ALIBABA CLOUD

阿里云

容器服务Kubernetes版

产品公告

文档版本：20201026

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.容器服务控制台导航栏改版公告

为了优化容器服务控制台的交互体验，阿里云以集群为核心调整优化了控制台导航栏，将原先在导航栏中平铺的功能菜单归入集群管理页面。

主要变更点

- 主导航栏

变更项	变更前	变更后	说明
整体目录			简化一级目录。将以下菜单移至集群管理页面： ○ 应用 ○ 路由与负载均衡 ○ Knative ○ 应用配置 Serverless集群移至一级目录。
市场			**镜像**改为**容器镜像服务**，单击之后跳转至容器镜像服务控制台。

- 集群管理页面导航栏

变更项	变更前	变更后	说明
整体目录			将导航栏主菜单中以集群为操作对象的功能菜单归入集群管理页面。新增以下菜单： ○ 命名空间 ○ 存储卷 ○ 工作负载 ○ 服务 ○ 路由 ○ 发布 ○ 应用配置 ○ 运维管理：将变更前的集群升级、集群审计、集群拓扑、事件列表移至此处。

变更项	变更前	变更后	说明
工作负载			将变更前**应用**中的以下菜单合并，以页签形式在**工作负载**页面呈现。 ○ 无状态 ○ 有状态 ○ 守护进程集 ○ 任务 ○ 定时任务 ○ 容器组
路由、服务			将变更前**路由与负载均衡**中的以下菜单，移至集群管理页面的一级目录。 ○ 路由 ○ 服务
配置管理			将变更前**应用配置**中的以下菜单合并，以页签形式在**配置管理**页面呈现。 ○ 配置项 ○ 保密字典
运维管理			将变更前的**组件管理**、**事件列表**、**集群升级**、**运行时升级**移至变更后的**运维管理**类目中。

2.升级CoreDNS至1.6.2新版本公告

为了提升ACK集群内域名解析服务的稳定性，建议您升级集群的CoreDNS至1.6.2及以上版本。本文介绍如何手动升级CoreDNS的版本。

背景信息

低版本CoreDNS（1.4及之前的版本）存在的以下两个问题，影响了ACK 1.16以前版本集群内域名解析服务的稳定性：

- 因为CoreDNS需要通过watch apiserver拿到Service数据，所以health插件会检查CoreDNS与apiserver的连通性。如果连通性不正常（如网络抖动、apiserver重启等情况），健康检查接口会报错。CoreDNS在3次健康检查失败后会重启，重启过程中将导致服务不可以用。详情请参见coredns。
- CoreDNS会受到klog缺陷的影响：CoreDNS与apiserver断连后，klog尝试向一个不存在的目录*/tmp*写错误日志，此行为会失败并进一步导致CoreDNS奔溃。详情请参见add mount of /tmp #137。

您可以选择以下两种升级方案以解决低版本CoreDNS带来的稳定性问题：

- 长期解决方案：升级Kubernetes集群到1.16及以上版本，集群升级时会自动将CoreDNS升级到1.6.2及以上版本。有关在控制台中升级集群的具体操作步骤，请参见升级集群；有关通过API升级集群的详细信息，请参见升级集群。
- 短期解决方案：如果不方便升级集群版本，您可以选择手动升级CoreDNS到1.6.2及以上版本。有关如何手动升级CoreDNS版本的具体步骤，请参见本文升级步骤。

> 注意 对于1.4及之前的版本的CoreDNS，您才需要进行手动升级。

升级步骤

1. 确认集群版本与CoreDNS版本的兼容性。

   您需先确认集群版本号，然后进一步确认与CoreDNS 1.6.2版本的兼容性。ACK Kubernetes集群版本与CoreDNS 1.6.2版本兼容情况如下表（Kubernetes 1.11/1.12/1.14/1/16均兼容CoreDNS 1.6.2版本）。

版本	兼容信息			
Kubernetes版本	1.11	1.12	1.14	1.16
CoreDNS	1.6.2	1.6.2	1.6.2	1.6.2

   确认集群版本号的操作步骤如下：

   i. 登录容器服务管理控制台。

   ii. 在控制台左侧导航栏中，单击**集群**。

   iii. 在集群列表中，找到目标集群，然后查看集群Kubernetes版本。

2. 确认集群CoreDNS的版本。
   - 您可以在ACK控制台确认CoreDNS的版本。

     a. 登录容器服务管理控制台.

     b. 在控制台左侧导航栏，单击**集群**，然后单击目标集群右侧**操作**列下的**应用管理**。

c. 在**无状态**页签中，选择**kube-system**命名空间，然后查看CoreDNS的版本。

- 您还可以通过以下**kubectl**命令查找CoreDNS的版本。

```
kubectl get deployment coredns -n kube-system -o jsonpath="{.spec.template.spec.containers[0].image}"
```

输出：

```
registry-vpc.cn-hangzhou.aliyuncs.com/acs/coredns:1.3.1
```

3. 变更CoreDNS配置项。

1.6.2版本CoreDNS废弃了Proxy插件，使用forward来替代。您需要先将kube-system命名空间下的配置项**coredns**内的proxy字段替换为forward字段。

- 您可以在ACK控制台上直接更新配置项**coredns**。

a. 登录容器服务管理控制台.

b. 在控制台左侧导航栏，单击**集群**，然后单击目标集群名称。

c. 在集群管理左侧导航栏，单击**配置管理**。

d. 在**配置项**页签，找到并单击**coredns**右侧的**查看Yaml**。

e. 在**编辑YAML**页面，将**proxy**修改为**forward**。

- 您还可以通过**kubectl**命令变更配置项CoreDNS。

```
# 打开编辑。
kubectl edit configmap/coredns -n kube-system


# 替换proxy字段为forward。
# 保存并退出。
```

更新完配置后，查看CoreDNS Pod的标准输出是否正常重新加载了配置（一般需要30s时间来热加载新配置）。

a. 执行以下命令查看集群内的CoreDNS Pod，确定其是否处于运行状态。

```
kubectl get pods -n kube-system | grep coredns
```

输出：

```
coredns-78d4b8bd88-6g62w                1/1   Running   0      9d
coredns-78d4b8bd88-n6wjm                1/1   Running   0      9d
```

b. 执行以下命令查看CoreDNS Pod的日志。

```
kubectl logs coredns-78d4b8bd88-n6wjm -n kube-system
```

输出：

```
.:53
[INFO] plugin/reload: Running configuration MD5 = 71c5f1ff539d304c630521f315dc2ac2
CoreDNS-1.6.7
linux/amd64, go1.13.6, da7f65b
[INFO] 127.0.0.1:48329 - 42313 "HINFO IN 1108347002237365533.4506541768939609094. udp 57
false 512" NXDOMAIN qr,rd,ra 132 0.008874794s
```

当出现plugin/reload信息时，说明重新加载了CoreDNS新配置。

4. 变更CoreDNS应用。变更CoreDNS应用内镜像版本到1.6.2。
   - 通过控制台操作。
     a. 登录容器服务管理控制台.
     b. 在控制台左侧导航栏，单击集群，然后单击目标集群右侧操作列下的应用管理。
     c. 在无状态页签，找到coredns，然后在其右侧选择更多 > 查看Yaml。
     d. 在编辑YAML页面，更新image中的版本为1.6.2。
   - 通过kubectl命令操作。

```
# 打开编辑。
kubectl edit deployment/coredns -n kube-system

# 变更镜像版本到1.6.2。
# 保存并退出。
```

5. 验证结果。

   执行以下命令查看集群内容所有CoreDNS Pod是否都处于Running的正常状态。

```
kubectl get pods -n kube-system | grep coredns
```

输出：

```
coredns-78d4b8bd88-6g62w                1/1     Running   0          9d
coredns-78d4b8bd88-n6wjm                1/1     Running   0          9d
```

3.Helm V2 Tiller升级公告

近期阿里云容器服务Kubernetes版（ACK）新建集群中安装的Helm已全面升级至v3版本。由于Helm v2 Tiller服务端在社区一直存在已知的安全问题，攻击者可以通过tiller在集群内安装未经授权的应用，因此推荐您升级至Helm v3版本。

影响范围

首先执行命令kubectl get deploy -n kube-system tiller-deploy查看是否存在tiller deployment。如果存在，判断以下条件：

- ACK集群访问密钥（kubeconfig）是否提供给外部客户使用。
- 阿里云容器服务控制台是否提供给外部客户登录访问。
- ACK集群是否应用在多租户场景下，且有用户之间权限隔离的情况存在。

如果满足以上任何一点，建议您将安装的Helm升级到Helm v3系统。

未在上述范围或者暂时无法升级Helm v3

对于不在影响范围内或暂时无法升级Helm v3的用户可以手动升级Helm v2 tiller到最新版本，以获取更加强健的安全性保障。升级方式如下。

1. 执行以下命令。

   ```
   helm init --tiller-image registry.cn-hangzhou.aliyuncs.com/acs/tiller:v2.16.3 --upgrade
   ```

2. 待tiller健康检查通过后，执行命令helm version查看版本升级情况。

   这里只会升级 Helm服务端。客户端在各平台的最新版下载地址，请参见下载地址。

> 说明 未在上述范围内的用户，或者暂时无法升级Helm v3的用户，将Tiller升级到最新版即可，不需要再执行下面的操作，后续可以根据自己需求逐步地迁移至Helm v3。

前置检查

升级Helm v2之前，请进行前置检查。

1. 首先判断自己集群内是否含有tiller。执行命令kubectl get deploy -n kube-system tiller-deploy查看是否存在此deployment。
2. 如果存在，执行命令helm ls -a查看是否已经安装了应用。
3. 如果安装了应用，需要先删除应用，因为Helm v2与Helm v3数据不兼容。

> 注意 Helm社区提供了Helm v2 to Helm v3插件，但是请慎重使用，以免出现数据丢失情况。Helm v2 to Helm v3插件信息，请参见helm-2to3。

升级步骤

1. 确保前置检查通过。
2. 执行命令kubectl delete deploy tiller-deploy -n kube-system。
3. 下载helm v3客户端安装新的应用。

> **注意**
>
> 安装新的应用前：
>
> - 需要将原有Helm v2安装的应用使用Helm v3重装一遍，请评估对业务的影响。
> - 重装应用会导致原有数据丢失，请注意数据备份与保护。

相关文档

- Helm v3 Change log
- Helm v3与Helm v2的区别
- Helm v2如何迁移到Helm v3

4.容器服务即将停止对Swarm的技术支持

容器服务即将于2019年年底停止对Swarm的技术支持，感谢您在过去几年对容器服务的支持，我们将在容器服务Kubernetes版（ACK）继续为您提供稳定、可靠的企业级容器服务。现将Swarm的下线计划向您通知，以助您更好地规划业务的迁移工作。

1. 自2019年7月1日起，停止用户在控制台创建Swarm集群。如您有特别需求，请工单联系我们。
2. 自2019年12月31日起，下线Swarm相关的控制台和文档，并停止对Swarm集群的技术支持。您仍旧可以通过API来运维您的集群。

为了帮助您迁移容器集群至ACK，我们特别发布了Swarm迁移Kubernetes的指南，您可在官网查阅迁移方案概述。如您在使用中遇到任何问题，可与我们取得联系。

5.升级Terway组件的公告

- v1.0.9.15-g3957085-aliyun

  修复了偶发的升级失败的问题。

- v1.0.9.14-ga0346bb-aliyun
  - 修复Terway获取弹性网卡信息时偶发性失败的问题。
  - 修复创建容器时上报failed to move veth to host netns: file exists 的问题。
  - 新增对弹性网卡状态定期扫描，对于异常释放的弹性网卡会定期回收的功能。
  - 优化健康检查：Terway健康检查方式从HTTP路径检查优化成TCP端口检查。

请前往容器服务控制台升级最新的Terway系统组件，此次升级不会对业务造成影响。

6.升级Cloud Controller Manager组件的公告

v1.9.3.105-gfd4e547-aliyun

- 修复了annotation配置不生效的问题。
- 新增支持在控制台上重新命名SLB的功能。如果您是从v1.9.3.10及以前的版本升级上来的，还需要参考旧版本CCM如何支持SLB重命名为之前创建的SLB打上相应的tag以支持重命名。

请前往容器服务控制台，组件升级页面单击 Cloud Controller Manager 组件升级。

7.Kubernetes版本支持的公告

为了能够更好地方便您使用容器服务，确保您使用稳定又可靠的 Kubernetes 版本，我们推出 Kubernetes 版本支持机制，将同时支持四个版本的维保，每个版本的支持周期为一年，请您务必在维保周期结束之前升级您的 Kubernetes 集群。

更多信息请参见Kubernetes版本支持机制。

8.容器服务升级安全策略的公告

容器服务将在一周后升级集群授权管理安全策略，禁止所有未授权的子账号访问集群资源，请您及时参考配置子账号RBAC权限，对管理范围内的集群进行子账号应用权限设置及RAM授权操作。升级后子账号将只拥有授权域内集群的指定访问权限，在授权域外的原有兼容访问模式将被禁止，感谢您的配合。

9.修复部分集群节点未成功挂载数据盘的公告

我们发现近期有部分多可用区集群节点未能成功挂载数据盘，容器服务现已修复，新创建的集群将不再出现此问题。对于已经创建了的多可用区集群，如果您运行了较多的应用或者拉取镜像的数量不断增加时，可能会导致那些没有为Docker挂载数据盘的节点磁盘空间不足，为此我们也推出了解决方案，请参见集群节点挂载数据盘。如果您对修复有任何问题或者需要支持，请通过钉钉联系容器服务值班答疑。

10.Serverless Kubernetes 底层 ECI 容器实例即将商用收费的公告

Serverless Kubernetes 底层所调度的 ECI 容器实例服务即将于 2019 年 1 月 22 日10:00 商用收费，详情请参见产品定价，如果您拥有 Serverless Kubernetes 集群并已创建相应的容器实例，请提前做好预算规划，容器实例在存续时间内会收取您相应的费用。如果您已不再使用容器实例，请提前将其删除，以免扣费。Serverless Kubernetes 不会收费，将继续为您提供免费服务。

11.托管集群节点RAM角色收敛公告

当前托管集群节点默认的WorkerRolePolicy权限较大，为了进一步加强托管集群节点在多租户场景下的安全隔离性，容器服务Kubernetes版ACK（Container Service for Kubernetes）已收敛托管集群节点RAM角色绑定的权限。

角色授权

原有的RAM角色绑定权限被收敛后，原有节点角色中用于集群系统addon组件的权限策略将被删除，同时增加addon各组件对应的ACK系统角色。角色权限收敛后您在ACK控制台创建托管集群时，系统会提示进行以下系统角色授权，您可以使用主账号或具有AliyunRAMFullAccess或AdministratorAccess授权的子账号单击**前往RAM进行授权**，进入RAM的批量授权页面进行授权。

> **说明** 如果您使用OpenAPI创建集群，请使用授权链接进行授权。

角色授权

在批量授权页面最下方，单击**同意授权**后，重新登录容器服务管理控制台即可创建集群。

角色授权

上述批量授权将增加以下系统角色的授权，用于集群addon组件的OpenAPI调用：

- AliyunCSManagedLogRole
- AliyunCSManagedCmsRole
- AliyunCSManagedCsiRole
- AliyunCSManagedVKRole
- AliyunCSManagedNetworkRole
- AliyunCSManagedArmsRole

收敛后的默认WorkerRole的RAM策略定义如下。

```
{
  "Version": "1",
  "Statement": [{
```

```
    "Action": [
      "ecs:DescribeInstanceAttribute",
      "ecs:DescribeInstanceTypesNew",
      "ecs:DescribeInstances"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "log:GetProject",
      "log:GetLogStore",
      "log:GetConfig",
      "log:GetMachineGroup",
      "log:GetAppliedMachineGroups",
      "log:GetAppliedConfigs",
      "log:GetIndex",
      "log:GetSavedSearch",
      "log:GetDashboard",
      "log:GetJob"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "cr:GetAuthorizationToken",
      "cr:ListInstanceEndpoint",
      "cr:PullRepository"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow"
  }
 ]
}
```

```
}
```

12.升级Metrics Server组件公告

Metrics-Server组件底层依赖的网络http2库在网络抖动的场景下，偶发出现 `http2: no cached connection was available` 的报错，可能造成 `kubectl top node/pod` 无返回结果、HPA无法生效、删除namespace阻塞等现象。

影响范围

受此影响的版本可以通过升级组件的方式修复，v0.2.3-8a48069-aliyun及以上版本默认已修复，无需升级。

- 影响版本：v0.2.2-473c961-aliyun、v0.2.2-b4bf266-aliyun
- 修复版本：v0.2.3-8a48069-aliyun及以上

升级组件

1. 登录容器服务管理控制台。
2. 在控制台左侧导航栏中，单击**集群**。
3. 在**集群列表**页面单击目标集群**操作**列下的**更多**，选择**系统组件管理**。
4. 在组件管理页面单击Metrics-Server组件**操作**列下的**升级**，在**确认**对话框中单击**确定**。
   当Metrics-Server组件的**状态**列显示成功，表明组件升级成功。

13.漏洞修复公告

13.1. 修复Kubernetes Dashboard漏洞CVE-2018-18264的公告

阿里云容器服务Kubernetes 已修复Dashboard漏洞*CVE-2018-18264*，本文介绍该漏洞的影响版本及解决方法。阿里云容器服务Kubernetes内建的Kubernetes Dashboard是托管形态且已进行过安全增强，不受此漏洞影响。

背景信息

Kubernetes社区发现Kubernetes Dashboard安全漏洞*CVE-2018-18264*：使用Kubernetes Dashboard v1.10及以前的版本有跳过用户身份认证，及使用Dashboard登录账号读取集群密钥信息的风险 。

阿里云容器服务Kubernetes内建的Kubernetes Dashboard是托管形态且已进行过安全增强，不受此漏洞影响。

安全漏洞*CVE-2018-18264*的详细信息，请参见：

- kubernetes/dashboard/pull/3289
- kubernetes/dashboard/pull/3400
- kubernetes/dashboard/releases/tag/v1.10.1

影响版本

如果您的Kubernetes集群中独立部署了Kubernetes Dashboard v1.10及之前版本（v1.7.0-v1.10.0），同时支持登录功能且使用了自定义证书。

解决方法

- 如果您不需要独立部署的Dashboard，请执行以下命令，将Kubernetes Dashboard从集群中删除。

  ```
  kubectl --namespace kube-system delete deployment kubernetes-dashboard
  ```

- 如果您需要独立部署的Dashboard，请将Dashboard升级到v1.10.1版本，请参见升级Dashboard。
- 如果您使用阿里云容器服务Kubernetes版本托管的Dashboard，由于阿里云容器服务Kubernetes版本对此进行过安全增强，不受此漏洞影响，您仍可以直接在容器服务管理控制台上使用Dashboard。

13.2. 修复Kubernetes漏洞CVE-2018-1002105公告

阿里云容器服务Kubernetes 已修复漏洞*CVE-2018-1002105*，本文介绍该漏洞的影响及解决方法。

背景信息

Kubernetes社区发现安全漏洞：*CVE-2018-1002105*。Kubernetes用户可通过伪造请求，在已建立的API Server连接上提升权限访问后端服务，目前阿里云容器服务Kubernetes 已第一时间修复此漏洞，请登录容器服务管理控制台升级您的Kubernetes版本。

漏洞*CVE-2018-1002105*详细信息，请参见CVE-2018-1002105。

影响版本

- Kubernetes v1.0.x-1.9.x
- Kubernetes v1.10.0-1.10.10 (fixed in v1.10.11)
- Kubernetes v1.11.0-1.11.4 (fixed in v1.11.5)
- Kubernetes v1.12.0-1.12.2 (fixed in v1.12.3)

影响配置

- 容器服务Kubernetes集群启用了扩展API Server，并且kube-apiserver与扩展API Server的网络直接连通。
- 容器服务Kubernetes集群开放了 pod exec/attach/portforward 接口，用户可以利用该漏洞获得所有的kubelet API访问权限。

阿里云容器服务Kubernetes集群配置

- 阿里云容器服务Kubernetes集群的API Server默认开启了RBAC，通过主账号授权管理默认禁止了匿名用户访问。同时Kubelet 启动参数为 `anonymous-auth=false` ，提供了安全访问控制，防止外部入侵。
- 对于使用子账号的多租户容器服务Kubernetes集群用户，子账号可能通过pod exec/attach/portforward 接口越权访问。如果集群只有管理员用户，则无需过度担心。
- 子账号在不经过主账号自定义授权的情况下默认不具有聚合API资源的访问权限。

解决方法

请登录容器服务管理控制台，升级您的集群，升级的注意事项及具体的操作步骤，请参见升级集群。

- 如果您的集群版本为1.11.2请升级到1.11.5。
- 如果您的集群版本为1.10.4请升级到1.10.11或1.11.5版本。
- 如果您的集群版本为1.9及以下版本，请升级到1.10.11或1.11.5版本。在1.9版本升级1.10或1.11版本时，如集群使用了云盘数据卷，需在控制台先升级flexvolume插件。

> 说明 在容器服务管理控制台上，选择目标集群，单击导航栏更多 > 系统组件升级，在系统组件升级页面，选择flexvolume组件，单击升级。

由于Serverless Kubernetes在此漏洞发生前已进行加固，用户不受影响。

13.3. 修复runc漏洞CVE-2019-5736的公告

阿里云容器服务已修复runc漏洞CVE-2019-5736。本文介绍该漏洞的影响范围及解决方法。

背景信息

Docker、containerd或者其他基于runc的容器在运行时存在安全漏洞，攻击者可以通过特定的容器镜像或者exec操作获取到宿主机runc执行时的文件句柄并修改掉runc的二进制文件，从而获取到宿主机的root执行权限。

漏洞CVE-2019-5736的详细信息，请参见CVE-2019-5736。

影响范围

- 对于阿里云容器服务而言，影响范围如下：

Docker版本 < 18.09.2 的所有Docker Swarm集群和Kubernetes集群（不包含Serverless Kubernetes集群）。

- 对于用户自建的Docker/Kubernetes环境而言，影响范围如下：

  Docker版本 < 18.09.2 或者使用 runc版本 <= 1.0-rc6的环境。

解决方法

阿里云容器服务已经修复该漏洞，新创建的1.11或1.12版本的Kubernetes集群中的Docker版本已修复该漏洞。您可以通过以下方法修复已有集群中的漏洞：

- 升级Docker。升级已有集群的Docker到18.09.2或以上版本。该方案会导致容器和业务中断。
- 仅升级runc（针对Docker版本17.06）。为避免升级Docker引擎造成的业务中断，可以按照以下步骤，逐一升级集群节点上的runc二进制。
  i. 执行以下命令定位docker-runc。docker-runc通常位于*/usr/bin/docker-runc*路径下。

  ```
  which docker-runc
  ```

  ii. 执行以下命令备份原有的runc：

  ```
  mv /usr/bin/docker-runc /usr/bin/docker-runc.orig.$(date -Iseconds)
  ```

  iii. 执行以下命令下载修复的runc：

  ```
  curl -o /usr/bin/docker-runc -sSL https://acs-public-mirror.oss-cn-hangzhou.aliyuncs.com/runc/docker-runc-17.06-amd64
  ```

  iv. 执行以下命令设置docker-runc的可执行权限：

  ```
  chmod +x /usr/bin/docker-runc
  ```

  v. 执行以下命令测试runc是否可以正常工作：

  ```
  docker-runc -v
  # runc version 1.0.0-rc3
  # commit: fc48a25bde6fb041aae0977111ad8141ff396438
  # spec: 1.0.0-rc5
  docker run -it --rm ubuntu echo OK
  ```

  vi. （可选）如果是Kubernetes集群中的GPU节点，需要完成以下步骤继续安装nvidia-runtime。
    a. 执行以下命令定位nvidia-container-runtime。nvidia-container-runtime通常位于*/usr/bin/nvidia-container-runtime*路径下。

    ```
    which nvidia-container-runtime
    ```

    b. 执行以下命令备份原有的nvidia-container-runtime：

    ```
    mv /usr/bin/nvidia-container-runtime /usr/bin/nvidia-container-runtime.orig.$(date -Iseconds)
    ```

c. 执行以下命令下载修复的nvidia-container-runtime：

```
curl -o /usr/bin/nvidia-container-runtime -sSL https://acs-public-mirror.oss-cn-hangzhou.aliyuncs.com/runc/nvidia-container-runtime-17.06-amd64
```

d. 执行以下命令设置nvidia-container-runtime的可执行权限：

```
chmod +x /usr/bin/nvidia-container-runtime
```

e. 执行以下命令测试nvidia-container-runtime是否可以正常工作：

```
nvidia-container-runtime -v
#  runc version 1.0.0-rc3
#  commit: fc48a25bde6fb041aae0977111ad8141ff396438-dirty
#  spec: 1.0.0-rc5

docker run -it --rm -e NVIDIA_VISIBLE_DEVICES=all ubuntu nvidia-smi -L
#  GPU 0: Tesla P100-PCIE-16GB (UUID: GPU-122e199c-9aa6-5063-0fd2-da009017e6dc)
```

> **说明** 本测试运行在GPU P100机型中，不同GPU型号测试方法会有区别。

13.4. 修复Kubectl cp漏洞CVE-2019-11246的公告

Kubernetes最近公布了另一个kubectl cp相关漏洞CVE-2019-11246，此漏洞可能允许攻击者利用kubectl cp命令，采用路径遍历（Path Traversal）的方式将容器tar包中的恶意文件写入所在主机上的任何路径，该过程仅受本地用户的系统权限限制。

背景信息

该漏洞与不久前的CVE-2019-1002101漏洞影响相似，由于之前的相关漏洞修复。

kubectl cp命令用于用户容器和主机之间的文件拷贝，当从容器中拷贝文件时，Kubernetes会首先在容器中执行tar命令创建相应的归档文件，然后发送给客户端，kubectl会在用户主机上进行相应解压操作。

如果容器tar包中包含恶意文件，当攻击者具有kubectl cp命令的执行权限时，可以利用路径遍历Path Traversal。

官方修复pr请参见CVE-2019-11246: Clean links handling in cp's tar code#76788。

影响范围

- kubectl v1.11.x 及以前版本
- kubectl v1.12.1-v1.12.8（fixed in v1.12.9）
- kubectl v1.13.1-v1.13.5（fixed in v1.13.6）
- kubectl v1.14.1（fixed in v1.14.2）

> **说明** 您可以通过运行 `kubectl version --client` 命令，来查看kubectl版本。

解决方案

通过升级kubectl的版本来修复该漏洞。请参见安装 Kubectl，升级kubectl客户端，安装成功后请再次确认客户端版本号。

- 如果您的kubectl版本为1.12.x 请升级到1.12.9。
- 如果您的kubectl版本为1.13.x 请升级到1.13.6。
- 如果您的kubectl版本为1.14.x，请升级到1.14.2。
- 如果您的kubectl版本为1.11及以下版本，请升级到1.12.9、1.13.6或1.14.2版本。

13.5. 修复Kubectl cp漏洞CVE-2019-11249的公告

Kubernetes官方公布了一个kubectl cp相关漏洞CVE-2019-11249 ，此漏洞可能允许恶意攻击者利用目录遍历（Directory Traversal）的方式将容器TAR包中的恶意文件写入或替换至所在主机上目标路径之外的其他位置，该过程仅受本地用户的系统权限限制。

背景信息

kubectl cp命令用于用户容器和主机之间的文件拷贝，当从容器中拷贝文件时，Kubernetes会首先在容器中执行tar命令创建相应的归档文件，然后发送给客户端，kubectl会在用户主机上进行相应解压操作。

如果容器TAR包中包含恶意文件，当攻击者具有kubectl cp命令的执行权限时，可以利用目录遍历Directory Traversal。

在本次修复中，cp命令在执行untar过程中对所有子文件的目标路径执行了更严格的校验，禁止所有在cp目标路径外的解压后拷贝动作，以防止 `untar` 过程中的恶意攻击。

有关详细信息，请参见Kubernetes披露。

有关官方修复PR，请参见漏洞 CVE-2019-11249。

影响范围

您可以通过运行 `kubectl version --client` 命令，查看kubectl版本。

在以下范围内的版本均受此次漏洞影响：

- kubectl 1.0.x-1.12.x
- kubectl 1.13.0-1.13.8（fixed in v1.13.9）
- kubectl 1.14.0-1.14.4（fixed in v1.14.5）
- kubectl 1.15.0-1.15.1（fixed in v1.15.2）

解决方案

通过升级kubectl的版本来修复该漏洞。请参见安装Kubectl，升级kubectl客户端。安装成功后请再次确认客户端版本号。

- 如果您的kubectl版本为1.13.x，请升级到1.13.9。
- 如果您的kubectl版本为1.14.x，请升级到1.14.5。
- 如果您的kubectl版本为1.15.x，请升级到1.15.2。
- 如果您的kubectl版本为1.12.x及以下版本，请升级到1.13.9、1.14.5或1.15.2版本。

13.6. 修复Kubernetes漏洞CVE-2019-11253的公告

阿里云容器服务Kubernetes版已修复漏洞*CVE-2019-11253*，本文介绍该漏洞的影响及解决方法。

背景信息

Kubernetes社区发现安全漏洞：*CVE-2019-11253*。Kubernetes用户可通过伪造指定格式YAML文件，发送POST请求对集群进行DoS攻击。目前阿里云容器服务Kubernetes版本已第一时间修复此漏洞，请登录容器服务管理控制台升级您的Kubernetes版本。

漏洞*CVE-2019-11253*详细信息，请参见CVE-2019-11253。

影响版本

- Kubernetes v1.0.x~1.12.x
- Kubernetes v1.13.0~1.13.11 （fixed in 1.13.12）
- Kubernetes v1.14.0~1.14.7 （fixed in 1.14.8 ）
- Kubernetes v1.15.0~1.15.4 （fixed in 1.15.5）
- Kubernetes v1.16.0~1.16.1 （fixed in 1.16.2）

解决方法

请登录容器服务管理控制台升级您的集群至1.14.8版本，升级的注意事项及具体的操作步骤，请参见升级集群。

如果由于其他原因暂时不能升级集群，您可以通过以下操作降低此漏洞带来的风险，等待合适的时机后再升级集群。

- 您可以遵循权限最小化原则，合理配置子账号对目标集群的访问权限，取消不必要的创建和修改集群资源的权限，请参见授权概述。
- 您可以通过吊销KubeConfig功能，请主账号对疑似泄露的Config及时进行吊销操作，请参见吊销集群的KubeConfig凭证。

13.7. 修复 golang 漏洞 CVE-2019-16276 的公告

阿里云容器服务 Kubernetes 已修复漏洞 *CVE-2019-16276*，本文介绍该漏洞的影响及解决方法。

背景信息

Golang官方发现安全漏洞：*CVE-2019-16276*。Kubernetes 用户可以通过编写特定格式的请求头绕开认证代理中的过滤条件，向后端 API Server 发送扮演为其他用户或组的已认证请求。目前 Golang 官方已第一时间修复此漏洞，请升级您的 Golang 的版本。

漏洞 *CVE-2019-16276* 详细信息，请参见 CVE-2019-16276。

影响版本

所有使用了 Authenticating Proxy 代理认证方式进行认证，并且该认证代理服务器使用 Go 语言编写的集群。

解决方法

通过升级 Golang 的版本修复该漏洞。请参见安装 Go，下载 Golang 1.12.10 或者 1.13.1 重新进行认证代理服务器的编译和部署，安装成功后通过go version 再次确认 Golang 的版本。

13.8. 修复Kubectl cp 漏洞CVE-2019-1002101的公告

Kubectl cp 命令允许用户在容器和用户机器之间拷贝文件，攻击者可能通过在镜像或运行容器中植入带有符号链接（symbolic links）头的恶意 tar 包，在 cp 命令执行解压过程中修改或监控符号链接头同名目录下的任意文件，造成破坏。该漏洞已经在Kubectl工具的 v1.11.9、v1.12.7、v1.13.5 和 v1.14.0 版本中修复，请参见Install and Set Up kubectl，使用以上版本的 Kubectl 来避免该问题。

13.9. 修复kube-controller-manager SSRF漏洞CVE-2020-8555的公告

阿里云容器服务Kubernetes版已修复kube-controller-manager组件中存在的SSRF漏洞*CVE-2020-8555*。通过认证鉴权的攻击者可能通过服务端请求伪造获取控制节点（Master Node）网络下未经认证鉴权保护接口返回的任意信息。本文介绍该漏洞的影响、解决办法及防范措施。

SSRF漏洞在CVSS的评分为3.0（CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N），威胁等级为中级。

影响范围

攻击前提：

- kube-apiserver暴露了非认证本地端口。
- 存在其他不受保护的服务被暴露于控制台节点（Master Node）网络下。
- 恶意用户在目标集群有创建Pod权限并有StorageClass的写权限。

下列版本均在此CVE影响范围：

- kube-controller-manager v1.16.0~v1.16.8
- kube-controller-manager<v1.15.11

受影响的存储类型有：GlusterFS、Quobyte、 StorageFS、ScaleIO。

解决办法

经过了认证鉴权的攻击者可以利用kube-controller-manager当前存在的SSRF漏洞，通过创建带有指定存储类型（GlusterFS、Quobyte、StorageFS、ScaleIO）的Pod或StorageClass完成对控制台节点（Master Node）网络下其他服务的GET或POST请求，从而对控制台节点网络下未经认证鉴权保护的服务进行网络探测或内网服务攻击，例如通过开启了非认证8080端口的apiserver获取secret信息。

ACK集群默认不开启8080非安全端口，同时所有子账号需要经过相应的RBAC授权。默认状态下所有子账号（集群创建者除外）没有Pod和StorageClass的创建权限。当前解决办法先合入pr.k8s.io/89794提及的修复方法并提供相应的kube-controller-manager组件升级能力，以规避暴露在控制台节点网络下其他未保护服务的信息泄露危险。

防范措施

> **说明** 当前ACK已提供了包含漏洞修复的1.16.9-aliyun.1版本，请您尽快升级至最新的1.16.9-aliyun.1版本。

如果您由于业务原因暂时无法升级集群，建议您采取以下安全防范措施：

- 当前ACK集群默认关闭apiserver 8080非认证端口，请不要手动开启该端口。
- 排查控制台节点网络下暴露的Service是否开启了认证鉴权，对未保护的服务评估影响，关闭其中可能造成信息泄露的服务。
- 限制可疑用户创建Pod和StorageClass的写权限。

13.10. 修复漏洞CVE-2020-8558的公告

kube-proxy组件在iptables和ipvs模式下均需要设置内核参数 `net.ipv4.conf.all.route_localnet=1` ，从而允许本地回环访问。攻击者可能通过共享主机网络的容器，或在集群节点上访问同一个LAN或二层网络下的相邻节点上绑定监听了本地127.0.0.1端口的TCP/UDP服务，从而获取接口信息。如果服务没有设置必要的安全认证，可能会造成信息泄露风险。

影响范围

在下列版本的kube-proxy组件均在此CVE的影响范围内：

- kube-proxy v1.18.0~v1.18.3
- kube-proxy v1.17.0~v1.17.6
- kube-proxy≤v1.16.10

当前ACK集群节点中默认监听127.0.0.1的系统服务是需要认证的，且API Server也统一禁用了非认证端口。唯一暴露的是kubelet 10255的非认证只读端口，由于kubelet只读接口同样监听在0.0.0.0，因此即使修复了该漏洞在本地或特权容器中也同样可以获取到接口信息。综上，该CVE对ACK集群影响不大。

漏洞影响

当攻击者拥有主机网络配置能力或运行在一个具备了CAP_NET_RAW能力的容器实例时，就可以获取在目标节点上监听了127.0.0.1的服务socket信息。如果在目标主机上存在127.0.0.1可以访问到且不需要任何认证鉴权的暴露服务，那么该服务信息就能被攻击者获取。问题详情请参见issue。

漏洞评分：

- 如果集群API Server开启了非认证端口（默认8080），那么攻击者可能获取到API Server接口相关信息，威胁等级为高危漏洞，评分为8.8分。
- 如果集群API Server默认关闭了非认证端口，威胁等级为中危漏洞，评分为5.4分

可能的攻击者：

- 同一交换机内的其他共享主机实例。
- 本机的运行容器。

防范措施

建议您采取以下安全防范措施：

- 当前ACK集群默认关闭API Server 8080非认证端口，请勿手动开启该端口。
- 执行以下命令，在集群中配置iptables规则，用于拒绝非本地对127.0.0.1的访问流量。

```
iptables -I INPUT --dst 127.0.0.0/8 ! --src 127.0.0.0/8 -m conntrack ! --ctstate RELATED,ESTABLISHED,
DNAT -j DROP
```

- 严格控制集群节点共享主机的登录权限，及时吊销可能泄露的kubeconfig集群访问凭证。
- 禁止Container开启CAP_NET_RAW能力，执行以下命令，可以在pod spec中关闭Container的CAP_NET_RAW能力。

```
securityContext:
    capabilities:
     drop: ["NET_RAW"]
```

- 通过PodSecurityPolicy策略限制部署特权或共享主机网络容器，另外可以通过在策略中配置requiredDropCapabilities强制容器部署关闭CAP_NET_RAW能力。

13.11. 修复漏洞CVE-2020-13401的公告

CVE-2020-13401漏洞源于IPv6动态分配提供了IPv6的DHCP技术外，还支持Router Advertisement技术。路由器会定期向节点通告网络状态，包括路由记录。客户端会通过NDP进行自身网络配置。本文介绍该漏洞的影响。

> 注意 由于ACK未开启IPv6，所有ACK集群不受该漏洞影响，您无需做任何操作。

影响范围

对操作系统中启用了IPv6并且容器网络的CNI Plugins小于 V0.8.6版的节点有影响。

漏洞影响

恶意攻击者可以篡改主机上其他容器或主机本身的IPv6路由记录，实现中间人攻击。即使现在系统或者服务上没有直接使用IPv6地址进行网络请求通知，但是如果DNS返回了A(IPv4)和AAAA(IPv6)记录，许多HTTP库都会尝试IPv6进行连接，如果再回退到IPv4。

以下kubelet版本都包含了kubernetes-cni服务，所以都会受到该漏洞影响：

- kubelet v1.18.0~v1.18.3
- kubelet v1.17.0~v1.17.6
- kubelet<v1.16.11

> 注意 由于ACK未开启IPv6，所有ACK集群不受该漏洞影响，您无需做任何操作。

13.12. 修复漏洞CVE-2020-8559的公告

近日Kubernetes官方披露了kube-apiserver组件的安全漏洞，攻击者可以通过截取某些发送至节点kubelet的升级请求，通过请求中原有的访问凭据转发请求至其他目标节点，从而造成节点的权限提升漏洞。本文介绍该漏洞的影响范围、漏洞影响和防范措施。

影响范围

从v1.6.0之后到下列修复版本的所有kube-apiserver组件均包含漏洞代码：

- kube-apiserver v1.18.6

- kube-apiserver v1.17.9
- kube-apiserver v1.16.13

下列应用场景在此次漏洞的影响范围内：

- 如果集群运行业务中存在多租户场景，且以节点作为不同租户间隔离的安全边界。
- 不同集群间共享使用了相同的集群CA和认证凭据。

漏洞影响

- 由于kube-apiserver中在升级请求的代理后端中允许将请求传播回源客户端，攻击者可以通过截取某些发送至节点kubelet的升级请求，通过请求中原有的访问凭据转发请求至其他目标节点，从而造成被攻击节点的权限提升漏洞。该漏洞为中危漏洞，CVSS评分为6.4。
- 如果有多个集群共享使用了相同的CA和认证凭证，攻击者可以利用此漏洞攻击其他集群，这种情况下该漏洞为高危漏洞。

防范措施

对于此次漏洞的跨集群攻击场景，ACK集群使用了独立签发的CA，同时不同集群间认证凭据完全隔离。

对于集群内跨节点的攻击，建议您采取以下安全防范措施：

- 开启集群kube-apiserver审计日志，如果下列资源模型请求的请求响应码在300~399之间，则该集群可能已经被攻击：
  - pods/exec
  - pods/attach
  - pods/portforward
  - 任意资源模型的proxy类型（比如pods/proxy、services/proxy）
- 及时吊销可能泄露的kubeconfig凭证，并且遵循权限最小化原则，收敛子账号不必要的pods/exec、pods/attach、pods/portforward和proxy类型的资源模型RBAC权限。

13.13. 修复漏洞CVE-2020-8557的公告

kubelet的驱逐管理器（eviction manager）中没有包含对Pod中挂载的*/etc/hosts*文件的临时存储占用量管理，因此在特定的攻击场景下，一个挂载了*/etc/hosts*的Pod可以通过对该文件的大量数据写入占满节点的存储空间，从而造成节点的拒绝访问（Denial of Service）。本文介绍该漏洞的影响范围、漏洞影响和防范措施。

影响范围

下列版本的kubelet组件均在此CVE的影响范围内：

- kubelet v1.18.0~v1.18.5
- kubelet v1.17.0~v1.17.9
- kubelet<v1.16.13

漏洞影响

kubelet的驱逐管理器（eviction manager）中没有包含对Pod中挂载的*/etc/hosts*文件的临时存储占用量管理，因此在特定的攻击场景下，一个挂载了*/etc/hosts*的Pod可以通过对该文件的大量数据写入占满节点的存储空间，从而造成节点的拒绝访问（Denial of Service）。该漏洞为中危漏洞，CVSS评分为5.5。

具备以下特权的Pod拥有节点上*/etc/hosts*文件的写入权限：

- Pod中的容器具备CAP_DAC_OVERRIDE系统权限（默认具备）。
- Pod以root（UID为0）用户启动或者Pod Security Context中的allowPrivilegeEscalation设置为true（默认为true）。

防范措施

建议您采取以下安全防范措施：

- 通过使用集群Pod安全策略或其他admission准入机制强制Pod删除CAP_DAC_OVERRIDE系统权限，详情请参见使用Pod安全策略。
- 通过使用集群Pod安全策略或其他admission准入机制限制以root用户启动容器，或设置参数allowPrivilegeEscalation为false，详情请参见使用Pod安全策略。
- 对节点上的*/etc/hosts*文件进行有效的监控，比如在云安全中心中启用网页防篡改保护，详情请参见启用网页防篡改保护。
- 在集群节点上执行以下命令，可以发现运行在该节点上的Pod存在异常大小的*etc-hosts*文件。

```
find /var/lib/kubelet/pods/*/etc-hosts -size +1M
```

13.14. 修复漏洞CVE-2020-14386的公告

近日Linux社区披露了编号为CVE-2020-14386的内核漏洞。该漏洞源自packet socket包中的漏洞，攻击者可以通过漏洞实现越界写，能够写的长度为1~10个字节（来自漏洞发现者描述），除了可能造成提权和容器逃逸等风险，该攻击还可能造成集群节点内存耗尽并影响节点上运行的业务应用。

Linux社区披露编号为CVE-2020-14386的内核漏洞，详情请参见CVE-2020-14386。

影响范围

集群节点内核版本高于4.6的不同操作系统的Linux发行版均在此次漏洞的影响范围内，包括：

- Ubuntu Bionic (18.04) and newer
- Debian 9
- Debian 10
- CentOS 8/RHEL 8

对于容器服务ACK集群：

- 如果您的集群节点操作系统选择的是Alibaba Cloud Linux 2（内核版本为4.19.91-19.1.al7），您的集群会受到此次漏洞的影响。
- 如果您的集群节点操作系统是CentOS，由于当CentOS内核版本较低（3.10.0-1062），不在此漏洞影响范围内。

漏洞影响

CVE-2020-14386是内核af_packet模块中存在的内存溢出漏洞。漏洞触发需要CAP_NET_RAW权限。非Root用户没有该权限，但是在高版本Linux（内核版本高于4.6）上非特权用户能够创建user namespace，在该user namespace中会有CAP_NET_RAW权限。K8s或Docker容器默认具有CAP_NET_RAW权限，在高版本Linux中也存在触发该漏洞的可能。该漏洞能够允许攻击者实现越界写，能够写的长度为1~10个字节（来自漏洞发现者描述），可能造成提权或容器逃逸。Alibaba Cloud Linux 2的官方公告请参见漏洞公告 | Linux内核漏洞（CVE-2020-14386）。Alibaba Cloud Linux 2.1903安全漏洞修复信息，请参见Security Advisories 。

防范措施

- 在容器应用中通过securityContext删除CAP_NET_RAW权限，从而可以阻止进入到容器触发此漏洞。

```
spec:
 containers:
  -name: target-container
   ...
  securityContext:
   capabilities:
    drop:
     -NET_RAW
```

触发此漏洞的前提是攻击者具有CAP_NET_RAW权限，而大多数容器应用场景并不需要CAP_NET_RAW权限，可以通过PodSecurityPolicy（PSP）策略强制校验Pod中是否删除了CAP_NET_RAW权限对应的内核能力，以下为PSP策略模板。

> 说明 在ACK容器服务控制台可以开启PSP特性，并创建和绑定PSP策略，详情请参见使用PSP安全策略。

```
apiversion: extensions/v1beta1
kind: PodSecurityPolicy
metadata:
 name: no-cap-net-raw
spec:
 requiredDropCapabilities:
  -NET_RAW
   ...
```

- 通过组件管理安装gatekeeper组件，并确保已经安装了官方的constraint template。此时您可以创建下面的约束实例来限制容器应用中对CAP_NET_RAW的使用。

```
# Dropping CAP_NET_RAW with Gatekeeper
# (requires the K8sPSPCapabilities template)
apiversion: constraints.gatekeeper.sh/v1beta1
kind:  K8sPSPCapabilities
metadata:
  name: no-cap-net-raw
spec:
  match:
    kinds:
      - apiGroups: [""]
        kinds: ["Pod"]
    namespaces:
      #List of namespaces to enforce this constraint on
      - default
    # If running gatekeeper >= v3.1.0-beta.5,
    # you can exclude namespaces rather than including them above.
    excludedNamespaces:
      - kube-system
  parameters:
    requiredDropCapabilities:
      - "NET_RAW"
```

- Alibaba Cloud Linux 2已经发布关于本漏洞的最新公告和相关升级说明，如果您的节点使用的是Alibaba Cloud Linux 2操作系统，建议您参照下列步骤升级内核版本。
  i. 执行命令 `yum -y install kernel-4.19.91-21.2.al7` ，升级内核至修复版本。 或执行命令 `yum -y update kernel` ，直接升级至最新内核。
  ii. 重启系统，使新内核生效。如果节点上有正在运行的单点服务，请选择非业务高峰时段将节点排水后再重启节点。
  iii. 更多Alibaba Cloud Linux 2.1903安全漏洞修复信息，请参考Security Advisories 。