# 阿里云
# 大数据轻量专有云

## 安全白皮书

产品版本：V1.1.0

文档版本：20180327

# 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 |
| --- | --- | --- |
|  | 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。 |  **禁止**：<br>重置操作将丢失用户配置数据。 |
|  | 该类警示信息可能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**：<br>重启操作将导致业务中断，恢复业务所需时间约10分钟。 |
|  | 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**：<br>您也可以通过按**Ctrl** + **A**选中全部文件。 |
| > | 多级菜单递进。 | **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。 | 单击 **确定**。 |
| courier字体 | 命令。 | 执行 cd /d C:/windows 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。 | swich *{stand \| slave}* |

# 目录

# 1 安全白皮书介绍

数据安全和用户隐私是阿里云大数据轻量专有云最重要的原则，阿里云致力于打造公共、开放、安全的专有云云计算服务平台。通过技术创新，不断提升计算能力与规模效益，将云计算变成真正意义上的基础设施。

阿里云大数据轻量专有云竭诚为用户提供稳定、可靠、安全、合规的云计算基础服务，帮助保护用户的系统及数据的可用性、机密性和完整性。

本白皮书介绍了阿里云大数据轻量专有云云安全体系，主要包括下列内容：

- 安全责任共担
- 安全合规和隐私
- 专有云平台架构安全
- 专有云各云产品提供的安全功能

同时，本白皮书提供了安全使用阿里云大数据产品的最佳实践来帮助您更好地使用阿里云大数据轻量专有云平台以及理解安全控制整体环境。

# 2 安全责任共担

基于大数据轻量专有云平台的用户应用，其安全责任由双方共同承担：阿里云确保专有云平台本身架构的安全性，用户负责专有云平台运营以及基于专有云平台构建的应用系统的安全。

**阿里云**

阿里云负责专有云飞天分布式云操作系统及之上的各种云服务产品本身的安全，从而为用户提供高可用和高安全的专有云平台。

**用户**

用户负责以安全的方式配置和使用云平台等云产品，并基于这些云产品以安全可控的方式构建自己的应用。

## 2.1 阿里云安全责任

阿里云负责分布式云操作系统及云服务产品本身的安全，并为用户提供保护专有云平台、云端应用及数据的技术手段。

- 保障专有云云平台架构安全
- 提供及时发现专有云云平台的安全漏洞并修复（修复漏洞过程不影响业务可用性）的安全服务及技术

## 2.2 用户安全责任

用户基于阿里云提供的大数据轻量专有云平台构建自己的云端应用系统，综合运用大数据轻量专有云产品的安全功能及服务保护自己的专有云环境。

用户应妥善管理专有云环境中的账户，为每个运维管理人员授予完成运维管理工作需要的最小权限，通过群组授权实现职责分离。同时，通过操作审计服务记录管理控制台操作及OpenAPI调用日志。

对于专有云提供的其他服务，例如大数据计算服务（MaxCompute），用户需要管理这些服务的账户及授权，并使用这些服务提供的安全功能。

# 3 阿里云专有云安全架构

阿里云为专有云设计了多个层面的纵深防御安全体系，包括基础设施安全、云操作系统安全、网络服务安全、应用安全、大数据计算安全、数据安全、云产品代码安全、安全审计等云平台层面的安全架构保障。

## 3.1 云平台安全架构

### 3.1.1 基础设施安全

#### 3.1.1.1 物理安全

对于委托运营商建设的专有云机房物理安全，主要包括但不限于双路供电、访问控制、视频监控、火灾检测、热备机房等安全措施。

**双路供电**

为保障业务7*24小时持续运行，专有云的数据中心机房的每一个负载均由两个电源供电，两个电源之间可以进行切换。若电源发生故障，在其中一个电源失电的情况下可以投切到另一个电源供电。

**访问控制**

对于专有云数据中心的物理设备和机房的访问要具备访问控制，包括机房的进出访问控制。例如，对于进出机房或者携带设备进出机房，物理设备的配置、启动、关机、故障恢复等，均需具备相应的访问控制策略。

**视频监控**

专有云数据中心机房应装设视频监控系统或者有专人24小时值守，对通道等重要部位进行监视。例如，对出入通道进行视频监控，同时报警设备应该能与视频监控系统或者出入口控制设备联动，实现对于监控点的有效监视。

**火灾检测**

专有云数据中心机房应配备火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等。火灾自动报警系统能够对于火灾发生的部位以声、光或点的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。

# 3.1.1.2 网络设备安全

**账号安全**

针对网络设备的账号口令策略、密码配置文件的存储加密进行安全加固。

- 为网络设备建立只读账号，只允许查看配置，实现读、改配置的账号分离。
- 通过集中管控策略，实现账号的统一管理。
- 采用多因素认证的方式保障网络设备的账号安全。

**服务**

禁用网络设备上的服务，减少网络设备的受攻击面；并且禁用与网络设备不相关的功能。

**日志集中化**

将网络设备产生的日志进行集中化收集和管理。

# 3.1.1.3 基础网络安全

云平台对大数据轻量专有云网络环境中的管理网络（OPS）、业务网络、物理网络进行了三网安全隔离。OPS网络、业务网络、物理网络三张网络之间通过网络访问控制策略实现三网逻辑隔离，彼此之间不能互相访问。同时，采取网络控制措施防止非授权设备私自连接云平台内部网络，并防止云平台物理服务器主动外连。

# 3.1.2 云操作系统安全

# 3.1.2.1 虚拟化安全

虚拟化技术是云计算平台的主要技术支撑，通过计算虚拟化、存储虚拟化、网络虚拟化来保障云计算环境下的多租户隔离。阿里云的虚拟化安全技术主要包括租户隔离、补丁热修复、逃逸检测三大基础安全部分来保障专有云平台虚拟化层的安全。

**租户隔离**

虚拟化管理层在租户隔离中起到至关重要的作用。基于硬件虚拟化技术的虚拟机管理，将多个计算节点的虚拟机在系统层面进行隔离，租户不能访问相互之间未授权的系统资源，从而保障计算节点的基本计算隔离。同时，虚拟化管理层还提供存储隔离和网络隔离。

- **计算隔离**

  专有云平台提供各种基于云的计算服务，包括各种计算实例和服务，同时支持自动伸缩以满足应用程序及各用户的需求。这些计算实例和服务从多个级别提供计算隔离以保护数据，同时保障用

户需求的配置灵活性。计算隔离中关键的隔离边界是管理系统与用户虚拟机之间、以及用户虚拟机之间的隔离，这种隔离由Hypervisor直接提供。在专有云平台使用的虚拟化环境中，将用户实例作为独立的虚拟机运行，并且通过使用物理处理器权限级别强制执行隔离，确保用户虚拟机无法通过未授权的方式访问物理主机和其他用户虚拟机的系统资源。

- **存储隔离**

  作为云计算虚拟化基础设计的一部分，阿里云将基于虚拟机的计算与存储分离。这种分离使得计算和存储可以独立扩展，从而更容易提供多租户服务。在虚拟化层，Hypervisor采用分离设备驱动模型实现I/O虚拟化。虚拟机所有I/O操作都会被Hypervisor截获并处理，保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。用户实例服务器释放后，原有的磁盘空间将会被可靠地清零以保障用户数据安全。

- **网络隔离**

  为了支持ECS虚拟机实例使用网络连接，阿里云将虚拟机连接到专有云的虚拟网络。虚拟网络是建立在物理网络结构之上的逻辑结构，每个逻辑虚拟网络与所有其他虚拟网络隔离。这种隔离有助于确保部署中的网络流量数据不能被其它ECS虚拟机访问。

## 3.1.2.2 基础系统服务安全

**飞天操作系统**

- **分布式文件系统安全**

  分布式文件系统使用三副本技术，将系统中的数据保存三份。如果其中一份副本丢失，系统会自动进行三副本的拷贝操作，始终保持拥有三份副本。同时，根据安全策略，三份副本不会存储在同一个物理存储介质上，保持存储的分离操作。

  所有访问分布式文件系统的操作，必须通过Capability认证，只有携带了允许的Capability才能与系统进行通信，从而解决未经授权访问的操作。

  存储在分布式文件系统中的数据，采用二进制格式化存储的方式，避免直接查看到明文信息，造成信息泄露。

- **远程过程调用模块安全**

  远程过程调用模块在飞天操作系统进行通信时，采用指定的二进制格式进行通信，保证传输过程中的效率以及传输的安全，保证即使数据被中间人劫持也无法还原数据。

- **任务调度模块安全**

  任务调度模块采用沙箱的方式对程序进行隔离。

**基础设施**

针对NTP、DNS服务部署DDoS攻击防护、DNS区域传送、DNS放大攻击防御、NTP放大攻击防御等安全措施，保障NTP和DNS服务器的安全。

## 3.1.2.3 系统管理和调度安全

专有云平台管理系统采用Docker容器化的部署方式。由阿里云安全专家对云平台管理系统进行SDL安全审核，通过代码审核、线上测试、需求分析、威胁建模的方式，保障云平台管理系统的整体安全性。

## 3.1.2.4 云服务器安全

**宿主机的操作系统**

专有云平台云服务器宿主机的操作系统采用阿里云根据云特点定制的、重新增减并进行编译的加固操作系统。同时，对操作系统的安全策略和安全访问上进行了大量的深度加固定制。

**实例的操作系统（Guest OS）**

用户拥有对云服务器ECS实例操作系统的完全控制权，阿里云没有任何权限访问用户的实例及实例上的操作系统。同时，阿里云强烈建议用户采用安全的方式对ECS实例上的操作系统进行访问和操作。例如，使用SSH公钥和私钥对，并妥善保存私钥（至少要求使用复杂密码，可在创建实例时设置）；采用更安全的SSHv2方式远程登录；采用 sudo指令的方式实现临时提权等。

**镜像**

阿里云基础镜像集成了所有已知的高危漏洞补丁，最大限度防止ECS实例上线后即处于高风险状态。同时，阿里云使用数据校验算法和单向散列算法确保镜像完整性，防止被恶意篡改。在发现新的高危安全漏洞后，用户应迅速更新基础镜像。同时，用户可以完全自主地对ECS实例上的操作系统进行升级或漏洞修复。

强烈建议在不影响用户业务部署的情况下，使用阿里云的基础镜像作为上云的第一步。

## 3.1.3 网络服务安全

## 3.1.3.1 负载均衡

负载均衡是对多台云服务器进行流量分发的负载均衡服务。负载均衡可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

## 3.1.4 大数据计算安全

### 3.1.4.1 授权管理

项目空间（Project）是专有云平台大数据计算服务实现多租户体系的基础，是用户管理数据和计算的基本单位。当用户申请创建一个项目空间之后，该用户就是这个空间的所有者（Owner）。也就是说，这个项目空间内的所有对象（如表、实例、资源、UDF等）都属于该用户。除了Owner之外，任何人都无权访问此项目空间内的对象，除非获得Owner的授权许可。

当项目空间的Owner决定对另一个用户授权时，Owner需要先将该用户添加到自己的项目空间中，只有添加到项目空间中的用户才能够被授权。

角色（Role）是一组访问权限的集合。当需要对一组用户赋予相同的权限时，可以使用角色来授权。基于角色的授权可以大大简化授权流程，降低授权管理成本。当需要对用户授权时，应当优先考虑是否应该使用角色来完成。

大数据计算服务支持对项目空间里的用户或角色，针对Project、Table、Function、Resource Instance四种对象，授予不同权限。

### 3.1.4.2 跨项目空间的资源分享

假设用户是项目空间的Owner或管理员（admin角色），其它用户需要申请访问用户的项目空间资源。如果申请人属于该用户的项目团队，建议用户使用项目空间的用户与授权管理功能；如果申请人并不属于该用户的项目团队，可以使用基于Package的跨项目空间的资源分享功能。

Package是一种跨项目空间共享数据及资源的机制，主要用于解决跨项目空间的用户授权问题。使用Package后，A项目空间管理员可以对B项目空间需要使用的对象进行打包授权（也就是创建一个Package），然后许可B项目空间安装这个Package。在B项目空间管理员安装Package后，就可以自行管理Package是否需要进一步授权给自己Project下的用户。

### 3.1.4.3 数据保护机制

如果项目空间中的数据非常敏感，绝对不允许流出到其他项目空间时，可以使用项目空间保护机制（设置ProjectProtection）。明确要求该项目空间中的数据只能流入，不能流出。

## 3.1.5 数据安全

### 3.1.5.1 数据安全体系

阿里云数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期（数据生产、数据存储、数据使用、数据传输、数据传播、数据销毁）各环节进行数据安全管理管控，实现数据安全目标。

专有云平台在数据安全生命周期的每一个阶段，都有相应的安全管理制度以及安全技术保障。

### 3.1.5.2 数据所有权

2015年7月，阿里云发起中国云计算服务商首个“数据保护倡议”，这份公开倡议书明确：运行在云计算平台上的开发者、公司、政府、社会机构的数据，所有权绝对属于用户；云计算平台不得将这些数据移作它用。平台方有责任和义务，帮助用户保障其数据的私密性、完整性和可用性。

### 3.1.5.3 多副本冗余存储

专有云使用分布式存储技术，将文件分割成许多数据片段分散存储在不同的设备上，并且将每个数据片段存储多个副本。分布式存储不但提高了数据的可靠性，也提高了数据的安全性。

### 3.1.5.4 镜像管理

专有云平台的云服务器提供快照与自定义镜像功能，快照可以保留某个时间点上的系统数据状态，用于数据备份，便于用户快速实现灾难恢复。用户可以使用快照创建自定义镜像，将快照的操作系统、数据环境信息完整地包含在镜像中。快照采用增量方式，两个快照之间只有数据变化的部分才会被拷贝。

### 3.1.5.5 残留数据清除

对于曾经存储过用户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖。

### 3.1.5.6 运维数据安全

运维人员未经用户许可，不得以任意方式访问用户未经公开的数据内容。

专有云平台遵循生产数据不出生产集群的原则，从技术上控制了生产数据流出生产集群的通道，防止运维人员从生产系统拷贝数据。

### 3.1.6 云产品代码安全

在云产品安全生命周期（SPLC）中，阿里云安全专家在各个开发节点中都进行严格审核并评估代码的安全性，保障阿里云提供给用户的产品的代码安全。

云产品安全生命周期（Secure Product Lifecycle，简称SPLC）是阿里云为云上产品量身定制的云产品安全生命周期，目标是将安全融入到整个产品开发生命周期中。SPLC在产品架构审核、开发、测试审核、应急响应的各个环节层层把关，每个节点都有完整的安全审核机制确保产品的安全性能够满足严苛的云上要求，从而有效地提高云产品的安全能力并降低安全风险。整个云产品安全生命周期可以分为六大阶段：产品立项、安全架构审核、安全开发、安全测试审核、应用发布、应急响应。

- **在产品立项阶段**，安全架构师和产品方一同根据业务内容、业务流程、技术框架建立功能需求文档（FRD）、绘制详细架构图，并在阿里云产品上云的所有安全基线要求中确认属于产品范围的《安全基线要求》。同时，本阶段会安排针对性的安全培训课程与考试给产品方人员，从而避免在后续产品开发中出现明显的安全风险。
- **在安全架构审核阶段**，安全架构师在上一阶段产出的FRD和架构图的基础上对产品进行针对性的安全架构评估并做出产品的威胁建模。在威胁建模的过程中，安全架构师会对产品中的每一个需要保护的资产、资产的安全需求、可能的被攻击场景做出详细的模型，并提出相对应的安全解决方案。安全架构师会综合《安全基线要求》和威胁建模中的安全解决方案，一并与产品方确认对于该产品的所有《安全要求》。
- **在安全开发阶段**，产品方会根据《安全要求》在产品开发中遵守安全编码规范，并实现产品的相关安全功能和要求。为了保证云产品快速持续的开发、发布与部署效率，产品方会在本阶段进行自评确认《安全要求》都已经实现，并提供相对应的测试信息（如代码实现地址，自测结果报告等）给负责测试的安全工程师，为下一阶段的安全测试审核做好准备。
- **在安全测试审核阶段**，安全工程师会根据产品的《安全要求》对其进行架构设计、服务器环境等全方位的安全复核，并对产品的代码进行代码审核和渗透测试。在此阶段发现的安全问题会要求产品方进行安全修复和加固。
- **在应用发布阶段**，只有经过安全复核并且得到安全审批许可后，产品才能通过标准发布系统部署到生产环境，以防止产品携带安全漏洞在生产环境运行。
- **在应急响应阶段**，安全应急团队会不断监控云平台可能的安全问题，并通过外部渠道（如ASRC等）或者内部渠道（如内部扫描器、安全自测等）得知安全漏洞。在发现漏洞后应急团队会对安全漏洞进行快速评级，确定安全漏洞的紧急度和修复排期，从而合理分配资源，做到快速并合理的修复安全漏洞，保障阿里云用户、自身的安全。

## 3.2 云用户（租户）侧安全

专有云在用户侧安全提供了多个层面的安全保障，其中包括了账户安全、主机安全、应用安全、数据安全、云盾、安全运营服务、以及安全最佳实践。

### 3.2.1 账户安全

专有云平台提供多种安全机制来帮助用户保护账户安全，防止未授权的用户操作。这些安全机制包括云账户登录、创建子用户、集中管理子用户权限、数据传输加密、子用户操作审计等，用户可以使用这些机制来保护云账户的安全。

### 3.2.2 主机安全

**入侵检测**

专有云平台用户可以通过在主机上配置云盾服务器安全系统（安骑士），实现与云端安全中心的联动，获取入侵检测的安全能力。主机的入侵检测包括异地登录提醒、识别暴力破解攻击、网站后门查杀、主机异常检测等功能。

**漏洞管理**

专有云用户可以通过在主机上配置服务器安全系统（安骑士），实现与云端安全中心的联动，获取漏洞管理的安全能力。主机的漏洞管理综合了多套扫描引擎（网络端、本地端、PoC验证），全面批量检测出系统存在的所有漏洞，并提供一键修复、生成修复命令、一键批量验证功能，实现漏洞管理的闭环。

**镜像加固**

镜像是云服务器 ECS 虚拟机实例运行环境的模板，一般包括操作系统和预装的软件。ECS租户可以使用镜像创建新的ECS实例或更换ECS实例的系统盘。阿里云基础镜像（支持Linux和Windows的多个发行版本）安全主要包括镜像基础安全配置、镜像漏洞修复、默认镜像主机安全软件三个部分。同时，阿里云保持对基础镜像操作系统漏洞以及三方软件漏洞的实时监测，确保所有阿里云提供的基础镜像的高危漏洞在第一时间得到修复。基础镜像默认采用主机最佳安全实践配置，并且所有阿里云基础镜像会默认添加阿里云主机安全软件以保障租户在实例启动时第一时间得到安全保障。

## 3.2.3 应用安全

**Web应用防护**

通过Web应用防火墙，防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站应用的安全与可用性。

**代码安全**

在云产品安全生命周期（SPLC）中，阿里云的安全专家在各个开发节点中都会严格审核和评估代码的安全性，从而保障阿里云提供给用户的产品的代码安全质量。同时，阿里云强烈建议企业用户对其上线的应用进行黑白盒代码安全检测，务求上线后的应用不会存在安全漏洞，增加用户本身的业务的安全强壮性。

## 3.2.4 数据安全

对于用户云平台上的数据安全进行保护，包括数据脱敏、数据发现、数据水印等：

- **数据发现**是数据安全的基础，通过数据发现来发现敏感的数据，并且根据数据类型进行自定义化的数据安全控制；数据发现主要包括身份证、手机号、银行卡号、家庭地址等敏感信息。
- **数据脱敏**主要解决敏感数据的脱敏操作，把原始数据转化成可以特定格式但是没有特殊含义的数据。
- **数据水印**是将数据库的数据通过增加伪行和伪列的形式插入到原始数据中，一旦发生大规模窃取的情况下，可以进行溯源操作。伪行和伪列的数据都是模拟的真实数据，黑客无法通过肉眼来进行数据的辨别以及伪行、伪列的数据删除以及数据水印的清除操作。

# 4 专有云云产品安全

## 4.1 运维权限管理（OAM）

运维权限管理系统（Operation Administrator Manager，简称OAM）是阿里云专有云运维系统统一的权限管理平台。OAM采用一种简化的基于角色的访问控制（RBAC）模型，管理者可以通过OAM为运维人员授予角色，运维人员依据各自的角色，对各运维系统拥有相应的操作权限。

## 4.2 天基权限管理（数据中心管理）

天基是一套自动化的数据中心管理系统，管理专有云数据中心的硬件生命周期与各类静态资源，包括程序、配置、操作系统镜像、数据等。

天基为飞天系统及专有云各种产品的应用及服务提供了一套通用的版本管理、部署以及热升级方案，使得基于天基的服务在大规模分布式的环境下达到自动化运维的效果，极大地提高运维效率，并提高系统可用性。

**权限管理**

天基的权限管理也采用OAM系统。天基用户权限包括天基Admin权限、Project权限和Service权限：

- **Admin权限**：Admin用户可以对整个天基平台的页面进行操作。
- **Project权限**：
  - 普通用户需要由管理员开通Project权限，才能查看天基平台中**运维** > **Project**中的Project信息。
  - 普通用户需要由管理员开通Project权限，才能查看天基平台中**运维** > **集群管理**中的集群信息并执行该节点下的相关操作。
- **Service权限**：普通用户需要由管理员开通Service权限，才能查看天基平台中**运维** > **Service** > **运维**中的服务信息并执行该节点下的相关操作。

## 4.3 访问控制RAM

云租户可以使用RAM建立主子账号体系。

访问控制管理（Resource Access Management，简称RAM）是专有云平台为用户提供的用户身份管理与访问控制服务。通过RAM，可以创建、管理用户账号（比如员工、系统或应用程序），并可

以分配这些用户账号对其名下资源具有的操作权限。当存在多用户协同操作资源时，使用RAM可以避免与其他用户共享云账号密码或访问密钥，按需为用户分配最小权限，从而降低信息安全风险。

## 4.4 MaxCompute

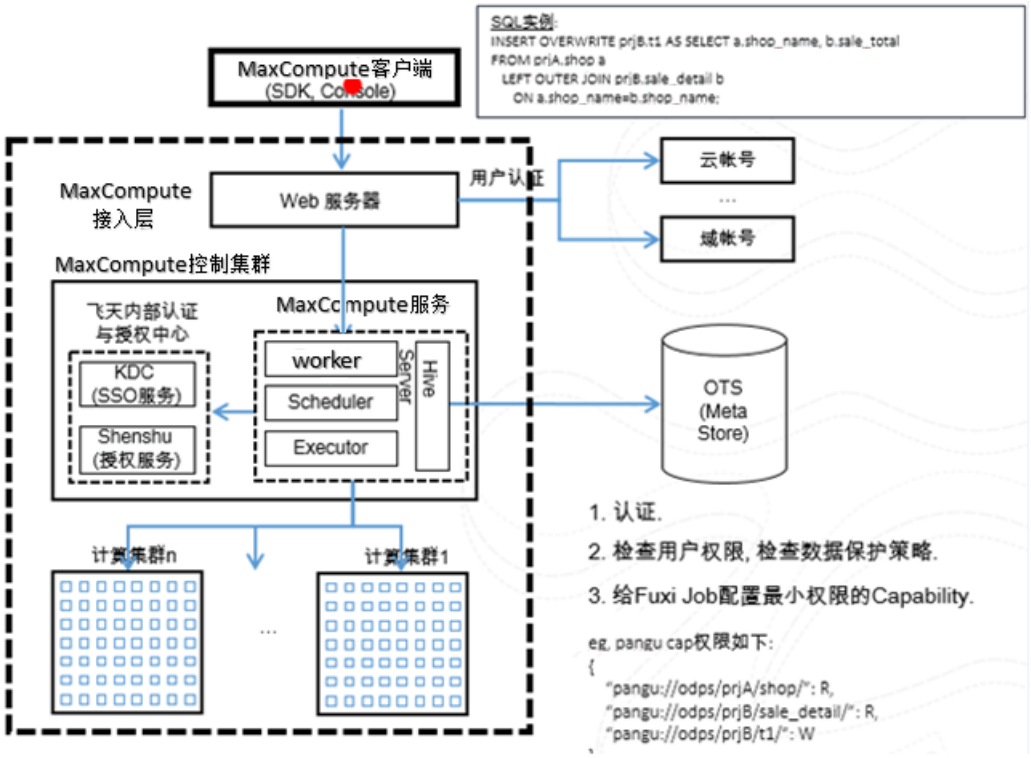
阿里云大数据计算服务（MaxCompute）是一种快速、完全托管的GB/TB/PB级数据仓库解决方案。MaxCompute为用户提供了完善的数据导入方案以及多种经典的分布式计算模型，能够更快速的解决海量数据计算问题，有效降低企业成本，并保障数据安全。

阿里云大数据计算服务（MaxCompute）的安全体系具有如下特点：

- 支持多租户的使用场景，同时满足多用户协同、数据共享、数据保密和安全的需要。
- 用户访问需要认证，用户操作需要鉴权，所有操作记录审计日志。
- 支持ACL授权、policy授权、角色授权、跨项目空间授权等多种权限管理方法，满足多种场景的需求。
- 同时提供DAC和MAC的安全管理方案，满足对于部分敏感数据的管理需求，可以提供精确到列级别的数据管理。
- 对于安全等级较高的数据，提供项目保护模式，防止数据泄露。
- 所有计算在受限的沙箱中运行，多层次的应用沙箱、系统沙箱配合请求鉴权管理机制，保证数据的安全。

阿里云大数据计算服务（MaxCompute）的安全架构如下所示：

**图 4-1: 安全架构**




## 4.4.1 身份认证

MaxCompute支持两种账号体系：专有云云账号体系和RAM账号体系。

**说明**：
在默认情况下，MaxCompute项目只能够识别专有云云账号系统。

## 4.4.2 授权管理

项目空间（Project）是MaxCompute实现多租户体系的基础，是用户管理数据和计算的基本单位。当用户申请创建一个项目空间之后，该用户就是这个空间的所有者（Owner）。也就是说，这个项目空间内的所有对象（例如，表、实例、资源、UDF等）都属于该用户。除了Owner之外，任何人都无权访问此项目空间内的对象，除非有Owner的授权许可。

当项目空间的Owner决定对另一个用户授权时，Owner需要先将该用户添加到自己的项目空间中来。只有添加到项目空间中的用户才能够被授权。

角色（Role）是一组访问权限的集合。当需要对一组用户赋予相同的权限时，可以使用角色来授权。基于角色的授权可以大大简化授权流程，降低授权管理成本。当需要对用户授权时，应当优先考虑是否应该使用角色来完成。

MaxCompute可以对项目空间里的用户或角色，针对Project、Table、Function、Resource Instance四种对象，授予不同权限。

MaxCompute支持两种授权机制来完成对用户或角色的授权：

- **ACL授权**：ACL授权是一种基于对象的授权。通过ACL授权的权限数据（即访问控制列表，Access Control List）被看做是该对象的一种子资源，只有当对象已经存在时，才能进行ACL授权操作。当对象被删除时，通过ACL授权的权限数据会被自动删除。ACL授权支持的授权方法是采用类似SQL92定义的GRANT/REVOKE命令进行授权，通过对应的授权命令来完成对已存在的项目空间对象的授权或撤销授权。
- **Policy授权**：Policy授权是一种基于策略的授权。通过Policy授权的权限数据（即访问策略）被看做是授权主体的一种子资源。只有当主体（用户或角色）存在时，才能进行Policy授权操作。当主体被删除时，通过Policy授权的权限数据会被自动删除。Policy授权使用MaxCompute自定义的一种访问策略语言来进行授权，允许或禁止主体对项目空间对象的访问权限。

两套体系的关系如下表所示：

**表 4-1: ACL授权和Policy授权的关系**

| ACL授权 | Policy授权 |
| --- | --- |
| 每次权限管理操作均是对效果（授权、撤销）、对象（如表、资源等）、主体（用户或是角色）、操作（读、写、删除等）的组合描述，例如“允许用户zinan.tang读取表table1中的数据”。 | |
| N/A | 支持条件授权，目前支持20种条件操作。 |
| N/A | 支持Allow（允许访问）和Deny（拒绝访问）授权。 |
| 授权或撤销授权时，对象和主体必须存在。 | 支持对“不存在”或“不确定”的对象和主体授权，授权时不会验证授权存在性，支持用通配符描述对象或主体。 |
| 删除一个对象时，会自动撤销与该对象关联的授权。 | 删除一个对象时，系统不会自动修改与该对象关联的Policy。 |
| 支持经典的Grant/Revoke语句。 | 通过上传Policy文本描述授权操作。 |

## 4.4.2.1 ACL授权

- 对已存在的对象和用户进行授权管理。
- 用户必须存在于project中。

- 角色（role）是一组权限的集合。
- 系统预设admin角色。
- 对象删除时，所有相关的ACL也被删除。

**示例如下**：

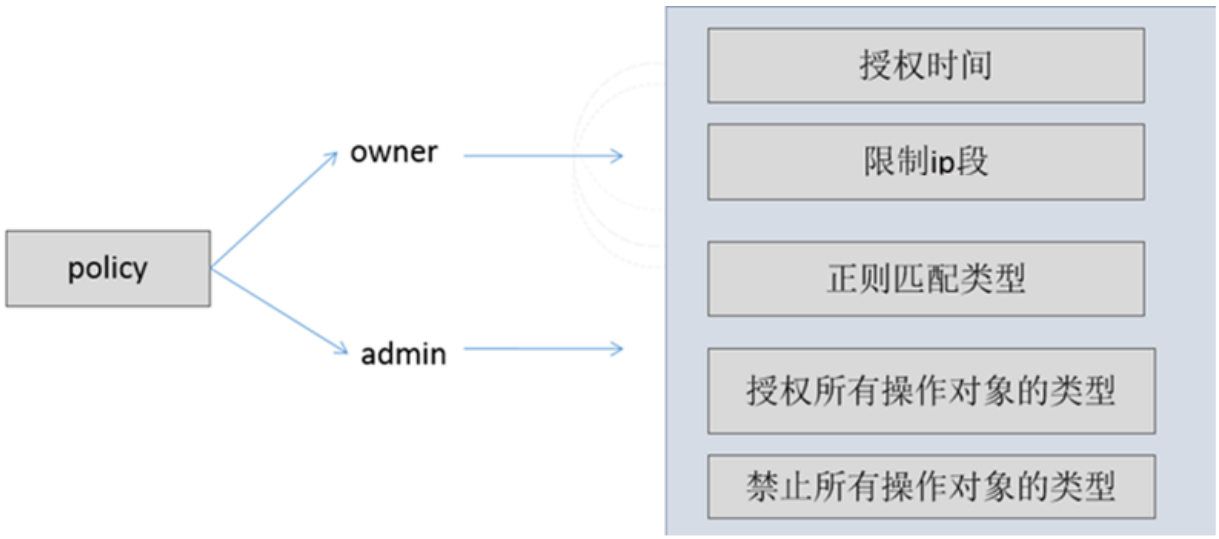
```
grant CreateTable, CreateInstance, List on project myprj to user Alice;
-- 增加用户权限。
grant worker to aliyun$abc@aliyun.com;
-- 加用户进角色。
revoke CreateTable on project myprj from user Alice;
-- 删除用户权限。
```

## 4.4.2.2 Policy授权

Policy授权策略描述了授权的具体内容，它是一种规则，例如：允许所有用户读所有开发环境的表、允许A用户从某个IP访问数据；当管理的数据对象和用户数非常多时，可以极大的减轻管理负担；存在于project和角色上，分为project Policy与role Policy，不会随表的删除而消失。

```
GET POLICY
PUT POLICY <policyFile>;
GET POLICY ON ROLE <roleName>;
PUT POLICY <policyFile> ON ROLE <roleName>;
```

**图 4-2: policy授权**




**示例如下**：

```
{
"Version": "1",
"Statement":
 [{
 "Effect":"Allow",
```

```
 "Principal":"ALIYUN$alice@aliyun.com",  "Action":["odps:CreateTable","odps:CreateInstance","
odps:List"],  "Resource":"acs:odps:*:projects/test_project", "Condition":{    "DateLessThan": { "
acs:CurrentTime":"2013-11-11T23:59:59Z" },
  "IpAddress": { "acs:SourceIp":"10.32.180.0/23" }
 }
 },
{
 "Effect":"Deny",
 "Principal":"ALIYUN$alice@aliyun.com",
 "Action":"odps:Drop", "Resource":"acs:odps:*:projects/test_project/tables/*"
}
] }
```

### 4.4.3 跨项目空间的资源分享

假设用户是项目空间的Owner或管理员（admin角色），有人需要申请访问用户的项目空间资源。如果申请人属于用户的项目团队，此时建议用户使用项目空间的用户与授权管理功能。但是如果申请人并不属于用户的项目团队， 此时用户可以使用基于Package的跨项目空间的资源分享功能。

Package是一种跨项目空间共享数据及资源的机制，主要用于解决跨项目空间的用户授权问题。

使用Package之后，A项目空间管理员可以对B项目空间需要使用的对象进行打包授权（也就是创建一个Package），然后许可B项目空间安装这个Package。在B项目空间管理员安装Package之后，就可以自行管理Package是否需要进一步授权给自己Project下的用户。

### 4.4.4 列级别访问控制

基于标签的安全（LabelSecurity）是项目空间级别的一种强制访问控制策略（Mandatory Access Control, MAC），它的引入可以让项目空间管理员更加灵活地控制用户对列级别敏感数据的访问。

LabelSecurity需要将数据和访问数据的人进行安全等级划分。一般来讲，会将数据的敏感度标记分为如下四类：

- 0级（不保密，Unclassified）。
- 1级（秘密，Confidential）。
- 2级（机密，Sensitive）。
- 3级（高度机密，Highly Sensitive）。

MaxCompute也遵循这一分类方法，ProjectOwner需要定义明确的数据敏感等级和访问许可等级划分标准。默认时所有用户的访问许可等级为0级，数据安全级别默认为0级。

LabelSecurity对敏感数据的粒度可以支持列级别，管理员可以对表的任何列设置敏感度标记（Label），一张表可以由不同敏感等级的数据列构成。而对于view，也支持和表相同的设置，即管理员可

以对view设置label等级。View的等级和它对应的基表的label等级是独立的，在view创建时，默认的等级也是0级。

在对数据和人分别设置安全等级标记之后，LabelSecurity的默认安全策略如下：

- No-ReadUp：不允许用户读取敏感等级高于用户等级的数据，除非显式授权。
- Trusted-User：允许用户写任意等级的数据，新建数据默认为0级（不保密）。

**说明**：

- 在一些传统的强制访问控制系统中，为了防止数据在项目空间内部的任意分发，一般还支持更多复杂的安全策略，例如：不允许用户写敏感等级不高于用户等级的数据（No-WriteDown）。但在MaxCompute平台中，考虑到项目空间管理员对数据敏感等级的管理成本，默认安全策略并不支持No-WriteDown，如果项目空间管理员有类似需求 ， 可以通过修改项目空间安全配置（ SetObjectCreatorHasGrantPermission=false）以达到控制目的。
- 如果是为了控制数据在不同项目空间之间的流动，则可以将项目空间设置为受保护状态（ProjectProtection）。设置之后，只允许用户在项目空间内访问数据，这样可以有效防止数据流出道项目空间之外。

项目空间中的LabelSecurity安全机制默认是关闭的，ProjectOwner需要自行开启。需要注意，LabelSecurity安全机制一旦开启，上述的默认安全策略将被强制执行。此时，当用户访问数据表时，除了必须拥有Select权限外，还必须获得读取敏感数据的相应许可等级。

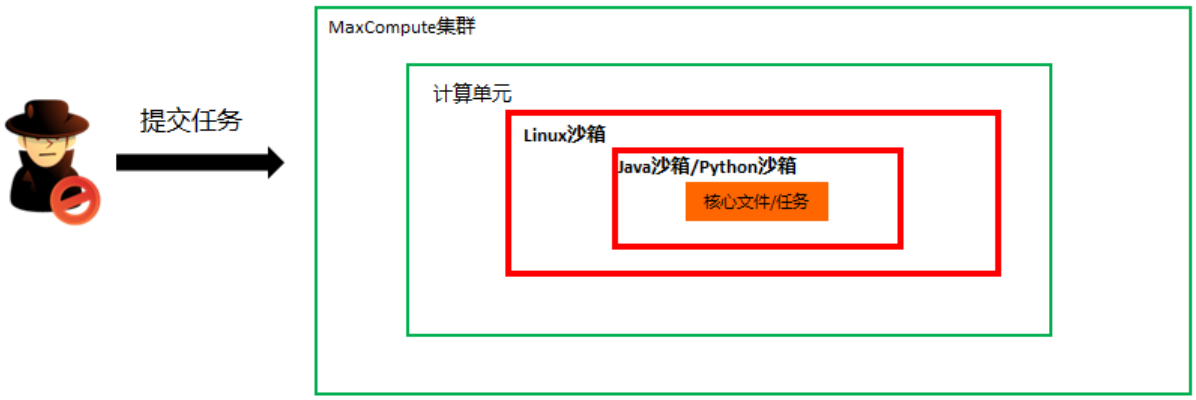
## 4.4.5 数据保护机制（Project Protection）

如果项目空间中的数据非常敏感，绝对不允许流出到其他项目空间中去，那么可以使用项目空间保护机制——设置ProjectProtection，明确要求项目空间中**“数据只能本地循环，允许写入，不能读出”**。

## 4.4.6 沙箱保护

MaxCompute中所有计算是在受限的沙箱中运行的，多层次的应用沙箱，从KVM级到Kernel级。系统沙箱配合鉴权管理机制，用来保证数据的安全，以避免出现内部人员恶意或粗心造成服务器故障。

**图 4-3: 沙箱保护**




## 4.4.7 特殊说明

MaxCompute允许project的所有者定制project的安全属性，满足project对安全的特殊需求，包括：

- 是否支持使用ACL权限（CheckPermissionUsingAcl）。
- 是否支持使用Policy权限（CheckPermissionUsingPolicy）。
- 对象所有者是否自动拥有对象所有权限（ObjectCreatorHasAccessPermission）。
- 是否允许对象所有者对对象授权（ObjectCreatorHasGrantPermission）。
- 是否启用项目空间的数据保护机制（Project Protection）。

> **说明**：
> MaxCompute提供了一个机制，允许用户定义一个exception policy，经过第二次的显示授权，对特定对象和主体打破数据保护机制的限制。

- 添加受信项目（trustedproject）：受信项目是与被保护项目关联的概念。对于一个受保护的项目prj1，如果添加了一个受信项目prj2，则运行在prj2中的instance可以将数据从prj1写到prj2。通过组合定义保护项目和受信项目，可以实现受保护的项目群的概念，即数据在多个project中可以相互流动，但是不能流出。
- 添加IP白名单：限制对该project的访问仅能从某些IP发起。MaxCompute会记录所有REST API调用的日志，并存储在MaxCompute内部的某个project中，供审计使用；可以使用MaxCompute的多种task对审计日志进行处理，生成各类报表。