 定义

```

apiVersion: route.openshift.io/v1
kind: Route
metadata:
  name: frontend-gnztq
  ownerReferences:
  - apiVersion: networking.k8s.io/v1
    controller: true

```

```

kind: Ingress
name: frontend
uid: 4e6c59cc-704d-4f44-b390-617d879033b6
spec:
  host: www.example.com
  path: /
  port:
    targetPort: https
  tls:
    certificate: |
      -----BEGIN CERTIFICATE-----
      [...]
      -----END CERTIFICATE-----
    insecureEdgeTerminationPolicy: Redirect
  key: |
    -----BEGIN RSA PRIVATE KEY-----
    [...]
    -----END RSA PRIVATE KEY-----
  termination: reencrypt
to:
  kind: Service
  name: frontend

```

15.2. 安全路由

安全路由提供以下几种 TLS 终止功能来为客户端提供证书。以下小节介绍了如何使用自定义证书创建重新加密、边缘和透传路由。



重要

如果您在 Microsoft Azure 中创建通过公共端点的路由，则资源名称会受到限制。您不能创建使用某些词语的资源。如需 Azure 限制词语的列表，请参阅 Azure 文档中的[解决预留资源名称错误](#)。

15.2.1. 使用自定义证书创建重新加密路由

您可以通过 **oc create route** 命令，使用重新加密 TLS 终止和自定义证书配置安全路由。

先决条件

- 您必须在 PEM 编码文件中有一个证书/密钥对，其中的证书对路由主机有效。
- 您可以在 PEM 编码文件中有一个单独的 CA 证书来补全证书链。
- 您必须在 PEM 编码文件中有单独的目标 CA 证书。
- 您必须具有要公开的服务。



注意

不支持密码保护的密钥文件。要从密钥文件中删除密码，使用以下命令：

```
$ openssl rsa -in password_protected_tls.key -out tls.key
```

流程

此流程使用自定义证书和重新加密 TLS 终止创建 **Route** 资源。以下步骤假定证书/密钥对位于当前工作目录下的 **tls.crt** 和 **tls.key** 文件中。您还必须指定一个目标 CA 证书，使 Ingress Controller 信任服务的证书。您也可以根据需要指定 CA 证书来补全证书链。替换 **tls.crt**、**tls.key**、**ca.crt** 和（可选）**ca.crt** 的实际路径名称。替换您要为 **frontend** 公开的 **Service** 资源的名称。使用适当的主机名替换 **www.example.com**。

- 使用重新加密 TLS 终止和自定义证书，创建安全 **Route** 资源：

```
$ oc create route reencrypt --service=frontend --cert=tls.crt --key=tls.key --dest-ca-cert=destca.crt --ca-cert=ca.crt --hostname=www.example.com
```

如果您检查生成的 **Route** 资源，它应该类似于如下：

安全路由 YAML 定义

```
apiVersion: v1
kind: Route
metadata:
  name: frontend
spec:
  host: www.example.com
  to:
    kind: Service
    name: frontend
  tls:
    termination: reencrypt
    key: |-
      -----BEGIN PRIVATE KEY-----
      [...]
      -----END PRIVATE KEY-----
    certificate: |-
      -----BEGIN CERTIFICATE-----
      [...]
      -----END CERTIFICATE-----
    caCertificate: |-
      -----BEGIN CERTIFICATE-----
      [...]
      -----END CERTIFICATE-----
    destinationCACertificate: |-
      -----BEGIN CERTIFICATE-----
      [...]
      -----END CERTIFICATE-----
```

如需了解更多选项，请参阅 **oc create route reencrypt --help**。

15.2.2. 使用自定义证书创建边缘路由

您可以通过 **oc create route** 命令，使用边缘 TLS 终止和自定义证书配置安全路由。使用边缘路由时，Ingress Controller 在将流量转发到目标 pod 之前终止 TLS 加密。该路由指定了 Ingress Controller 用于路由的 TLS 证书和密钥。

先决条件

- 您必须在 PEM 编码文件中有一个证书/密钥对，其中的证书对路由主机有效。
- 您可以在 PEM 编码文件中有一个单独的 CA 证书来补全证书链。
- 您必须具有要公开的服务。



注意

不支持密码保护的密钥文件。要从密钥文件中删除密码，使用以下命令：

```
$ openssl rsa -in password_protected_tls.key -out tls.key
```

流程

此流程使用自定义证书和边缘 TLS 终止创建 **Route** 资源。以下步骤假定证书/密钥对位于当前工作目录下的 **tls.crt** 和 **tls.key** 文件中。您也可以根据需要指定 CA 证书来补全证书链。替换 **tls.crt**、**tls.key** 和（可选）**ca.crt** 的实际路径名称。替换您要为 **frontend** 公开的服务名称。使用适当的主机名替换 **www.example.com**。

- 使用边缘 TLS 终止和自定义证书，创建安全 **Route** 资源：

```
$ oc create route edge --service=frontend --cert=tls.crt --key=tls.key --ca-cert=ca.crt --hostname=www.example.com
```

如果您检查生成的 **Route** 资源，它应该类似于如下：

安全路由 YAML 定义

```
apiVersion: v1
kind: Route
metadata:
  name: frontend
spec:
  host: www.example.com
  to:
    kind: Service
    name: frontend
  tls:
    termination: edge
    key: |-
      -----BEGIN PRIVATE KEY-----
      [...]
      -----END PRIVATE KEY-----
    certificate: |-
      -----BEGIN CERTIFICATE-----
      [...]
      -----END CERTIFICATE-----
    caCertificate: |-
      -----BEGIN CERTIFICATE-----
      [...]
      -----END CERTIFICATE-----
```

如需了解更多选项，请参阅 **oc create route edge --help**。

15.2.3. 创建 passthrough 路由

您可以使用 `oc create route passthrough` 命令使用 passthrough 终止配置安全路由。如果 passthrough 终止，加密的流量会直接发送到目的地，而路由器不会提供 TLS 终止。因此，路由不需要密钥或证书。

先决条件

- 您必须具有要公开的服务。

流程

- 创建 **Route** 资源：

```
$ oc create route passthrough route-passthrough-secured --service=frontend --port=8080
```

如果您检查生成的 **Route** 资源，它应该类似于如下：

使用 Passthrough 终止的安全路由

```
apiVersion: v1
kind: Route
metadata:
  name: route-passthrough-secured 1
spec:
  host: www.example.com
  port:
    targetPort: 8080
  tls:
    termination: passthrough 2
    insecureEdgeTerminationPolicy: None 3
  to:
    kind: Service
    name: frontend
```

- 1 对象的名称，长度限于 63 个字符。
- 2 `termination` 字段设置为 `passthrough`。这是唯一需要 `tls` 的字段。
- 3 可选的 `insecureEdgeTerminationPolicy`。禁用后唯一有效的值是 `None`、`Redirect` 或为空。

目标 pod 负责为端点上的流量提供证书。目前，这是唯一支持需要客户端证书的方法，也称双向验证。

第 16 章 配置集群入口流量

16.1. 集群入口流量配置概述

OpenShift Container Platform 提供了以下从集群外部与集群中运行的服务进行通信的方法。

建议采用以下方法，它们按顺序或首选程度排列：

- 如果您有 HTTP/HTTPS，请使用 Ingress Controller。
- 如果您有 HTTPS 之外的 TLS 加密协议，比如对于使用 SNI 标头的 TLS，请使用 Ingress Controller。
- 否则，请使用负载均衡器、外部 IP 或 **NodePort**。

方法	用途
使用 Ingress Controller	允许访问 HTTP/HTTPS 流量和 HTTPS 以外的 TLS 加密协议（例如，使用 SNI 标头的 TLS）。
使用负载均衡器服务自动分配外部 IP	允许流量通过从池分配的 IP 地址传到非标准端口。
手动将外部 IP 分配给服务	允许流量通过特定的 IP 地址传到非标准端口。
配置一个 NodePort	在集群中的所有节点上公开某一服务。

16.2. 为服务配置 EXTERNALIP

作为集群管理员，您可以指定可向集群中服务发送流量的集群外部 IP 地址块。

这个功能通常最适用于在裸机硬件上安装的集群。

16.2.1. 先决条件

- 您的网络基础架构必须将外部 IP 地址的流量路由到集群。

16.2.2. 关于 ExternalIP

对于非云环境，OpenShift Container Platform 支持通过 **ExternalIP** 工具将外部 IP 地址分配给 **Service** 对象的 **spec.externalIPs[]** 字段。通过设置此字段，OpenShift Container Platform 为服务分配额外的虚拟 IP 地址。IP 地址可以在为集群定义的服务网络之外。配置了 ExternalIP 功能的服务与具有 **type=NodePort** 的服务类似，允许您将流量定向到本地节点以进行负载均衡。

您必须配置网络基础架构，以确保您定义的外部 IP 地址块路由到集群。

OpenShift Container Platform 通过添加以下功能来扩展 Kubernetes 中的 ExternalIP 功能：

- 通过可配置策略对用户外部 IP 地址的限制
- 根据请求自动将外部 IP 地址分配给服务



警告

默认情况下禁用，使用 ExternalIP 功能可能会造成安全隐患，因为集群内到一个外部 IP 地址的流量会定向到那个服务。这可让集群用户拦截用于外部资源的敏感流量。



重要

这个功能只在非云部署中被支持。对于云部署，使用负载均衡器服务自动部署云负载均衡器，以服务端点为目标。

您可以使用以下方法分配外部 IP 地址：

自动分配一个外部 IP

当创建了一个带有 `spec.type=LoadBalancer` 设置的 **Service** 对象时，OpenShift Container Platform 会从 `autoAssignCIDRs` CIDR 块中自动为 `spec.externalIPs[]` 分配一个 IP 地址。在本例中，OpenShift Container Platform 实现了负载均衡器服务类型的非云版本，并为服务分配 IP 地址。默认情况下，自动分配被禁用，且必须由集群管理员配置，如以下部分所述。

手动分配外部 IP

OpenShift Container Platform 在创建 **Service** 对象时使用分配给 `spec.externalIPs[]` 数组的 IP 地址。您不能指定已经被其他服务使用的 IP 地址。

16.2.2.1. 配置 ExternalIP

在 OpenShift Container Platform 中使用外部 IP 地址取决于名为 `cluster` 的 `Network.config.openshift.io` CR 中的以下字段：

- `spec.externalIP.autoAssignCIDRs` 定义了一个负载均衡器在为服务选择外部 IP 地址时使用的 IP 地址块。OpenShift Container Platform 只支持单个 IP 地址块进行自动分配。当手工为服务分配 ExternalIPs 时，这比管理有限共享 IP 地址的端口空间更简单。如果启用了自动分配，则会为带有 `spec.type=LoadBalancer` 的 **Service** 对象分配一个外部 IP 地址。
- 在手动指定 IP 地址时，`spec.externalIP.policy` 定义了允许的 IP 地址块。OpenShift Container Platform 不会将策略规则应用到 `spec.externalIP.autoAssignCIDRs` 定义的 IP 地址块。

如果路由正确，来自配置的外部 IP 地址块的外部流量可以通过服务公开的任何 TCP 或 UDP 端口访问服务端点。



重要

您必须确保分配的 IP 地址块在集群中的一个或多个节点上终止。

OpenShift Container Platform 支持自动和手动分配 IP 地址，并且保证每个地址都被分配到最多一个服务。这样可保证，无论由其他服务公开的端口是什么，每个服务都可以公开选择的端口。



注意

要使用 OpenShift Container Platform 中由 `autoAssignCIDRs` 定义的 IP 地址块，您必须为主机网络配置必要的 IP 地址分配和路由。

以下 YAML 描述了配置了外部 IP 地址的服务：

带有 `spec.externalIPs[]` 设置的示例 Service 对象

```
apiVersion: v1
kind: Service
metadata:
  name: http-service
spec:
  clusterIP: 172.30.163.110
  externalIPs:
  - 192.168.132.253
  externalTrafficPolicy: Cluster
  ports:
  - name: highport
    nodePort: 31903
    port: 30102
    protocol: TCP
    targetPort: 30102
  selector:
    app: web
  sessionAffinity: None
  type: LoadBalancer
status:
  loadBalancer:
    ingress:
    - ip: 192.168.132.253
```

16.2.2.2. 对外部 IP 地址分配的限制

作为集群管理员，您可以指定允许和拒绝的 IP 地址块。

限制只针对没有 `cluster-admin` 权限的用户。集群管理员始终可以将服务 `spec.externalIPs[]` 字段设置为任何 IP 地址。

您可以使用一个通过指定 `spec.ExternalIP.policy` 字段来定义的一个 `policy` 对象来配置 IP 地址策略。策略对象有以下内容：

```
{
  "policy": {
    "allowedCIDRs": [],
    "rejectedCIDRs": []
  }
}
```

在配置策略限制时，会应用以下规则：

- 如果设置了 `policy={}`，那么创建带有 `spec.ExternalIPs[]` 设置的 `Service` 对象将失败。这是 OpenShift Container Platform 的默认设置。这与设置 `policy=null` 的行为相同。
- 如果设置了 `policy`，并且设置了 `policy.allowedCIDRs[]` 或 `policy.rejectedCIDRs[]`，则应用以下规则：
 - 如果同时设置了 `allowedCIDRs[]` 和 `rejectedCIDRs[]`，则 `allowedCIDRs[]` 的设置高于 `rejectedCIDRs[]`。

- 如果设置了 `allowedCIDRs[]`，只有在允许指定的 IP 地址时，创建带有 `spec.ExternalIPs[]` 的 `Service` 对象才能成功。
- 如果设置了 `rejectedCIDRs[]`，只有在指定的 IP 地址未被拒绝时，创建带有 `spec.ExternalIPs[]` 的 `Service` 对象才能成功。

16.2.2.3. 策略对象示例

下面的例子演示了几个不同的策略配置。

- 在以下示例中，策略会防止 OpenShift Container Platform 使用指定的外部 IP 地址创建任何服务：

拒绝为 `Service` 对象 `spec.externalIPs[]` 指定的任何值的策略示例

```
apiVersion: config.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  externalIP:
    policy: {}
  ...
```

- 在以下示例中，设置了 `allowedCIDRs` 和 `rejectedCIDRs` 字段。

包括允许和拒绝 CIDR 块的策略示例

```
apiVersion: config.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  externalIP:
    policy:
      allowedCIDRs:
        - 172.16.66.10/23
      rejectedCIDRs:
        - 172.16.66.10/24
  ...
```

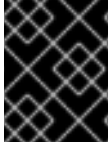
- 在以下示例中，`policy` 被设置为 `null`。如果设为 `null`，则通过输入 `oc get network.config.openshift.io -o yaml` 来检查配置对象时，`policy` 项不会出现在输出中。

允许为 `Service` 对象 `spec.externalIPs[]` 指定的任何值的示例策略

```
apiVersion: config.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  externalIP:
    policy: null
  ...
```

16.2.3. ExternalIP 地址块配置

ExternalIP 地址块的配置由名为 **cluster** 的网络自定义资源（CR）定义。Network CR 是 **config.openshift.io** API 组的一部分。



重要

在集群安装过程中，Cluster Version Operator（CVO）会自动创建一个名为 **cluster** 的网络 CR。不支持创建此类型的任何其他 CR 对象。

以下 YAML 描述了 ExternalIP 配置：

network.config.openshift.io CR 名为 cluster

```
apiVersion: config.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  externalIP:
    autoAssignCIDRs: [] 1
    policy: 2
    ...
```

- 1** 定义 CIDR 格式的 IP 地址块，可用于自动将外部 IP 地址分配给服务。只允许一个 IP 地址范围。
- 2** 定义手动为服务分配 IP 地址的限制。如果没有定义限制，则不允许在 **Service** 对象中指定 **spec.externalIP** 字段。默认情况下，不会定义任何限制。

以下 YAML 描述了 **policy** 小节的字段：

network.config.openshift.io policy 小节

```
policy:
  allowedCIDRs: [] 1
  rejectedCIDRs: [] 2
```

- 1** CIDR 格式允许的 IP 地址范围列表。
- 2** CIDR 格式拒绝的 IP 地址范围列表。

外部 IP 配置示例

以下示例中显示了外部 IP 地址池的一些可能配置：

- 以下 YAML 描述了启用自动分配外部 IP 地址的配置：

带有 spec.externalIP.autoAssignCIDRs 的配置示例

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

```
spec:
  ...
  externalIP:
    autoAssignCIDRs:
      - 192.168.132.254/29
```

- 以下 YAML 为允许的和被拒绝的 CIDR 范围配置策略规则：

带有 `spec.externalIP.policy` 的示例配置

```
apiVersion: config.openshift.io/v1
kind: Network
metadata:
  name: cluster
spec:
  ...
  externalIP:
    policy:
      allowedCIDRs:
        - 192.168.132.0/29
        - 192.168.132.8/29
      rejectedCIDRs:
        - 192.168.132.7/32
```

16.2.4. 为集群配置外部 IP 地址块

作为集群管理员，可以配置以下 ExternalIP 设置：

- OpenShift Container Platform 用来自动填充 **Service** 对象的 `spec.clusterIP` 字段的 ExternalIP 地址块。
- 用于限制可手动分配给 **Service** 对象的 `spec.clusterIP` 数组的 IP 地址的策略对象。

先决条件

- 安装 OpenShift CLI (**oc**)。
- 使用具有 **cluster-admin** 角色的用户访问集群。

流程

1. 可选：要显示当前的外部 IP 配置，请输入以下命令：

```
$ oc describe networks.config cluster
```

2. 要编辑配置，请输入以下命令：

```
$ oc edit networks.config cluster
```

3. 修改 ExternalIP 配置，如下例所示：

```
apiVersion: config.openshift.io/v1
kind: Network
metadata:
```



```

name: cluster
spec:
...
externalIP: 1
...

```

- 1 指定 **externalIP** 小节的配置。

4. 要确认更新的 ExternalIP 配置，请输入以下命令：

```
$ oc get networks.config cluster -o go-template='{{.spec.externalIP}}{\n}'
```

16.2.5. 后续步骤

- [为服务外部 IP 配置 ingress 集群流量](#)

16.3. 使用 INGRESS CONTROLLER 配置集群入口流量

OpenShift Container Platform 提供了从集群外部与集群中运行的服务进行通信的方法。此方法使用了 Ingress Controller。

16.3.1. 使用 Ingress Controller 和路由

Ingress Operator 管理 Ingress Controller 和通配符 DNS。

使用 Ingress Controller 是允许从外部访问 OpenShift Container Platform 集群的最常用方法。

Ingress Controller 配置为接受外部请求并根据配置的路由进行代理。这仅限于 HTTP、使用 SNI 的 HTTPS 以及使用 SNI 的 TLS，对于通过使用 SNI 的 TLS 工作的 Web 应用程序和服务而言已经足够。

与管理员合作将 Ingress Controller 配置为接受外部请求并根据配置的路由进行代理。

管理员可以创建通配符 DNS 条目，再设置 Ingress Controller。然后，您可以处理边缘 Ingress Controller，无需与管理员联系。

默认情况下，集群中的每个入口控制器可以接受集群中任何项目中创建的任何路由。

Ingress Controller：

- 默认有两个副本；即，它应该在两个 worker 节点上运行。
- 可以纵向扩张，以在更多节点上具有更多副本。



注意

这部分中的流程需要由集群管理员执行先决条件。

16.3.2. 先决条件

在开始以下流程前，管理员必须：

- 设置集群联网环境的外部端口，使请求能够到达集群。

- 确定至少有一个用户具有集群管理员角色。要将此角色添加到用户，请运行以下命令：

```
$ oc adm policy add-cluster-role-to-user cluster-admin username
```

- 有一个 OpenShift Container Platform 集群，其至少有一个 master 和至少一个节点，并且集群外有一个对集群具有网络访问权限的系统。此流程假设外部系统与集群位于同一个子网。不同子网上外部系统所需要的额外联网不在本主题的讨论范围内。

16.3.3. 创建项目和服务

如果您要公开的项目和服务尚不存在，请首先创建项目，再创建服务。

如果项目和服务都已存在，跳到公开服务以创建路由这一步。

先决条件

- 按照 **oc** CLI 并以一个集群管理员身份登陆。

流程

1. 运行 **oc new-project** 命令为您的服务创建一个新项目：

```
$ oc new-project myproject
```

2. 使用 **oc new-app** 命令创建服务：

```
$ oc new-app nodejs:12~https://github.com/sclorg/nodejs-ex.git
```

3. 要验证是否已创建该服务，请运行以下命令：

```
$ oc get svc -n myproject
```

输出示例

```
NAME      TYPE      CLUSTER-IP    EXTERNAL-IP  PORT(S)    AGE
nodejs-ex ClusterIP  172.30.197.157 <none>      8080/TCP   70s
```

默认情况下，新服务没有外部 IP 地址。

16.3.4. 通过创建路由公开服务

您可以使用 **oc expose** 命令，将服务公开为路由。

流程

公开服务：

1. 登录 OpenShift Container Platform。
2. 登录您想公开的服务所在的项目。

```
$ oc project myproject
```

- 运行 **oc expose service** 命令来公开路由：

```
$ oc expose service nodejs-ex
```

输出示例

```
route.route.openshift.io/nodejs-ex exposed
```

- 要验证服务是否已公开，您可以使用 cURL 等工具来确保可从集群外部访问该服务。

- 使用 **oc get route** 命令查找路由的主机名：

```
$ oc get route
```

输出示例

NAME	HOST/PORT	PATH	SERVICES	PORT	TERMINATION
WILDCARD					
nodejs-ex	nodejs-ex-myproject.example.com		nodejs-ex	8080-tcp	None

- 使用 cURL 检查主机是否响应 GET 请求：

```
$ curl --head nodejs-ex-myproject.example.com
```

输出示例

```
HTTP/1.1 200 OK
...
```

16.3.5. 通过路由标签（label）配置 Ingress Controller 分片

使用路由标签进行 Ingress Controller 分片，意味着 Ingress Controller 提供由路由选择器选择的任意命名空间中的所有路由。

在一组 Ingress Controller 之间平衡传入的流量负载时，以及在将流量隔离到特定 Ingress Controller 时，Ingress Controller 分片会很有用处。例如，A 公司的流量使用一个 Ingress Controller，B 公司的流量则使用另外一个 Ingress Controller。

流程

- 编辑 **router-internal.yaml** 文件：

```
# cat router-internal.yaml
apiVersion: v1
items:
- apiVersion: operator.openshift.io/v1
  kind: IngressController
  metadata:
    name: sharded
    namespace: openshift-ingress-operator
  spec:
    domain: <apps-sharded.basedomain.example.net>
```

```

nodePlacement:
  nodeSelector:
    matchLabels:
      node-role.kubernetes.io/worker: ""
routeSelector:
  matchLabels:
    type: sharded
status: {}
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""

```

- 应用 Ingress Controller **router-internal.yaml** 文件 :

```
# oc apply -f router-internal.yaml
```

Ingress Controller 选择具有 **type: sharded** 标签的任意命名空间中的路由。

16.3.6. 使用命名空间标签配置 Ingress Controller 分片

使用命名空间标签进行 Ingress Controller 分片，意味着 Ingress Controller 提供由命名空间选择器选择的任意命名空间中的所有路由。

在一组 Ingress Controller 之间平衡传入的流量负载时，以及在将流量隔离到特定 Ingress Controller 时，Ingress Controller 分片会很有用处。例如，A 公司的流量使用一个 Ingress Controller，B 公司的流量则使用另外一个 Ingress Controller。



警告

如果部署 Keepalived Ingress VIP，请不要为 **endpointPublishingStrategy** 参数部署一个值为 **HostNetwork** 的非默认 Ingress Controller。这样做可能会导致问题。将值 **NodePort** 而不是 **HostNetwork** 用于 **endpointPublishingStrategy**。

流程

- 编辑 **router-internal.yaml** 文件 :

```
# cat router-internal.yaml
```

输出示例

```

apiVersion: v1
items:
- apiVersion: operator.openshift.io/v1
  kind: IngressController
  metadata:
    name: sharded
    namespace: openshift-ingress-operator

```

```
spec:
  domain: <apps-sharded.basedomain.example.net>
  nodePlacement:
    nodeSelector:
      matchLabels:
        node-role.kubernetes.io/worker: ""
  namespaceSelector:
    matchLabels:
      type: sharded
  status: {}
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""
```

- 应用 Ingress Controller **router-internal.yaml** 文件：

```
# oc apply -f router-internal.yaml
```

Ingress Controller 选择由命名空间选择器选择的具有 **type: sharded** 标签的任意命名空间中的路由。

16.3.7. 其他资源

- Ingress Operator 管理通配符 DNS。如需更多信息，请参阅 [OpenShift Container Platform 中的 Ingress Operator](#)、[在裸机上安装集群](#)和[在 vSphere 上安装集群](#)。

16.4. 使用负载均衡器配置集群入口流量

OpenShift Container Platform 提供了从集群外部与集群中运行的服务进行通信的方法。此方法使用了负载均衡器。

16.4.1. 使用负载均衡器使流量进入集群

如果不需要具体的外部 IP 地址，您可以配置负载均衡器服务，以便从外部访问 OpenShift Container Platform 集群。

负载均衡器服务分配唯一 IP。负载均衡器有单一边缘路由器 IP，它可以是虚拟 IP (VIP)，但仍然是一台用于初始负载均衡的计算机。



注意

如果配置了池，则会在基础架构一级进行，而不是由集群管理员完成。



注意

这部分中的流程需要由集群管理员执行先决条件。

16.4.2. 先决条件

在开始以下流程前，管理员必须：

- 设置集群联网环境的外部端口，使请求能够到达集群。

- 确定至少有一个用户具有集群管理员角色。要将此角色添加到用户，请运行以下命令：

```
$ oc adm policy add-cluster-role-to-user cluster-admin username
```

- 有一个 OpenShift Container Platform 集群，其至少有一个 master 和至少一个节点，并且集群外有一个对集群具有网络访问权限的系统。此流程假设外部系统与集群位于同一个子网。不同子网上外部系统所需要的额外联网不在本主题的讨论范围内。

16.4.3. 创建项目和服务

如果您要公开的项目和服务尚不存在，请首先创建项目，再创建服务。

如果项目和服务都已存在，跳到公开服务以创建路由这一步。

先决条件

- 按照 **oc** CLI 并以一个集群管理员身份登陆。

流程

1. 运行 **oc new-project** 命令为您的服务创建一个新项目：

```
$ oc new-project myproject
```

2. 使用 **oc new-app** 命令创建服务：

```
$ oc new-app nodejs:12~https://github.com/sclorg/nodejs-ex.git
```

3. 要验证是否已创建该服务，请运行以下命令：

```
$ oc get svc -n myproject
```

输出示例

```
NAME      TYPE      CLUSTER-IP    EXTERNAL-IP  PORT(S)    AGE
nodejs-ex ClusterIP  172.30.197.157 <none>       8080/TCP   70s
```

默认情况下，新服务没有外部 IP 地址。

16.4.4. 通过创建路由公开服务

您可以使用 **oc expose** 命令，将服务公开为路由。

流程

公开服务：

1. 登录 OpenShift Container Platform。
2. 登录您想公开的服务所在的项目。

```
$ oc project myproject
```

3. 运行 **oc expose service** 命令来公开路由：

```
$ oc expose service nodejs-ex
```

输出示例

```
route.route.openshift.io/nodejs-ex exposed
```

4. 要验证服务是否已公开，您可以使用 cURL 等工具来确保可从集群外部访问该服务。

- a. 使用 **oc get route** 命令查找路由的主机名：

```
$ oc get route
```

输出示例

NAME	HOST/PORT	PATH	SERVICES	PORT	TERMINATION
WILDCARD					
nodejs-ex	nodejs-ex-myproject.example.com		nodejs-ex	8080-tcp	None

- b. 使用 cURL 检查主机是否响应 GET 请求：

```
$ curl --head nodejs-ex-myproject.example.com
```

输出示例

```
HTTP/1.1 200 OK
...
```

16.4.5. 创建负载均衡器服务

使用以下流程来创建负载均衡器服务。

先决条件

- 确保您要公开的项目和服务已经存在。

流程

创建负载均衡器服务：

1. 登录 OpenShift Container Platform。
2. 加载您要公开的服务所在的项目。

```
$ oc project project1
```

3. 在 control plane 节点上打开文本文件（也称为 master 节点）并粘贴以下文本，根据需要编辑该文件：

负载均衡器配置文件示例

```

apiVersion: v1
kind: Service
metadata:
  name: egress-2 ❶
spec:
  ports:
  - name: db
    port: 3306 ❷
  loadBalancerIP:
  loadBalancerSourceRanges: ❸
  - 10.0.0.0/8
  - 192.168.0.0/16
  type: LoadBalancer ❹
  selector:
    name: mysql ❺

```

- ❶ 为负载均衡器服务输入一个描述性名称。
- ❷ 输入您要公开的服务所侦听的同一个端口
- ❸ 输入特定 IP 地址列表来限制通过负载均衡器的流量。如果 cloud-provider 不支持这个功能，则此字段将被忽略。
- ❹ 输入 **Loadbalancer** 作为类型。
- ❺ 输入服务的名称。



注意

要将通过负载均衡器的流量限制为特定的 IP 地址，建议使用 **service.beta.kubernetes.io/load-balancer-source-ranges** 注解，而不是设置 **loadBalancerSourceRanges** 字段。通过注释，您可以更轻松地迁移到 OpenShift API，后者将在未来的发行版中实施。

4. 保存并退出文件。
5. 运行以下命令来创建服务：

```
$ oc create -f <file-name>
```

例如：

```
$ oc create -f mysql-lb.yaml
```

6. 执行以下命令以查看新服务：

```
$ oc get svc
```

输出示例

```

NAME          TYPE          CLUSTER-IP      EXTERNAL-IP      PORT(S)
AGE

```



```
egress-2 LoadBalancer 172.30.22.226 ad42f5d8b303045-487804948.example.com
3306:30357/TCP 15m
```

如果启用了云供应商，该服务会自动分配到一个外部 IP 地址。

7. 在 master 上，使用 cURL 等工具来确保您可以通过公共 IP 地址访问该服务：

```
$ curl <public-ip>:<port>
```

例如：

```
$ curl 172.29.121.74:3306
```

此部分中的示例使用 MySQL 服务，这需要客户端应用程序。如果您得到一串字符并看到 **Got packets out of order** 消息，则您已连接到该服务。

如果您有 MySQL 客户端，请使用标准 CLI 命令登录：

```
$ mysql -h 172.30.131.89 -u admin -p
```

输出示例

```
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.

MySQL [(none)]>
```

16.5. 使用网络负载均衡器在 AWS 上配置集群入口流量

OpenShift Container Platform 提供了从集群外部与集群中运行的服务进行通信的方法。此方法使用 Network Load Balancer (NLB)，它会将客户端的 IP 地址转发到节点。您可以在新的或现有 AWS 集群上配置 NLB。

16.5.1. 使用网络负载均衡器替换 Ingress Controller Classic 负载均衡器

您可以将正在使用 Classic Load Balancer(CLB)的 Ingress Controller 替换为在 AWS 上使用网络负载均衡器(NLB)的 Ingress Controller。



警告

这个过程会导致预期的中断，由于新的 DNS 记录传播、新的负载均衡器置备及其他因素，可能会持续几分钟。应用此流程后，Ingress Controller 负载均衡器的 IP 地址和规范名称可能会改变。

流程

1. 使用新的默认 Ingress Controller 创建一个文件。以下示例假定您的默认 Ingress Controller 具有 **外部** 范围，且没有其他自定义：

ingresscontroller.yml 文件示例

```

apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  creationTimestamp: null
  name: default
  namespace: openshift-ingress-operator
spec:
  endpointPublishingStrategy:
    loadBalancer:
      scope: External
      providerParameters:
        type: AWS
      aws:
        type: NLB
      type: LoadBalancerService

```

如果您的默认 Ingress Controller 有其他自定义，请确保相应地修改该文件。

2. 强制替换 Ingress Controller YAML 文件：

```
$ oc replace --force --wait -f ingresscontroller.yml
```

等待 Ingress Controller 替换。预期服务器停机。

16.5.2. 在现有 AWS 集群上配置 Ingress Controller 网络负载均衡器

您可以在当前集群中创建一个由 AWS Network Load Balancer (NLB) 支持的 Ingress Controller。

先决条件

- 您必须已安装 AWS 集群。
- 基础架构资源的 **PlatformStatus** 需要是 AWS。
 - 要验证 **PlatformStatus** 是否为 AWS，请运行：

```
$ oc get infrastructure/cluster -o jsonpath='{.status.platformStatus.type}'
AWS
```

流程

在现有集群中，创建一个由 AWS NLB 支持的 Ingress Controller。

1. 创建 Ingress Controller 清单：

```
$ cat ingresscontroller-aws-nlb.yaml
```

输出示例

```

apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:

```

```

name: $my_ingress_controller ❶
namespace: openshift-ingress-operator
spec:
  domain: $my_unique_ingress_domain ❷
  endpointPublishingStrategy:
    type: LoadBalancerService
  loadBalancer:
    scope: External ❸
    providerParameters:
      type: AWS
      aws:
        type: NLB

```

- ❶ 将 **\$my_ingress_controller** 替换为 Ingress Controller 的唯一名称。
- ❷ 将 **\$my_unique_ingress_domain** 替换为集群中所有 Ingress Controller 的唯一域名。
- ❸ 您可以将 **External** 替换为 **Internal**，以使用内部 NLB。

2. 在集群中创建资源：

```
$ oc create -f ingresscontroller-aws-nlb.yaml
```



重要

在新 AWS 集群上配置 Ingress Controller NLB 之前，您必须完成 [创建安装配置文件的步骤](#)。

16.5.3. 在新 AWS 集群上配置 Ingress Controller 网络负载均衡

您可在新集群中创建一个由 AWS Network Load Balancer（NLB）支持的 Ingress Controller。

先决条件

- 创建 **install-config.yaml** 文件并完成对其所做的任何修改。

流程

在新集群中，创建一个由 AWS NLB 支持的 Ingress Controller。

1. 进入包含安装程序的目录并创建清单：

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

- ❶ 对于 **<installation_directory>**，请指定含有集群的 **install-config.yaml** 文件的目录的名称。

2. 在 **<installation_directory>/manifests/** 目录中创建一个名为 **cluster-ingress-default-ingresscontroller.yaml** 的文件：

```
$ touch <installation_directory>/manifests/cluster-ingress-default-ingresscontroller.yaml ❶
```

- 1 对于 `<installation_directory>`，请指定包含集群的 `manifests/` 目录的目录名称。

创建该文件后，`manifests/` 目录中会包含多个网络配置文件，如下所示：

```
$ ls <installation_directory>/manifests/cluster-ingress-default-ingresscontroller.yaml
```

输出示例

```
cluster-ingress-default-ingresscontroller.yaml
```

3. 在编辑器中打开 `cluster-ingress-default-ingresscontroller.yaml` 文件，并输入描述您想要的 Operator 配置的 CR:

```
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  creationTimestamp: null
  name: default
  namespace: openshift-ingress-operator
spec:
  endpointPublishingStrategy:
    loadBalancer:
      scope: External
      providerParameters:
        type: AWS
      aws:
        type: NLB
    type: LoadBalancerService
```

4. 保存 `cluster-ingress-default-ingresscontroller.yaml` 文件并退出文本编辑器。
5. 可选：备份 `manifests/cluster-ingress-default-ingresscontroller.yaml` 文件。创建集群时，安装程序会删除 `manifests/` 目录。

16.5.4. 其他资源

- [使用自定义网络在 AWS 上安装集群。](#)
- 如需更多信息，请参阅 [AWS 上的网络负载均衡支持。](#)

16.6. 为服务外部 IP 配置 INGRESS 集群流量

您可以将外部 IP 地址附加到服务，使其可用于集群外的流量。这通常只适用于在裸机硬件上安装的集群。必须正确配置外部网络基础架构，将流量路由到该服务。

16.6.1. 先决条件

- 您的集群被配置为启用了 ExternalIP。如需更多信息，请参阅 [为服务配置 ExternalIPs。](#)

16.6.2. 将 ExternalIP 附加到服务

您可以将 ExternalIP 附加到服务。如果您的集群被配置为自动分配 ExternalIP，您可能不需要手动将 ExternalIP 附加到该服务。

流程

1. 可选：要确认为 ExternalIP 配置了哪些 IP 地址范围，请输入以下命令：

```
$ oc get networks.config cluster -o jsonpath='{.spec.externalIP}'
```

如果设置了 **autoAssignCIDRs**，在没有指定 **spec.externalIPs** 字段的情况下，OpenShift Container Platform 会自动为新的 **Service** 对象分配一个 ExternalIP。

2. 为服务附加一个 ExternalIP。

- a. 如果要创建新服务，请指定 **spec.externalIPs** 字段，并提供包括一个或多个有效 IP 地址的数组。例如：

```
apiVersion: v1
kind: Service
metadata:
  name: svc-with-externalip
spec:
  ...
  externalIPs:
  - 192.174.120.10
```

- b. 如果您要将 ExternalIP 附加到现有服务中，请输入以下命令。将 **<name>** 替换为服务名称。将 **<ip_address>** 替换为有效的 ExternalIP 地址。您可以提供多个以逗号分开的 IP 地址。

```
$ oc patch svc <name> -p \
{
  "spec": {
    "externalIPs": [ "<ip_address>" ]
  }
}
```

例如：

```
$ oc patch svc mysql-55-rhel7 -p '{"spec":{"externalIPs":["192.174.120.10"]}]'
```

输出示例

```
"mysql-55-rhel7" patched
```

3. 要确认一个 ExternalIP 地址已附加到该服务，请输入以下命令。如果为新服务指定 ExternalIP，您必须首先创建该服务。

```
$ oc get svc
```

输出示例

```
NAME          CLUSTER-IP    EXTERNAL-IP    PORT(S)    AGE
mysql-55-rhel7 172.30.131.89 192.174.120.10 3306/TCP   13m
```

16.6.3. 其他资源

- [为服务配置 ExternalIP](#)

16.7. 使用 NODEPORT 配置集群入口流量

OpenShift Container Platform 提供了从集群外部与集群中运行的服务进行通信的方法。此方法使用了 **NodePort**。

16.7.1. 使用 NodePort 使流量进入集群

使用 **NodePort** 类型的 **Service** 资源，在集群中所有节点的特定端口上公开服务。端口在 **Service** 资源的 `.spec.ports[*].nodePort` 字段中指定。



重要

使用节点端口需要额外的端口资源。

NodePort 在节点 IP 地址的静态端口上公开服务。默认情况下，**NodePort** 在 **30000** 到 **32767** 的范围内，这意味着，**NodePort** 不可能与服务的预期端口匹配。例如：端口 **8080** 可能会在节点的端口 **31020** 中公开。

管理员必须确保外部 IP 地址路由到节点。

NodePort 和外部 IP 地址互相独立，可以同时使用它们。



注意

这部分中的流程需要由集群管理员执行先决条件。

16.7.2. 先决条件

在开始以下流程前，管理员必须：

- 设置集群联网环境的外部端口，使请求能够到达集群。
- 确定至少有一个用户具有集群管理员角色。要将此角色添加到用户，请运行以下命令：

```
$ oc adm policy add-cluster-role-to-user cluster-admin <user_name>
```

- 有一个 OpenShift Container Platform 集群，其至少有一个 master 和至少一个节点，并且集群外有一个对集群具有网络访问权限的系统。此流程假设外部系统与集群位于同一个子网。不同子网上外部系统所需要的额外联网不在本主题的讨论范围内。

16.7.3. 创建项目和服务

如果您要公开的项目和服务尚不存在，请首先创建项目，再创建服务。

如果项目和服务都已存在，跳到公开服务以创建路由这一步。

先决条件

- 按照 **oc** CLI 并以一个集群管理员身份登陆。

流程

1. 运行 **oc new-project** 命令为您的服务创建一个新项目：

```
$ oc new-project myproject
```

2. 使用 **oc new-app** 命令创建服务：

```
$ oc new-app nodejs:12~https://github.com/sclorg/nodejs-ex.git
```

3. 要验证是否已创建该服务，请运行以下命令：

```
$ oc get svc -n myproject
```

输出示例

```
NAME      TYPE      CLUSTER-IP    EXTERNAL-IP  PORT(S)    AGE
nodejs-ex ClusterIP  172.30.197.157 <none>      8080/TCP   70s
```

默认情况下，新服务没有外部 IP 地址。

16.7.4. 通过创建路由公开服务

您可以使用 **oc expose** 命令，将服务公开为路由。

流程

公开服务：

1. 登录 OpenShift Container Platform。
2. 登录您想公开的服务所在的项目。

```
$ oc project myproject
```

3. 要为应用程序公开节点端口，请输入以下命令。OpenShift Container Platform 会自动在 **30000-32767** 范围内选择可用端口。

```
$ oc expose service nodejs-ex --type=NodePort --name=nodejs-ex-nodeport --generator="service/v2"
```

输出示例

```
service/nodejs-ex-nodeport exposed
```

4. 可选：要使用公开的节点端口确认该服务可用，请输入以下命令：

```
$ oc get svc -n myproject
```

输出示例

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
nodejs-ex	ClusterIP	172.30.217.127	<none>	3306/TCP	9m44s
nodejs-ex-ingress	NodePort	172.30.107.72	<none>	3306:31345/TCP	39s

5. 可选：要删除由 `oc new-app` 命令自动创建的服务，请输入以下命令：

```
$ oc delete svc nodejs-ex
```

16.7.5. 其他资源

- [配置节点端口服务范围](#)

第 17 章 配置集群范围代理

生产环境可能会拒绝直接访问互联网，而是提供 HTTP 或 HTTPS 代理。您可以通过[修改现有集群的 Proxy 对象](#)或在新集群的 `install-config.yaml` 文件中配置代理设置，将 OpenShift Container Platform 配置为使用代理。

17.1. 先决条件

- 查看 [集群需要访问的站点](#) 中的内容，决定这些站点中的任何站点是否需要绕过代理。默认情况下，所有集群系统的出站流量都需经过代理，包括对托管集群的云供应商 API 的调用。系统范围的代理仅会影响系统组件，而不会影响用户工作负载。若有需要，将站点添加到 Proxy 对象的 `spec.noProxy` 字段来绕过代理服务器。



注意

Proxy 对象 `status.noProxy` 字段使用安装配置中的 `networking.machineNetwork[].cidr`、`networking.clusterNetwork[].cidr` 和 `networking.serviceNetwork[]` 字段的值填充。

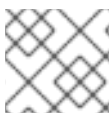
对于在 Amazon Web Services(AWS)、Google Cloud Platform(GCP)、Microsoft Azure 和 Red Hat OpenStack Platform(RHOSP)上安装，**Proxy** 对象 `status.noProxy` 字段也会使用实例元数据端点填充(169.254.169.254)。

17.2. 启用集群范围代理

Proxy 对象用于管理集群范围出口代理。如果在安装或升级集群时没有配置代理，则 Proxy 对象仍会生成，但它会有一个空的 `spec`。例如：

```
apiVersion: config.openshift.io/v1
kind: Proxy
metadata:
  name: cluster
spec:
  trustedCA:
    name: ""
status:
```

集群管理员可以通过修改这个 `cluster` Proxy 对象来配置 OpenShift Container Platform 的代理。



注意

只支持名为 `cluster` 的 Proxy 对象，且无法创建额外的代理。

先决条件

- 集群管理员权限
- 已安装 OpenShift Container Platform **oc** CLI 工具

流程

1. 创建包含代理 HTTPS 连接所需的额外 CA 证书的 ConfigMap。



注意

如果代理的身份证书由来自 RHCOS 信任捆绑包的颁发机构签名，您可以跳过这一步。

- a. 利用以下内容，创建一个名为 **user-ca-bundle.yaml** 的文件，并提供 PEM 编码证书的值：

```
apiVersion: v1
data:
  ca-bundle.crt: | 1
    <MY_PEM_ENCODED_CERTS> 2
kind: ConfigMap
metadata:
  name: user-ca-bundle 3
  namespace: openshift-config 4
```

- 1** 这个数据键必须命名为 **ca-bundle.crt**。
- 2** 一个或多个 PEM 编码的 X.509 证书，用来为代理的身份证书签名。
- 3** 要从 Proxy 对象引用的 ConfigMap 名称。
- 4** ConfigMap 必须在 **openshift-config** 命名空间中。

- b. 从此文件创建 ConfigMap：

```
$ oc create -f user-ca-bundle.yaml
```

2. 使用 **oc edit** 命令修改 Proxy 对象：

```
$ oc edit proxy/cluster
```

3. 为代理配置所需的字段：

```
apiVersion: config.openshift.io/v1
kind: Proxy
metadata:
  name: cluster
spec:
  httpProxy: http://<username>:<pswd>@<ip>:<port> 1
  httpsProxy: https://<username>:<pswd>@<ip>:<port> 2
  noProxy: example.com 3
  readinessEndpoints:
  - http://www.google.com 4
  - https://www.google.com
  trustedCA:
    name: user-ca-bundle 5
```

- 1** 用于创建集群外 HTTP 连接的代理 URL。URL 必须是 **http**。
- 2** 用于创建集群外 HTTPS 连接的代理 URL。

- 3 要排除代理的目标域名、域、IP 地址或其他网络 CIDR 的逗号分隔列表。

在域前面加 `.` 来仅匹配子域。例如：`.y.com` 匹配 `x.y.com`，但不匹配 `y.com`。使用 `*` 可对所有目的地绕过所有代理。如果您扩展了未包含在安装配置中 `networking.machineNetwork[].cidr` 字段定义的 worker，您必须将它们添加到此列表中，以防止连接问题。

如果未设置 `httpProxy` 或 `httpsProxy` 字段，则此字段将被忽略。

- 4 将 `httpProxy` 和 `httpsProxy` 值写进状态之前，执行就绪度检查时要使用的一个或多个集群外部 URL。
- 5 引用 `openshift-config` 命名空间中的 ConfigMap，其包含代理 HTTPS 连接所需的额外 CA 证书。注意 ConfigMap 必须已经存在，然后才能在这里引用它。此字段是必需的，除非代理的身份证书由来自 RHCOS 信任捆绑包的颁发机构签名。

4. 保存文件以使改变生效。

17.3. 删除集群范围代理服务器

`cluster Proxy` 对象不能被删除。要从集群中删除代理，请删除 Proxy 对象的所有 `spec` 字段。

先决条件

- 集群管理员权限
- 已安装 OpenShift Container Platform `oc` CLI 工具

流程

1. 使用 `oc edit` 命令来修改代理：

```
$ oc edit proxy/cluster
```

2. 删除 Proxy 对象的所有 `spec` 字段。例如：

```
apiVersion: config.openshift.io/v1
kind: Proxy
metadata:
  name: cluster
spec: {}
status: {}
```

3. 保存文件以使改变生效。

其他资源

- [替换 CA 捆绑证书](#)
- [代理证书自定义](#)

第 18 章 配置自定义 PKI

有些平台组件，如 Web 控制台，使用 Routes 进行通信，且必须信任其他组件的证书与其交互。如果您使用的是自定义公钥基础架构 (PKI)，您必须将其配置为在集群中识别其私有签名的 CA 证书。

您可以使用 Proxy API 添加集群范围的可信 CA 证书。您必须在安装过程中或运行时执行此操作。

- 在安装过程中，配置集群范围代理。您需要在 `install-config.yaml` 文件中的 `additionalTrustBundle` 设置中定义私有签名的 CA 证书。安装程序生成名为 `user-ca-bundle` 的 ConfigMap，其中包含您定义的附加 CA 证书。然后，Cluster Network Operator 会创建 `trusted-ca-bundle` ConfigMap，将这些内容与 Red Hat Enterprise Linux CoreOS (RHCOS) 信任捆绑包合并，Proxy 对象的 `trustedCA` 字段中也会引用此 ConfigMap。
- 在运行时，修改 default Proxy 对象，使其包含您私有签名的 CA 证书（集群代理启用 workflow 的一部分）。这涉及创建包含集群应信任的私有签名 CA 证书的 ConfigMap，然后使用 `trustedCA` 引用私有签名证书的 ConfigMap 修改代理服务器资源。



注意

安装程序配置的 `additionalTrustBundle` 字段和 proxy 资源的 `trustedCA` 字段被用来管理集群范围信任捆绑包；在安装时会使用 `additionalTrustBundle`，并在运行时使用代理的 `trustedCA`。

`trustedCA` 字段是对包含集群组件使用的自定义证书和密钥对的 ConfigMap 的引用。

18.1. 在安装过程中配置集群范围代理

生产环境可能会拒绝直接访问互联网，而是提供 HTTP 或 HTTPS 代理。您可以通过在 `install-config.yaml` 文件中配置代理设置，将新的 OpenShift Container Platform 集群配置为使用代理。

先决条件

- 您有一个现有的 `install-config.yaml` 文件。
- 您检查了集群需要访问的站点，并决定是否需要绕过代理。默认情况下代理所有集群出口流量，包括对托管云供应商 API 的调用。您需要将站点添加到 Proxy 对象的 `spec.noProxy` 字段来绕过代理。



注意

Proxy 对象 `status.noProxy` 字段使用安装配置中的 `networking.machineNetwork[].cidr`、`networking.clusterNetwork[].cidr` 和 `networking.serviceNetwork[]` 字段的值填充。

对于在 Amazon Web Services(AWS)、Google Cloud Platform(GCP)、Microsoft Azure 和 Red Hat OpenStack Platform(RHOSP)上安装，Proxy 对象 `status.noProxy` 字段也会使用实例元数据端点填充(169.254.169.254)。

流程

1. 编辑 `install-config.yaml` 文件并添加代理设置。例如：

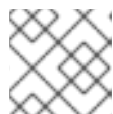
```
apiVersion: v1
```

```

baseDomain: my.domain.com
proxy:
  httpProxy: http://<username>:<pswd>@<ip>:<port> ❶
  httpsProxy: https://<username>:<pswd>@<ip>:<port> ❷
  noProxy: example.com ❸
additionalTrustBundle: | ❹
  -----BEGIN CERTIFICATE-----
  <MY_TRUSTED_CA_CERT>
  -----END CERTIFICATE-----
...

```

- ❶ 用于创建集群外 HTTP 连接的代理 URL。URL 必须是 **http**。
- ❷ 用于创建集群外 HTTPS 连接的代理 URL。
- ❸ 要排除在代理中的目标域名、IP 地址或其他网络 CIDR 的逗号分隔列表。在域前面加 **.** 来仅匹配子域。例如：**.y.com** 匹配 **x.y.com**，但不匹配 **y.com**。使用 ***** 绕过所有目的地的代理。
- ❹ 如果提供，安装程序会在 **openshift-config** 命名空间中生成名为 **user-ca-bundle** 的配置映射来保存额外的 CA 证书。如果您提供 **additionalTrustBundle** 和至少一个代理设置，则 **Proxy** 对象会被配置为引用 **trustedCA** 字段中的 **user-ca-bundle** 配置映射。然后，Cluster Network Operator 会创建一个 **trusted-ca-bundle** 配置映射，该配置映射将为 **trustedCA** 参数指定的内容与 RHCOS 信任捆绑包合并。**additionalTrustBundle** 字段是必需的，除非代理的身份证书由来自 RHCOS 信任捆绑包的颁发机构签名。



注意

安装程序不支持代理的 **readinessEndpoints** 字段。

2. 保存该文件，并在安装 OpenShift Container Platform 时引用。

安装程序会创建一个名为 **cluster** 的集群范围代理，该代理使用提供的 **install-config.yaml** 文件中的代理设置。如果没有提供代理设置，仍然会创建一个 **cluster Proxy** 对象，但它会有一个空 **spec**。



注意

只支持名为 **cluster** 的 **Proxy** 对象，且无法创建额外的代理。

18.2. 启用集群范围代理

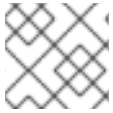
Proxy 对象用于管理集群范围出口代理。如果在安装或升级集群时没有配置代理，则 **Proxy** 对象仍会生成，但它会有一个空的 **spec**。例如：

```

apiVersion: config.openshift.io/v1
kind: Proxy
metadata:
  name: cluster
spec:
  trustedCA:
    name: ""
status:

```

集群管理员可以通过修改这个 **cluster** Proxy 对象来配置 OpenShift Container Platform 的代理。



注意

只支持名为 **cluster** 的 Proxy 对象，且无法创建额外的代理。

先决条件

- 集群管理员权限
- 已安装 OpenShift Container Platform **oc** CLI 工具

流程

1. 创建包含代理 HTTPS 连接所需的额外 CA 证书的 ConfigMap。



注意

如果代理的身份证书由来自 RHCOS 信任捆绑包的颁发机构签名，您可以跳过这一步。

- a. 利用以下内容，创建一个名为 **user-ca-bundle.yaml** 的文件，并提供 PEM 编码证书的值：

```
apiVersion: v1
data:
  ca-bundle.crt: | 1
    <MY_PEM_ENCODED_CERTS> 2
kind: ConfigMap
metadata:
  name: user-ca-bundle 3
  namespace: openshift-config 4
```

- 1** 这个数据键必须命名为 **ca-bundle.crt**。
- 2** 一个或多个 PEM 编码的 X.509 证书，用来为代理的身份证书签名。
- 3** 要从 Proxy 对象引用的 ConfigMap 名称。
- 4** ConfigMap 必须在 **openshift-config** 命名空间中。

- b. 从此文件创建 ConfigMap：

```
$ oc create -f user-ca-bundle.yaml
```

2. 使用 **oc edit** 命令修改 Proxy 对象：

```
$ oc edit proxy/cluster
```

3. 为代理配置所需的字段：

```
apiVersion: config.openshift.io/v1
kind: Proxy
```

```

metadata:
  name: cluster
spec:
  httpProxy: http://<username>:<pswd>@<ip>:<port> ❶
  httpsProxy: http://<username>:<pswd>@<ip>:<port> ❷
  noProxy: example.com ❸
  readinessEndpoints:
    - http://www.google.com ❹
    - https://www.google.com
  trustedCA:
    name: user-ca-bundle ❺

```

❶ 用于创建集群外 HTTP 连接的代理 URL。URL 必须是 **http**。

❷ 用于创建集群外 HTTPS 连接的代理 URL。

❸ 要排除代理的目标域名、域、IP 地址或其他网络 CIDR 的逗号分隔列表。

在域前面加 `.` 来仅匹配子域。例如：`.y.com` 匹配 `x.y.com`，但不匹配 `y.com`。使用 `*` 可对所有目的地绕过所有代理。如果您扩展了未包含在安装配置中 `networking.machineNetwork[].cidr` 字段定义的 worker，您必须将它们添加到此列表中，以防止连接问题。

如果未设置 `httpProxy` 或 `httpsProxy` 字段，则此字段将被忽略。

❹ 将 `httpProxy` 和 `httpsProxy` 值写进状态之前，执行就绪度检查时要使用的一个或多个集群外部 URL。

❺ 引用 `openshift-config` 命名空间中的 ConfigMap，其包含代理 HTTPS 连接所需的额外 CA 证书。注意 ConfigMap 必须已经存在，然后才能在这里引用它。此字段是必需的，除非代理的身份证书由来自 RHCOS 信任捆绑包的颁发机构签名。

4. 保存文件以使改变生效。

18.3. 使用 OPERATOR 进行证书注入

在您的自定义 CA 证书通过 ConfigMap 添加到集群中后，Cluster Network Operator 会将用户提供的证书和系统 CA 证书合并到单一捆绑包中，并将合并的捆绑包注入请求信任捆绑包注入的 Operator。

Operator 通过创建一个带有以下标签的空 ConfigMap 来请求此注入：

```
config.openshift.io/inject-trusted-cabundle="true"
```

空 ConfigMap 的示例：

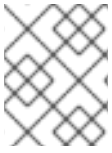
```

apiVersion: v1
data: {}
kind: ConfigMap
metadata:
  labels:
    config.openshift.io/inject-trusted-cabundle: "true"
  name: ca-inject ❶
  namespace: apache

```

- 1 指定空 ConfigMap 名称。

Operator 将这个 ConfigMap 挂载到容器的本地信任存储中。



注意

只有在 Red Hat Enterprise Linux CoreOS (RHCOS) 信任捆绑包中没有包括证书时才需要添加可信的 CA 证书。

证书注入不仅限于 Operator。当使用 **config.openshift.io/inject-trusted-cabundle=true** 标记 (label) 创建一个空的 ConfigMap 时，Cluster Network Operator 会跨命名空间注入证书。

ConfigMap 可以驻留在任何命名空间中，但 ConfigMap 必须作为卷挂载到需要自定义 CA 的 pod 中的每个容器。例如：

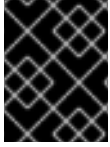
```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-example-custom-ca-deployment
  namespace: my-example-custom-ca-ns
spec:
  ...
  spec:
    ...
    containers:
      - name: my-container-that-needs-custom-ca
        volumeMounts:
          - name: trusted-ca
            mountPath: /etc/pki/ca-trust/extracted/pem
            readOnly: true
        volumes:
          - name: trusted-ca
            configMap:
              name: trusted-ca
              items:
                - key: ca-bundle.crt 1
                  path: tls-ca-bundle.pem 2
```

- 1 **CA-bundle.crt** 需要作为 ConfigMap 密钥。
- 2 **TLS-ca-bundle.pem** 需要作为 ConfigMap 的路径。

第 19 章 RHOSP 负载均衡

19.1. 使用带有 KURYR SDN 的 OCTAVIA OVN 负载均衡器供应商驱动

如果您的 OpenShift Container Platform 集群使用 Kuryr，并安装在稍后升级到 RHOSP 16 的 Red Hat OpenStack Platform (RHOSP) 13 云上，您可以将其配置为使用 Octavia OVN 供应商驱动程序。



重要

在更改供应商驱动程序后，Kuryr 会替换现有的负载均衡器。这个过程会产生一些停机时间。

先决条件

- 安装 RHOSP CLI **openstack**。
- 已安装 OpenShift Container Platform CLI (**oc**)。
- 验证 RHOSP 上 Octavia OVN 驱动程序是否启用。

提示

要查看可用 Octavia 驱动程序列表，请在命令行中输入 **openstack loadbalancer provider list**。命令的输出中会显示 **ovn** 驱动。

流程

把 Octavia Amphora 供应商驱动改为 Octavia OVN:

1. 打开 **kuryr-config** ConfigMap。在命令行中运行：

```
$ oc -n openshift-kuryr edit cm kuryr-config
```

2. 在 ConfigMap 中，删除包含 **kuryr-octavia-provider: default** 的行。例如：

```
...
kind: ConfigMap
metadata:
  annotations:
    networkoperator.openshift.io/kuryr-octavia-provider: default 1
...
```

- 1** 删除这一行。集群将会重新生成，并带有 **ovn** 值。

等待 Cluster Network Operator 检测修改并重新部署 **kuryr-controller** 和 **kuryr-cni** pod。这可能需要几分钟。

3. 验证 **kuryr-config** ConfigMap 注解是否带有 **ovn** 作为其值。在命令行中运行：

```
$ oc -n openshift-kuryr edit cm kuryr-config
```

ovn 供应商值会在输出中显示：

```
...
kind: ConfigMap
metadata:
  annotations:
    networkoperator.openshift.io/kuryr-octavia-provider: ovn
...
```

4. 验证 RHOSP 是否已重新创建其负载均衡器。

- a. 在命令行中运行：

```
$ openstack loadbalancer list | grep amphora
```

此时会显示一个 Amphora 负载均衡器。例如：

```
a4db683b-2b7b-4988-a582-c39daaad7981 | ostest-7mbj6-kuryr-api-loadbalancer |
84c99c906edd475ba19478a9a6690efd | 172.30.0.1 | ACTIVE | amphora
```

- b. 输入以下内容查找 **ovn** 负载均衡器：

```
$ openstack loadbalancer list | grep ovn
```

显示 **ovn** 类型的负载均衡器。例如：

```
2dffe783-98ae-4048-98d0-32aa684664cc | openshift-apiserver-operator/metrics |
84c99c906edd475ba19478a9a6690efd | 172.30.167.119 | ACTIVE | ovn
0b1b2193-251f-4243-af39-2f99b29d18c5 | openshift-etcd/etcd |
84c99c906edd475ba19478a9a6690efd | 172.30.143.226 | ACTIVE | ovn
f05b07fc-01b7-4673-bd4d-adaa4391458e | openshift-dns-operator/metrics |
84c99c906edd475ba19478a9a6690efd | 172.30.152.27 | ACTIVE | ovn
```

19.2. 使用 OCTAVIA 为应用程序流量扩展集群

在 Red Hat OpenStack Platform (RHOSP) 上运行的 OpenShift Container Platform 集群可以使用 Octavia 负载均衡服务在多个虚拟机 (VM) 或浮动 IP 地址间分配流量。这个功能减少了单一机器或地址生成的瓶颈。

如果您的集群使用 Kuryr, Cluster Network Operator 会在部署时创建一个内部 Octavia 负载均衡器。您可以使用此负载均衡器进行应用程序网络扩展。

如果您的集群没有使用 Kuryr, 则需要创建自己的 Octavia 负载均衡器将其用于应用程序网络扩展。

19.2.1. 使用 Octavia 扩展集群

如果要使用多个 API 负载均衡器, 或者集群没有使用 Kuryr, 请创建一个 Octavia 负载均衡器, 然后配置集群使用它。

先决条件

- Octavia 包括在您的 Red Hat OpenStack Platform (RHOSP) 部署中。

流程

1. 在命令行中创建一个使用 Amphora 驱动程序的 Octavia 负载均衡器：

```
$ openstack loadbalancer create --name API_OCP_CLUSTER --vip-subnet-id
<id_of_worker_vms_subnet>
```

可以使用自己选择的名称而不是 **API_OCP_CLUSTER**。

2. 负载均衡器成为活跃后，创建监听程序：

```
$ openstack loadbalancer listener create --name API_OCP_CLUSTER_6443 --protocol
HTTPS--protocol-port 6443 API_OCP_CLUSTER
```



注意

要查看负载均衡器的状态，请输入 **openstack loadbalancer list**。

3. 创建一个使用轮循算法的池，并启用了会话持久性：

```
$ openstack loadbalancer pool create --name API_OCP_CLUSTER_pool_6443 --lb-
algorithm ROUND_ROBIN --session-persistence type=<source_IP_address> --listener
API_OCP_CLUSTER_6443 --protocol HTTPS
```

4. 为确保 control plane 机器可用，创建一个健康监控器：

```
$ openstack loadbalancer healthmonitor create --delay 5 --max-retries 4 --timeout 10 --type
TCP API_OCP_CLUSTER_pool_6443
```

5. 将 control plane 机器作为负载均衡器池的成员添加：

```
$ for SERVER in $(MASTER-0-IP MASTER-1-IP MASTER-2-IP)
do
  openstack loadbalancer member create --address $SERVER --protocol-port 6443
  API_OCP_CLUSTER_pool_6443
done
```

6. 可选：要重复使用集群 API 浮动 IP 地址，取消设置它：

```
$ openstack floating ip unset $API_FIP
```

7. 为创建的负载均衡器 VIP 添加未设置的 **API_FIP** 或一个新地址：

```
$ openstack floating ip set --port $(openstack loadbalancer show -c <vip_port_id> -f value
API_OCP_CLUSTER) $API_FIP
```

您的集群现在使用 Octavia 进行负载平衡。



注意

如果 Kuryr 使用 Octavia Amphora 驱动程序，则所有流量都通过单个 Amphora 虚拟机 (VM) 路由。

您可以重复这个过程来创建其他负载均衡器，这样可降低瓶颈。

19.2.2. 通过 Octavia 扩展使用 Kuryr 的集群

如果您的集群使用 Kuryr，将集群的 API 浮动 IP 地址与预先存在的 Octavia 负载均衡器相关联。

先决条件

- OpenShift Container Platform 集群使用 Kuryr。
- Octavia 包括在您的 Red Hat OpenStack Platform (RHOSP) 部署中。

流程

1. 可选：在命令行中，为了重新使用集群 API 浮动 IP 地址取消设置它：

```
$ openstack floating ip unset $API_FIP
```

2. 为创建的负载均衡器 VIP 添加未设置的 **API_FIP** 或一个新地址：

```
$ openstack floating ip set --port $(openstack loadbalancer show -c <vip_port_id> -f value ${OCP_CLUSTER}-kuryr-api-loadbalancer) $API_FIP
```

您的集群现在使用 Octavia 进行负载平衡。



注意

如果 Kuryr 使用 Octavia Amphora 驱动程序，则所有流量都通过单个 Amphora 虚拟机 (VM) 路由。

您可以重复这个过程来创建其他负载均衡器，这样可降低瓶颈。

19.3. 使用 RHOSP OCTAVIA 为入站流量扩展

您可以使用 Octavia 负载均衡器来扩展使用 Kuryr 的集群中的 Ingress 控制器。

先决条件

- OpenShift Container Platform 集群使用 Kuryr。
- Octavia 可用于您的 RHOSP 部署。

流程

1. 要复制当前的内部路由器服务，在命令行中输入：

```
$ oc -n openshift-ingress get svc router-internal-default -o yaml > external_router.yaml
```

- 在 `external_router.yaml` 文件中，将 `metadata.name` 和 `spec.type` 的值改为 `LoadBalancer`。

路由器文件示例

```

apiVersion: v1
kind: Service
metadata:
  labels:
    ingresscontroller.operator.openshift.io/owning-ingresscontroller: default
  name: router-external-default 1
  namespace: openshift-ingress
spec:
  ports:
    - name: http
      port: 80
      protocol: TCP
      targetPort: http
    - name: https
      port: 443
      protocol: TCP
      targetPort: https
    - name: metrics
      port: 1936
      protocol: TCP
      targetPort: 1936
  selector:
    ingresscontroller.operator.openshift.io/deployment-ingresscontroller: default
  sessionAffinity: None
  type: LoadBalancer 2

```

- 1 确保此值具有描述性，如 `router-external-default`。
- 2 确定这个值是 `LoadBalancer`。



注意

您可以删除与负载均衡相关的时间戳和其他信息。

1. 在命令行中，从 `external_router.yaml` 文件创建服务：

```
$ oc apply -f external_router.yaml
```

2. 验证服务的外部 IP 地址是否与与负载均衡器关联的 IP 地址相同：

- a. 在命令行中检索服务的外部 IP 地址：

```
$ oc -n openshift-ingress get svc
```

输出示例

```

NAME                TYPE          CLUSTER-IP    EXTERNAL-IP  PORT(S)
AGE
router-external-default LoadBalancer  172.30.235.33  10.46.22.161

```

```
80:30112/TCP,443:32359/TCP,1936:30317/TCP 3m38s
router-internal-default ClusterIP 172.30.115.123 <none>
80/TCP,443/TCP,1936/TCP 22h
```

- b. 检索负载均衡器的 IP 地址：

```
$ openstack loadbalancer list | grep router-external
```

输出示例

```
| 21bf6afe-b498-4a16-a958-3229e83c002c | openshift-ingress/router-external-default |
66f3816acf1b431691b8d132cc9d793c | 172.30.235.33 | ACTIVE | octavia |
```

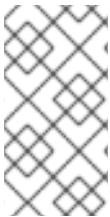
- c. 验证您在前面的步骤中获取的地址是否在浮动 IP 列表中相互关联：

```
$ openstack floating ip list | grep 172.30.235.33
```

输出示例

```
| e2f80e97-8266-4b69-8636-e58bacf1879e | 10.46.22.161 | 172.30.235.33 | 655e7122-
806a-4e0a-a104-220c6e17bda6 | a565e55a-99e7-4d15-b4df-f9d7ee8c9deb |
66f3816acf1b431691b8d132cc9d793c |
```

现在，您可以使用 **EXTERNAL-IP** 值作为新的入口地址。



注意

如果 Kuryr 使用 Octavia Amphora 驱动程序，则所有流量都通过单个 Amphora 虚拟机 (VM) 路由。

您可以重复这个过程来创建其他负载均衡器，这样可降低瓶颈。

第 20 章 将二级接口指标与网络附加关联

20.1. 将二级接口指标与网络附加关联

二级设备或接口用于不同目的。为了对采用相同分类的二级设备的指标数据进行汇总，需要有一个方法来对它们进行分类。

公开的指标会包括接口，但不会指定接口的起始位置。这在没有其他接口时是可行的。但如果添加了二级接口，则很难使用这个指标，因为仅使用接口名称作为标识符很难识别不同的接口。

在添加二级接口时，它们的名称取决于添加它们的顺序，不同的二级接口可能属于不同的网络，并可用于不同的目的。

通过使用 `pod_network_name_info`，可以使用标识接口类型的额外信息来扩展当前的指标。这样，就可以聚合指标，并为特定接口类型添加特定的警告。

网络类型使用相关的 `NetworkAttachmentDefinition` 名称生成，该名称反过来用于区分不同类别的次要网络。例如，属于不同网络或使用不同的 CNI 的不同接口使用不同的网络附加定义名称。

20.1.1. 网络指标守护进程

网络指标守护进程是收集并发布与网络相关的指标的守护进程组件。

kubelet 已经发布了您可以观察到的网络相关指标。这些指标是：

- `container_network_receive_bytes_total`
- `container_network_receive_errors_total`
- `container_network_receive_packets_total`
- `container_network_receive_packets_dropped_total`
- `container_network_transmit_bytes_total`
- `container_network_transmit_errors_total`
- `container_network_transmit_packets_total`
- `container_network_transmit_packets_dropped_total`

这些指标中的标签包括：

- Pod 名称
- Pod 命名空间
- 接口名称（比如 `eth0`）

这些指标在为 Pod 添加新接口之前（例如通过 `Multus`）可以正常工作。在添加了新接口后，无法清楚地知道接口名称代表什么。

`interface` 标签指向接口名称，但它不知道接口的作用是什么。在有多个不同接口的情况下，无法了解您监控的指标代表什么网络。

现在引入了新的 `pod_network_name_info` 可以帮助解决这个问题。

20.1.2. 带有网络名称的指标

此 daemonset 发布一个 `pod_network_name_info` 指标，固定值为 0:

```
pod_network_name_info{interface="net0",namespace="namespace",network_name="namespace/firstNAD",pod="podname"} 0
```

使用 Multus 所添加的注解生成网络名称标签。它是网络附加定义所属命名空间的连接，加上网络附加定义的名称。

新的指标本身不会提供很多值，但与网络相关的 `container_network_*` 指标一起使用，可以为二集网络的监控提供更好的支持。

使用类似以下的 `promql` 查询时，可以获取包含这个值的新指标，以及从 `k8s.v1.cni.cncf.io/networks-status` 注解中检索的网络名称：

```
(container_network_receive_bytes_total) + on(namespace,pod,interface) group_left(network_name) (
pod_network_name_info )
(container_network_receive_errors_total) + on(namespace,pod,interface) group_left(network_name) (
pod_network_name_info )
(container_network_receive_packets_total) + on(namespace,pod,interface)
group_left(network_name) ( pod_network_name_info )
(container_network_receive_packets_dropped_total) + on(namespace,pod,interface)
group_left(network_name) ( pod_network_name_info )
(container_network_transmit_bytes_total) + on(namespace,pod,interface) group_left(network_name)
( pod_network_name_info )
(container_network_transmit_errors_total) + on(namespace,pod,interface) group_left(network_name)
( pod_network_name_info )
(container_network_transmit_packets_total) + on(namespace,pod,interface)
group_left(network_name) ( pod_network_name_info )
(container_network_transmit_packets_dropped_total) + on(namespace,pod,interface)
group_left(network_name)
```