ALIBABA CLOUD

Alibaba Cloud

访问控制

快速入门

文档版本：20220511

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 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。	`switch {active|stand}`

目录

1.入门概述

当企业接入阿里云，需要通过访问控制（RAM）进行安全管控。本文为您介绍一系列入门操作，方便您快速上手和使用。

前提条件

请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

入门操作

- 为了保护账号安全，请先设置安全策略。请参见设置RAM用户安全策略。
- RAM用户对应某一个操作实体，如运维操作人员或应用程序，您可以创建RAM用户进行日常管理。请参见创建RAM用户。
- 通过创建用户组对职责相同的RAM用户进行分类并授权，从而更好的管理用户。请参见创建用户组。
- 为创建好的RAM用户授权后，RAM用户便可以访问相应的阿里云资源。请参见为RAM用户授权。
- 如果系统策略不能满足您的需求，可以通过创建自定义策略满足细粒度的要求，从而实现更灵活的权限管理。请参见创建自定义权限策略。
- 基础操作配置完成后，RAM用户便可以登录控制台访问相应阿里云资源并进行日常工作。请参见RAM用户登录阿里云控制台。

更多信息

您可以通过RAM学习路径图快速了解RAM，学习相关的基础操作，并利用丰富的API、SDK包和便捷工具进行二次开发。

2.设置RAM用户安全策略

阿里云账号可以通过修改RAM用户安全设置更好地管理RAM用户的权限。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 设置**。
3. 在**安全设置**页签，单击**修改用户安全设置**。
4. 在**修改用户安全设置**面板，设置参数。
   - **保存MFA验证状态7天**：表示RAM用户使用多因素认证登录后，是否允许保存多因素认证的验证状态，其有效期为7天。
   - **自主管理密码**：表示是否允许RAM用户修改密码。
   - **自主管理AccessKey**：表示是否允许RAM用户管理访问密钥。
   - **自主管理MFA设备**：表示是否允许RAM用户绑定或解绑多因素认证设备。
   - **登录时必须使用MFA**：表示是否强制所有RAM用户在通过用户名和密码登录时必须启用多因素认证。如果不强制，则依赖每个RAM用户自身的多因素认证配置。

     > **说明** 如果强制登录时必须使用MFA，则敏感操作二次验证功能会对所有RAM用户启用。即当RAM用户登录控制台进行敏感操作时，会触发风控拦截，要求其进行二次MFA身份验证。更多信息，请参见敏感操作二次验证。

   - **自主管理钉钉**：表示是否允许RAM用户绑定或解绑钉钉账号。
   - **登录会话的过期时间**：表示RAM用户登录的有效期，单位为小时。取值范围1~24小时，默认值为6小时。

     > **说明** 通过切换角色或角色SSO登录控制台时，登录会话有效期也会受到**登录会话的过期时间**的限制，即最终的登录会话有效期将不会超过此参数设置的值。详情请参见使用RAM角色、角色SSO的SAML响应。

   - **登录掩码设置**：登录掩码决定哪些IP地址会受到登录控制台的影响。默认为空，表示不限制登录IP地址。如果设置了登录掩码，使用密码登录或单点登录（SSO登录）时会受到影响，但使用访问密钥发起的API访问不受影响。最多配置25个登录掩码，多个登录掩码之间用半角分号（;）分隔，总长度最大512个字符。
5. 单击**确定**。

   > **说明** 设置成功后，此规则适用于所有RAM用户。

相关文档

- SetSecurityPreference

3.创建RAM用户

RAM用户是RAM中的一种身份，对应某一个操作实体（运维操作人员或应用程序）。通过创建新的RAM用户并授权，RAM用户便可以访问相关资源。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击**创建用户**。
4. 在**创建用户**页面的**用户账号信息**区域，输入**登录名称**和**显示名称**。

   > **说明** 单击**添加用户**，可一次性创建多个RAM用户。

5. 在**访问方式**区域，选择访问方式。
   - **控制台访问**：设置控制台登录密码、重置密码策略和多因素认证策略。

     > **说明** 自定义登录密码时，密码必须满足密码复杂度规则。关于如何设置密码复杂度规则，请参见设置RAM用户密码强度。

   - **OpenAPI调用访问**：自动为RAM用户生成访问密钥（AccessKey），支持通过API或其他开发工具访问阿里云。

     > **说明** 为了保障账号安全，建议仅为RAM用户选择一种登录方式，避免RAM用户离开组织后仍可以通过访问密钥访问阿里云资源。

6. 单击**确定**。

后续步骤

- RAM用户创建成功后，可以使用RAM用户登录控制台。具体操作，请参见RAM用户登录阿里云控制台。
- 可以为RAM用户添加权限策略，使RAM用户具有资源的访问能力。具体操作，请参见为RAM用户授权。
- 可以将RAM用户添加到用户组，对RAM用户进行分类并授权。具体操作，请参见为用户组添加RAM用户。

相关文档

- CreateUser

4.创建用户组

如果阿里云账号下有多个RAM用户，您可以通过创建用户组对职责相同的RAM用户进行分类并授权，从而更好的管理RAM用户及其权限。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户组**。
3. 在**用户组**页面，单击**创建用户组**。
4. 在**创建用户组**页面，输入**用户组名称**、**显示名称**和**备注**。
5. 单击**确定**。

后续步骤

可以为用户组添加一个或多个权限策略，具体操作，请参见为用户组授权。

相关文档

- CreateGroup

5.创建自定义权限策略

如果系统权限策略不能满足您的需求，您可以通过创建自定义权限策略实现精细化权限管理。

创建方式

- 通过可视化编辑模式创建自定义权限策略

  RAM提供所见即所得的可视化编辑界面，您只需选择效果、云服务、操作、资源和条件，就可以生成自定义权限策略。同时，提供的智能校验功能，帮助您提高权限策略的正确性和有效性。该方式操作简单，易于上手。

- 通过脚本编辑模式创建自定义权限策略

  RAM提供JSON脚本编辑界面，您需要按照权限策略语法和结构编写自定义权限策略。该方式使用灵活，适用于对权限策略语法比较熟悉的用户。

- 通过导入模板创建自定义权限策略

  基于长期的业务实践，RAM提供了常见场景的权限策略模板。例如：系统管理员、财务人员、网络管理员等。您只需要导入合适的权限策略模板，然后基于模板进行简单修改，就能一键轻松创建自定义策略。

- 通过导入系统策略创建自定义权限策略

  您可以通过导入一个系统策略模板，然后基于规范化的系统策略模板修改适合实际业务的内容，更加方便快捷地创建自定义权限策略。

通过可视化编辑模式创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击**可视化编辑**页签。
5. 配置权限策略，然后单击**下一步：编辑基本信息**。
   i. 在**效果**区域，选择**允许**或**拒绝**。
   ii. 在**服务**区域，选择云服务。

   > **说明** 支持可视化编辑模式的云服务以控制台界面显示为准。

   iii. 在**操作**区域，选择**全部操作**或**指定操作**。

   系统会根据您上一步选择的云服务，自动筛选出可以配置的操作。如果您选择了**指定操作**，您需要继续选择具体的操作。

   iv. 在**资源**区域，选择**全部资源**或**指定资源**。

   系统会根据您上一步选择的操作，自动筛选出可以配置的资源类型。如果您选择了**指定资源**，您需要继续单击**添加资源**，配置具体的资源ARN。您可以使用**匹配全部**功能，快速选择对应配置项的全部资源。

   > **说明** 为了权限策略的正常生效，对操作关联的必要资源ARN标识了**必要**，强烈建议您配置该资源ARN。

v. （可选）在**条件**区域，单击**添加条件**，配置条件。

条件包括阿里云通用条件和服务级条件，系统会根据您前面配置的云服务和操作，自动筛选出可以配置的条件列表。您只需要选择对应条件键配置具体内容。

vi. 单击**添加语句**，重复上述步骤，配置多条权限策略语句。

6. 输入权限策略**名称**和**备注**。
7. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：
     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：
     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。
8. 单击**确定**。

通过脚本编辑模式创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击**脚本编辑**页签。
5. 输入权限策略内容，然后单击**下一步：编辑基本信息**。

   关于权限策略语法结构的详情，请参见权限策略语法和结构。
6. 输入权限策略**名称**和**备注**。
7. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：
     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：
     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。
8. 单击**确定**。

通过导入模板创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击页面右上角的**导入策略模板**。
5. 在**导入策略模板**对话框，导入权限策略模板。
   i. 选择权限策略模板。

   > **说明** 支持的权限策略模板列表，请以控制台显示为准。

   ii. （可选）部分模板需要根据实际业务配置模板参数。
   iii. 选择新导入的权限策略模板的覆盖规则。
      - 覆盖（默认）：新导入的权限策略模板内容完全覆盖已有的内容。
      - 追加：新导入的权限策略模板内容添加到已有内容的末尾。

   iv. 单击**导入**。
6. 在可视化编辑或脚本编辑模式下，查看和修改已导入的权限策略内容，然后单击**下一步：编辑基本信息**。

   导入的权限策略模板默认以可视化模式展示，方便您查看和修改。 您也可以选择脚本编辑模式进行修改。
7. 输入权限策略**名称**和**备注**。
8. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：
     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：
     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。
9. 单击**确定**。

通过导入系统策略创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击页面右上角的**导入系统策略**。
5. 在**导入系统策略**对话框，导入系统策略。

i. 选择系统策略。

ii. 选择新导入的系统策略的覆盖规则。

- 覆盖：新导入的系统策略内容完全覆盖已有的内容。
- 追加（默认）：新导入的系统策略内容添加到已有内容的末尾。

iii. 单击**导入**。

6. 在可视化编辑或脚本编辑模式下，查看和修改已导入的系统策略内容，然后单击**下一步：编辑基本信息**。

   导入的系统策略默认以可视化模式展示，方便您查看和修改。 您也可以选择脚本编辑模式进行修改。

7. 输入权限策略**名称**和**备注**。
8. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：

     - 删除不必要的条件。
     - 删除不必要的数组。

   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：

     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。

9. 单击**确定**。

相关文档

- CreatePolicy

6.为RAM用户授权

为RAM用户授权后，RAM用户可以访问相应的阿里云资源。本文为您介绍为RAM用户授权的几种方式。

方式一：在用户页面为RAM用户授权

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。
4. 在**添加权限**面板，为RAM用户添加权限。
   i. 选择授权应用范围。
      - **整个云账号**：权限在当前阿里云账号内生效。
      - **指定资源组**：权限在指定的资源组内生效。

        > **说明** 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见支持资源组的云服务。

   ii. 输入被授权主体。

   被授权主体即需要授权的RAM用户，系统会自动填入当前的RAM用户，您也可以添加其他RAM用户。

   iii. 选择权限策略。

   > **说明** 每次最多绑定5条策略，如需绑定更多策略，请分次操作。

5. 单击**确定**。
6. 单击**完成**。

方式二：在授权页面为RAM用户授权

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 授权**。
3. 在**授权**页面，单击**新增授权**。
4. 在**新增授权**页面，为RAM用户添加权限。
   i. 选择授权应用范围。
      - **整个云账号**：权限在当前阿里云账号内生效。
      - **指定资源组**：权限在指定的资源组内生效。

        > **说明** 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见支持资源组的云服务。

   ii. 输入被授权主体。

   被授权主体即需要授权的RAM用户。

iii. 选择权限策略。

> **说明** 每次最多绑定5条策略，如需绑定更多策略，请分次操作。

5. 单击**确定**。
6. 单击**完成**。

相关文档

- AttachPolicyToUser

7.RAM用户登录阿里云控制台

本文为您介绍RAM用户如何登录阿里云控制台，包括登录入口和操作步骤。

登录入口

RAM用户登录阿里云控制台的入口有以下几种：

- 通用登录地址
  - 在阿里云账号登录页面，单击**RAM用户登录**。

  - 直接访问阿里云控制台页面。
- 阿里云账号专属登录地址

  阿里云账号登录RAM控制台，在**概览**页的**账号管理**区域，获取RAM用户登录地址（例如：`https://signin.alibabacloud.com/example.onaliyun.com/login.htm`）。RAM用户使用该地址登录阿里云控制台。
- RAM用户专属登录地址

  在登录地址中使用`username`参数指定RAM用户名，登录过程中免输用户名，直接单击**下一步**输入密码即可。`username`使用UPN（User Principal Name）格式，即RAM控制台用户列表中所见的用户登录名称。例如：一个名为Alice@example.onaliyun.com的RAM用户可以使用`https://signin.alibabacloud.com/login.htm?username=Alice@example.onaliyun.com`登录阿里云控制台。

使用RAM用户名密码登录

以下操作以RAM用户使用通用登录地址登录阿里云控制台为例。

1. RAM用户登录阿里云控制台。
2. 在**RAM用户登录**页面，输入RAM用户名，单击**下一步**。
   - 方式一：使用默认域名登录。RAM用户的登录格式为`<UserName>@<AccountAlias>.onaliyun.com`，例如：username@company-alias.onaliyun.com。

     > **说明** `<UserName>`为RAM用户名称，`<AccountAlias>.onaliyun.com`为默认域名。关于默认域名的更多信息，请参见基本概念和查看和修改默认域名。

   - 方式二：使用账号别名登录。RAM用户的登录格式为`<UserName>@<AccountAlias>`，例如：username@company-alias。

> **说明** `<UserName>` 为RAM用户名称，`<AccountAlias>` 为账号别名。关于账号别名的更多信息，请参见基本概念和查看和修改默认域名。

- 方式三：如果创建了域别名，也可以使用域别名登录。RAM用户的登录格式为 `<UserName>@<DomainAlias>` ，例如：username@example.com。

  > **说明** `<UserName>` 为RAM用户名称，`<DomainAlias>` 为域别名。关于域别名的更多信息，请参见基本概念和创建并验证域别名。

3. 输入RAM用户的登录密码，然后单击**登录**。
4. （可选）如果您开启了多因素认证（MFA），则需要输入虚拟MFA设备生成的验证码，或通过U2F安全密钥认证。

   更多信息，请参见多因素认证（MFA）和为RAM用户启用多因素认证。