ALIBABA CLOUD

阿里云

配置审计

快速入门

文档版本：20201013

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

当您初次使用配置审计时，可以快速了解其操作流程、操作场景和功能之间的关联关系。

快速入门操作流程

通过配置审计快速入门操作流程，来指导您快速授权配置审计，并使用其监控和审计资源。

配置审计快速入门的操作流程说明如下表所示。

序号	操作方法	操作场景
1	服务授权	在您使用配置审计之前，需要先授权配置审计服务。
2	查看资源列表	配置审计服务授权后，会自动扫描您账号下各区域的资源，并生成跨区域聚合的资源列表。您可以查看并管理自己账号下的所有资源。
3	设置审计规则	配置审计通过审计规则来判断资源的合法性，您可以根据业务所需配置资源的审计规则。
4	（可选）设置监控范围	当您开始使用配置审计服务时，默认将支持的所有资源类型纳入监控范围，初始化过程会扫描您账户下的所有资源。如果您有其他监控方案，则请自定义资源类型。
5	（可选）开启等保预检	当您需要持续检测配置是否合规时，请开启等保预检。

功能关联关系

配置审计的核心要素是资源和规则，及相应的配置信息、配置历史信息、变更信息、规则信息、合规评估结果、合规评估历史等信息。为方便您查阅所需功能，提供如下信息关联关系图。

2.服务授权

在您使用配置审计之前，必须先授权。

前提条件

请确保您已完成阿里云账号注册和实名认证。

背景信息

服务授权仅获取您资源配置的只读权限，不会对您其他服务的运行产生任何影响。

操作步骤

1. 登录配置审计控制台。
2. 单击**允许创建**。

> **说明** 配置审计需要2~10分钟时间对您的资源进行扫描，构建资源列表，请耐心等待。

3.查看资源列表

配置审计服务授权后，会自动扫描您账号下各地域的资源，并生成跨地域聚合的资源列表。

前提条件

请确保您已授权配置审计服务，操作方法请参见服务授权。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**查看全局资源**。
3. 在**资源列表**页面，您可以通过资源ID、资源类型、所属地域、合规状态和资源状态快速而准确地过滤出所需资源。
4. 单击目标资源的**资源ID/资源名称**链接。

   在**资源详情**页面，您可以查看如下信息：

   - 在**资源信息**页签，查看基本信息、资源核心配置信息和最新审计结果。
   - 在**关联资源**页签，查看当前资源关联的资源列表。
   - 在**配置时间线**页签，查看资源的历史配置记录。
   - 在**合规时间线**页签，查看资源的历史合规记录。

4.设置审计规则

配置审计通过审计规则来判断资源的合法性，您可以根据业务所需设置资源的审计规则。

背景信息

在设置审计规则之前，您可以先了解规则的定义及运行原理。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**管理合规规则**。
3. 在**管理合规规则**页面，单击**新建规则**。
4. 在**基本设置**页面，选择**规则配置方式**，并配置相关参数，单击**下一步**。

   

   - 当您选择**使用托管规则**时，系统已为您提供多款托管规则，您可以直接选择所需规则，并设置风险等级。
   - 当您选择**通过函数计算**时，需要选择函数ARN，设置规则名称和风险等级。

     请确保您已在函数计算中完成规则函数的开发，才能选择函数，操作方法请参见新建函数。
   - 当您选择**通过可视化编辑器**时，只需要设置规则名称和风险等级。
5. 在**参数设置**页面，设置规则参数，单击**下一步**。

   

   - 当您选择**基本设置**页面的**规则配置方式**为**使用托管规则**时，只能设置规则入参的阈值。
   - 当您选择**基本设置**页面的**规则配置方式**为**通过函数计算**时，可以设置规则触发机制、资源类型、规则入参以及阈值。

     当您设置规则参数时，需要根据自定义函数的逻辑设置入参的名称和阈值。该参数必须与函数的入参名称和资源实际配置的属性名称保持一致。
   - 当您选择**基本设置**页面的**规则配置方式**为**通过可视化编辑器**时，可以设置资源类型和合规条件。
6. 在**修正设置**页面，**修正执行方式**默认为**不执行修正**，单击**提交**。

   如果您需要为当前规则绑定修正模板，请参见设置自动修正或设置手动修正。
7. 查看规则新建结果。在**完成**页面，您可以查看规则新建结果。
   - 单击**查看规则详情**，您可以查看当前规则的**规则详情**和**修正详情**。
   - 单击**返回规则列表**，您可以在**管理合规规则**列表中查看该规则，规则状态为**应用中**。

5.设置监控范围

开始使用配置审计服务时，默认将所有资源类型纳入监控范围，初始化过程会扫描您账户下的所有资源。如果您有其他监控方案，则请根据本操作设置您需要监控的资源类型。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**设置 > 设置监控范围**。
3. 在**设置监控范围**页面，单击**编辑**。
4. 选择监控的资源类型。
   - 如果您选择**服务支持的全部资源类型**，则当配置审计对接新产品时，新产品也会纳入监控范围。
   - 如果您选择**自定义资源类型**，则可以根据所需选择指定资源。
5. 单击**确定**。
6. 在**手机验证**对话框中，单击**点击获取**。阿里云会向您绑定的手机发送一个校验码。
7. 输入**校验码**，单击**确定**。

6.开启等保预检

配置审计提供等保2.0预检能力，为您动态且持续地监控阿里云上资源的合规性，从而避免正式检测时反复整改，帮助您快速通过等保检测。

背景信息

等保预检的使用限制如下：

- 等保2.0条例所需的产品未能完全接入配置审计，部分条例的检测尚不能支持。
- 等保检测仅能在预检和整改环节为您提供辅助信息，所得的检测报告并不能直接用于等保2.0的正式检测。您仍需请公安部授权的检测机构为您做最终认证。

操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**启用合规场景 > 法则标准 > 等保预检**。
3. 单击**开启持续检测**，为当前账号开启持续的等保预检。

7.配置审计服务关联角色

配置审计服务关联角色（AliyunServiceRoleForConfig）是在某些场景下，为了完成配置审计的某个功能，需要获取其他云服务的访问权限而提供的RAM角色。

> 说明 更多关于服务关联角色的信息，请参见服务关联角色。

应用场景

配置审计服务关联角色的应用场景如下：

- 当配置审计调用各云服务的OpenAPI查询接口，获取当前账号下云资源的配置信息时，需要通过服务关联角色获取云资源配置信息的读取权限。
- 当您设置OSS Bucket地址用于接收资源变更历史快照时，配置审计需向您指定的OSS Bucket写入快照文件，需要通过服务关联角色获取OSS Bucket的写入权限。

创建服务关联角色

在配置审计控制台上，创建服务关联角色的操作方法如下：

- 个人版配置审计

  阿里云账号使用配置审计服务之前，需要创建服务关联角色，操作方法请参见服务授权。

- 企业版配置审计

  当企业管理账号将个人版配置审计升级为企业版时，单击**升级企业版**，配置审计将自动为所有成员账号创建服务关联角色。

  更多关于企业版配置审计的信息，请参见企业版配置审计概述。

删除服务关联角色

如果您需要删除服务关联角色，则请登录RAM控制台，执行删除操作，详情请参见删除服务关联角色。

角色说明

配置审计服务关联角色的详细信息如下：

- 角色名称：AliyunServiceRoleForConfig。
- 角色权限策略名称：AliyunServiceRolePolicyForConfig。
- 角色权限策略说明：授予配置审计服务读取当前账号下云资源配置信息的权限，以及资源配置变更快照写入OSS Bucket的权限。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "ecs:Describe*",
        "ess:Describe*",
        "vpc:Describe*",
        "rds:DescribeDBInstance*",
```

```
"rds:DescribeRegions",
"rds:DescribeBackup*",
"slb:Describe*",
"*:DescribeTags",
"oss:GetService",
"oss:GetBucket*",
"oss:ListBuckets",
"oss:ListObjects",
"ram:List*",
"ram:Get*",
"actiontrail:LookupEvents",
"actiontrail:Describe*",
"actiontrail:Get*",
"ots:BatchGet*",
"ots:Describe*",
"ots:Get*",
"ots:List*",
"ocs:Describe*",
"cms:Get*",
"cms:List*",
"cms:Query*",
"cms:BatchQuery*",
"cms:Describe*",
"kvstore:Describe*",
"fc:Get*",
"fc:List*",
"kms:DescribeKey",
"kms:DescribeRegions",
"kms:ListAliases",
"kms:ListAliasesByKeyId",
"kms:ListKeys",
"cdn:Describe*",
"yundun*:Get*",
"yundun*:Describe*",
"yundun*:Query*",
"yundun*:List*",
"polardb:Describe*",
"dds:Describe*",
"cen:Describe*",
"mns:ListTopic",
"mns:GetTopicAttributes",
```

```
            "resourcemanager:GetAccount",
            "resourcemanager:ListAccountsForParent",
            "resourcemanager:ListAccounts",
            "resourcemanager:GetFolder",
            "resourcemanager:ListFoldersForParent",
            "resourcemanager:ListAncestors",
            "resourcemanager:GetResourceDirectory",
            "composer:GetFlow",
            "composer:DescribeFlow",
            "nas:Describe*",
            "hbase:Describe*",
            "hbase:Get*",
            "hbase:List*",
            "hbase:Query*",
            "cs:Get*"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "oss:PutObject",
            "fc:InvokeFunction",
            "mns:PublishMessage",
            "composer:GroupInvokeFlow",
            "log:PostLogStoreLogs"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "config:*"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": "ram:DeleteServiceLinkedRole",
        "Resource": "*",
```

```
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "ram:ServiceName": "config.aliyuncs.com"
          }
        }
      }
    ]
}
```