目录

目录 1
实例管理 3
前提条件 3
创建实例 3
查看实例基本信息 3
删除实例 3
概述 3
配置公网访问控制 3
前提条件 3
相关操作 3
配置内网访问控制 4
前提条件 4
相关操作 4
访问凭证配置 4
操作步骤 4
自定义域名配置 4
前提条件 4
操作步骤 5
授权KCR访问KCM 5
创建自定义域名 5
设置访问控制和域名解析 5
其他操作 5
概述 5
基于IAM权限访问控制 5
非资源鉴权 5
资源鉴权 6
资源类型 6
资源规则 6
策略配置 7
系统策略 7
KCRFullAccess：容器镜像服务（KCR）全读写权限 7
KCRReadOnlyAccess：容器镜像服务（KCR）只读权限 7
授予系统策略操作步骤 8
自定义策略 8
授予自定义策略操作步骤 9
创建自定义策略 9
授予用户自定义策略 9
其他 9
管理命名空间 9
创建命名空间 9
管理镜像仓库 9
推送容器镜像至镜像仓库 9
镜像仓库相关操作 10
查看镜像仓库基本信息 10
删除镜像仓库 10
管理镜像版本 10
镜像安全扫描 10
删除镜像版本 10
容器镜像安全扫描 10
触发器(Webhook) 10

创建触发器 11
触发器相关操作 11
修改触发器状态 11
查看触发记录 11
修改触发器 11
删除触发器 11
相关信息 11
Webhook请求格式参考 11
清理镜像版本 11
操作步骤 12
创建版本保留规则 12
设置执行策略 12
查看执行日志 12
KS3镜像清理 12
注意事项 12
操作步骤 12
模拟运行清理 12
立即执行清理 13
执行结果 13
相关文档 13

实例管理

在使用容器镜像服务托管您的镜像之前，您需要创建容器镜像服务KCR实例。

前提条件

- 已注册金山云账号，详情请参考
- 已开通容器镜像服务所关联的KS3产品。具体操作请参见开通KS3服务。
- 已在容器镜像服务控制台按照界面提示为容器镜像服务授权。

创建实例

1. 登录容器镜像服务控制台。
2. 在**实例列表**页面，单击**创建实例**。
3. 在**创建容器镜像服务实例**页面，完成基本信息的配置，配置完成后点击**立即购买**。
   - 实例名称：自定义实例的名称，长度为2-30个字符，支持填写小写英文字母和数字，且不能以数字开头。
   - 计费方式：支持包年包月、按量付费两种计费模式，可根据实际需求进行选择。
   - 数据中心：按需选择实例所在地域，目前仅支持北京。
   - 实例规格：目前支持基础版、高级版两种实例规格，可根据实际需求进行选择。
   - 实例存储：默认在您账号下创建并关联金山云对象存储KS3 Bucket托管云原生制品，实例内镜像等数据将存储在该Bucket中，根据您的实际使用情况收取存储及流量费用，收费详情参考KS3计费说明。
   - 购买时长：针对包年包月实例，目前支持1-11个月以及1-3年可供选择。

     注：您可按需设置是否到期自动续费。

   - 所属项目：按需选择实例所属项目。
   - 服务协议：阅读并勾选《容器镜像服务公测试用服务协议》。
4. 在订单页点击**提交订单**即可。

查看实例基本信息

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏点击**基本信息**，即可查看相关详情。如下图所示：

删除实例

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 选择需要删除的容器镜像服务实例，点击**删除**，如下图所示：
4. 在跳出的弹窗中，可按需选择是否同步删除节点池内节点，如下图所示：
5. 点击**确定**，即可删除容器镜像服务实例。

注：包年包月实例不支持手动在容器镜像服务控制台删除，如需退订，请参考 退费说明

概述

容期镜像服务KCR为您提供网络访问控制能力，多方面保障您的数据安全，新创建的KCR实例默认拒绝所有外部访问，配置相应访问策略后，才可以访问该实例。

配置公网访问控制

镜像服务KCR支持配置公网访问控制，可基于白名单策略限制来自公网环境的客户端对实例的访问，保障实例内的数据隐私安全，新创建的KCR企业版实例默认不开启公网访问入口。

前提条件

- 企业版实例创建后，默认不允许通过公网访问。因此在配置公网的访问控制策略前，需要先打开公网的访问入口。

相关操作

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**访问控制** > **公网访问**，在**公网访问**页面单击**开启公网访问入口**。 待该按钮状态变为**已生效**，且添加公网白名单为可选择状态，则说明入口已开启。如下图所示： 入口开启后，仍默认拒绝全部来源的公网访问。
5. 在开启公网访问入口后，点击**添加公网白名单**。 **所属实例**：配置公网访问策略的目标实例。 **白名单地址**：可输入多个来源地址，支持多种格式：单个IP/CIDR/所有IPV4；支持换行或使用英文逗号输入多个地址段。

   注：容器镜像服务暂不支持同时使用公网访问控制和内网访问控制；实例域名在私有网络内将解析至内网 IP x.x.x.x ，不再默认解析至实例公网访问地址。

配置内网访问控制

容器镜像服务KCR支持配置内网访问控制，通过将私有网络与KCR实例打通，您可以指定私有网络内的云服务器通过内网拉取KCR实例内的容器镜像。

前提条件

- 已成功创建容器镜像服务实例。
- 已开通金山云 PrivateLink、内网DNS服务，用于内网推送、拉取镜像。

相关操作

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**访问控制** > **内网访问**，在**内网访问**页面单击**新建**。
5. 在新建内网访问链路弹窗中，可按需对私有网络以及终端子网进行配置，如下图所示：
6. 内网访问链路建立成功后，默认未配置该实例域名在接入的私有网络VPC内的解析，请单击**管理解析**，开启内网域名解析。

   注：开启后，本实例域名在私有网络内将解析至内网 IP x.x.x.x ，不再默认解析至实例公网访问地址。

访问凭证配置

使用Docker客户端上传下载容器镜像时，首先需要使用访问凭据信息登录实例，即在访问客户端中执行 `docker login` 命令并输入用户名及密码。通过配置访问凭证，您可以更安全地管理容器镜像的上传和下载。

操作步骤

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**访问凭证**，然后点击**新建访问凭证**。
5. 在弹出的“新建访问凭证”弹窗中，选择过期时间，点击**确认**。
6. 在“保存访问凭证”步骤中，点击**确认**进行保存。

   注：这是唯一一次复制当前访问凭证的机会，请您在关闭本弹窗前点击**确认**保存该访问凭证。

7. 创建完成后即可在**访问凭证**列表中查看，您还可进行访问凭证的**禁用**、**修改**过期时间及**删除**操作。

自定义域名配置

容器镜像服务KCR支持自定义域名配置，您可使用自定义域名功能添加自定义域名以及相应的SSL证书，通过HTTPS协议来访问实例。

前提条件

- 已拥有域名。详情介绍可参考域名注册介绍。
- 已为域名签发的SSL证书。

注：目前自定义域名功能只支持获取上传至SSL证书管理控制台的证书，您可提前将已签发的SSL证书上传至SSL证书管理控制台。详情请参考上传证书。请您确认已签发的SSL证书可用并已绑定实例需要使用的自定义域名。

- 已开通金山云内网DNS服务，用于域名解析。

操作步骤

授权KCR访问KCM

在使用域名管理功能之前，您需为容器镜像服务KCR授予访问SSL证书管理KCM的权限，KCR才能正常访问该SSL证书。

创建自定义域名

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**域名管理**，然后点击**添加域名**。
5. 在弹出的“添加域名”弹窗中，按需配置自定义域名以及选择已绑定自定义域名的证书，点击**确认**。

注：请确保填写的域名为已注册域名，若您填写的域名为其他用户已正式注册的域名，您的域名有可能被收回。

设置访问控制和域名解析

您可在私有网络VPC内使用自定义域名服务。

1. 配置内网访问控制，详情请参考配置内网访问控制。
2. 登录内网DNS控制台，新建实例，并为该实例关联已接入的VPC。

注：若您内网DNS已有实例，您直接为该实例关联VPC即可。

3. 使用该自定义域名新建Zone，并为该域名添加解析记录：使用A记录，且记录值为已创建内网访问链路的内网访问IP。具体详情页可点击**域名解析操作指南**进行参考： **完成以上配置后可在该私有网络VPC 内的机器上测试使用该自定义域名登录实例、拉取上传镜像。**

其他操作

您可以在域名管理页面单击目标域名操作列的**修改**更新域名证书，也可点击域名操作列的**删除**，删除该自定义域名。

概述

访问控制（ Identity and Access Management ，IAM）是金山云提供的管理用户身份与资源访问权限的基础服务。 可以实现安全且精细化管理金山云云服务和资源的访问。您可以通过IAM，将策略与用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。详情请参考IAM访问控制。

基于IAM权限访问控制

容器镜像服务KCR结合IAM管理访问权限能力，为您提供KCR授权管理功能。在该模式下，您可对KCR资源进行细颗粒度的权限访问控制，允许给单个用户或一组用户分配不同的资源及操作权限。 当用户访问容器镜像服务API时，容器镜像服务KCR会向IAM进行权限校验，以确保访问者拥有相应的权限。通过比对容器镜像服务API是否可以进行资源鉴权，KCR访问权限控制分为两种情形：**非资源鉴权**、**资源鉴权**。

非资源鉴权

非资源鉴权指的是能够指定允许用户是否可以对容器镜像服务API进行相关操作的能力。每个API的鉴权规则如下表所示：

API名称	鉴权Action	鉴权Resource
kcrs:CreateInstance创建实例	kcrs:CreateInstance	*
kcrs:DescribeInstance查询实例信息	kcrs:DescribeInstance	*
kcrs:DescribeInstanceUsage查询实例配额	kcrs:DescribeInstanceUsage	*
kcrs:DescribeNamespace查询命名空间	kcrs:DescribeNamespace	*
kcrs:DescribeNamespaceExist查询命名空间是否存在	kcrs:DescribeNamespaceExist	*

kcrs:DescribeRepository查询镜像仓库信息	kcrs:DescribeRepository	*
kcrs:StartImageScan镜像安全扫描	kcrs:StartImageScan	*
kcrs:DescribeImageScan获取镜像安全扫描结果	kcrs:DescribeImageScan	*

资源鉴权

资源级权限指的是能够指定允许用户对哪些资源具有执行操作的能力。容器镜像服务支持基于IAM 的资源级访问控制，控制颗粒度可至仓库级，即用户可通过配置IAM 策略实现授权子用户仅能够操作指定资源。

资源类型

通过IAM进行授权，指定允许用户对哪些资源具有执行操作的能力。

资源类型	授权策略中的资源描述
实例	krn:ksc:kcrs:***region***:***account-id***:instance/* krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
命名空间	krn:ksc:kcrs:***region***:***account-id***:namespace/***instanceid***/* krn:ksc:kcrs:***region***:***account-id***:namespace/***instanceid***/***namespace***
镜像仓库	krn:ksc:kcrs:***region***:***account-id***:repository/***instanceid***/***namespace***/* krn:ksc:kcrs:***region***:***account-id***:repository/***instanceid***/***namespace***/***repository***

注：***斜体***需要被替换为实际值。

参数说明：	参数说明	说明
region	地域信息，例如cn-beijing-6代表北京地域，所有地域可用*代替	
account-id	账号ID，可用*代替	
instanceid	容器镜像服务实例ID，所有实例可用*代替	
namespacename	容器镜像服务命名空间名称，所有命名空间可用*代替	
repositoryname	容器镜像服务镜像仓库名称，所有镜像仓库可用*代替	

资源规则

每个API的鉴权规则如下表所示： **实例级别相关接口**

API名称	鉴权Action	鉴权Resource
DeleteInstance删除实例	kcrs:DeleteInstance	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
CreateInstanceToken创建实例访问凭证	kcrs:CreateInstanceToken	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
ModifyInstanceTokenStatus修改访问凭证启用状态	kcrs:ModifyInstanceTokenStatus	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
ModifyInstanceTokenInformation修改访问凭证信息	kcrs:ModifyInstanceTokenInformation	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
DescribeInstanceToken查询访问凭证列表	kcrs:DescribeInstanceToken	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
DeleteInstanceToken删除访问凭证	kcrs:DeleteInstanceToken	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
CreateInternalEndpoint创建实例内网访问VPC链接	kcrs:CreateInternalEndpoint	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
DescribeInternalEndpoint查询实例内网访问VPC链接	kcrs:DescribeInternalEndpoint	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
DeleteInternalEndpoint删除实例内网访问VPC链接	kcrs:DeleteInternalEndpoint	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
CreateInternalEndpointDns创建实例私有域名解析	kcrs:CreateInternalEndpointDns	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
DescribeInternalEndpointDns查询实例私有域名解析	kcrs:DescribeInternalEndpointDns	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***
DeleteInternalEndpointDns删除实例私有域名解析	kcrs:DeleteInternalEndpointDns	krn:ksc:kcrs:***region***:***account-id***:instance/***instanceid***

注：若您需要指定用户授予内网访问控制相关权限时，因会查询您VPC列表，故需要您同时为该用户配置**vpc:Describe***鉴权ACtion。

命名空间级别相关接口	API名称	鉴权Action	鉴权Resource
CreateNamespace创建命名空间	kcrs:CreateNamespace	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*	
ModifyNamespaceType修改命名空间属性	kcrs:ModifyNamespaceType	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*namespace*	
DeleteNamespace删除命名空间	kcrs:DeleteNamespace	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*namespace*	
CreateWebhookTrigger创建触发器	kcrs:CreateWebhookTrigger	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*namespace*	
DescribeWebhookTrigger查询触发器	kcrs:DescribeWebhookTrigger	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*namespace*	
ModifyWebhookTrigger修改触发器	kcrs:ModifyWebhookTrigger	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*namespace*	
DescribeWebhookTriggerLog查询触发器日志	kcrs:DescribeWebhookTriggerLog	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*namespace*	
DeleteWebhookTrigger删除触发器	kcrs:DeleteWebhookTrigger	krn:ksc:kcrs:*region*:*account-id*:namespace/*instanceid*/*namespace*	

镜像仓库级别相关接口	API名称	鉴权Action	鉴权Resource
DeleteRepository删除镜像仓库	kcrs:DeleteRepository	krn:ksc:kcrs:*region*:*account-id*:repository/*instanceid*/*namespace*/*repository*	
ModifyRepoDesc修改镜像仓库描述信息	kcrs:ModifyRepoDesc	krn:ksc:kcrs:*region*:*account-id*:repository/*instanceid*/*namespace*/*repository*	
DescribeImages查询镜像列表	kcrs:DescribeImages	krn:ksc:kcrs:*region*:*account-id*:repository/*instanceid*/*namespace*/*repository*	
DeleteImages删除镜像	kcrs:DeleteImages	krn:ksc:kcrs:*region*:*account-id*:repository/*instanceid*/*namespace*/*repository*	
DeleteRepoTag删除镜像Tag	kcrs:DeleteRepoTag	krn:ksc:kcrs:*region*:*account-id*:repository/*instanceid*/*namespace*/*repository*	
PullRepository拉镜像	kcrs:PullRepository	krn:ksc:kcrs:*region*:*account-id*:repository/*instanceid*/*namespace*/*repository*	
PushRepository推镜像	kcrs:PushRepository	krn:ksc:kcrs:*region*:*account-id*:repository/*instanceid*/*namespace*/*repository*	

注：因Docker中Push镜像和Pull镜像操作耦合，故您授予PushRepository权限时需同步授予PullRepository权限。

策略配置

您可以按需选择已有的系统策略，也可以根据实际需求场景自定义策略。

系统策略

容器镜像服务KCR目前提供两种系统策略：**容器镜像服务（KCR）全读写权限KCRFullAccess**和**容器镜像服务（KCR）只读权限KCRReadOnlyAccess**，您直接授权即可使用。

KCRFullAccess：容器镜像服务（KCR）全读写权限

子用户拥有该授权后，将具有KCR全部资源的全部操作权限。

```
{
    "Version": "2015-11-01",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kcrs:*",
                "vpc:Describe*"
             ],
            "Resource": "*"
        }
    ]
}
```

KCRReadOnlyAccess：容器镜像服务（KCR）只读权限

子用户拥有该授权后，将具有KCR全部资源的只读权限，例如：可以查看仓库信息，Pull镜像等。

```
{
  "Version": "2015-11-01",
  "Statement": [
    {
      "Action": [
        "kcrs:Describe*",
        "kcrs:Get*",
    "kcrs:StartImageScan",
    "vpc:Describe*",
        "kcrs:Pull*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

授予系统策略操作步骤

以下以授权用户KCRFullAccess权限策略为例：

1. 登录访问管理控制台。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表，找到目标子用户，单击**操作**列的**添加权限**按钮。
4. 在**添加权限**页面中选择系统策略，在文本框中输入并勾选KCRFullAccess策略。
5. 单击**确定**，完成权限添加。

自定义策略

如果用户想对权限进行细粒度控制，可以自定义策略，然后授予子用户自定义策略权限即可。以下将提供典型场景下的策略配置来方便用户使用。

- 授权子用户管理指定实例并进行实例相关操作，例如主账号ID：12345，管理北京地域（cn-beijing-6）下的实例，实例ID：kcr-xxxxxxxx。

```
{
  "Version": "2015-11-01",
  "Statement": [
    {
      "Action": [
        "kcrs:*"
      ],
      "Resource": "krn:ksc:kcrs:cn-beijing-6:12345:instance/kcr-xxxxxxxx",
      "Effect": "Allow"
    }
  ]
}
```

- 授权子用户管理指定实例内的指定命名空间进行相关操作，例如主账号ID：12345，北京地域（cn-beijing-6）下的实例，实例ID：kcr-xxxxxxxx，命名空间名称为test。

```
{
    "Version": "2015-11-01",
    "Statement": [
        {
            "Action": [
                "kcrs:*"
            ],
            "Resource": "krn:ksc:kcrs:cn-beijing-6:12345:namespace/kcr-xxxxxxxx/test",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kcrs:DescribeInstance",
                "kcrs:DescribeInstanceUsage"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kcrs:DescribeNamespace",
                "kcrs:DescribeNamespaceExist"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
```

```
    ]
}
```

授予自定义策略操作步骤

创建自定义策略

相关操作您可以参考此文档：创建自定义策略

> 注：您可以在**设置策略类型**中选择通过**可视化配置**创建，也可以选择通过**策略语法**创建。

授予用户自定义策略

方法一：在策略页面为子用户授权

1. 登录访问控制控制台。
2. 选择**权限管理** > **策略**。
3. 在**自定义策略**列表页中，找到要授权的目标策略，单击**操作**列的**关联对象**按钮。
4. 在**关联对象**面板，选择要授权的子用户。
5. 单击**确定**，完成权限添加。

方法二：在策略页面为子用户授权

1. 登录访问管理控制台。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表，找到目标子用户，单击**操作**列的**添加权限**按钮。
4. 在**添加权限**页面中选择您创建的自定义策略。
5. 单击**确定**，完成权限添加。

其他

当您为指定用户授予创建实例策略时，因创建实例需要下订单，故您需要为该用户绑定**系统策略：PayOrderAccess**，避免您后续购买实例失败。

管理命名空间

通过配置命名空间，您可以有效管理该命名空间下的镜像仓库，例如管理多个具有关联属性的镜像仓库以及结合权限管理可实现不同的用户访问或操作指定命名空间。

创建命名空间

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**仓库管理** > **命名空间**。
5. 在**命名空间**页面单击**创建命名空间**。
6. 在**创建命名空间**弹窗中设置命名空间名称、命名空间类型，点击**确定**即可。

   > 注：若命名空间类型设置为公有，任何通过访问控制的客户端均无需登录即可拉取镜像。

7. 创建完成后即可在**命名空间**列表中查看，您还可进行命名空间的**删除**、**修改命名空间类型**操作。

   注：

   - 若您当前命名空间内仍有镜像仓库，则该命名空间无法删除。
   - 修改命名空间类型后，命名空间中的所有镜像仓库都将继承该属性。

管理镜像仓库

镜像仓库是用于存放容器镜像的地方，您可以使用镜像仓库管理不同版本的容器镜像。镜像仓库归属于命名空间，并继承命名空间的公有、私有类型属性。

推送容器镜像至镜像仓库

目前不支持通过控制台直接创建镜像仓库，您可以通过Docker客户端推送镜像时指定镜像仓库，操作步骤请参考**镜像操作指南**。

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**仓库管理 > 镜像仓库**。
5. 在**镜像仓库**页面单击**镜像操作指南**。
6. 在**镜像操作指南**弹窗中查看操作步骤。

镜像仓库相关操作

查看镜像仓库基本信息

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**仓库管理 > 镜像仓库**。
5. 在**镜像仓库**列表页单击目标镜像仓库。
6. 在**基本信息**页签中即可查看镜像仓库的基本信息。

删除镜像仓库

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**仓库管理 > 镜像仓库**。
5. 在**镜像仓库**列表页选择目标镜像仓库，单击**删除**即可进行删除操作。

> 注：删除镜像仓库，会将您镜像仓库内的所有镜像同步删除，请谨慎操作。

管理镜像版本

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**仓库管理 > 镜像仓库**。
5. 在**镜像仓库**列表页单击目标镜像仓库。
6. 在**镜像列表**页签中即可进行管理仓库内镜像版本、安全扫描等操作。

镜像安全扫描

单击指定镜像右侧操作中的**安全扫描**触发对该镜像进行安全漏洞扫描，待扫描结束后即可查看具体漏洞信息。

删除镜像版本

单击指定镜像右侧操作中的**删除**即可删除该镜像。

> 注：删除此镜像，则该镜像下的所有版本也将随镜像同步删除，请谨慎操作。

容器镜像安全扫描

容器镜像服务KCR支持对托管的容器镜像进行安全漏洞扫描并产生扫描结果，对漏洞信息进行评估并给出修复建议。您可以查看容器镜像内潜在的安全漏洞信息，有效降低实际业务漏洞风险。

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**仓库管理 > 镜像仓库**。
5. 在**镜像仓库**列表页单击目标镜像仓库。
6. 在**镜像列表**页签中选择目标镜像，单击**安全扫描**。
7. 在弹窗中单击**开始扫描**即可进行镜像安全扫描。
8. 扫描完成后，您可以查看扫描结果以及具体的漏洞信息，如下图所示：

触发器(Webhook)

容器镜像服务KCR支持配置并使用触发器（Webhook）功能，允许您自定义创建触发器规则，并支持查看触发日志。当触发动作发生时，自动执行您自定义的POST请求。

创建触发器

1. 登录容器镜像服务控制台。
2. 在顶部菜单栏，选择所需地域。
3. 在**实例列表**页面单击目标容器镜像服务实例。
4. 在容器镜像服务实例管理页面左侧导航栏选择**仓库管理 > 触发器**。
5. 在**触发器**列表页单击**创建触发器**。
6. 在**新建触发器**弹窗中配置相关信息，如下图所示：
   - 名称：触发器名称，2-256个字符，支持小写字母，数字，及 “- . _” 三种符号，且以字母数字开头。
   - 触发动作：目前支持推送镜像、删除镜像。

     注：若您选择删除镜像为触发动作，当您删除镜像tag时不会触发请求。

   - 触发规则：触发器生效的命名空间。
   - URL：触发器被触发后，发起请求的 URL地址。触发器将向该 URL 地址发起 POST 请求，请求 body 中将包含触发动作、触发规则等信息。
   - Header：触发器发起 POST 请求时，支持以 Key:Value 形式输入可携带的 Header 信息。
7. 单击**确认**即可完成创建触发器。

触发器相关操作

触发器创建成功后，即可进行查看触发记录以及修改、删除触发器等操作。

修改触发器状态

表示触发器启用，表示触发器禁用。

查看触发记录

单击指定触发器名称右侧的**触发记录**即可查看该规则触发日志。

修改触发器

重新配置触发器信息，注：触发规则中命名空间不可更改。

删除触发器

删除该触发器规则。

相关信息

Webhook请求格式参考

当您对符合触发的规则执行相应动作时，例如向指定镜像仓库推送新的镜像版本时，则相应的触发器将被触发，并向触发规则中配置的URL发起HTTP POST请求，请求Body中包含触发动作、仓库路径等信息。以下为推送镜像触发后并经解析的请求Body信息，可供开发Webhook服务端参考：

```
{
  "type": "PUSH_ARTIFACT",
  "occur_at": xxxxxxxx,
  "event_data": {
    "resources": [
      {
        "digest": "sha256:xxxxxxxxxxxx",
        "tag": "v1",
        "resource_url": "xxxxxx/xxxxxx/nginx:v1"
      }
    ],
    "repository": {
      "date_created": xxxxxx,
      "name": "nginx",
      "namespace": "xxxxxx",
      "repo_full_name": "xxxxxx/nginx",
      "repo_type": "public"
    }
  },
  "operator": "xxxxxxxxxx"
}
```

清理镜像版本

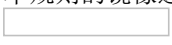
容器镜像服务KCR支持批量清理企业版实例的镜像版本。本文介绍如何通过设置版本保留策略来清理镜像版本。

操作步骤

创建版本保留规则

1. 登录容器镜像服务控制台。选择具体实例，点击进入；
2. 选择左侧导航栏中的版本保留；
3. 单击创建保留规则，在“新建版本保留规则”窗口中，参考以下提示进行规则配置。

- **所属实例**：当前已选择实例
- **命名空间**：版本保留规则生效的命名空间，每个命名空间最多支持创建15条规则
- **镜像仓库**：支持全选或选择部分仓库
- **保留策略**：支持根据镜像数量策略保留或根据镜像版本策略保留。镜像数量策略中，支持保留最近推送/拉取的指定数量镜像，或保留最近指定天数推送/拉取的镜像；镜像版本策略中，支持根据您配置的版本规则匹配镜像版本，对满足版本规则的镜像进行保留，此外对于无镜像版本的镜像，您可勾选是否将无镜像版本的镜像加入保留策略。


完成配置后，单击确定即可创建版本保留规则。

设置执行策略

版本保留规则成功创建后，即可在**版本保留**页面查看已创建的版本保留规则。  **保留策略**：配置多条保留规则时，多条规则将作为一个保留策略执行。

策略执行方式支持定时执行保留策略/手动执行保留策略： **定时执行保留策略**：您可配置定时执行保留策略的执行周期，支持按每小时、每天、每周、每月执行。 **手动执行保留策略**：您可配置立即运行或模拟运行，模拟运行可用于确认规则是否生效，但不实际清理镜像版本。

查看执行日志

在执行版本保留策略后，您可在执行日志列表中查看每次策略执行的关键日志信息。 

- **任务ID**：实例内唯一的版本保留执行任务ID
- **执行状态**：您可根据执行状态判断任务执行成功/失败/执行中
- **模拟运行**：任务是否为模拟运行，是则不实际清理镜像版本
- **执行方式**：根据执行方式区分手动/自动执行
- **开始时间**：版本保留执行任务开始的时间
- **持续时间**：完成全部版本保留执行任务消耗的时间

选择指定任务，可查看任务详情，点击**查看日志**可查询日志详情。

注：执行日志默认保留时长为7天。

KS3镜像清理

金山云容器镜像服务(Kingsoft Cloud Container Registry,KCR)在控制台删除镜像数据后，存储在实例关联的对象存储KS3内的镜像数据仍保留。 基于以上问题，可以设置制品清理任务，删除ks3存储空间中的无效镜像相关数据，清理存储空间，降低存储费用。

注意事项

制品清理功能请评估以下注意事项后谨慎操作：

清理ks3存储空间时，无效镜像相关数据将会被清理，此删除过程不可恢复，建议执行真实清理任务前，使用模拟运行评估影响范围。

操作步骤

模拟运行清理

1. 登录容器镜像服务控制台，指定具体实例，选择左侧导航栏中的制品清理。
2. 单击模拟运行清理，仔细阅读相关提示。
3. 单击确定即可执行模拟清理任务。

注：模拟运行制品清理将全面扫描实例内可清理的垃圾数据，并预估清理范围及清理时间。

立即执行清理

1. 登录容器镜像服务控制台，指定具体实例，选择左侧导航栏中的制品清理。
2. 单击立即执行清理，仔细阅读相关提示。

   注：期间实例基础功能不受影响，仍可推送和拉取制品，但密集计算任务可能会影响到实例部分功能响应性能。
3. 单击确定即可执行立即执行清理任务。

执行结果

在制品清理页面查看清理任务。当清理状态显示已完成，说明清理完成。

相关文档

- 清理镜像版本