黑石物理服务器1.0

访问管理

产品文档

腾讯云

文档目录

访问管理

概述

最近更新时间：2020-10-12 09:38:28

什么是访问管理?

访问管理（Cloud Access Management，CAM）是腾讯云提供的Web服务，主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。用户可以通过 CAM 创建、管理和销毁用户(组)，并使用身份管理和策略管理控制其他用户使用腾讯云资源的权限。

当您使用 CAM 的时候，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。有关 CAM 策略的更多相关基本信息，请参照 策略语法。有关 CAM 策略的更多相关使用信息，请参照 策略。

黑石物理服务器、黑石弹性公网 IP、黑石私有网络，黑石负载均衡都已经接入 CAM，您可以使用 CAM 对相关黑石资源实现精细化的权限控制需求。

相关概念

- **CAM用户：** CAM 用户 为您在腾讯云中创建的一个实体，每一个 CAM 用户仅同一个腾讯云账户关联。您注册的腾讯云账号身份为**主账号**，您可以通过 用户管理 来创建拥有不同权限的**子账号**协作您。子账号的类型分为 子用户、协作者 以及 消息接收人。
- **策略：** 用于定义和描述一条或多条权限的语法规范。腾讯云的策略类型分为预设策略和自定义策略。
  - 预设策略：预设策略 由腾讯云创建和管理，是被用户高频使用的一些常见权限集合，如资源全读写权限等。操作对象范围广，操作粒度粗。预设策略为系统预设，不可被用户编辑。
  - 自定义策略：由用户创建的策略，允许作细粒度的权限划分。例如，为某数据库管理员关联一条策略，使其有权管理云数据库实例，而无权管理云服务器实例。
- **资源：** 即 resource 元素，描述一个或多个操作对象。例如黑石服务器、黑石负载均衡等实例。

黑石相关预设策略

预设策略，不需要编写策略，即可帮助您快速授权，但其缺点是授权的精度略为粗糙。以下是黑石产品的所有预设策略，分别为：

预设策略名	授权范围描述
QcloudBMFullAccess	关联后，获得所有黑石所有产品（cpm，bmeip，bmlb，bmvpc 等）实例的增、删、改、查操作等操作权限
QcloudBMReadOnlyAccess	关联后，只能获得查询黑石所有产品（cpm，bmeip，bmlb，bmvpc 等）列表及基本信息的权限
QcloudBMInnerFullAccess	关联后，获得所有黑石服务器实例的增、删、改、查等操作的权限
QcloudBMInnerReadOnlyAccess	关联后，只能获得查询黑石服务器列表及基本信息的权限
QcloudBMEIPFullAccess	关联后，获得所有黑石弹性公网 IP 实例的增、删、改、查等操作的权限
QcloudBMEIPReadOnlyAccess	关联后，只能获得查询黑石弹性公网 IP 列表及基本信息的权限
QcloudBMLBFullAccess	关联后，获得所有黑石负载均衡实例的增、删、改、查等操作的权限
QcloudBMLBReadOnlyAccess	关联后，只能获得查询黑石负载均衡列表及基本信息的权限
QcloudBMVPCFullAccess	关联后，获得所有黑石私有网络实例的增、删、改、查操作的权限
QcloudBMVPCReadOnlyAccess	关联后，只能获得查询黑石私有网络实例列表及基本信息的权限

鉴权失败处理

当您在使用腾讯云控制台或者 API 遇到以下提示，说明您没有被授予操作权限。请联系 root 帐号管理员或者有 CAM 管理权限的人员为您的 CAM 账号关联相应策略。调用任一黑石 API 都要求通过 CAM 鉴权，您需要把用到的 API 和实例 ID 都添加到策略中，否则该提示会频繁出现。

授权方法如下：

- **复制提示中的 operation 以及 resource，并黏贴到策略的 action 和 resource 字段，再关联这个策略即可完成授权。**
- **使用预设策略，但预设策略的授权的粒度较粗。**

更多访问控制相关的说明，请参考 访问管理 相关官方文档。

黑石物理服务器

最近更新时间：2020-10-12 09:49:49

概述

黑石物理服务器支持细化到实例级别的权限管理，您可以为人员分配管理特定物理服务器实例的权限；或者属于特定 VPC 或者子网的所有物理服务器的管理权限。

预设策略

预设策略，能帮助您快速授权，而不需要编写策略，但授权粒度会粗些，以下是黑石服务器的两个预设策略，分别为：

预设策略名	授权范围描述
QcloudBMInnerFullAccess	关联后，获得所有黑石服务器实例的增、删、改、查等操作的权限
QcloudBMInnerReadOnlyAccess	关联后，只能获得查询黑石服务器列表及基本信息的权限

Action、Resource、Condition 列表

以下表格，罗列了在配置黑石服务器的策略时，需要用到的 action、resource、condition。相关概念请参考 访问管理 章节。

- **Action**：即操作，对应的是 API。编写策略时，您可以复制表格里内容并粘贴在 Action 字段中。关联该策略后，即可获得特定 API 的调用权限。
- **Resource**：即云资源，当列表中 Action 的鉴权参数不为空时，则表示在调用 API 需要指定云资源，否则不需要指定。编写策略时，您可以复制表格里内容并粘贴在策略生成器的 Resource 字段中，但请记得替换 $region、$instanceId、$eipId 为真实的实例 ID。关联该策略后，即可获得特定资源的操作权限。

> ⚠ 注意：
> 部分 API 鉴权时需要两种产品的实例 ID，例如绑定 EIP，分别需要被绑定的黑石服务器以及用于绑定的黑石弹性公网 IP 的实例 ID，这时需要把两种云产品的资源描述都写在 Resource 里。

- **Condition**：即生效条件。换句话说 Action 和 Resource 需要在特定的生效条件下，才能鉴权通过。您可以灵活使用 condition 以做到 VPC 或者 Subnet 粒度的权限管理，例如授权人员管理特定 VPC 内的所有黑石服务器。

> ⚠ 注意：
> Describe 或者 Get 指查询操作，例如拉取多个实例详情等，查询操作鉴权通过后可能会把所有实例信息都返回，而无法区别哪些是有权限哪些是没有权限的实例。但再修改、删除实例时，会再次鉴权。

Action	鉴权参数	功能描述	条件密钥
bm:OfflineDevice	qcs::bm:$region::instance/$instanceId	退还后付费实例	bmvpc:unVpcId bmvpc:unSubnetId
bm:ModifyPayModePre2Post	qcs::bm:$region::instance/$instanceId	将设备从预付费转换为后付费	bmvpc:unVpcId bmvpc:unSubnetId
bm:ModifyDeviceAutoRenewFlag	qcs::bm:$region::instance/$instanceId	设置物理机服务器自动续费标志	bmvpc:unVpcId bmvpc:unSubnetId
bm:GetDeviceDeployProcess	qcs::bm:$region::instance/$instanceId	机器部署重装进度查询	bmvpc:unVpcId bmvpc:unSubnetId
bm:DescribeDevicePrice	qcs::bm:$region::instance/$instanceId	获取服务器的价格	bmvpc:unVpcId bmvpc:unSubnetId
bm:DescribeDevicePartition	qcs::bm:$region::instance/$instanceId	获取物理机的分区格式	bmvpc:unVpcId bmvpc:unSubnetId
bm:GetDeviceOutBandInfo	qcs::bm:$region::instance/$instanceId	获取设备的带外信息	bmvpc:unVpcId bmvpc:unSubnetId
bm:UnbindEip	qcs::bm:$region::instance/$instanceId qcs::bmeip::uin/:eipId/$eipId	解绑EIP	bmvpc:unVpcId bmvpc:unSubnetId
bm:BindEip	qcs::bm:$region::instance/$instanceId	绑定 EIP	bmvpc:unVpcId

	qcs::bmeip::uin/:eipId/$eipId		bmvpc:unSubnetId
bm:ResetDevicePasswd	qcs::bm:$region::instance/$instanceId	重置密码	bmvpc:unVpcId bmvpc:unSubnetId
bm:ReloadDeviceOs	qcs::bm:$region::instance/$instanceId	重装操作系统	bmvpc:unVpcId bmvpc:unSubnetId
bm:DescribeDeviceOperationLog	qcs::bm:$region::instance/$instanceId	获取设备的操作日志	bmvpc:unVpcId bmvpc:unSubnetId
bm:ModifyDeviceAlias	qcs::bm:$region::instance/$instanceId	批量修改设备名称	bmvpc:unVpcId bmvpc:unSubnetId
bm:StartDevice	qcs::bm:$region::instance/$instanceId	开机	bmvpc:unVpcId bmvpc:unSubnetId
bm:ShutdownDevice	qcs::bm:$region::instance/$instanceId	关闭服务器	bmvpc:unVpcId bmvpc:unSubnetId
bm:RebootDevice	qcs::bm:$region::instance/$instanceId	重启机器	bmvpc:unVpcId bmvpc:unSubnetId
bm:DescribeDevice	-	获取物理服务器列表	-
bm:DescribeDeviceWeb	-	获取黑石物理服务器列表	-
bm:DescribeDeviceTrash	-	获取黑石物理服务器回收站列表	-
bm:SetOutBandVPNAuthPwd	-	设置带外 VPN 认证用户密码	-
bm:GetOutBandVPNAuthInfo	-	获取带外 VPN 认证信息	-
bm:BuyDevice	-	获取设备的带外信息	-
bm:RunUserCmd	-	运行自定义脚本	-
bm:GetUserCmdTaskDetail	-	查任务详细信息	-
bm:GetUserCmdTaskDetailList	-	获取任务详细信息列表	-
bm:GetUserCmdTaskList	-	获取任务列表	-
bm:DeleteUserCmd	-	删除自定义脚本	-
bm:GetUserCmd	-	查自定义脚本内容	-
bm:GetUserCmdList	-	查询自定义脚本列表	-
bm:ModifyUserCmd	-	修改自定义脚本	-
bm:AddUserCmd	-	新建自定义脚本	-

Condition（生效条件）

灵活使用 Condition，即可做到 VPC 或者 Subnet 粒度的权限管理，例如授权管理特定 VPC 内的所有黑石服务器。

> ⚠ 注意：
> 在使用 Condition 时，做到 VPC 或者 Subetnet 粒度的授权，策略的 Resource 字段建议只需填写 * 。

书写规范

```
"condition":
{
"Option1":{"key1":["value1","value2"]),"key2":["value1","value2"])},
"Option2":{"key1":["value1","value2"]),"key2":["value1","value2"])}
}
```

Option 即操作符，理解为传入的鉴权参数和 key 的运算规则。Key 和 Value 是对应的，以下是对应关系。传入的鉴权参数经过运算后应该满足 key 和 value 的要求。

key	value
bmvpc:unVpcId	vpc-yyyyyy（VPC 的实例 Id）
bmvpc:unSubnetId	subnet-xxxxx（Subnet 的实例 Id）

操作符（Option）

黑石服务器只推荐使用 `string_equal` 以及 `for_all_value:string_equal_if_exist`：

- string_equal，用于 condition 只有一个 key 和一个 value 的情况，要求传入的鉴权参数满足 key:value，可以做到特定 VPC 或者 subnet 的授权。
- for_all_value:string_equal_if_exist，用于 condition 有一个 key 多个 value 的情况。key:value1,value2，可以做到多个 VPC 或者 subnet 的授权。

例子

策略如下：

```
{
"version": "2.0",
"statement": {
"effect": "allow",
"action": "bm:ModifyDeviceAlias",
"resource": "*",
"condition": {
"string_equal": {
"bmvpc:unVpcId": "vpc-12345"
}
}
}
}
```

场景：调用 ModifyDeviceAlias 修改 cpm-678910 的别名。

评估逻辑：

1. 鉴权逻辑发现关联了 effect:allow 的策略且 action:bm:ModifyDeviceAlias 和 resource:*，即允许修改任一实例的别名。
2. 但前提是实例要在 vpc-12345里，鉴权才能通过。

最佳实践

本章节，我们举例两个场景的策略内容和评估逻辑，帮助您了解如何实现黑石服务器的权限分配。

- 场景 1：授权将 eip-34lvo6ir 绑定在 cpm-ftukx3a
- 场景 2：授权重启 vpc-34cxlz7z 内的所有物理服务器

场景 1

策略如下：

```
{
"version": "2.0",
"statement": [{
"effect": "allow",
"action": [
"name/bm:BindEip"
],
"resource": [
"qcs::bm:::instance/cpm-ftukx3aj",
"qcs::bmeip::: eipId / eip - 34 lvo6ir "
]
```

```
}]
}
```

评估逻辑：
当调用 BindEip 时，CAM 会判断传入的 InstanceId 和 EipId 是否为 cpm-ftukx3aj 和 eip-34lvo6ir，【是】则鉴权通过。

场景 2

策略如下：

```
{
"version": "2.0",
"statement": [{
"effect": "allow",
"action": [
"name/bm:RebootDevice"
],
"resource": [
"*"
],
"condition": {
"for_all_value:string_equal_if_exist": {
"bmvpc:unVpcId": ["vpc-34cxlz7z", "vpc-34cxlz12"]
}
}
}]
}
```

评估逻辑：
当调用 RebootDevice 时，CAM 对传入的 instanceId 做鉴权，发现满足 resource（*）的要求。
但要求 instanceId在vpc-34cxlz7z 或者 vpc-34cxlz12 里，【是】则鉴权通过，【否】则鉴权失败。

黑石弹性公网 IP

最近更新时间：2020-10-12 11:21:06

概述

黑石弹性公网 IP 支持细化到实例级别的权限管理，您可以为人员分配管理特定弹性公网 IP 实例的权限；或者属于特定 VPC 的所有弹性公网 IP 的管理权限。

预设策略

预设策略，能帮助您快速授权，而不需要编写策略，但授权粒度会粗些，以下是黑石弹性公网 IP 的两个预设策略，分别为：

预设策略名	授权范围描述
QcloudBMEIPFullAccess	关联后，获得所有黑石弹性公网 IP 实例的增、删、改、查等操作的权限
QcloudBMEIPReadOnlyAccess	关联后，只能获得查询黑石弹性公网 IP 列表及基本信息的权限

Action、Resource、Condtion 列表

以下表格，罗列了在配置黑石弹性公网 IP 的策略时，需要用到的 action、resource、condition。相关概念请参考 访问管理 章节。

- **Action**：即操作，对应的是 API。编写策略时，您可以复制表格里内容并粘贴在 Action 字段中。关联该策略后，即可获得特定 API 的调用权限。
- **Resource**：即云资源，当列表中 Action 的鉴权参数不为空时，则表示在调用 API 需要指定云资源，否则不需要指定。编写策略时，您可以复制表格里内容并粘贴在策略生成器的 Resource 字段中，但请记得替换 $eipId、$InstanceId 为真实的实例 ID；关联该策略后，即可获得特定资源的操作权限。

> ⚠ 注意：
> 部分 API 鉴权时需要两种类型的实例 ID，例如绑定 EIP，分别需要被绑定的黑石服务器以及用于绑定的黑石弹性公网 IP 的实例 ID，这时需要把两种云产品的资源描述都写在 Resource 里。

- **Condition**：即生效条件。换句话说 Action 和 Resource 需要在特定的生效条件下，才能鉴权通过。您可以灵活使用 condtion 以做到 VPC 或者 Subnet 粒度的权限管理，例如授权人员管理特定VPC内的所有黑石服务器。

> ⚠ 注意：
> Describe* 或者 Get* 指查询操作，例如拉取多个实例详情等，查询操作鉴权通过后可能会把所有实例信息都返回，而无法区别哪些是有权限哪些是没有权限的实例。但再修改、删除实例时，会再次鉴权。

Action	鉴权参数	功能描述	条件密钥
bmeip:EipBmUnBindVpcIp	qcs::bmeip:::eipId/$eipId	黑石 EIP 解绑 VPCIP 云服务器或者托管	bmvpc:unVpcId
bmeip:EipBmBindVpcIp	qcs::bmeip:::eipId/$eipId	黑石 EIP 绑定 VPCIP（云服务器或者托管）	bmvpc:unVpcId
bm:UnbindEip	qcs::bmeip:::eipId/$eipId qcs::bm:::instance/$InstanceId	解绑黑石 EIP	bmvpc:unVpcId
bm:BindEip	qcs::bmeip:::eipId/$eipId qcs::bm:::instance/$InstanceId	绑定黑石 EIP	bmvpc:unVpcId
bmeip:EipBmModifyCharge	qcs::bmeip:::eipId/$eipId	黑石 EIP 修改计费方式	bmvpc:unVpcId
bmeip:ModifyEipAlias	qcs::bmeip:::eipId/$eipId	更新黑石 EIP 名称	bmvpc:unVpcId
bmeip:EipBmDelete	qcs::bmeip:::eipId/$eipId	释放黑石 EIP	bmvpc:unVpcId
bmeip:EipBmApply	qcs::bmvpc:::unVpcId/vpc-xxx	创建黑石 EIP	-
bmeip:DescribeEipBm	-	黑石 EIP 查询接口	-

Condition（生效条件）

灵活使用 Condtion，即可做到 VPC 粒度的权限管理，例如授权管理特定 VPC 内的黑石弹性公网 IP 实例。

> 注意：
> 在使用Condtion时，做到 VPC 粒度的授权，策略的 Resource 字段建议只需填写 * 。

书写规范

```
"condition":
{
"Option1":{"key1":["value1","value2"]),"key2":["value1","value2"])},
"Option2":{"key1":["value1","value2"]),"key2":["value1","value2"])}
}
```

Option 即操作符，理解为传入的鉴权参数和 key 的运算规则。Key 和 Value 是对应的，以下是对应关系。传入的鉴权参数经过运算后应该满足 key 和 value 的要求。

key	value
bmvpc：unVpcId	vpc-yyyyyy（VPC 的实例 ID）

操作符（Option）

黑石弹性公网IP只推荐使用 `for_all_value:string_equal_if_exist`：

for_all_value:string_equal_if_exist，用于 condition 有一个 key 多个 value 的情况。key:value1,value2，可以做到多个 VPC 或者 subnet 的授权。

例子

策略如下：

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":[
"bmeip:EipBmModifyCharge"
],
"resource":[
"*"
],
"condition":{
"for_all_value:string_equal_if_exist":{
"bmvpc:unVpcId":"vpc-34cxlz7z"
}
}
}
]
}
```

场景：调用 EipBmModifyCharge 修改 vpc-34cxlz7z 的任一 EIP 实例的别名。

评估逻辑：

1. 鉴权逻辑关联了 effect:allow 的策略且 action:bmeip:EipBmModifyCharge 和 resource:*，即允许修改任一实例的别名。
2. 但前提是，实例要在 vpc-34cxlz7z 里才能鉴权通过。

最佳实践

本章节，我们举例两个场景的策略内容和评估逻辑，帮助您了解如何实现黑石服务器的权限分配。

- 场景 1：授权释放 eip-adt6pq7f

- 场景 2：授权绑定 vpc-34cxlz7z 和 vpc-muinpf9p 里内所有的物理服务器和 EIP

场景1

策略如下：

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":[
"bmeip:EipBmDelete"
],
"resource":[
"qcs::bmeip:::eipId/eip-adt6pq7f"
]
}
]
}
```

评估逻辑：

当调用 EipBmDelete 时，CAM会判断传入的 EipId 是否为 eip-adt6pq7f，【是】则鉴权通过，【否】则鉴权失败。

场景2

策略如下：

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":[
"bm:BindEip",
"bm:UnbindEip"
],
"resource":[
"*"
],
"condition":{
"for_all_value:string_equal_if_exist":{
"bmvpc:unVpcId":[
"vpc-34cxlz7z",
"vpc-muinpf9p"
]
}
}
}
]
}
```

评估逻辑：
当调用 BindEip 时，CAM 会对传入的 instanceId 和 EipID 做鉴权，发现满足 resource（*）的要求。
但要求 instanceId 和 EipID 在 vpc-34cxlz7z 或者 vpc-muinpf9p 里，【是】则鉴权通过，【否】则鉴权失败。

黑石负载均衡

最近更新时间：2020-10-12 11:56:29

概述

黑石负载均衡支持细化到实例级别的权限管理，您可以为人员分配管理特定负载均衡实例的权限；或者特定 VPC 内所有负载均衡或者监听器的管理权限。

预设策略

预设策略，能帮助您快速授权，而不需要编写策略，但授权粒度会粗些，以下是黑石负载均衡的两个预设策略，分别为：

预设策略名	授权范围描述
QcloudBMLBFullAccess	关联后，获得所有黑石负载均衡实例的增、删、改、查等操作的权限。
QcloudBMLBReadOnlyAccess	关联后，只能获得查询黑石负载均衡列表及基本信息的权限。

Action、Resource、Condtion 列表

以下表格，罗列了在编辑黑石负载均衡策略时，需要用到的 action、resource、condition。相关概念请参考 访问管理 章节。

- **Action**：即操作，对应的是 API。编写策略时，您可以复制表格里内容并粘贴在 Action 字段中。关联该策略后，即可获得特定 API 的调用权限。
- **Resource**：即云资源，当列表中 Action 的鉴权参数不为空时，则表示在调用 API 需要指定云资源，否则不需要指定。编写策略时，您可以复制表格里内容并粘贴在策略生成器的 Resource 字段中。但请记得替换 $VpcId、$lbId 及 $LblistenId 为真实的实例 ID；关联该策略后，即可获得特定资源的操作权限。

> ⚠ 注意：
> 部分 API 鉴权时需要不同类型的实例 ID，例如 CreateBmForwardRules，分别需要负载均衡和监听器的实例 ID，这时需要把两种资源描述都写在 Resource 里。

- **Condition**：即生效条件。换句话说 Action 和 Resource 需要在特定的生效条件下，才能鉴权通过。您可以灵活使用 condtion 以实现 VPC 或者 Subnet 粒度的权限管理，例如授权人员管理特定子网内的所有监听器。

> ⚠ 注意：
> Describe* 或者 Get* 指查询操作，例如拉取多个实例详情等，查询操作鉴权通过后可能会把所有实例信息都返回，而无法区别哪些是有权限哪些是没有权限的实例。但再修改、删除实例时，会再次鉴权。

Action	鉴权参数	功能描述	条件密钥
bmlb:CreateBmLoadBalancer	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc::uin/:unSubnetId/$SubnetId(内网)	创建负载均衡	-
bmlb:ModifyBmLoadBalancerAttributes	qcs::bmlb:::loadBalancerId/$Lbid	修改负载均衡属性信息	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:DeleteBmLoadBalancers	qcs::bmlb:::loadBalancerId/$Lbid	删除负载均衡	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:CreateBmListeners	qcs::bmlb:::loadBalancerId/$Lbid	创建负载均衡四层监听器	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmListener	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	创建负载均衡四层监听器	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:BindBmL4ListenerRs	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	绑定物理服务器到四层监听器	bmvpc:unVpcId bmvpc:unSubnetId

bmlb:BindBmL4ListenerVmIp	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	绑定虚机IP到负载均衡四层监听器	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmL4ListenerBackendWeight	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	修改负载均衡四层监听器后端实例权重	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmL4ListenerBackendPort	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	修改负载均衡四层监听器后端实例端口	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:UnbindBmL4ListenerRs	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	解绑负载均衡四层监听器物理服务器	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:UnbindBmL4ListenerVmIp	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	解绑负载均衡四层监听器虚机 IP	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:DeleteBmListeners	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	删除负载均衡四层监听器	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:CreateBmForwardListeners	qcs::bmlb:::loadBalancerId/$Lbid	创建负载均衡七层监听器	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmForwardListener	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	修改负载均衡七层监听器	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:CreateBmForwardRules	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	创建负载均衡七层转发规则	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmForwardLocation	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	修改负载均衡七层转发路径	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:BindBmLocationInstances	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	绑定物理服务器到七层转发路径	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:BindBmL7LocationVmIp	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	绑定虚机IP 到负载均衡七层转发路径	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmLocationBackendWeight	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	修改负载均衡七层转发路径后端实例权重	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmLocationBackendPort	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	修改负载均衡七层转发路径后端实例端口	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:UnbindBmLocationInstances	qcs::bmlb:::loadBalancerId/$Lbid	解绑物理	bmvpc:unVpcId

	qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	服务器到七层转发路径	bmvpc:unSubnetId
bmlb:UnbindBmL7LocationVmIp	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	解绑负载均衡七层转发路径虚机 IP	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:DeleteBmForwardRules	qcs::bmlb:::loadBalancerId/$Lbid	删除负载均衡七层转发规则	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmLoadBalancerChargeMode	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId	更改黑石 LB 的计费方式	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:ModifyBmL4ListenerBackendProbePort	qcs::bmlb:::loadBalancerId/$Lbid qcs::bmlb:::listenerId/$LlistenId qcs::bm:::instance/$InstanceId	修改4层 LB 后端实例探测端口	bmvpc:unVpcId bmvpc:unSubnetId
bmlb:DescribeBmListeners	-	获取负载均衡四层监听器	-
bmlb:DescribeBmListenerInfo	-	获取负载均衡四层监听器详细信息	-
bmlb:DescribeBmBindInfo	-	获取主机的负载均衡的绑定详情	-
bmlb:DescribeBmVportInfo	-	获取负载均衡端口信息	-
bmlb:DescribeBmLoadBalancers	-	获取负载均衡实例列表	-
bmlb:DescribeBmL4ListenerBackends	-	获取负载均衡四层监听器绑定的主机列表	-
bmlb:DescribeBmForwardListeners	-	获取负载均衡七层监听器	-
bmlb:DescribeBmForwardListenerInfo	-	获取负载均衡七层监听器详细信息	-
bmlb:DescribeBmForwardRules	-	获取负载均衡七层转发规则	-
bmlb:DescribeBmLocationBackends	-	获取负载均衡七层转发路径绑定的主机列表	-
bmlb:UploadBmCert	-	创建负载均衡证书	-

bmlb:GetBmCertDetail	-	获取负载均衡证书详情	-
bmlb:ReplaceBmCert	-	更新负载均衡证书	qcs::bmlb::uin/:certId/$certId

Condition（生效条件）

灵活使用 Condtion，即可做到 VPC 或者 Subnet 粒度的权限管理，例如授权管理特定 VPC 内的所有负载均衡

> 注意：
> 在使用 Condtion时，要做到 Vpc 或者 Subetnet 粒度的授权，策略的 Resource 字段建议只需填写 * 。

书写规范

```
"condition":
{
"Option1":{"key1":["value1","value2"]),"key2":["value1","value2"])},
"Option2":{"key1":["value1","value2"]),"key2":["value1","value2"])}
}
```

Option 即操作符，理解为传入的鉴权参数和 key 的运算规则。Key 和 Value 是对应的，以下是对应关系。传入的鉴权参数经过运算后应该满足 key 和 value 的要求。

key	value
bmvpc:unVpcId	vpc-yyyyyy（VPC 的实例 ID）
bmvpc:unSubnetId	subnet-xxxxx（Subnet 的实例 ID）

操作符（Option）

黑石负载均衡只推荐使用 `string_equal` 以及 `for_all_value:string_equal_if_exist`：

- string_equal，用于 condition 只有一个 key 和一个 value 的情况，要求传入的鉴权参数满足 key:value，可以做到特定 VPC 或者 subnet 的授权。
- for_all_value:string_equal_if_exist，用于 condition 有一个 key 多个 value 的情况 key:value1,value2，可以做到多个 VPC 或者 subnet 的授权。

例子

策略如下：

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":[
"bmlb:BindBmL4ListenerRs"
],
"resource":[
"qcs::bmlb:::loadBalancerId/lb-dtrzsshx",
"qcs::bmlb:::listenerId/lbl-6l1q8cdf",
"qcs::bm:::instance/*"
],
"condition":{
"for_all_value:string_equal_if_exist":{
"bmvpc:unSubnetId":[
"subnet-1so5ae8m",
"subnet-jv24ivq0"
]
```

```
}
}
}
]
}
```

场景：调用 BindBmL4ListenerRs，为内网 LB 监听器 lbl-6l1q8cdf 绑定同 vpc 的物理服务器 cpm-6y3le68b 时。

1. 鉴权逻辑发现关联了 effect:allow 的策略且 action:bm:BindBmL4ListenerRs 和 lb、listen、cpm 等实例
2. 但前提是，上述三种资源需要在 subnet-1so5ae8m 或者 subnet-jv24ivq0 才能鉴权通过。

最佳实践

本章节，我们举例两个场景的策略内容和评估逻辑，帮助您了解如何实现黑石服务器的权限分配。

- 场景 1：授权在 vpc-muinpf9p 里创建一个外网监听器
- 场景 2：授权在 subnet-c6bzyq4a 里的所有内网负载均衡七层监听器创建七层转发路径

场景1

策略如下:

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":[
"bmlb:CreateBmLoadBalancer"
],
"resource":[
"qcs::bmvpc:::unVpcId/vpc-muinpf9p"
]
}
]
}
```

评估逻辑:

调用 CreateBmLoadBalancer时，CAM 判断传入的 VpcId 参数是否为 vpc-muinpf9p，【是】则鉴权通过，【否】则鉴权失败。

场景2

策略如下:

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":[
"bmlb:CreateBmForwardRules"
],
"resource":[
"qcs::bmlb:::loadBalancerId/*",
"qcs::bmlb:::listenerId/*"
],
"condition":{
"string_equal":{
"bmvpc:unSubnetId":"subnet-c6bzyq4a"
```

```
}
}
}
]
}
```

评估逻辑：
当调用 CreateBmForwardRules时，CAM 会对传入 loadBalancerId 和 listenerId 做鉴权，发现满足 resource（*）的要求。
但要求两个资源都在子网 subnet-c6bzyq4a 里，【是】则鉴权通过，【否】则鉴权失败。

黑石私有网络

最近更新时间：2020-10-13 09:30:04

概述

黑石私有网络支持细化到实例级别的权限管理，您可以为人员分配管理特定 VPC 实例的管理权限。

预设策略

预设策略，能帮助您快速授权，而不需要编写策略，但授权粒度会粗些，以下是黑石私有网络的两个预设策略，分别为：

预设策略名	授权范围描述
QcloudBMVPCFullAccess	关联后，获得所有黑石私有网络实例的增、删、改、查操作的权限。
QcloudBMVPCReadOnlyAccess	关联后，只能获得查询黑石私有网络实例列表及基本信息的权限。

Action、Resource、Condtion 列表

以下表格，罗列了在配置黑石私有网络的策略时，需要用到的 action、resource、condition。相关概念请参考 访问管理 章节。

- **Action**：即操作，对应的是 API。编写策略时，您可以复制表格里内容并粘贴在 Action 字段中。关联该策略后，即可获得特定 API 的调用权限。
- **Resource**：即云资源，当列表中 Action 的鉴权参数不为空时，则表示在调用 API 需要指定云资源，否则不需要指定。编写策略时，您可以复制表格里内容并粘贴在策略生成器的 Resource 字段中，但请记得替换 $unVpcId、$unSubnetId、$NatId、$PeerId 为真实的实例 ID；关联该策略后，即可获得特定资源的操作权限。

> ⚠ 注意：
> 部分 API 鉴权时需要两种类型的实例 ID，例如黑石 NAT 网关绑定 EIP，分别需要被绑定的 NAT 网关以及用于绑定的黑石弹性公网 IP 的实例 ID，这时需要把两种云产品的资源描述都写在 Resource 里。

- **Condition**：即生效条件。换句话说 Action 和 Resource 需要在特定的生效条件下，才能鉴权通过。您可以灵活使用 condtion 以做到 VPC 或者 Subnet 粒度的权限管理，例如授权人员管理特定 VPC 内的所有黑石服务器。

> ⚠ 注意：
> Describe 或者 Get 指查询操作，例如拉取多个实例详情等，查询操作鉴权通过后可能会把所有实例信息都返回，而无法区别哪些是有权限哪些是没有权限的实例。但再修改、删除实例时，会再次鉴权。

Action	鉴权参数	功能描述	条件密钥
bmvpc:SubnetBindBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	黑石 NAT 网关绑定子网	-
bmvpc:SubnetUnBindBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	黑石网关解绑子网	-
bmvpc:EipUnBindBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatIdx qcs::bmeip:::eipId/$EipId	黑石网关解绑 EIP	-
bmvpc:EipBindBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId qcs::bmeip:::eipId/$EipId	黑石 NAT 网关绑定 EIP	-
bmvpc:UpgradeBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	升级黑石 NAT 网关	-
bmvpc:DeleteBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	删除黑石 NAT 网关	-
bmvpc:CreateBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId	创建黑石 NAT 网关	-
bmvpc:UpdateBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	更新黑石 NAT 网关绑定信息	-

bmvpc:UnbindIpsToBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	黑石 NAT 网关解绑 IP	-
bmvpc:BindIpsToBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	黑石 NAT 网关绑定 IP	-
bmvpc:ModifyBmNatGateway	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::natId/$NatId	修改黑石 NAT 网关名称	-
bmvpc:RegisterBatchIp	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::unSubnetId/$unSubnetId	指定 VPC 内网 IP 注册	-
bmvpc:ApplyIps	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::unSubnetId/$unSubnetId	VPC 内网 IP 申请	-
bmvpc:ModifySubnetDhcpRelayFlag	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::unSubnetId/$unSubnetId	修改子网 Dhcp	-
bmvpc:ModifyBmSubnetAttribute	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::unSubnetId/$unSubnetId	修改黑石私有网络中的子网属性	-
bmvpc:DeleteBmSubnet	qcs::bmvpc:::unVpcId/$unVpcId qcs::bmvpc:::unSubnetId/$unSubnetId	删除黑石私有网络的子网	-
bmvpc:ModifyBmVpcPeeringConnection	qcs::bmvpc:::vpcPeerId/$PeerId	黑石修改对等连接属性	-
bmvpc:DeleteBmVpcPeeringConnection	qcs::bmvpc:::vpcPeerId/$PeerId	黑石删除对等连接	-
bmvpc:CreateBmVpcPeeringConnection	qcs::bmvpc:::vpcPeerId/$PeerId	黑石创建对等连接	-
bmvpc:EnableBmVpcPeeringConnection	qcs::bmvpc:::vpcPeerId/$PeerId	黑石激活对等连接申请	-
bmvpc:RejectBmVpcPeeringConnection	qcs::bmvpc:::vpcPeerId/$PeerId	黑石拒绝对等连接	-
bmvpc:AcceptBmVpcPeeringConnection	qcs::bmvpc:::vpcPeerId/$PeerId	黑石接受对等连接	-
bmvpc:ReturnIps	qcs::bmvpc:::unVpcId/$unVpcId	回收 VPC 子网 IP	-
bmvpc:ModifyBmRouteTableAttribute	qcs::bmvpc:::unVpcId/$unVpcId	修改黑石路由表项	-
bmvpc:ModifyBmVpcAttribute	qcs::bmvpc:::unVpcId/$unVpcId	修改黑石 VPC 属性	-
bmvpc:CreateBmSubnet	qcs::bmvpc:::unVpcId/$unVpcId	创建黑石私有网络的子网	-
bmvpc:DelBmInterface	qcs::bmvpc:::unVpcId/$unVpcId	物理机从带 VLANTAG 子网中移除	-
bmvpc:DescribeBmNatSubnetEx	-	查询子网被 NAT 网关使用情况信息	-
bmvpc:DescribeBmNatGateway	-	黑石 NAT 网关列表	-
bmvpc:DescribeBmVpcPeeringConnections	-	查询黑石对等连接	-
bmvpc:DescribeBmVpcEx	-	查询黑石私有网络列表	-
bmvpc:DescribeBmSubnetEx	-	查询黑石私有网络中的子网信息	-
bmvpc:DescribeBmSubnetAvailableIp	-	获取 VPC 子网内可用 IP	-
bmvpc:DescribeBmNatSubnetBindIps	-	查看给定 NAT 下子网绑定的 IP	-
bmvpc:DescribeBmSubnetIpInfo	-	查看给定子网下的 IP 信息	-
bmvpc:DescribeBmSubnetIps	-	拉取子网已分配的 IP 列表	-
bmvpc:DescribeBmSubnetByCpmId	-	拉取物理机加入的所有子网列表	-

bmvpc:DescribeBmCpmBySubnetId	-	拉取加入子网的所有物理机列表	-
bmvpc:DescribeBmRouteTableEx	-	获取黑石路由表详情	-
bmvpc:CreateBmVpc	-	创建黑石私有网络和子网	bmvpc:unVpcId bmvpc:$unSubnetId
bmvpc:CreateBmInterface	qcs::bmvpc:::unVpcId/$unVpcId	物理机加入带VLANTAG 子网	bmvpc:unVpcId bmvpc:$unSubnetId

最佳实践

本章节，我们举例两个场景的策略内容和评估逻辑，帮助您了解如何实现黑石服务器的权限分配。

场景：授权将 eip-b2h2rhs5 绑定到属于 vpc-34cxlz7z 的 NAT 网关：nat-am27agoo 以及解绑权限。

场景

策略如下：

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":[
"bmvpc:EipBindBmNatGateway",
"bmvpc:EipUnBindBmNatGateway"

],
"resource":[
"qcs::bmvpc:::natId/nat-am27agoo",
"qcs::bmvpc:::unVpcId/vpc-34cxlz7z",
"qcs::bmeip:::eipId/eip-b2h2rhs"

]
}
]
}
```

评估逻辑：
当调用 EipBindBmNatGateway 或者 EipUnBindBmNatGateway 时，CAM 会判断传入的 NatId、EipId、VpcId 是否为 nat-am27agoo、vpc-34cxlz7z、eip-b2h2rhs。【是】则鉴权通过，【否】则鉴权失败。