ALIBABA CLOUD

Alibaba Cloud

容器服务Kubernetes版

产品公告

文档版本：20220111

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.公告概览 06
2.【产品变更】容器服务OpenAPI鉴权优化公告 09
3.【系统恢复】容器服务关于2021年02月23日阿里云ECS管控API异常问题... 15
4.【产品变更】ACK Pro版集群商用通知 17
5.【产品变更】容器服务控制台导航栏调整公告 18
6.【产品变更】ACK关于K8s Dashboard功能下线公告 21
7.【K8s版本】关于Kubernetes 1.12.6及以前版本过期的公告 22
8.【组件升级】升级CCM组件公告 23
9.【组件升级】CoreDNS升级公告 24
10.【组件升级】Helm V2 Tiller升级公告 25
11.【产品变更】容器服务即将停止对Swarm的技术支持 27
12.【组件升级】升级Terway组件的公告 28
13.【K8s版本】Kubernetes版本支持的公告 29
14.【产品变更】容器服务升级安全策略的公告 30
15.【系统恢复】修复部分集群节点未成功挂载数据盘的公告 31
16.【产品变更】Serverless Kubernetes底层ECI容器实例商用收费的公告 32
17.【产品变更】托管集群节点RAM角色收敛公告 33
18.【CVE安全】漏洞修复公告 36
18.1. 漏洞CVE-2021-25742公告 36
18.2. 漏洞CVE-2021-41103公告 36
18.3. 漏洞CVE-2021-25741公告 37
18.4. 漏洞CVE-2021-25740公告 38
18.5. 修复漏洞CVE-2021-25738公告 41
18.6. 修复漏洞CVE-2021-25737公告 42
18.7. 修复漏洞CVE-2021-30465公告 42
18.8. 修复漏洞CVE-2021-3121公告 43

18.9. 漏洞CVE-2020-8562公告 44
18.10. 修复漏洞CVE-2021-25735公告 44
18.11. 修复NVIDIA GPU驱动漏洞CVE-2021-1056公告 45
18.12. 修复漏洞CVE-2020-8554公告 47
18.13. 修复漏洞CVE-2020-15257公告 48
18.14. 修复Kubernetes Dashboard漏洞CVE-2018-18264的公告 49
18.15. 修复Kubernetes漏洞CVE-2018-1002105公告 50
18.16. 修复runc漏洞CVE-2019-5736的公告 51
18.17. 修复Kubectl cp漏洞CVE-2019-11246的公告 52
18.18. 修复Kubectl cp漏洞CVE-2019-11249的公告 53
18.19. 修复Kubernetes漏洞CVE-2019-11253的公告 54
18.20. 修复 GoLang 漏洞 CVE-2019-16276 的公告 54
18.21. 修复Kubectl cp 漏洞CVE-2019-1002101的公告 55
18.22. 修复kube-controller-manager SSRF漏洞CVE-2020-8555的公... 55
18.23. 修复漏洞CVE-2020-8558的公告 56
18.24. 修复漏洞CVE-2020-13401的公告 57
18.25. 修复漏洞CVE-2020-8559的公告 57
18.26. 修复漏洞CVE-2020-8557的公告 58
18.27. 修复漏洞CVE-2020-14386的公告 59
18.28. 修复漏洞CVE-2020-8564、CVE-2020-8565、CVE-2020-8566... 61

1.公告概览

本文列举容器服务ACK发布的公告，类型包括近期发布、产品变更、K8s版本、组件升级、CVE安全、系统恢复。

◉ 近期发布 ○ 产品变更 ○ K8s版本 ○ 组件升级 ○ CVE安全 ○ 系统恢复

公告标题	公告时间
【CVE安全】漏洞CVE-2021-25741公告	2021年09月17日
【产品变更】容器服务OpenAPI鉴权优化公告	2021年08月10日
【K8s版本】关于Kubernetes 1.12.6及以前版本过期的公告	2021年04月24日
【系统恢复】容器服务关于2021年02月23日阿里云ECS管控API异常问题的公告	2021年02月23日
【组件升级】升级CCM组件公告	2021年01月07日
【产品变更】容器服务控制台导航栏调整公告	2020年12月16日
【产品变更】ACK Pro版集群商用通知	2020年11月26日
【产品变更】ACK关于K8s Dashboard功能下线公告	2020年10月23日
【组件升级】升级CoreDNS至1.6.2新版本公告	2020年10月23日
【组件升级】升级Metrics Server组件公告	2020年08月21日

公告标题	公告时间
【产品变更】容器服务OpenAPI鉴权优化公告	2021年08月10日
【产品变更】容器服务控制台导航栏调整公告	2020年12月16日
【产品变更】ACK Pro版集群商用通知	2020年11月26日
【产品变更】ACK关于K8s Dashboard功能下线公告	2020年10月23日
【产品变更】托管集群节点RAM角色收敛公告	2020年04月27日
【产品变更】容器服务即将停止对Swarm的技术支持	2019年07月23日
【产品变更】容器服务升级安全策略的公告	2019年05月08日
【产品变更】Serverless Kubernetes底层ECI容器实例商用收费的公告	2019年05月08日

公告标题	公告时间
【K8s版本】关于Kubernetes 1.12.6及以前版本过期的公告	2021年04月24日
【K8s版本】Kubernetes版本支持的公告	2019年07月24日

公告标题	公告时间
【组件升级】升级CCM组件公告	2021年01月07日
【组件升级】升级CoreDNS至1.6.2新版本公告	2020年10月23日
【组件升级】Helm V2 Tiller升级公告	2020年03月07日
【组件升级】升级Terway组件的公告	2019年07月23日

公告标题	公告时间
【CVE安全】漏洞CVE-2021-25741公告	2021年09月17日
【CVE安全】漏洞CVE-2021-25740公告	2021年07月23日
【CVE安全】修复漏洞CVE-2021-25738公告	2021年06月10日
【CVE安全】修复漏洞CVE-2021-25737公告	2021年06月10日
【CVE安全】修复漏洞CVE-2021-30465公告	2021年06月02日
【CVE安全】修复漏洞CVE-2021-3121公告	2021年05月25日
【CVE安全】漏洞CVE-2020-8562公告	2021年05月25日
【CVE安全】修复漏洞CVE-2021-25735公告	2021年04月15日
【CVE安全】修复NVIDIA GPU驱动漏洞CVE-2021-1056公告	2021年04月09日
【CVE安全】修复漏洞CVE-2020-8554公告	2020年12月08日
【CVE安全】修复漏洞CVE-2020-15257公告	2020年12月02日
【CVE安全】修复漏洞CVE-2020-8564、CVE-2020-8565、CVE-2020-8566的公告	2020年11月02日
【CVE安全】修复漏洞CVE-2020-14386的公告	2020年09月18日
【CVE安全】修复漏洞CVE-2020-8559的公告	2020年07月15日
【CVE安全】修复漏洞CVE-2020-8557的公告	2020年07月15日
【CVE安全】修复漏洞CVE-2020-8558的公告	2020年07月08日
【CVE安全】修复kube-controller-manager SSRF漏洞CVE-2020-8555的公告	2020年06月01日
【CVE安全】修复漏洞CVE-2020-13401的公告	2020年06月01日
【CVE安全】修复Kubernetes漏洞CVE-2019-11253的公告	2019年11月14日
【CVE安全】修复Golang漏洞CVE-2019-16276的公告	2019年11月15日

【CVE安全】修复Kubectl cp漏洞CVE-2019-11249的公告	2019年08月06日
【CVE安全】修复Kubectl cp漏洞CVE-2019-11246的公告	2019年07月01日
【CVE安全】修复Kubectl cp漏洞CVE-2019-1002101的公告	2019年05月08日
【CVE安全】修复runc漏洞CVE-2019-5736的公告	2019年02月12日
【CVE安全】修复Kubernetes Dashboard漏洞CVE-2018-18264的公告	2019年01月07日
【CVE安全】修复Kubernetes漏洞CVE-2018-1002105公告	2018年12月05日

公告标题	公告时间
【系统恢复】容器服务关于2021年02月23日阿里云ECS管控API异常问题的公告	2021年02月23日
【系统恢复】修复部分集群节点未成功挂载数据盘的公告	2019年08月05日

2.【产品变更】容器服务OpenAPI鉴权优化公告

阿里云容器服务Kubernetes版（ACK）将于2021年08月18日开始陆续加强部分OpenAPI对RAM用户（即子账号）和角色的权限控制，请您及时检查阿里云账号（即主账号）下RAM用户或角色的绑定权限，添加可能遗漏的权限策略，避免未授权的RAM用户或角色访问OpenAPI发生鉴权错误。

影响范围

本次鉴权优化完成后，若RAM用户或角色执行的操作没有对应权限，控制台或OpenAPI会提示包含 `RAM policy Forbidden` 或 `STSToken policy Forbidden` 的错误信息，同时错误信息中会包含所需权限的RAM Action名称。

错误信息示例（下面错误信息中包含的RAM Action名称为cs:DescribeEvents）：

```
RAM policy Forbidden for action cs:DescribeEvents
```

若您的RAM用户或角色使用了下表中的OpenAPI接口并且未授权，请您参考接口对应的RAM Action，及时前往RAM控制台添加指定RAM用户或角色的授权：

API名称	RAM Action	说明
DescribeEvents	cs:DescribeEvents	查询用户操作事件
StartAlert	cs:StartAlert	启动报警规则
StopAlert	cs:StopAlert	停止报警规则
DeleteAlertContact	cs:DeleteAlertContact	删除报警联系人
DeleteAlertContactGroup	cs:DeleteAlertContactGroup	删除报警联系人分组
OpenAckService	cs:OpenAckService	开通容器服务ACK
DescribeClusterResources	cs:DescribeClusterResources	根据集群ID查询该集群的所有资源
DescribeUserQuota	cs:DescribeUserQuota	查询集群及节点配额
DescribeClustersV1	cs:DescribeClustersV1	查询已创建的所有ACK集群的详情
DescribeExternalAgent	cs:DescribeExternalAgent	根据集群ID查询集群中部署注册集群的代理配置
DescribeKubernetesVersionMetadata	cs:DescribeKubernetesVersionMetadata	查询ACK支持的Kubernetes版本详情
DescribeClusterAddonUpgradeStatus	cs:DescribeClusterAddonUpgradeStatus	查询集群Addons升级状态
DescribeClusters	cs:DescribeClusters	查看容器服务中创建的所有集群（包括Swarm和Kubernetes集群）

API名称	RAM Action	说明
DescribeClusterNamespaces	cs:DescribeClusterNamespaces	查询集群命名空间
ModifyCluster	cs:ModifyCluster	根据集群ID修改该集群配置
MigrateCluster	cs:MigrateCluster	迁移集群
UpdateK8sClusterUserConfigExpire	cs:UpdateK8sClusterUserConfigExpire	更新用户自定义配置过期时间
DescribeClusterNodes	cs:DescribeClusterNodes	根据集群ID，查询该集群中的所有节点的详情
DescribeClusterAttachScripts	cs:DescribeClusterAttachScripts	查询手动添加实例到集群的脚本
GetUpgradeStatus	cs:GetUpgradeStatus	根据集群ID，查询该集群的升级状态
UpgradeCluster	cs:UpgradeCluster	根据集群ID，升级指定集群
PauseClusterUpgrade	cs:PauseClusterUpgrade	暂停用户集群升级
CancelClusterUpgrade	cs:CancelClusterUpgrade	取消处于升级状态的ACK集群
CreateTemplate	cs:CreateTemplate	创建一个编排模板
DescribeTemplates	cs:DescribeTemplates	查询已创建的所有编排模板详情
DescribeTemplateAttribute	cs:DescribeTemplateAttribute	根据编排模板ID，查询该编排模板的详情
UpdateTemplate	cs:UpdateTemplate	根据编排模板ID，更新编排模板
DeleteTemplate	cs:DeleteTemplate	根据编排模板ID，删除指定编排模板
CreateKubernetesTrigger	cs:CreateKubernetesTrigger	为应用创建触发器
GetKubernetesTrigger	cs:GetKubernetesTrigger	根据应用名称查询该应用的触发器
DeleteKubernetesTrigger	cs:DeleteKubernetesTrigger	根据应用触发器ID，删除应用触发器
InstallClusterAddons	cs:InstallClusterAddons	为集群安装组件
DescribeAddons	cs:DescribeAddons	查询平台支持的所有组件的详情
DescribeClusterAddonsUpgradeStatus	cs:DescribeClusterAddonsUpgradeStatus	根据组件名称查询该组件升级状态
DescribeClusterAddonsVersion	cs:DescribeClusterAddonsVersion	根据集群ID，查询集群中已安装的所有组件的详情
ModifyClusterConfiguration	cs:ModifyClusterConfiguration	只针对托管版集群

API名称	RAM Action	说明
UpgradeClusterAddons	cs:UpgradeClusterAddons	根据组件名称，将指定组件升级到指定版本
PauseComponentUpgrade	cs:PauseComponentUpgrade	暂停组件升级
ResumeComponentUpgrade	cs:ResumeComponentUpgrade	重新开始组件升级
CancelComponentUpgrade	cs:CancelComponentUpgrade	取消集群组件升级
UnInstallClusterAddons	cs:UnInstallClusterAddons	根据组件名称，卸载指定集群的组件
CreateAutoscalingConfig	cs:CreateAutoscalingConfig	创建自动伸缩配置

RAM权限策略修改示例

本示例介绍如何修改RAM用户或角色的RAM权限策略。关于RAM授权的相关操作，请参见自定义RAM授权策略。

场景一：RAM用户只对指定集群有cs:Get*权限，需要拥有指定集群所有OpenAPI的只读权限

例如，当前RAM用户只拥有指定集群的 `cs:Get*` ，对应的RAM权限策略如下：

```
{
    "Statement": [
        {
            "Action": "cs:Get*",
            "Effect": "Allow",
            "Resource": [
                "acs:cs:*:*:cluster/c2e63856bcd714197****"
            ]
        }
    ],
    "Version": "1"
}
```

若需要RAM用户在OpenAPI鉴权优化后仍具有原有集群所有OpenAPI的只读权限，修改后的RAM权限策略如下所示：

```
{
    "Statement": [
        {
            "Action": [
                "cs:Get*",
                "cs:List*",
                "cs:Describe*"
            ],
            "Effect": "Allow",
            "Resource": [
                "acs:cs:*:*:cluster/c2e63856bcd714197****"
            ]
        }
    ],
    "Version": "1"
}
```

> **说明** 若只包含 `cs:Get*` Action并不能匹配所有只读OpenAPI，需要再增加 `cs:List*` 和 `cs:Describe*` 。

场景二：为RAM用户授权指定集群的单个OpenAPI的操作权限

若您需要为RAM用户授权指定集群的单个OpenAPI操作权限，在该RAM权限策略中增加该OpenAPI对应的RAM Action即可。

例如，当前RAM权限策略如下：

```
{
    "Statement": [
        {
            "Action": [
                "cs:Get*",
                "cs:List*",
                "cs:Describe*"
            ],
            "Effect": "Allow",
            "Resource": [
                "acs:cs:*:*:cluster/c2e63856bcd714197****"
            ]
        }
    ],
    "Version": "1"
}
```

若需要授权OpenAPI `ModifyCluster` ，其对应RAM Action为 `cs:ModifyCluster` ，修改后的RAM权限策略如下所示：

```
{
    "Statement": [
        {
            "Action": [
                "cs:Get*",
                "cs:List*",
                "cs:Describe*",
                "cs:ModifyCluster"
            ],
            "Effect": "Allow",
            "Resource": [
                "acs:cs:*:*:cluster/c2e63856bcd714197****"
            ]
        }
    ],
    "Version": "1"
}
```

场景三：为RAM用户授权无法指定集群的OpenAPI的操作权限

部分OpenAPI无法指定集群授权（例如，`CreateCluster`、`DescribeClusters`及`DescribeEvents`等），若您需要给RAM用户授权这些无法指定集群的OpenAPI的操作权限，请不要在`Resource`中限定集群ID。

例如，当前RAM权限策略如下：

```
{
    "Statement": [
        {
            "Action": [
                "cs:Get*",
                "cs:List*",
                "cs:Describe*"
            ],
            "Effect": "Allow",
            "Resource": [
                "acs:cs:*:*:cluster/c2e63856bcd714197****"
            ]
        }
    ],
    "Version": "1"
}
```

若您需要授权无法指定集群的OpenAPI`DescribeEvents`，其对应的RAM Action为`cs:DescribeEvents`，修改后的RAM权限策略如下所示：

```
{
    "Statement": [
        {
            "Action": [
                "cs:DescribeEvents"
            ],
            "Effect": "Allow",
            "Resource": [
              "*"
            ]
        },
        {
            "Action": [
                "cs:Get*",
                "cs:List*",
                "cs:Describe*"
            ],
            "Effect": "Allow",
            "Resource": [
                "acs:cs:*:*:cluster/c2e63856bcd714197****"
            ]
        }
    ],
    "Version": "1"
}
```

3.【系统恢复】容器服务关于2021年02月23日阿里云ECS管控API异常问题的公告

背景

因02月23日ECS管控API发生异常，ACK及ACK Pro集群网络模式若为Terway（独占ENI或ENI多IP模式），部分用户在异常时间段所创建的Pod的IP会由于信息不一致而导致网络不通。我们建议相关用户核查此类Pod，如有问题需要加以修复，具体操作如下。

检查流程

步骤一：运行脚本检查节点

在每个节点上运行如下脚本。

```
#!/bin/bash
set -e
err(){
    echo "error at line $1"
}
trap 'err $LINENO' ERR
check(){
    cid=$1
    pid=$(docker inspect $cid -f '{{.State.Pid}}')
    if [ -z "$pid" ]; then
        echo 'cannot get pid from container $cid'
        return 1
    fi
    nsenter -t $pid -n curl -s --connect-timeout 4 100.100.100.200 -o /dev/null
}
for line in $(docker ps|grep -v k8s_POD|awk '$NF~/^k8s_/{print $1"_"$NF}'|awk -F_ '{print $
1"_"$3"_"$4"_"$5}')
do
    IFS=_ read cid cname pod namespace <<< $line
    if ! check $cid; then
        echo "pod $namespace/$pod has connectivity issues"
    fi
    if [[ "$cname" == "terway" && "$namespace" == "kube-system"  && "$pod" =~ ^(terway-|ter
way-eniip-|terway-eni-) ]]; then
        terway_container=$cid
    fi
done
if [ -n "$terway_container" ]; then
   for pod in $(docker exec -it $terway_container terway-cli mapping|sed -r "s/\x1B\[([0-9]
{1,3}(;[0-9]{1,2})?)?[mGK]//g"|awk '$3=="X"{print $1}')
   do
        echo "pod $pod on this host has connectivity issues"
   done
fi
```

预期输出：

```
pod *** has connectivity issues
```

如果输出以上信息，表示对应的Pod可能分配了一个有问题的IP。

步骤二：修复有问题的Pod

1. 重建Terway Pod。

```
kubectl -n kube-system delete pod -l app=terway
kubectl -n kube-system delete pod -l app=terway-eniip
kubectl -n kube-system delete pod -l app=terway-eni
```

2. 重建受影响的Pod。
   - 如果是通过Deployment或DaemonSet方式创建的Pod，您可以直接删除Pod，等待系统直接创建。
   - 如果是您直接创建的Pod，你需要删除Pod之后重新创建。

说明 以上脚本是对于网络通信异常的Pod节点进行网络插件重加载操作，运行完成之后，您可以再次运行检查流程中**步骤一：运行脚本检查节点**，以确认集群是否加固完成。如仍出现异常信息，请提交工单。

4.【产品变更】ACK Pro版集群商用通知

阿里云容器服务ACK Pro版集群于2020年10月23日00:00正式商用。

收费说明

阿里云容器服务ACK Pro版集群转为商用后，关于定价计费的更多信息，请参见产品计费。

ACK Pro版集群特性

针对许多对于生产环境有着高稳定性和高安全性要求的企业客户，ACK Pro版集群在ACK托管版集群的基础上进一步增强了可靠性、安全性，并且提供可赔付的SLA。更多信息，请参见ACK Pro版集群概述。

5.【产品变更】容器服务控制台导航栏调整公告

为了优化容器服务控制台的交互体验，阿里云容器服务对控制台的主导航栏和集群管理页面导航栏进行了聚合与分类的优化。

变更项	变更前	变更后	说明
主导航栏			• **Serverless集群**合并入**集群**。 • **服务网格**做跳转至服务网格ASM控制台，且转移至**多集群**导航栏中。 • **微服务治理**转移至集群管理页面的**应用**导航栏中。

变更项	变更前	变更后	说明
集群管理页面导航栏			二级导航栏调整后包含的功能菜单明细如下： • 节点管理：节点池、节点。 • 工作负载：无状态、有状态、守护进程集、任务、定时任务、容器组和自定义资源。 • 服务与路由：服务、路由。 • 配置管理：配置项、保密字典。 • 存储：存储声明、存储卷和存储类。 • 应用：Helm、灰度发布（公测）、微服务治理、服务网格、knative和工作流。 说明　**工作流**功能菜单只有申请了白名单的用户才能使用。 • 运维管理：事件列表、Prometheus监控、集群拓扑、组件管理、集群检查、集群升级和运行时升级。 • 安全管理：授权、集群审计、策略管理、配置巡检和运行时安全监控。

变更项	变更前	变更后	说明

6.【产品变更】ACK关于K8s Dashboard功能下线公告

阿里云容器服务ACK从K8s 1.18版本开始，已不再支持K8s Dashboard功能。如果您需要继续使用Dashboard功能，建议您在应用目录中安装kubernetes-dashboard应用。登录容器服务管理控制台安装kubernetes-dashboard。

7.【K8s版本】关于Kubernetes 1.12.6及以前版本过期的公告

根据阿里云容器服务Kubernetes版（ACK）的版本支持机制，Kubernetes 1.12.6及以前版本现已过期，ACK将不再为这些版本提供技术支持。请您尽快升级您的集群版本，关于如何升级集群，请参见升级ACK集群K8s版本。

关于ACK的版本支持机制，请参见版本机制。

8.【组件升级】升级CCM组件公告

为了提升ACK集群内LoadBalancer服务的稳定性，建议您升级集群的Cloud Controller Manager组件至最新版本。本文介绍如何升级Cloud Controller Manager组件版本。

背景信息

低于v1.9.3.380版本的Cloud Controller Manager组件存在以下问题，可能会影响ACK集群内LoadBalancer服务的稳定性：

- 默认服务器组更新异常。
- 存在同名虚拟服务器组，导致虚拟服务器组更新异常。

具体信息，请参见Cloud Controller Manager。

升级CCM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**页面中，单击目标集群名称或者目标集群右侧**操作**列下的**详情**。
4. 在集群管理页左侧导航栏中，选择**运维管理 > 组件管理**。
5. 在**组件管理**页面**核心组件**页签下单击**Cloud Control Manager**面板上的**升级**。

   > **说明** 若Cloud Control Manager面板上无升级按钮，说明CCM组件已是最新版本，无需升级。

6. 在**提示**对话框中单击**确认**。

9.【组件升级】CoreDNS升级公告

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至最新版本。本文介绍如何升级CoreDNS的版本。

背景信息

低于1.7.0版本的CoreDNS存在以下问题，可能会影响ACK集群内域名解析服务的稳定性：

- CoreDNS与APIServer连通性异常（例如APIServer重启、APIServer迁移、网络抖动）时，CoreDNS会因错误日志写入失败导致容器重启。更多信息，请参见Set klog's logtostderr flag。
- CoreDNS启动时会占用额外内存，默认采用的Memory Limit在较大规模集群下可能触发OOM（Out Of Memory）问题，严重时可能导致CoreDNS Pod反复重启无法自动恢复。更多信息，请参见CoreDNS uses a lot memory during initialization phase。
- CoreDNS存在若干可能影响Headless Service域名、集群外部域名解析的问题。更多信息，请参见plugin/kubernetes: handle tombstones in default processor和Data is not synced when CoreDNS reconnects to kubernetes api server after protracted disconnection。
- 在集群节点异常情况下，部分旧版本CoreDNS默认采用的容忍策略可能会导致CoreDNS Pod无法被驱逐，继而导致域名解析异常。

升级方式

升级CoreDNS前，请仔细阅读Core DNS变更记录和Core DNS社区介绍，了解不同版本间的差异和注意事项。

CoreDNS支持两种方式升级：自动升级和手动升级，具体的使用场景如下：

- 自动升级CoreDNS：如果您在ACK控制台的**组件管理**页面CoreDNS组件上可以看到升级按钮，说明该版本的CoreDNS组件支持自动升级。具体操作，请参见CoreDNS自动升级。
- 手动升级CoreDNS：如果您在ACK控制台的**组件管理**页面CoreDNS组件上无法看到升级按钮，且当前组件版本较低，说明您的Kubernetes集群版本过低，已不再维护。由于过低版本的Kubernetes集群不支持升级到最新的CoreDNS，针对这种情况，您需要手动升级CoreDNS至1.6.2版本后，再升级Kubernetes集群版本，然后按照自动升级方案将CoreDNS升级到最新版本。关于手动升级的具体操作，请参见CoreDNS手动升级。

相关文档

- CoreDNS
- CoreDNS自动升级
- CoreDNS手动升级

10.【组件升级】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

11.【产品变更】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。

12.【组件升级】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。

13.【K8s版本】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。

更多信息请参见版本机制。

14.【产品变更】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RAM用户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。

15.【系统恢复】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。

16.【产品变更】Serverless Kubernetes底层ECI容器实例商用收费的公告

Serverless Kubernetes底层所调度的ECI容器实例服务于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。

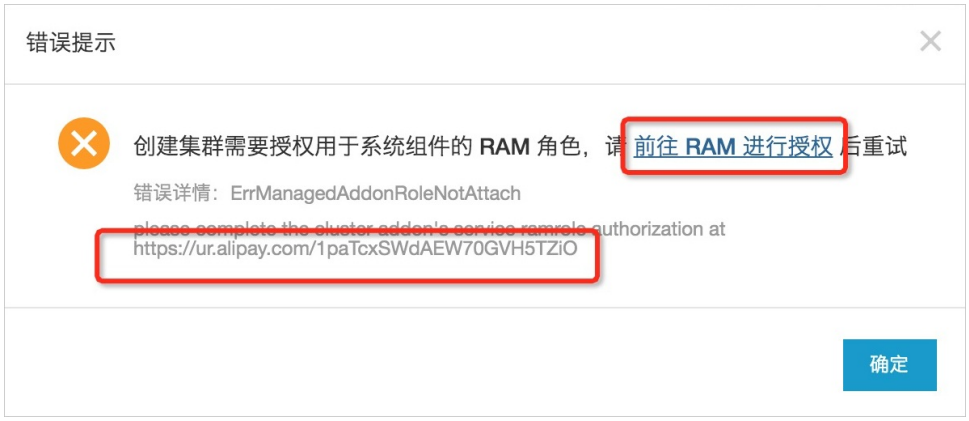
17.【产品变更】托管集群节点RAM角色收敛公告

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。

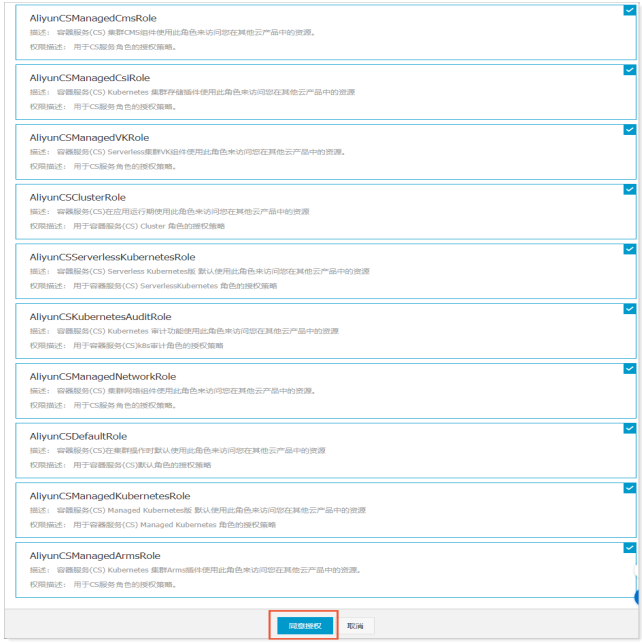
角色授权

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。



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。



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"
     }
  ]
}
```

18.【CVE安全】漏洞修复公告

18.1. 漏洞CVE-2021-25742公告

Kubernetes社区公布了安全漏洞CVE-2021-25742，攻击者可以通过定制化的Snippets特性创建或修改集群中的Ingress实例，从而获取集群中所有的Secret实例信息。本文介绍该漏洞的影响和影响范围，以及防范措施。

CVE-2021-25742漏洞被评估为高危漏洞，在CVSS的评分为7.6。

影响范围

以下枚举的ingress-nginx组件均在该漏洞影响范围内：

- v1.0.0
- ≤v0.49.0

Kubernetes社区在以下版本的ingress-nginx组件中修复了该漏洞：

- v1.0.1
- v0.49.1

关于漏洞的详细信息，请参见CVE-2021-25742。

漏洞影响

当集群运行在多租户场景下，如果存在非管理员用户拥有Ingress实例的创建和修改权限，那么该用户可以通过定制化的Snippets特性获取集群所有Secret实例信息，造成跨租户的越权访问和集群维度的敏感信息泄露。

防范措施

执行以下命令，修改kube-system命名空间下的nginx-configuration。

```
kubectl edit configmap -nkube-system nginx-configuration
```

在返回结果中设置 `allow-snippet-annotations` 为 `false` ：

```
data:
  allow-snippet-annotations: “false”
```

18.2. 漏洞CVE-2021-41103公告

Containerd社区公布了安全漏洞CVE-2021-41103，该漏洞源于Containerd中的缺陷，在容器根目录和一些系统插件中缺少必要的权限约束时，可使一个非特权的主机Linux用户拥有遍历容器文件系统并执行目标程序的权限。本文介绍该漏洞的影响和影响范围，以及防范措施。

CVE-2021-41103漏洞被评估为中危漏洞，在CVSS的评分为5.9。

影响范围

以下枚举的Containerd版本均在该漏洞影响范围内：

- <v1.4.11
- <v1.5.7

Containerd社区在以下版本的Containerd中修复了该漏洞：

- v1.14.11
- v1.5.7

关于漏洞的详细信息，请参见CVE-2021-41103。

漏洞影响

在多租户场景下，如果集群节点中的容器包含扩展权限（例如setuid），非特权的Linux用户可能发现并执行该程序。如果非特权的主机Linux用户UID碰撞到了容器中执行程序的所属用户或组，这个非特权的Linux用户可以读写该文件从而导致越权访问。

防范措施

1. 保证集群节点登录用户都是可信用户，限制非受信用户对集群节点的访问权限。
2. 收敛容器bundles目录中不必要的扩展权限。

18.3. 漏洞CVE-2021-25741公告

Kubernetes社区公布了安全漏洞CVE-2021-25741，该漏洞可使攻击者使用软链接的方式在容器中挂载指定subPath配置的目录逃逸到主机敏感目录。本文介绍该漏洞的影响和影响范围，以及防范措施。

CVE-2021-25741漏洞被评估为高危漏洞，在CVSS的评分为8.8。

影响范围

以下枚举的Kubernetes集群版本所安装的kubelet组件均存在该漏洞：

- v1.22.0~v1.22.1
- v1.21.0~v1.21.4
- v1.20.0~v1.20.10
- ≤v1.19.14

Kubernetes社区在以下版本修复了该漏洞：

- v1.22.2
- v1.21.5
- v1.20.11
- v1.19.15

关于该漏洞的详细信息，请参见#104980。

漏洞影响

在多租户场景下，拥有以Root用户启动容器权限的恶意攻击者可以利用该漏洞逃逸至主机文件系统，获取主机敏感目录的读写权限。

修复措施

阿里云容器服务Kubernetes 1.20.11-aliyun.1版本已修复该漏洞，建议尽快升级到该修复版本。

18.4. 漏洞CVE-2021-25740公告

Kubernetes社区公布了安全漏洞CVE-2021-25740，该漏洞可使攻击者利用混淆代理的方式访问到他们原本无法访问的集群服务。本文介绍该漏洞的影响和影响范围，以及检测方法和防范措施。

CVE-2021-25740漏洞被评估为低危漏洞，在CVSS的评分为3.0。

影响范围

当前所有Kubernetes集群版本均受该漏洞影响。关于该漏洞的详细信息，请参见#103675。

漏洞影响

如果攻击者拥有编辑或者创建Endpoints或者EndpointSlices的权限，可以通过Kubernetes API修改Endpoints指向的地址，则攻击者可能会利用LoadBalancer或Ingress来访问本不应访问的服务后端IP地址。另外如果目标NetworkPolicy已经信任LoadBalancer或Ingress，则NetworkPolicy不能用于阻止跨命名空间服务的暴露。

检测方法

当Services对象没有指定Selector且依赖自定义Endpoints时，容易受到该漏洞的攻击，建议您执行以下命令，手动筛查集群中所有Service和Selector。

```
kubectl get svc --all-namespaces -o=custom-columns='NAME:metadata.name,NAMESPACE:metadata.n
amespace,SELECTOR:spec.selector'
```

> **说明** 当 `default/kubernetes Service` 没有指定Selector但拥有自己的Endpoints时，该Endpoints被API Server管理，属正常现象。

防范措施

该漏洞暂时没有修复版本，只能通过限制易受攻击的功能来进行缓解。为了降低风险，建议您执行以下命令更新 `system:aggregate-to-edit` 角色来限制对Endpoints和EndpointSlices的写访问权限，从 `admin` 和 `edit` 角色中删除对Endpoints的写访问权限。

```
# Allow kubectl auth reconcile to work
kubectl annotate --overwrite clusterrole/system:aggregate-to-edit rbac.authorization.kubern
etes.io/autoupdate=true
# Test reconcile, then run for real if happy
kubectl auth reconcile --remove-extra-permissions -f aggregate_to_edit_no_endpoints.yaml.tx
t --dry-run
kubectl auth reconcile --remove-extra-permissions -f aggregate_to_edit_no_endpoints.yaml.tx
t
# Prevent autoreconciliation back to old state
kubectl annotate --overwrite clusterrole/system:aggregate-to-edit rbac.authorization.kubern
etes.io/autoupdate=false
```

上述命令中涉及的*aggregate_to_edit_no_endpoints.yaml.txt*样例如下：

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
```

```
  annotations:
    rbac.authorization.kubernetes.io/autoupdate: "true"
  creationTimestamp: null
  labels:
    kubernetes.io/bootstrapping: rbac-defaults
    rbac.authorization.k8s.io/aggregate-to-edit: "true"
  name: system:aggregate-to-edit
rules:
- apiGroups:
  - ""
  resources:
  - pods/attach
  - pods/exec
  - pods/portforward
  - pods/proxy
  - secrets
  - services/proxy
  verbs:
  - get
  - list
  - watch
- apiGroups:
  - ""
  resources:
  - serviceaccounts
  verbs:
  - impersonate
- apiGroups:
  - ""
  resources:
  - pods
  - pods/attach
  - pods/exec
  - pods/portforward
  - pods/proxy
  verbs:
  - create
  - delete
  - deletecollection
  - patch
  - update
- apiGroups:
  - ""
  resources:
  - configmaps
  - persistentvolumeclaims
  - replicationcontrollers
  - replicationcontrollers/scale
  - secrets
  - serviceaccounts
  - services
  - services/proxy
  verbs:
  - create
```

```
  - delete
  - deletecollection
  - patch
  - update
- apiGroups:
  - apps
  resources:
  - daemonsets
  - deployments
  - deployments/rollback
  - deployments/scale
  - replicasets
  - replicasets/scale
  - statefulsets
  - statefulsets/scale
  verbs:
  - create
  - delete
  - deletecollection
  - patch
  - update
- apiGroups:
  - autoscaling
  resources:
  - horizontalpodautoscalers
  verbs:
  - create
  - delete
  - deletecollection
  - patch
  - update
- apiGroups:
  - batch
  resources:
  - cronjobs
  - jobs
  verbs:
  - create
  - delete
  - deletecollection
  - patch
  - update
- apiGroups:
  - extensions
  resources:
  - daemonsets
  - deployments
  - deployments/rollback
  - deployments/scale
  - ingresses
  - networkpolicies
  - replicasets
  - replicasets/scale
  - replicationcontrollers/scale
  verbs:
```

```
  verbs:
  - create
  - delete
  - deletecollection
  - patch
  - update
- apiGroups:
  - policy
  resources:
  - poddisruptionbudgets
  verbs:
  - create
  - delete
  - deletecollection
  - patch
  - update
- apiGroups:
  - networking.k8s.io
  resources:
  - ingresses
  - networkpolicies
  verbs:
  - create
  - delete
  - deletecollection
  - patch
  - update
```

通过上述操作，您可以阻止新版本的Kubernetes修改 `system:aggregate-to-edit` 角色的默认权限。从Kubernetes v1.14.0之后就没有新的默认权限被添加到这个角色。但是只要Kubernetes后期修复了此漏洞，建议您主动去除 `autoupdate=false` 这个注解。

对于因为业务需要，确实需要拥有编辑Endpoints和EndpointSlices权限的用户，建议您新创建一个角色，赋予其想要的权限，专门用于该业务。

类似的攻击也可能发生在使用Ingress，并支持转发ExternalName Services流量的场景中。在该场景下，攻击者同样可跨Namespace转发流量，访问到敏感Endpoint的内容。如果您正在使用Ingress API，建议您确认所用Ingress是否支持ExternalName Services的流量转发，如果不支持该功能则不受影响。如果支持ExternalName Services的流量转发，则需要暂时禁用该功能。

18.5. 修复漏洞CVE-2021-25738公告

近日Kubernetes官方披露了Java客户端的相关漏洞，攻击者可以利用指定的特殊YAML模板进行代码执行攻击。本文介绍该漏洞的影响范围和防范措施。

CVE-2021-25738漏洞在CVSS的评分为6.7。

影响范围

下列版本的官方Java客户端都包含该漏洞：

- Kubernetes Java Client=v12.0.0
- Kubernetes Java Client≤v11.0.1
- Kubernetes Java Client≤v10.0.1

- Kubernetes Java Client≤v9.0.2

社区在下列版本修复了该漏洞：

- Kubernetes Java Client master：1676
- Kubernetes Java Client≥v12.0.1：1691
- Kubernetes Java Client≥v11.0.2：1692

防范措施

在应用中，使用官方推荐的修复版本Java客户端访问集群。关于漏洞的更多信息，请参见 1698。

18.6. 修复漏洞CVE-2021-25737公告

Kubernetes社区披露了**kube-apiserver**组件的相关漏洞。由于Kubernetes集群没有校验EndpointSlices实例的端点IP是否合法，攻击者可能重定向访问集群节点的本地网络。本文介绍该漏洞，以及漏洞的影响范围和防范措施。

CVE-2021-25737漏洞在CVSS的评分为2.7，威胁等级属于低级。

漏洞现象

通过Kubectl命令行或API的方式，列举集群中存在的EndpointSlices实例。如果EndpointSlices实例的端点包含 `127.0.0.0/8` 和 `169.254.0.0/16` 网段内的某个地址，则该集群可能会受到该漏洞攻击。关于该漏洞的详细信息，请参见 #101084。

漏洞影响

下列官方**kube-apiserver**组件版本均包含该漏洞：

- v1.21.0
- v1.20.0 ~ v1.20.6
- v1.19.0 ~ v1.19.10
- v1.16.0 ~ v1.18.18

> **说明** 在v1.16~v1.18中默认没有开启EndpointSlices特性，如果在这个版本区间的EndpointSlices特性没有开启，您就不会受到该漏洞影响 。

Kubernetes社区在下列版本中修复了该漏洞：

- v1.21.1
- v1.20.7
- v1.19.11
- v1.18.19

防范措施

您可以通过部署**gatekeeper**组件创建Validating Admission Webhook，强制阻止在 `127.0.0.0/8` 和 `169.254.0.0/16` 网段的EndpointSlices实例 。具体操作，请参见gatekeeper。

18.7. 修复漏洞CVE-2021-30465公告

Open Containers社区披露了runC相关的漏洞，攻击者通过创建恶意Pod，利用符号链接以及条件竞争漏洞将宿主机目录挂载至容器中，最终可能导致容器逃逸问题。本文介绍该漏洞，以及该漏洞影响、影响范围和防范措施。

漏洞描述

对于K8s集群，攻击者将目标挂载路径设置为一个容器Volume在主机上的根目录的软链接（比如，emptyDir卷对应的软链接路径为*/var/lib/kubelet/pods/$MY_POD_UID/volumes/kubernetes.io~empty-dir*），以此来获取主机上的挂载点。由于挂载的源路径是攻击者可以控制的目录，攻击者可以将源路径中的子目录软链接到主机根目录上，并通过条件竞争TOCTTOU（Time Of Check To Time Of Use）的特定手段在一定条件让恶意容器中的指定目录挂载到主机的根目录。

CVE-2021-30465漏洞为高危漏洞，CVSS漏洞评分为7.6。更多信息，请参见官方公告。

漏洞影响

当Pod中启动多个容器时，攻击者可以利用条件竞争，通过构造一个恶意Pod并挂载包含了软链接的目标路径，在特定条件下可以逃逸并获取容器 `rootfs` 之外的主机文件系统访问权限。

影响范围

runC小于等于1.0.0-rc94的版本均包含该漏洞。

该漏洞的修复版本为runC 1.0.0-rc95。更多信息，请参见runC v1.0.0-rc95。

防范措施

手动升级Containerd至最新版本，关于Containerd的最新版本信息，请参见v1.0.0-rc95。

18.8. 修复漏洞CVE-2021-3121公告

Kubernetes社区披露了编号为CVE-2021-3121的安全漏洞，存在该漏洞的程序可能会因为处理了包含恶意Protobuf消息而崩溃。如果您使用的Gogo Protobuf编译器版本过低，可能存在该漏洞。本文介绍该漏洞的影响和影响范围，以及防范措施。

漏洞影响

kubernetes系统组件由于自身有应对崩溃的恢复机制，当遇到恶意提交的Protobuf消息时不会中断服务，所以不在该漏洞的影响范围内。

在应用系统中程序接收处理Protobuf消息时，如果组件没有应对崩溃的恢复机制，那么这类程序都在该漏洞影响范围内，且被恶意攻击时服务可能会中断。

影响范围

Kubernetes社区经过测试验证API Server不受该漏洞的影响，但为了避免您受到该安全漏洞隐患的影响，社区对相关Protobuf文件进行了升级，具体修复版本如下：

- 1.21版本：1.21.0、1.21.1。
- 1.20版本：1.20.6、1.20.7。
- 1.19版本：1.19.10、1.19.11。
- 1.18版本：1.18.18、1.18.19。

防范措施

如果在您的应用系统代码中使用了自动生成的Protobuf消息，并且发现相关组件因为以下异常退出，则可能存在该漏洞。

```
panic: runtime error: index out of range [-9223372036854775804]
goroutine 1 [running]:
v1.(*MessageName).Unmarshal(0xc000057ef8, 0xc0000161a0, 0xa, 0x10, 0xc000057ec8, 0x1)
        .../protofile.pb.go:250 +0xb86
```

如果您使用了Protobuf消息的相关组件，推荐将Gogo Protobuf编译器升级到漏洞修复版本（v1.3.2或更高的版本），再基于升级后的Protobuf编译器重新生成相关的Protobuf消息。

18.9. 漏洞CVE-2020-8562公告

K8s社区披露了编号为CVE-2020-8562的安全漏洞。攻击者可以通过某种方式绕过API Server对内网Proxy请求的IP限制，访问到集群内网中的ControlPlane管控组件，从而造成越权访问的问题。本文介绍该漏洞的影响和影响范围，以及防范措施。

CVE-2020-8562漏洞在CVSS的评分为2.2，威胁等级属于低级。

漏洞影响

由于安全原因，Kubernetes社区已经禁止了由用户触发的对Services，Pods，Nodes，StorageClass对象的内网Proxy访问权限。在这个禁止触发流程中，Kubernetes首先会对请求进行域名解析，并且校验Proxy请求的IP地址是否属于本地地址（169.254.0.0/16或127.0.0.1/8）的范围。然后再进行第二次域名解析，且不再进行IP地址的校验。如果一个非标准的DNS服务器不断返回不同的非缓存解析请求，攻击者可以利用竞争条件绕过代理IP地址限制，并成功访问内网ControlPlane管控组件。

攻击者能够成功绕过拦截的前提是拥有节点的创建或修改权限，并且能够以Proxy的方式访问节点。或者拥有对StorageClass对象的创建和修改权限，并且能够获取到kube-controller-manager的组件日志。

漏洞现象

从集群API Server审计日志中寻找关键字为address not allowed的日志，当有大量相关日志时，说明该集群可能受到该漏洞攻击。

> **说明** 正常情况下集群API Server审计日志中不会有关键字为address not allowed的日志。

影响范围

以下枚举的Kubernetes集群版本所安装的kube-apiserver均存在该漏洞：

- Kubernetes≤v1.21.0
- Kubernetes≤v1.20.6
- Kubernetes≤v1.19.10
- Kubernetes≤v1.18.18

K8s社区尚未发布针对该漏洞的修复版本。

防范措施

遵循权限最小化原则，对节点和StorageClass对象的创建和修改权限严格限制。

18.10. 修复漏洞CVE-2021-25735公告

近日Kubernetes官方披露了kube-apiserver组件的安全漏洞，攻击者可以在某些场景下绕过Validating Admission Webhook的准入机制更新节点。本文介绍该漏洞的影响和影响范围，以及防范措施。

CVE-2021-25735漏洞评级为中危漏洞，CVSS漏洞评分为3.0。

影响范围

该漏洞仅影响使用了Validating Admission Webhook，并且该Webhook会依赖节点更新前原状态的某些字段进行准入校验的集群。

以下枚举的kube-apiserver版本均包含该漏洞：

- kube-apiserver v1.20.0 ~ v1.20.5
- kube-apiserver v1.19.0 ~ v1.19.9
- kube-apiserver<=v1.18.17

该漏洞的修复版本为：

- kube-apiserver v1.21.0
- kube-apiserver v1.20.6
- kube-apiserver v1.19.10
- kube-apiserver v1.18.18

漏洞影响

> **说明**
> - 如果您的集群使用默认配置，没有扩展新的Validating Admission Webhook，不在该漏洞影响范围内。
> - 集群默认的NodeRestriction准入插件不在该漏洞的影响范围内。

如果您的集群中存在使用Validating Admission机制进行节点更新准入校验的Webhook，并且该Webook的准入依赖节点原状态的某些字段，则攻击者可以通过某些手段绕过准入校验完成对节点实例模型的修改。

防范措施

如果集群存在上述所描述的影响范围内的Validating Admission Webhook，在集群升级到修复版本前无法保证现有准入机制的安全性，请通过RBAC授权管理等其他途径限制对Node节点的更新权限。具体操作，请参见配置RAM用户RBAC权限。

18.11. 修复NVIDIA GPU驱动漏洞CVE-2021-1056公告

NVIDIA公布了关于NVIDIA驱动的一个漏洞CVE-2021-1056，该漏洞是NVIDIA GPU驱动程序与设备隔离相关的安全漏洞。Kubernetes集群中如果存在阿里云GPU（EGS）的节点，都有可能存在该漏洞。本文介绍该漏洞的背景信息、影响范围和解决方案。

背景信息

漏洞CVE-2021-1056是NVIDIA GPU驱动程序与设备隔离相关的安全漏洞。当容器以非特权模式启动，攻击者利用这个漏洞，在容器中创建特殊的字符设备文件后，能够获取宿主机上所有GPU设备的访问权限。

关于漏洞的详细信息，请参见CVE-2021-1056。

影响范围

按照NVIDIA官方给出的漏洞说明信息，目前受影响的NVIDIA GPU驱动版本如下图所示。更多信息，请参见NVIDIA官网。

CVE IDs Addressed	Software Product	Operating System	Driver Branch	Affected Versions	Updated Driver Version
CVE-2021-1052 CVE-2021-1053	GeForce	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
	NVIDIA RTX/Quadro, NVS	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
	Tesla	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
CVE-2021-1056	GeForce	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
	NVIDIA RTX/Quadro, NVS	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
			R390	All version prior to 390.141	390.141
	Tesla	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
			R418	All versions prior to 418.181.07	418.181.07

- 如果您选择自定义安装或更新GPU驱动，请参考上图确认您安装的GPU驱动是否受该漏洞影响。
- 如果您选择由阿里云容器服务Kubernetes版集群默认安装NVIDIA GPU驱动。依据NVIDIA官方信息，目前已验证受影响的容器服务Kubernetes集群版本包括：
  - ACK 1.16.9-aliyun.1（默认安装GPU驱动版本为418.87.01版本）
  - ACK 1.18.8-aliyun.1（默认安装GPU驱动版本为418.87.01版本）

> **说明** 其他版本的ACK集群，GPU节点默认安装的NVIDIA GPU驱动，尚未出现在NVIDIA官方信息中。如果将来有新的官方信息变化，阿里云容器服务团队将及时跟进帮助您升级修复。

确认GPU节点NVIDIA驱动版本

登录到GPU节点，执行以下命令，查看驱动版本。

> **说明** 关于如何登录到GPU节点，请参见通过密码认证登录Linux实例或通过密码认证登录Windows实例。

```
nvidia-smi
```

预期输出：

```
Fri Apr 16 10:58:19 2021
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 418.87.01    Driver Version: 418.87.01    CUDA Version: 10.1     |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla V100-SXM2...  On   | 00000000:00:07.0 Off |                    0 |
| N/A   34C    P0    37W / 300W |      0MiB / 16130MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID   Type   Process name                             Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

从上述输出的信息，可以知道该节点的GPU驱动版本为418.87.01。

解决方案

> **注意** 升级节点GPU驱动的过程需要重启节点，节点上的业务将受到影响。

请您根据上图的NVIDIA官方信息，将节点升级到对应驱动版本进行漏洞修复：

- R390系列：请升级至390.141版本。
- R418系列：请升级至418.181.07版本。
- R450系列：请升级至450.102.04版本。
- R460系列：请升级至460.32.03版本。

关于升级ACK集群GPU节点驱动方法，请参见通过节点池升级已有节点的NVIDIA驱动、手动升级GPU节点驱动和通过节点池创建新NVIDIA驱动版本的节点。

18.12. 修复漏洞CVE-2020-8554公告

近日Kubernetes社区披露了使用LoadBalancer或External IPs进行中间人攻击的漏洞，在一个多租集群中攻击者可以通过创建和更新Service实例状态等字段来劫持集群中来自其他Pod的流量。

目前CVE-2020-8554漏洞评级为中危漏洞，CVSS漏洞评分为3.0。

影响范围

当前所有版本的Kubernetes集群均在该漏洞影响范围内，该漏洞源自Kubernetes设计上的安全缺陷，明确的修复计划将在issue 97110中给出。

对于ACK集群用户，如果您的集群运行在多租户场景下，或者集群中运行的应用可能来自非受信的用户所部署，此时您可以通过在apiserver审计日志中搜寻Service的status对象的patch事件来发现可疑事件。具体操作，请参见查看详细日志记录。

漏洞描述

在多租集群中，攻击者可以通过下面两种方式完成对指定Service的流量劫持。

- 创建ClusterIP类型的Service，并设置服务实例spec中的externalIP字段来指定劫持该IP内的流量。
- 对于LoadBalancer类型的Service，攻击者可以通过设置Service实例中的spec.loadBalancerIP字段并且修改status.loadBalancer.ingress.ip达到流量劫持的目的。

防范措施

目前Kubernetes社区官方还没有提供针对该漏洞的修复方案，由于漏洞修复可能涉及原生模型较大的改动，预计在官方正式修复版本发布前还需一段较长的时间。建议您优先采用以下方案防范攻击：

- 对于external IPs的使用建议如下：
  - 通过admission webhook的准入校验方式限制external IPs的使用，详情请参见Kubernetes官方给出的externalip-webhook源码和部署说明。
  - 通过OPA Gatekeeper来限制external IPs的使用范围，具体操作，请参见gatekeeper。ConstraintTemplate和Constraint的示例模板请参考externalip。
- 对于LoadBalancer类型的IP使用建议如下：
  - 尽可能收敛对Service的status对象的patch权限。
  - 可采用上述external IPs的使用建议，通过admission webhook或OPA Gatekeeper的方式来限制对LoadBalancer IP的使用。

18.13. 修复漏洞CVE-2020-15257公告

近日containerd社区披露了编号为CVE-2020-15257的GHSA-36xw-fx78-c5r4安全漏洞。一个使用Host Networking Namespace的容器，且容器内UID设置为0时，攻击者可以通过containerd-shim API来操作宿主机上其他的containerd-shim进程，从而发生提权攻击。本文主要描述了该漏洞的影响范围，漏洞产生的原因和防范措施。

目前CVE-2020-15257漏洞评级为中危漏洞，CVSS漏洞评分为5.2。

影响范围

containerd社区在1.3.9和1.4.3版本修复了该漏洞，当前ACK所有版本的k8s集群均在该漏洞影响范围内。您可以使用以下kubectl命令查看集群内有哪些Pod共享了主机网络。

```
kubectl get pods -A -o json |
  jq -c '.items[] | select(.spec.hostNetwork==true) |[.metadata.namespace, .metadata.name]'
```

漏洞描述

containerd和containerd-shim之间采用abstract socket通信，当容器共享了宿主机的网络namespace且容器内部UID设置为0时，攻击者就可以以Root用户访问宿主机上的containerd-shim进程，进而逃逸出容器并使用containerd-shim的相关接口发起下一步的提权攻击。

> **说明**
> - containerd作为支撑Kubernetes集群运行时，负责管理底层的runC容器，通常包含一个守护进程并通过本地的Unix套接字暴露gRPC服务接口用于容器生命周期的各种管理操作。
> - containerd-shim作为containerd的一个组件，用于隔离containerd守护进程和容器进程，并且通过containerd-shim调用runC接口直接和容器交互。

防范措施

为了尽可能降低您受到提权攻击的概率，您需要尽可能地让业务应用运行在独立的五个核心Net、Mount、IPC、PID或UTS Namespace内，与宿主机共享的namespace越多，被攻击的概率就越高。您也尽可能不要在Pod配置中使用Host Networking配置，可以通过以下方式限制Host Networking的使用：

- 开启PSP特性，通过PSP策略中的hostNetwork配置可以限制指定namespace的Pod无法使用共享主机网络。ACK容器服务提供了PSP安全策略的控制台配置能力，具体操作，请参见配置容器安全策略（旧版）。
- 装gatekeeper组件，具体操作，请参见gatekeeper。基于示例OPA策略。

如果因为业务原因必须使用Host Networking配置， 建议您在Pod的securityContext中配置以非Root用户启动，设置allowPrivilegeEscalation参数为*false*。具体配置样例如下：

```
hostNetwork: true    #特殊原因必须使用主机共享网络。
containers:
- name: foo
  securityContext:
    runAsUser: 12345
    allowPrivilegeEscalation: false
```

18.14. 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。

18.15. 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ACK集群K8s版本。

- 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。

18.16. 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。

18.17. 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。

18.18. 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。

18.19. 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ACK集群K8s版本。

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。

18.20. 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。

18.21. 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。

18.22. 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。

18.23. 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。

18.24. 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。

18.25. 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。

18.26. 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
```

18.27. 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，详情请参见配置容器安全策略（旧版）。

```
apiversion: policy/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 。

18.28. 修复漏洞CVE-2020-8564、CVE-2020-8565、CVE-2020-8566的公告

近日Kubernetes社区披露了多个组件的日志级别≥指定日志级别时，存在敏感信息泄露的问题，涉及kube-apiserver、kube-controller-manager、kubectl客户端等多个组件。

目前CVE-2020-8564、CVE-2020-8565、CVE-2020-8566的漏洞评级为中危漏洞。

影响范围

- 对于社区Kubernetes。

  当前1.19.2之前的所有Kubernetes发行版本均存在漏洞，以下为修复措施：

  - 关于如何修复CVE-2020-8564漏洞，请参见94712。
  - 关于如何修复CVE-2020-8565漏洞，请参见95316。
  - 关于如何修复CVE-2020-8566漏洞，请参见95245。

- 对于ACK集群。
  - 如果您的集群是标准托管版或Serverless集群，不在该漏洞影响范围内。
  - 如果您的集群是标准专有版集群且没有修改系统组件的日志级别，也不在该漏洞的影响范围内。
  - 如果您的集群是标准专有版集群，且指定组件的日志级别高于触发漏洞的日志级别，则存在漏洞。更多信息，请参见防范措施。

漏洞影响

- CVE-2020-8564

  当在Docker Config文件中配置了用于拉取私仓镜像的密钥，且kubelet组件的日志级别≥4时，攻击者可以通过kubelet日志查看密钥信息。

- CVE-2020-8565

  当kube-apiserver的日志级别≥9时，用于鉴权的 `bearer token` 或 `basic auth token` 存在泄露风险。

- CVE-2020-8566

  当kube-controller-manager日志级别≥4且应用中使用了Ceph RBD块存储时，攻击者可以通过controller-manager日志获取RBD Admin密钥。

防范措施

如果您的标准专有版集群中有指定组件的日志级别高于触发漏洞的日志级别，建议您采取以下防范措施：

- 请确保对应组件的日志读取权限在一个可信范围。
- 如果存在攻击者可能读取日志的场景，请及时轮转对应密钥，调整日志级别。
- 使用漏洞代码的一些客户端工具（例如kubectl）也存在信息泄露的风险。当使用指定日志级别的kubectl操作时，请确保输出日志的安全性。