

目录

目录	1
概述	3
权限(Permission)	3
权限策略(Policy)	3
授权	3
鉴权逻辑	3
策略文档元素解析	3
使用元素及规则	3
策略语法说明	4
策略文档的形式语法示例	4
策略文档示例	4
新建授权	4
操作步骤	4
解除授权	5
操作步骤	5
全局系统策略	5
产品线无关系统内置策略	5
策略概要	5
策略详情	5
CDN相关系统内置策略	5
策略概要	5
策略详情	5
KEC相关系统内置策略	5
策略概要	5
策略详情	6
VPC相关系统内置策略	6
策略概要	6
策略详情	6
EIP相关系统内置策略	6
策略概要	6
策略详情	6
SLB相关系统内置策略	7
策略概要	7
策略详情	7
IAM相关系统内置策略	7
策略概要	7
策略详情	7
裸金属服务器相关系统内置策略	8
策略概要	8
策略详情	8
KMR相关系统内置策略	8
策略概要	8
策略详情	8
DNS相关系统内置策略	8
策略概要	8
策略详情	8
WAF相关系统内置策略	8
策略概要	8
策略详情	9
KAS相关系统内置策略	9

策略概要	9
策略详情	9
KAD相关系统内置策略	9
策略概要	9
策略详情	9
KRDS相关系统内置策略	9
策略概要	9
策略详情	9
KIS相关系统内置策略	9
策略概要	9
策略详情	9
BWS相关系统内置策略	10
策略概要	10
策略详情	10
创建自定义策略	10
前提条件	10
操作步骤	10
后续步骤	10
修改自定义策略内容	11
操作步骤	11
管理自定义策略版本	11
限制说明	11
操作步骤	11
金山云KRN	11

概述

权限指在某种条件下允许或拒绝对某些资源执行某些操作，权限策略是一组访问权限的集合。

权限(Permission)

权限是指是否允许用户对某种资源执行某种操作，权限分为：允许(Allow)或拒绝(Deny)。

权限策略(Policy)

权限策略是用语法结构描述的一组权限的集合，可以精确地描述被授权的资源集、操作集以及授权条件。

IAM支持以下两种权限策略：

- 金山云管理的系统策略：统一由金山云创建，用户只能使用不能修改，策略的版本更新由金山云维护。
- 客户管理的自定义策略：用户可以自主创建、更新和删除，策略的版本更新由客户自己维护。

授权

授权是您将用户完成具体工作需要的权限策略授予给对应用户身份（IAM子用户、用户组、IAM角色）。对应用户身份获取到云服务权限后，可以对云服务进行操作。

- 授权的权限策略可以是系统策略也可以是自定义策略。
- 如果授权的权限策略被更新，更新后的权限策略自动生效，无需重新绑定权限策略。

鉴权逻辑

判断流程如下：

1. 如果使用主账户的安全信任状（即AccessKey）进行签名发起请求，且访问对象Resource的属主是该主账户，那么授权通过，否则授权不通过
2. 如果请求使用子用户的安全信任状进行签名发起请求，且访问对象Resource的属组是其所属主账户，那么此时调用权限评估接口，根据子用户身上附加的策略集合来判断是否授权通过。
3. 在评估子用户身上的附加策略时采用默认/隐式拒绝（default /implicit deny）的原则：
 - 3.1 如果操作请求被“显示拒绝（explicit deny）”，则返回“授权不通过”，否则进入下一步
 - 3.2 如果操作请求被“显示授权（explicit allow）”，则返回“授权通过”，否则进入下一步
 - 3.3 默认/隐式拒绝（default /implicit deny）所有操作请求，返回“授权不通过”

即显示拒绝>“显示授权”>“默认/隐式拒绝”

策略文档元素解析

金山云IAM的策略文档采用AWS的策略文档的语法和规范，但在支持的元素的数量上有所区别。

使用元素及规则

元素名称	是否必须	描述
Version（版本）	否	形如“Version”：“2015-11-01”，用于说明策略文档的版本。 目前金山云的策略文档版本只有一个取值，2015-11-01，如果策略中没有Version元素，其默认值为2015-11-01
Statement（授权规则）	是	形如“Statement”：[{... }, { ... }, { ... }]，策略的主元素，用于说明具体授权规则。 每个Statement元素可以包含多条语句，每条语句用 {} 括起来说明。
Sid	否	形如“Sid”：“1”，Statement的语句标识符，可被省略，在一个策略中需要保持唯一性。
Effect（效力）	是	形如“Effect”：“Allow”，Statement的授权规则的组成元素，每条授权规则必须包括该元素 (1) 只有两种取值Allow或者Deny，分别表明“显示授权”和“显示拒绝”。 (2) 权限策略中既有允许(Allow)又有拒绝(Deny)的授权语句时，遵循Deny优先的原则。

Action（操作）	是	<p>形如"Action": "iam:CreateUser", Statement的授权规则的组成元素，每条授权规则必须包括该元素。</p> <p>(1) 操作支持多值，取值为：云服务所定义的API操作名称。</p> <p>(2) 格式：:，其中service-name是金山云服务名称，而、action-name是相关API操作接口名称。</p> <p>(3) service-name和action-name的值不区分大小写，操作名称可以包含通配符*。</p>
Resource（资源）	是	<p>形如"Resource": "KRN", Resource是被授权的具体资源对象。</p> <p>(1) 每种service的resource各不相同，可以使用*来表示全体资源对象。</p> <p>(2) 同时也遵金山云KRN的统一命名规范，详细格式请查看金山云KRN。</p>

策略语法说明

- 每个策略文档可以包含多条策略语句
- 每个策略组成元素中包含的同名称元素不能重复，只能出现一次，比如不能在一个策略语句中出现两次Effect元素块
- 策略文档中各元素块的显示顺序无限制
- 策略文档中的白空格（whiteSpace）被忽略

策略文档的形式语法示例

```

policy = {
  <version_block?>
  <statement_block>
}
<version_block> = "Version" : "2015-11-01"
<statement_block> = "Statement" : [<statement>, <statement>, ...]
<statement> = {
  <sid_block?>,
  <effect_block>,
  <action_block>,
  <resoure_block>
}
<sid_block> = "Sid" : <sid_string>
<effect_block> = "Effect" : ("Allow" | "Deny")
<action_block> = "Action" : ( "*" | [<action_string>, <action_string>, ...])
<resoure_block> = "Resource" : ( "*" | [<resoure_string>, <resoure_string>, ...])
<action_string> = "service_name : action_name"
<resource_string> = "KRN"

```

策略文档示例

云主机（KEC）管理员的权限的策略文档示例

```

{
  "Version" : "2015-11-01",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "KEC:*",
      "Resource" : "*"
    }
  ]
}

```

新建授权

授权是您将用户完成具体工作需要的权限策略授予给对应用户身份（IAM子用户、用户组、IAM角色）。对应用户身份获取到云服务权限后，可以对云服务进行操作。

操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**权限管理** > **授权**。
3. 在**授权列表**页面，单击**新建授权**按钮。
4. 在**新建授权**面板，在**被授权主体**区域选择要授权的主体。

被授权主体支持用户、用户组、角色。最多同时选择5个授权主体。

5. 在**选择权限**区域，选择要授权的策略。

支持选择系统策略或自定义策略。

6. 单击**确定**，完成权限添加。

解除授权

当IAM子用户、用户组或角色不再需要某些权限时，可以在授权列表将这些权限移除。

操作步骤

1. 登录[访问控制控制台](#)。
2. 选择权限管理 > 授权。
3. 在授权列表页面，单击目标授权操作列的解除操作按钮。
4. 在确认弹窗中，单击确定解除。

全局系统策略

目前金山云内置的系统全局策略如下表：

产品线无关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
系统管理员	AdministratorAccess	karn:ksc:iam::ksc:policy/AdministratorAccess	提供系统管理员的管理权限（最大权限）	v1	是

策略详情

策略名称	策略文档	权限说明
AdministratorAccess	<pre>{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": "*", "Resource": "*" }] }</pre>	包括金山云全部产品（KEC、EIP、VPC、SLB、CDN、KMR、IAM、KRDS等）的管理权限

CDN相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
CDN管理员	CDNFullAccess	karn:ksc:iam::ksc:policy/CDNFullAccess	提供CDN功能全部管理权限	v1	是
CDN查询管理员	CDNReadOnlyAccess	karn:ksc:iam::ksc:policy/CDNReadOnlyAccess	提供CDN功能查询管理权限	v1	是

策略详情

策略名称	策略文档	权限说明
CDNFullAccess	<pre>{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": "cdn:*", "Resource": "*" }] }</pre>	包括刷新管理、预加载管理、流量带宽查询、实时命中率状态码、用户配额管理等全部功能的权限
CDNReadOnlyAccess	<pre>{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": ["cdn:Get*", "cdn:List*"], "Resource": "*" }] }</pre>	包括查询刷新列表和详情、查询预加载列表和详情、查询流量带宽、查询实时命中率状态码、查询用户配额和用量等权限

KEC相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
云主机系统管理员	KECAdminFullAccess	karn:ksc:iam::ksc:policy/KECAdminFullAccess	提供操作云主机运行所需要的全部管理权限	v1	是
云主机管理员（API）	KECFullAccess	karn:ksc:iam::ksc:policy/KECFullAccess	提供云主机openAPI接口全部管理权限	v1	是

云主机查询管理员 (API)	KECReadOnlyAccess	karn:ksc:iam::ksc:policy/KECReadOnlyAccess	提供云主机查询openAPI管理权限	v1	是
----------------	-------------------	--	--------------------	----	---

策略详情

策略名称	策略文档	权限说明
KECAdminFullAccess	{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": "kec:*", "Resource": "*" }, { "Effect": "Allow", "Action": "vpc:*", "Resource": "*" }, { "Effect": "Allow", "Action": "slb:*", "Resource": "*" }, { "Effect": "Allow", "Action": "eip:*", "Resource": "*" }] }	包括实例管理、VPC管理、负载均衡管理、弹性IP管理等全部功能的权限
KECFullAccess	{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": "kec:*", "Resource": "*" }] }	包括实例管理、映像管理、网络接口属性修改等全部openAPI功能的权限
KECReadOnlyAccess	{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": "kec:Describe*", "Resource": "*" }] }	包括查询主机信息、镜像信息openAPI的权限

VPC相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
VPC管理员 (API)	VPCFullAccess	karn:ksc:iam::ksc:policy/VPCFullAccess	提供虚拟专有网络全部openAPI接口管理权限	v1	是
VPC查询管理员 (API)	VPCReadOnlyAccess	karn:ksc:iam::ksc:policy/VPCReadOnlyAccess	提供虚拟专有网络查询openAPI接口管理权限	v1	是
VPC管理员 (控制台)	VPCConsoleFullAccess	karn:ksc:iam::ksc:policy/VPCConsoleFullAccess	提供虚拟专有网络和EIP控制台功能全部管理权限	v1	是
VPC查询管理员 (控制台)	VPCConsoleReadOnlyAccess	karn:ksc:iam::ksc:policy/VPCConsoleReadOnlyAccess	提供虚拟专有网络控制台查询功能全部管理权限	v1	是

策略详情

策略名称	策略文档	权限说明
VPCFullAccess	{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": "vpc:*", "Resource": "*" }] }	包括vpc管理、子网管理、路由管理、网络ACL管理、NAT管理、隧道网关管理、对等连接管理等全部openAPI功能的权限
VPCReadOnlyAccess	{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": "vpc:Describe*", "Resource": "*" }] }	包括查询vpc、子网、路由、网络ACL、NAT等信息的openAPI管理权限
VPCConsoleFullAccess	{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": ["vpc:*", "eip:*", "kec:DescribeInstances", "epc:ListEpcs"], "Resource": "*" }] }	包括vpc管理、子网管理、路由管理、网络ACL管理、NAT管理、隧道网关管理、对等连接管理、弹性IP管理、端口映射管理等全部功能的控制台管理权限
VPCConsoleReadOnlyAccess	{ "Version": "2015-11-01", "Statement": [{ "Effect": "Allow", "Action": ["vpc:Describe*", "eip:Describe*", "kec:DescribeInstances", "epc:ListEpcs"], "Resource": "*" }] }	包括查询vpc、子网、路由、网络ACL、NAT、EIP、端口映射等信息的控制台管理权限

EIP相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
弹性IP管理员 (API)	EIPFullAccess	karn:ksc:iam::ksc:policy/EIPFullAccess	提供弹性IP全部openAPI接口管理权限	v1	是
弹性IP查询管理员 (API)	EIPReadOnlyAccess	karn:ksc:iam::ksc:policy/EIPReadOnlyAccess	提供弹性IP查询openAPI接口管理权限	v1	是
弹性IP管理员 (控制台)	EIPConsoleFullAccess	karn:ksc:iam::ksc:policy/EIPConsoleFullAccess	提供弹性IP控制台功能全部管理权限	v1	是
弹性IP查询管理员 (控制台)	EIPConsoleReadOnlyAccess	karn:ksc:iam::ksc:policy/EIPConsoleReadOnlyAccess	提供弹性IP控制台查询功能全部管理权限	v1	是

策略详情

策略名称	策略文档	权限说明
EIPFullAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "eip:*", "Resource": "*"}]}</code>	包括弹性IP管理、端口映射管理等全部功能的openAPI的管理权限
EIPReadOnlyAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["eip:Describe*", "eip:GetLines"], "Resource": "*"}]}</code>	包括查询链路、弹性IP、端口映射等信息的openAPI管理权限
EIPConsoleFullAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["eip:*", "vpc:DescribeNetworkInterfaces", "kec:DescribeInstances", "epc:ListEpcs"], "Resource": "*"}]}</code>	包括弹性IP管理、端口映射管理等功能的控制台全部管理权限
EIPConsoleReadOnlyAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["eip:Describe*", "vpc:DescribeNetworkInterfaces", "kec:DescribeInstances", "epc:ListEpcs"], "Resource": "*"}]}</code>	包括弹性IP管理、端口映射管理等控制台查询功能的全部管理权限

SLB相关系统内置策略

策略概要

策略中文名称	策略名称	策略ARN	策略描述	策略版本	是否默认策略
负载均衡管理员 (API)	SLBFullAccess	karn:ksc:iam::ksc:policy/SLBFullAccess	提供负载均衡全部openAPI功能管理权限	v1	是
负载均衡查询管理员 (API)	SLBReadOnlyAccess	karn:ksc:iam::ksc:policy/SLBReadOnlyAccess	提供负载均衡查询openAPI的管理权限	v1	是
负载均衡管理员 (控制台)	SLBConsoleFullAccess	karn:ksc:iam::ksc:policy/SLBConsoleFullAccess	提供负载均衡和EIP控制台全部管理权限	v1	是
负载均衡查询管理员 (控制台)	SLBConsoleReadOnlyAccess	karn:ksc:iam::ksc:policy/SLBConsoleReadOnlyAccess	提供负载均衡控制台查询功能全部管理权限	v1	是

策略详情

策略名称	策略文档	权限说明
SLBFullAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "slb:*", "Resource": "*"}]}</code>	包括负载均衡器管理、监听器管理、健康检查管理、真实服务器管理等全部功能的openAPI管理权限
SLBReadOnlyAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "slb:Describe*", "Resource": "*"}]}</code>	包括查询负载均衡器、监听器、健康检查、真实服务器等信息查询openAPI的管理权限
SLBConsoleFullAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["slb:*", "eip:*", "vpc:DescribeNetworkInterfaces", "vpc:DescribeVpcs", "vpc:DescribeSubnets", "kec:DescribeInstances", "epc:ListEpcs"], "Resource": "*"}]}</code>	包括负载均衡器管理、监听器管理、健康检查管理、真实服务器管理、弹性IP管理、端口映射管理等功能的控制台全部管理权限
SLBConsoleReadOnlyAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["slb:Describe*", "eip:Describe*", "vpc:DescribeNetworkInterfaces", "vpc:DescribeVpcs", "vpc:DescribeSubnets", "kec:DescribeInstances", "epc:ListEpcs"], "Resource": "*"}]}</code>	包括负载均衡器管理、监听器管理、健康检查管理、真实服务器管理、弹性IP管理、端口映射管理等控制台查询功能的全部管理权限

IAM相关系统内置策略

策略概要

策略中文名称	策略名称	策略ARN	策略描述	策略版本	是否默认策略
IAM管理员 (控制台&openAPI)	IAMFullAccess	karn:ksc:iam::ksc:policy/IAMFullAccess	提供IAM功能全部管理权限 (控制台&openAPI)	v1	是
IAM查询管理员 (控制台&openAPI)	IAMReadOnlyAccess	karn:ksc:iam::ksc:policy/IAMReadOnlyAccess	提供IAM查询管理 (控制台&openAPI) 权限	v1	是

策略详情

策略名称	策略文档	权限说明
IAMFullAccess	<code>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "iam:*", "Resource": "*"}]}</code>	包括用户管理、访问密钥管理、策略及授权管理等全部功能的权限 (控制台&openAPI)

IAMReadOn lyAccess n:{"iam:Get*", "iam:List*"}, "Resource": "*"}] 包括查询用户、访问密钥、策略及授权等信息的权限（控制台&openAPI）

裸金属服务器相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
裸金属服务器管理员（控制台&openAPI）	EPCFullAccess	krn:ksc:iam::ksc:policy/EPCFullAccess	提供裸金属服务器功能全部管理权限（控制台&openAPI）	v1	是
裸金属服务器查询管理员（控制台&openAPI）	EPCReadOnlyAccess	krn:ksc:iam::ksc:policy/EPCReadOnlyAccess	提供裸金属服务器查询管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
EPCFullAccess	{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "epc:*", "Resource": "*"}]}	包括裸金属服务器生命周期管理、子网管理、镜像管理等全部功能的权限（控制台&openAPI）
EPCReadOnlyAccess	{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["epc:Get*", "epc:List*"], "Resource": "*"}]}	包括查询裸金属服务器、镜像等信息的权限（控制台&openAPI）

KMR相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
KMR管理员（控制台&openAPI）	KMRFullAccess	krn:ksc:iam::ksc:policy/KMRFullAccess	提供托管hadoop产品全部控制台管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
KMRFullAccess	{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "kmr:*", "Resource": "*"}]}	包括集群管理、ssh密钥管理、作业管理、eip管理等全部功能的权限（控制台&openAPI）

DNS相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
DNS管理员（控制台&openAPI）	DNSFullAccess	krn:ksc:iam::ksc:policy/DNSFullAccess	提供DNS的全部管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
DNSFullAccess	{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "dns:*", "Resource": "*"}]}	包括域名管理、域名记录管理全部功能的权限（控制台&openAPI）

WAF相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
WAF管理员（控制台&openAPI）	WAFFullAccess	krn:ksc:iam::ksc:policy/WAFFullAccess	提供web防火墙产品全部管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
WAFFullAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "waf:*", "Resource": "*"}]}</pre>	包括web防火墙全部功能的权限（控制台&openAPI）

KAS相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
KAS管理员（控制台&openAPI）	KASFullAccess	krn:ksc:iam::ksc:policy/KASFullAccess	提供安全服务产品全部管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
KASFullAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "kas:*", "Resource": "*"}]}</pre>	包括安全服务全部功能的权限（控制台&openAPI）

KAD相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
KAD管理员（控制台&openAPI）	KADFullAccess	krn:ksc:iam::ksc:policy/KADFullAccess	提供高防IP产品全部管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
KADFullAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "kad:*", "Resource": "*"}]}</pre>	包括高防IP全部功能的权限（控制台&openAPI）

KRDS相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
KRDS管理员（控制台&openAPI）	KRDSFullAccess	krn:ksc:iam::ksc:policy/KRDSFullAccess	提供关系型数据库产品全部管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
KRDSFullAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "krd:s:*", "Resource": "*"}]}</pre>	包括关系型数据库全部功能的权限（控制台&openAPI）

KIS相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
KIS管理员（控制台&openAPI）	KISFullAccess	krn:ksc:iam::ksc:policy/KISFullAccess	提供云IDC产品全部管理权限（控制台&openAPI）	v1	是

策略详情

策略名称	策略文档	权限说明
KISFullAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "kis:*", "Resource": "*"}]}</pre>	包括云IDC产品全部功能的权限（控制台&openAPI）

BWS相关系统内置策略

策略概要

策略中文名称	策略名称	策略KRN	策略描述	策略版本	是否默认策略
BWS管理员(API)	BWSFullAccess	karn:ksc:iam::ksc:policy/BWSFullAccess	提供共享带宽全部openAPI接口管理权限	v1	是
BWS查询管理员(API)	BWSReadOnlyAccess	karn:ksc:iam::ksc:policy/BWSReadOnlyAccess	提供共享带宽查询openAPI接口管理权限	v1	是
BWS管理员(控制台)	BWSConsoleFullAccess	karn:ksc:iam::ksc:policy/BWSConsoleFullAccess	提供共享带宽控制台功能全部管理权限	v1	是
BWS查询管理员(控制台)	BWSConsoleReadOnlyAccess	karn:ksc:iam::ksc:policy/BWSConsoleReadOnlyAccess	提供共享带宽控制台查询功能全部管理权限	v1	是

策略详情

策略名称	策略文档	权限说明
BWSFullAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "bws:*", "Resource": "*"}]}</pre>	包括创建、删除、绑定、解绑等全部openAPI功能的权限
BWSReadOnlyAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": "bws:Describe*", "Resource": "*"}]}</pre>	描述共享带宽openAPI管理权限
BWSConsoleFullAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["bws:*", "eip:*", "vpc:DescribeInternetGateways", "slb:DescribeLoadBalancers", "epc:ListEpcs", "kec:DescribeInstances"], "Resource": "*"}]}</pre>	包括共享带宽和eip等全部功能的控制台管理权限
BWSConsoleReadOnlyAccess	<pre>{"Version": "2015-11-01", "Statement": [{"Effect": "Allow", "Action": ["vpc:Describe*", "eip:Describe*", "kec:DescribeInstances", "epc:ListEpcs", "slb:DescribeLoadBalancers"], "Resource": "*"}]}</pre>	包括查询共享带宽、EIP、SLB、云主机等信息的控制台管理权限

创建自定义策略

如果系统策略无法满足您的需求，您可以创建自定义策略，自定义策略支持更细粒度的权限划分，可以灵活满足差异化权限管理需求。

前提条件

创建自定义策略前，需要先了解权限策略语言的基本结构和语法，请参见[策略文档元素解析](#)。

操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**权限管理 > 策略**，进入到权限策略管理页面。
3. 单击**自定义策略**页签，进入自定义策略列表页面。
4. 单击**新建策略**，进入新建自定义策略页面，输入策略名称和备注。
5. 在设置策略类型区域选择对应的类型。
 - **产品功能 / 项目权限**：按产品功能创建的策略，由用户设置，解决对权限划分有一定要求，但并不复杂的用户诉求。-**可视化配置**：通过自主择服务和操作，并定义资源，自动生成策略语法，简单灵活，优先推荐使用。
 - 策略语法**：由用户设置，权限粒度灵活，由用户把控，解决对权限精细划分有较高要求的用户诉求。
 - 按标签授权**：将具有一类标签属性的资源快速授权给用户或用户组。
6. 单击**确定**，完成自定义策略创建。

后续步骤

可以将自定义策略授权给IAM子用户或用户组或角色。

修改自定义策略内容

本文为您介绍如何修改自定义策略的内容。

操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**权限管理** > **策略**，进入到权限策略管理页面。
3. 单击**自定义策略**页签，进入自定义策略列表页面。
4. 在自定义策略列表页面，单击目标策略名称。
5. 在**策略内容**页签，单击**修改信任策略**按钮。
6. 修改策略内容面板，修改权限策略内容，然后单击保存。

修改完成后，系统会自动生成一个新的版本。如果需要该新版本作为当前默认版本生成，保存的时候需选择设置为默认版本。

管理自定义策略版本

本文为您介绍如何管理自定义策略版本，包括查看版本、设置默认版本和删除版本。

限制说明

- 一个自定义策略最多可以有5个版本。
- 当自定义策略版本达到5个，在控制台再次修改自定义策略时，需要删除不需要的版本。
- 对于一个存在多版本的自定义策略，只有一个版本是活跃的，即默认版本。
- 默认版本只能查看，不能删除。

操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**权限管理** > **策略**，进入到权限策略管理页面。
3. 单击**自定义策略**页签，进入自定义策略列表页面。
4. 在自定义策略列表页面，单击目标策略名称。
5. 在**版本管理**页签下，您可以查看版本、设置默认版本和删除版本。

(1) 查看版本：单击查看可以查看权限策略的版本号和策略内容。(2) 设置默认版本：单击操作列下的设为默认版本，可设置该版本为默认版本。(3) 删除版本：单击操作列下的删除，然后单击确定，删除不需要的版本。

金山云KRN

当前金山云IAM使用到的KRN如下表（**斜体**需要被替换为实际值）：

资源名称	英文名称	资源KRN
实例	instance	karn:ksc:kec:region:account-id:instance/instance-id
云主机镜像	image	karn:ksc:kec:region::image/image-id
安全组	security-group	karn:ksc:vpc:region:account-id:security-group/security-group-id
子网	subnet	karn:ksc:vpc:region:account-id:subnet/subnet-id
网络接口	network-interface	karn:ksc:vpc:region:account-id:network-interface/network-interface-id
虚拟专有网络	vpc	karn:ksc:vpc:region:account-id:vpc/vpc-id
网络ACL	network-acl	karn:ksc:vpc:region:account-id:network-acl/network-acl-id
路由	route	karn:ksc:vpc:region:account-id:route/route-id
本地地址转换	nat	karn:ksc:vpc:region:account-id:nat/nat-id
隧道网关	tunnel	karn:ksc:vpc:region:account-id:tunnel/tunnel-id
对等连接	vpc-peering-connection	karn:ksc:vpc:region:account-id:vpc-peering-connection/vpc-peering-connection-id
负载均衡器	loadbalancer	karn:ksc:slb:region:account-id:loadbalancer/load-balancer-id
监听器	listener	karn:ksc:slb:region:account-id:listener/listener-id
用户	user	karn:ksc:iam::account-id:user/user-name
策略	policy	karn:ksc:iam::account-id:policy/policy-name

裸金属服务器镜像	image	<code>krn:ksc:epc:region::image/image-id</code>
裸金属服务器实例	epc-host	<code>krn:ksc:epc:region:account-id:epc-host/epc-host-id</code>