# 阿里云安全架构设计

之 ACE 认证考试辅导版

## 目录





## 什么是访问控制

访问控制（RAM）是阿里云提供的管理用户身份与资源访问权限的服务。

RAM允许在一个云账号下创建并管理多个身份，并允许给单个身份或一组身份分配不同的权限，从而实现不同用户拥有不同资源访问权限的目的。

- RAM的功能特性如下：
  - 集中控制RAM用户及其密钥：管理每个RAM用户及其访问密钥，为用户绑定多因素认证（MFA）设备。
  - 集中控制RAM用户的访问权限：控制每个RAM用户访问资源的权限。
  - 集中控制RAM用户的资源访问方式：确保RAM用户在指定的时间和网络环境下，通过安全信道访问特定的阿里云资源。
  - 集中控制云资源：对RAM用户创建的实例或数据进行集中控制。当用户离开组织时，实例或数据不会丢失。
  - 单点登录管理（SSO）：支持与企业身份提供商（IdP）进行用户SSO或角色SSO。



## 用户身份类型

- 访问控制（RAM）中有三种身份：
  - RAM用户
    - RAM用户是RAM的一种实体身份类型，有确定的身份ID和身份凭证，它通常与某个确定的人或应用程序一一对应。
  - 用户组
    - 用户组是RAM的一种实体身份类型，用户组可以对职责相同的RAM用户进行分类并授权，从而更好的管理用户及其权限。
  - RAM角色
    - RAM角色是一种虚拟用户，RAM角色需要被一个受信的实体用户扮演。

## RAM 用户

RAM用户是RAM的一种实体身份类型，有确定的身份ID和身份凭证，它通常与某个确定的人或应用程序——对应。

- 一个阿里云账号下可以创建多个RAM用户，对应企业内的员工、系统或应用程序。
- RAM用户不拥有资源，不能独立计量计费，由所属阿里云账号统一控制和付费。
- RAM用户归属于阿里云账号，只能在所属阿里云账号的空间下可见，而不是独立的阿里云账号。
- RAM用户必须在获得阿里云账号的授权后才能登录控制台或使用API操作阿里云账号下的资源。



## RAM 用户组

访问控制（RAM）通过用户组对职责相同的RAM用户进行分类并授权，可以更加高效地管理RAM用户及其权限。

- 在RAM用户职责发生变化时，只需将其移动到相应职责的用户组下，不会对其他RAM用户产生影响。关于如何创建用户组，请参见创建用户组。
- 当用户组的权限发生变化时，只需修改用户组的权限策略，即可应用到所有RAM用户。关于如何为用户组授权，请参见为用户组授权。



## 权限策略

- 权限是用来描述用户、用户组、角色对具体资源的访问能力。
- 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。
- RAM支持以下两种权限策略：
  - 阿里云管理的系统策略：统一由阿里云创建，用户只能使用不能修改，策略的版本更新由阿里云维护。
  - 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。
- 为RAM主体授权，是指为用户、用户组或角色绑定一个或多个权限策略。



## 权限策略语言

**权限策略基本元素**

权限策略基本元素是权限策略的基本组成部分，RAM中使用权限策略来描述授权的具体内容。

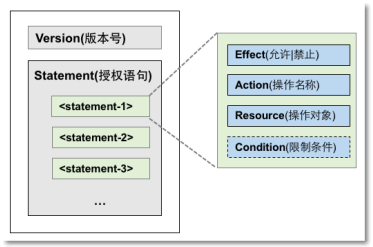
- 基本元素包括：
  - 效力（Effect），授权效力包括两种：允许（Allow）和拒绝（Deny）。
  - 操作（Action），操作是指对具体资源的操作。
  - 资源（Resource），资源是指被授权的具体对象。
  - 限制条件（Condition），限制条件是指授权生效的限制条件。

## 权限策略语言

**权限策略结构**

每条授权语句包括授权效力（Effect）、操作（Action）、资源（Resource）以及限制条件（Condition，可选项）。

- 版本：当前支持的权限策略版本，固定为1，不允许修改。
- RAM仅支持JSON格式。当创建或更新权限策略时，RAM会先检查JSON格式的正确性。






## 示例：重启ECS实例

```
{
  "Statement": [
    {
      "Action": "ecs:RebootInstance",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "Bool": {
          "acs:MFAPresent": "true"
        }
      }
    }
  ],
  "Version": "1"
}
```



## RAM角色

RAM角色（RAM role）与RAM用户一样，都是RAM身份类型的一种。RAM角色是一种虚拟用户，没有确定的身份认证密钥，需要被一个受信的实体用户扮演才能正常使用。

它与实体用户（云账号、RAM用户和云服务）和教科书式角色（Textbook role）不同。

- 实体用户：拥有确定的登录密码或访问密钥。
- 教科书式角色：教科书式角色或传统意义上的角色是指一组权限集合，类似于RAM里的权限策略。如果一个用户被赋予了这种角色，也就意味着该用户被赋予了一组权限，可以访问被授权的资源。
- RAM角色：RAM角色有确定的身份，可以被赋予一组权限策略，但没有确定的登录密码或访问密钥。RAM角色需要被一个受信的实体用户扮演，扮演成功后实体用户将获得RAM角色的安全令牌，使用这个安全令牌就能以角色身份访问被授权的资源。



## RAM角色类型

根据RAM可信实体的不同，RAM支持以下三种类型的角色：

- **阿里云账号**：允许RAM用户所扮演的角色。扮演角色的RAM用户可以属于自己的云账号，也可以属于其他云账号。此类角色主要用来解决跨账号访问和临时授权问题。
- **阿里云服务**：允许云服务所扮演的角色。此类角色主要用于授权云服务代理您进行资源操作。
- **身份提供商**：允许受信身份提供商下的用户所扮演的角色。此类角色主要用于实现与阿里云的SSO。

## RAM角色的使用方法

1. RAM角色指定可信实体，即指定可以扮演角色的实体用户身份。
2. 可信实体通过控制台或调用API扮演角色并获取角色令牌。
   - 通过控制台扮演角色：切换身份是在控制台中实体用户从当前登录身份切换到RAM角色身份的方法，详情请参见使用RAM角色。
   - 通过调用API扮演角色：一个实体用户通过调用AssumeRole可以获得角色令牌，使用角色令牌可以访问云服务API。
3. 为RAM角色绑定权限策略。
4. 受信实体通过扮演角色，使用角色令牌访问阿里云资源。



## RAM角色的应用场景

- 移动应用使用临时安全令牌访问阿里云
- 跨云账号的资源授权
- 对云上应用进行动态身份管理与授权



## 跨阿里云账号的资源授权

企业A购买了多种阿里云资源来开展业务，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。企业A希望将部分业务授权给企业B。

企业A有如下要求：

- 企业A希望能专注于业务系统，仅作为资源Owner。企业A希望可以授权账号B来操作部分业务，例如：云资源运维、监控以及管理等。
- 企业A希望当企业B的员工加入或离职时，无需做任何权限变更。企业B可以进一步将企业A的资源访问权限分配给企业B的RAM用户（员工或应用），并可以精细控制其员工或应用对资源的访问和操作权限。
- 企业A希望如果双方合同终止，企业A随时可以撤销企业B的授权。



## 对云上应用进行动态身份管理与授权

企业A购买了ECS实例，并计划在ECS中部署企业的应用程序。这些应用程序需要使用访问密钥（AccessKey）访问其它云服务API。

有两种做法：

- 将访问密钥直接嵌入在代码里。
- 将访问密钥保存在应用程序的配置文件中。

这样会带来两个问题：

- 保密性问题：如果访问密钥以明文形式存在于ECS实例中，可能会随着快照、镜像及镜像创建出来的实例泄露。
- 难运维问题：由于访问密钥存在于实例中，如果要更换访问密钥（例如：周期性轮转或切换用户身份），那么需要对每个实例和镜像进行更新并重新部署，这会增加对实例和镜像管理的复杂性。

## 利用标签对ECS实例进行分组授权

假设您的账号购买了10个ECS实例，其中5个想要授权给developer团队，另外5个授权给operator团队。企业希望每个团队只能查看被授权的ECS实例，未被授权的不允许查看。

应该怎么做？



## 移动应用使用临时安全令牌访问阿里云

企业A开发了一款移动应用（App），并购买了对象存储（OSS）服务。App需要直连OSS上传或下载数据，但是App运行在用户自己的移动设备上，这些设备不受企业A的控制。

企业A有如下要求：

- 直传数据：企业A不希望所有App都通过企业的服务端应用服务器（Application Server）来进行数据中转，而希望能够直连OSS上传或下载数据。
- 安全管控：企业A不希望将访问密钥（AccessKey）保存到移动设备中，因为移动设备是归属于用户控制，属于不可信的运行环境。
- 风险控制：企业A希望将风险控制到最小，每个App直连OSS时都必须拥有最小的访问权限且访问时效需要很短。



## 通过API使用实例RAM角色

可以通过API创建、授权实例RAM角色，并将其授予实例。但是有一些使用限制：

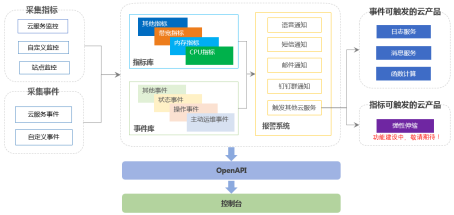
- 只有专有网络（VPC）网络类型的ECS实例才能使用实例RAM角色。
- 一个ECS实例一次只能授予一个实例RAM角色。
- 当您给ECS实例授予了实例RAM角色后，并希望在ECS实例内部部署的应用程序中访问云产品的API时，您需要通过实例元数据获取实例RAM角色的临时授权Token。
  - 检索名为EcsRamRoleDocumentTesting的实例RAM角色的临时授权Token。
  - 例如：curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting
- 如果您是通过RAM用户子账号使用实例RAM角色，您需要通过云账号授权RAM用户使用实例RAM角色。
  - 您授权RAM用户使用实例RAM角色时，您必须授权RAM用户对该实例RAM角色的PassRole权限。其中，PassRole决定该RAM用户能否直接执行角色策略赋予的权限。



## 目录

## 什么是云监控

- 云监控（CloudMonitor） 是一项针对阿里云资源和互联网应用进行监控的服务。云监控服务可用于收集获取阿里云资源的监控指标，探测互联网服务可用性，以及针对指标设置警报。






## 应用场景

- 云服务监控
- 系统监控
- 及时处理异常场景
- 及时扩容场景
- 站点监控
- 自定义监控



## 主机监控

- 云监控主机监控服务通过在服务器上安装插件，为您提供服务器的系统监控服务。
- 无论您的服务器是阿里云服务器ECS，还是其他云厂商的服务器或物理机，都可以使用主机监控服务。
- 主机监控服务通过安装在主机中的插件采集丰富的操作系统层面监控指标。您可以使用主机监控服务进行服务器资源使用情况查询以及排查故障时的监控数据查询。
- 主机监控为您提供CPU、内存、磁盘、网络等三十余种监控项，满足服务器的基本监控运维需求。
- 主机监控对以上所有监控项提供报警功能，您可以选择在实例、应用分组、全部资源三个角度设置报警规则。



## 站点监控

- 站点监控是一款定位于互联网网络探测的监控产品，主要用于通过遍布全国的互联网终端节点，发送模拟真实用户访问的探测请求，监控全国各省市运营商网络终端用户到您服务站点的访问情况。
- 支持多种探测协议
  - HTTP/HTTPS、PING、TCP、UDP、DNS、POP3、SMTP、FTP

## 报警服务

- 您可以对主机监控中的监控项、站点监控中的探测点、云服务监控中的实例和自定义监控中的监控项设置报警规则。您可以在全部资源、应用分组和单实例维度设置报警规则。
- 报警服务支持电话、短信、旺旺、邮件、钉钉机器人等多种方式。旺旺仅支持PC端报警消息推送。如果您安装了阿里云APP，也可以通过阿里云APP接收报警通知。



## ECS状态变化事件的自动化运维

- 阿里云ECS在已有的系统事件的基础上，通过云监控新发布了状态变化类事件和抢占型实例的中断通知事件。当ECS实例的状态发生变化时，会触发一条ECS实例状态变化事件。这种变化包括您在控制台、OpenAPI和SDK操作导致的变化，也包括弹性伸缩或欠费等原因而自动触发的变化，还包括因系统异常而触发的变化。

1. 创建消息队列
2. 创建事件报警规则
   - 注：云监控会将云服务器ECS所有的状态变化事件投递到消息队列中，再通过编写代码从消息队列获取消息并进行消息处理。
3. 添加Listener。当收到Stopped事件时，对该ECS执行命令**start**。



## 目录





## 是什么 DDos 攻击

- 分布式拒绝服务（Distributed Denial of Service，简称DDoS）将多台计算机联合起来作为攻击平台，通过远程连接利用恶意程序，对一个或多个目标发起DDoS攻击，消耗目标服务器性能或网络带宽，从而造成服务器无法正常地提供服务。
- 出现以下情况时，您的业务可能已遭受DDoS攻击：
  - 网络和设备正常的情况下，服务器突然出现连接断开、访问卡顿、用户掉线等情况。
  - 服务器CPU或内存占用率出现明显增长。
  - 网络出方向或入方向流量出现明显增长。
  - 您的业务网站或应用程序突然出现大量的未知访问。
  - 登录服务器失败或者登录过慢。

## DDoS原生防护

- DDoS原生防护是一款针对阿里云ECS、SLB、Web应用防火墙、EIP等产品直接提升DDoS防御能力的安全产品。相比于DDoS高防，DDoS原生防护可以直接把防御能力加载到云产品上，不需要更换IP，也没有四层端口、七层域名数等限制。DDoS原生防护部署简易，购买后只需要绑定需要防护的云产品的IP地址即可使用，几分钟内生效。
- DDoS原生防护（防护包）提供基础版和企业版套餐。
  - 基础版：默认为阿里云资源公网IP免费开启，无需购买。提供不超过5 Gbps的DDoS基础防护能力。
  - 企业版：购买后开启，提供20 Gbps的DDoS基础防护能力和共享全力防护能力。



## DDoS高防

- DDoS高防（Anti-DDoS）是阿里云提供的DDoS攻击代理防护服务。当您的互联网服务器遭受大流量的DDos攻击时，DDoS高防可以保护其应用服务持续可用。
- DDoS高防支持通过DNS解析和IP直接指向两种引流方式，实现网站域名和业务端口的接入防护。根据您在DDoS高防中为业务配置的转发规则，DDoS高防将业务的DNS域名解析或业务IP指向DDoS高防实例IP或CNAME地址进行引流。
- 来自公网的访问流量都将优先经过高防机房，恶意攻击流量将在高防流量清洗中心进行清洗过滤，正常的访问流量通过端口协议转发的方式返回给源站服务器，从而保障源站服务器的稳定访问。



## 阿里云DDoS防护解决方案

- DDoS基础防护
  - 购买阿里云产品即可获得的基础DDoS防护能力，仅可满足较低的安全需求，对于有最大安全防护需求的用户建议额外选择其他安全方案。
- DDoS原生防护（防护包）
  - 在线视频、直播答题等对业务流畅要求比较高（低延迟）的DDoS攻击防护。
  - 业务中存在大量端口、域名、IP的DDoS攻击防护。
- DDoS高防
  - 金融、电商、门户类网站的DDoS攻击防护。
  - 政府互联网出口、门户与开放平台的DDoS攻击防护。
  - 重大线上直播、活动推广促销场景的DDoS攻击防护。
  - 业务遭竞争对手恶意攻击、勒索场景的安全防护。
  - 移动业务（APP）遭恶意注册、刷单、刷流量场景的安全防护。



## 目录

## 什么是游戏盾

- 游戏盾是阿里云针对游戏行业面对的DDoS、CC攻击推出的针对性的网络安全解决方案，相比高防IP，除了能针对大型DDoS攻击（T级别）进行有效防御外，还具备彻底解决游戏行业特有的TCP协议的CC攻击问题能力，防护成本更低，效果更好！
- 与传统单点防御DDoS防御方案相比，游戏盾用数据和算法来实现智能调度，将“正常玩家”流量和“黑客攻击”流量快速分流至不同的节点，最大限度缓解大流量攻击；通过端到端加密，让模拟用户行为的小流量攻击也无法到达客户端。
- 同时，在传统防御中，黑客很容易锁定攻击目标IP，在攻击过程中受损非常小。而游戏盾的智能调度和识别，可让用户“隐形”，让黑客“显形” —— 每一次攻击都会让黑客受损一次，攻击设备和肉鸡不再重复可用。颠覆以往DDoS攻防资源不对等的状况。



## 核心原理

- 游戏盾的核心技术是弹性安全网络技术，简单地说，弹性安全网络将DDoS防御前置到网络边缘处。
- 游戏盾提供了一个只能由SDK接入的并且免疫DDoS/CC攻击的弹性安全网络。SDK通过服务本地化代理接入游戏盾的弹性安全网络，实现玩家（Token）由具体的游戏盾网络接入点（GroupName）访问防护目标（Dip）端口（Dport）的逻辑。



## 产品优势

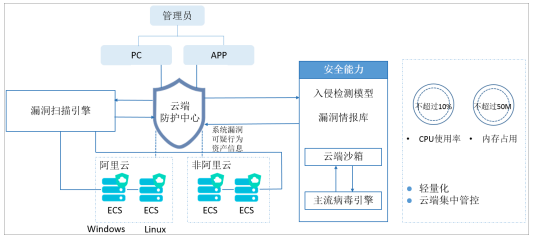
| 对比项 | 游戏盾 | 传统DDoS流量清洗机房 |
| --- | --- | --- |
| 游戏行业超大DDoS攻击 | 摆脱DDoS攻防军备竞赛，专业防御游戏行业超大DDoS攻击分布式抗D节点优质BGP接入，针对游戏提供高可用的网络环境 | 仅能靠一个本地机房，带宽无法扩展，无法防御更大的DDoS攻击 |
| 指纹加密/链路加密 | 支持TCP/HTTP/HTTPS适合手游、端游等各类业务场景支持云内/云外客户集成游戏SDK，数据报文全链路加密，防黑客破解端到端的加密，游戏安全接入支持防护针对模拟游戏协议的攻击支持解码游戏私有协议防护算法实时调整 | 传统清洗机房仅靠硬件设备来识别，无法解码游戏私有协议 |
| 支持解码游戏私有协议 | DPI深度报文检测技术，通过机器学习自动建立协议特征，仅放行满足协议特征请求 | 传统清洗机房仅靠硬件设备来识别，无法解码游戏私有协议 |
| 定制游戏防护算法 | 防御游戏空连接、慢连接、恶意踢人攻击全球僵尸网络库、神盾局攻击溯源 | 传统机房大多采购防火墙设备或者硬件设备，防御算法更新慢，自身没有调整防御算法的能力 |



## 目录

## 什么是安骑士？

- 阿里云安骑士是一款经受百万级主机稳定性考验的主机安全加固产品，支持自动化实时入侵威胁检测、病毒查杀、漏洞智能修复、基线一键检查、网页防篡改等功能，是构建主机安全防线的统一管理平台。






## 基本功能

- 安全预防
  - 漏洞管理
  - 基线检测
- 入侵检测
  - 异常登录
  - 网站后门查杀
  - 主机异常
  - 敏感数据篡改
  - 异常账号
- 精准防御
  - 病毒自动查杀
- 资产指纹
  - 主机管理
  - 资产清点：端口、账号、进程、软件
- 日志检索
  - 进程相关
  - 网络连接
  - 其他日志
- 网页防篡改
  - 网页防篡改



## 目录





## 什么是堡垒机

- 堡垒机是云盾提供的一个核心系统运维和安全审计管控平台。
- 云盾堡垒机集中了运维身份鉴别、账号管控、系统操作审计等多种功能。基于协议正向代理实现，通过正向代理的方式实现对SSH 、Windows远程桌面、及SFTP等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维审计的目的。

## 功能特性

- **操作审计**
  - 全面记录运维人员的操作行为，作为事件追溯的保障和事故分析的依据。
- **权限控制**
  - 通过账号管控和权限管理，实现人员和资产的权限管理。
- **安全认证**
  - 引入**双因子认证**机制，通过短信认证、动态令牌等技术，降低账号密码泄露风险，防止运维人员账号泄露被反复利用。
- **高效运维**
  - 从架构、工具、ECS接入、RDS接入等多方面提升运维效率。



## 使用流程

| 任务 | 描述 |
| --- | --- |
| 步骤1：同步阿里云ECS资产 | 在使用堡垒机进行主机运维前，管理员需要在堡垒机实例中添加要管理的主机资产。在该任务中，管理员将在堡垒机实例中同步导入当前阿里云账号下的ECS资产并新建主机账户。 |
| 步骤2：导入阿里云RAM用户 | 在使用堡垒机进行主机运维前，管理员需要在堡垒机实例中创建堡垒机用户。在该任务中，管理员在堡垒机实例中导入阿里云RAM用户（即阿里云子账号）作为堡垒机用户。 |
| 步骤3：创建运维规则 | 在使用堡垒机进行主机运维前，管理员需要创建运维规则，授权指定用户运维指定资产。在该任务中，管理员创建运维规则，授权指定用户运维指定主机和主机账户。 |
| 步骤4：主机运维 | 当管理员在堡垒机实例中完成主机资产、堡垒机用户、运维规则部署后，堡垒机用户可以通过CS运维方式访问已授权主机，进行运维操作。在该任务中，运维人员将了解CS运维的具体操作方法。 |
| 步骤5：审计运维会话 | 当运维人员通过SSH、RDP、SFTP协议方式登录云盾堡垒机并对已授权服务器进行运维操作时，管理员可以在云盾堡垒机Web管理页面查看用户会话的详细信息。在该任务中，管理员在堡垒机实例中进行审计查询和阻断高危会话操作。 |



# 谢 谢

xujiajie@hotmail.com