ALIBABA CLOUD

阿里云

资源编排

快速入门

文档版本：20211105

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.快速入门

资源编排服务ROS（Resource Orchestration Service）是阿里云提供的一项简化云计算资源管理的服务。首次使用ROS时，您可以编写模板，定义所需的云计算资源、资源间的依赖关系等，然后创建资源栈，快速创建资源。本文以快速创建专有网络和交换机为例，为您介绍具体的操作方法。

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。

步骤一：编写模板

模板是一个JSON、YAML或Terraform格式的文本文件，使用UTF-8编码。您需要使用模板定义阿里云资源和配置细节，并说明资源间的依赖关系，然后基于模板创建资源栈。您可以根据模板结构和资源类型自行编写模板，也可以直接使用模板示例。

关于模板结构的更多信息，请参见JSON和YAML类型模板结构和Terraform类型模板结构。

创建专有网络和交换机的模板示例如下：

模板含义如下：

- `ROSTemplateFormatVersion`：模板的版本号，当前版本号：2015-09-01。
- `Description`：模板的描述信息，可用于说明模板的适用场景、架构说明等。通常情况下，对模板进行详细描述，有利于用户理解模板的内容。
- `Parameters`：模板的参数。示例中定义了专有网络名称（VpcName）、专有网络网段（VpcCidrBlock）、可用区ID（ZoneId）、交换机名称（VSwitchName）、交换机网段（VSwitchCidrBlock）和标签（Tags）等参数。关于参数定义的更多信息，请参见概览。
- `Resources`：模板所包含的阿里云资源。示例将创建一个专有网络和一个交换机。资源属性将引用`Parameters`中定义的参数。关于资源的更多信息，请参见ALIYUN::ECS::VPC和ALIYUN::ECS::VSwitch。
- `Outputs`：资源栈创建完成后，输出的资源信息。示例将输出专有网络ID和交换机ID。

Create a VPC and a VSwitch❯

步骤二：创建资源栈

您可以使用步骤一：编写模板编写的模板快速创建资源栈。

1. 登录资源编排控制台。
2. 在左侧导航栏，单击**资源栈**。
3. 在页面左上角的地域下拉列表，选择资源栈的所在地域，例如：华东1（杭州）。
4. 在**资源栈列表**页面，单击**创建资源栈**，然后在下拉列表中选择**使用新资源（标准）**。
5. 在**选择模板**页面，在**指定模板**区域单击**选择已有模板**、选择**模板录入方式**为**输入模板**，然后在**模板内容**区域的**ROS**页签输入步骤一：编写模板中编写的JSON格式的模板，最后单击**下一步**。
6. 在**配置模板参数**页面，输入资源栈名称，并设置以下参数。

参数	说明	示例
VpcName	专有网络名称。	myVPC

参数	说明	示例
VpcCidrBlock	专有网络网段。取值： ○ 10.0.0.0/8 ○ 172.16.0.0/12 ○ 192.168.0.0/16（默认值）	192.168.0.0/16
ZoneId	可用区ID。	华东1可用区K
VSwitchName	交换机名称。	myVSwitch
VSwitchCidrBlock	交换机网段。取值： ○ 10.0.0.0/24 ○ 172.16.0.0/24 ○ 192.168.0.0/24 **说明** 交换机跟专有网络需处于同一网段。	192.168.0.0/24
Tags	标签。 最多支持设置20个标签，每个标签由键值对组成。标签值可以为空。	[{"Key": "ros", "Value": "beginner-tutorial"}]

7. 单击**创建**。

步骤三：使用资源栈中的资源

资源栈创建成功后，您可以根据需要使用资源栈中的资源，例如：在专有网络的交换机中部署阿里云资源。

1. 在资源编排控制台的左侧导航栏，单击**资源栈**。
2. 在**资源栈列表**页面，单击目标资源栈ID。
3. 单击**资源**页签，然后单击交换机资源ID。
4. 在专有网络控制台，查看交换机基本信息，包括交换机ID、可用区、所属的专有网络ID等信息。
5. 在交换机中部署阿里云资源。

   具体操作，请参见创建云资源。

步骤四（可选）：更新资源栈

当您需要更新资源栈中的资源（例如：VpcName）时，可以更新资源栈。

1. 在资源编排控制台的左侧导航栏，单击**资源栈**。
2. 在**资源栈列表**页面，单击目标资源栈**操作**列的**更新**。
3. 在**配置模板参数**页面，更新参数信息（例如：将VpcName更新为testVPC）。
4. 单击**确认修改**。

步骤五（可选）：删除资源栈

当您不再需要已创建的资源时，可以删除资源栈，释放资源，以免产生不必要的费用。

1. 在资源编排控制台的左侧导航栏，单击**资源栈**。
2. 在**资源栈列表**页面，单击目标资源栈**操作**列的**删除**。

3. 在**删除资源栈**对话框，选择**删除方式**为**释放资源**。
4. 单击**确定**。

2.使用RAM控制资源访问

访问控制RAM（Resource Access Management）是阿里云提供的管理用户身份与资源访问权限的服务。通过RAM，您可以创建、管理RAM用户，并可以控制这些RAM用户对资源的操作权限。当您的企业存在多用户协同操作资源的场景时，RAM可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，从而降低企业的信息安全风险。

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**，设置RAM用户的安全策略。具体操作，请参见设置RAM用户安全策略。
3. 在左侧导航栏，选择**身份管理 > 用户**，创建RAM用户。具体操作，请参见创建RAM用户。
4. 创建ROS相关操作的自定义权限策略。具体操作，请参见创建自定义策略。

   > **说明**
   > - 关于权限策略语言的更多信息，请参见权限策略基本元素和权限策略语法和结构。
   > - 关于ROS权限策略的详情和示例，请参见ROS权限策略。其中操作可作为策略中的*Action*元素的内容，*Action*元素表示授权的操作，*Resource*表示授权操作的资源。*Action*和*Resource*元素一起可以组合出多种权限策略。

5. 在**用户**或**用户组**页面列表中，找到要授权的RAM用户或RAM用户组，并给其授予权限。

ROS权限策略

- ROS操作列表

操作（Action）	描述
ros:DescribeStacks	查看资源栈列表
ros:CreateStack	创建资源栈
ros:DeleteStack	删除资源栈
ros:UpdateStack	更新资源栈
ros:CancelUpdateStack	取消资源栈更新
ros:AbandonStack	丢弃资源栈
ros:ValidateTemplate	校验模板
ros:DescribeStackDetail	查看资源栈详情
ros:DescribeStackResources	查看资源列表
ros:DescribeStackResourceDetail	查看资源详情
ros:DescribeStackEvents	查看事件列表
ros:DescribeStackTemplate	查看模板内容

操作（Action）	描述
ros:SetDeletionProtection	启用或禁用删除保护

- ROS资源描述符
  RAM的策略定义中，可以通过下面的方式描述ROS资源栈。其中的变量可以用星号（*）来表示所有。如授权查看某一地域内的资源栈列表和详情的描述结构为：

  ```
  acs:ros:{region_id}:{owner_id}:stack/{stack_name}/{stack_id}
  ```

  示例：

  ```
  acs:ros:cn-beijing:*:stack/myStack/94dd5431-2df6-4415-81ca-732a7082****
  ```

- ROS权限策略示例
  - 以下策略授予查看cn-beijing地域的所有资源栈列表和资源栈详情的权限。其中，星号（*）是一个通配符，它表示账号下cn-beijing地域的所有资源栈。

    ```
    {
     "Statement": [
      {
       "Action": [
        "ros:DescribeStacks",
        "ros:DescribeStackDetail"
       ],
       "Effect": "Allow",
       "Resource": "acs:ros:cn-beijing:*:stack/*"
      }
     ],
     "Version": "1"
    }
    ```

  - 以下策略可以授予用户在所有地域创建和查看资源栈的权限。

    ```
    {
     "Statement": [
      {
       "Action": [
        "ros:CreateStack",
        "ros:DescribeStacks",
        "ros:DescribeStackDetail",
        "ros:ValidateTemplate"
       ],
       "Effect": "Allow",
       "Resource": "*"
      }
     ],
     "Version": "1"
    }
    ```

- 以下策略授予ID为12345****的用户可以对名称为myStack，ID为94dd5431-2df6-4415-81ca-732a7082****的资源栈进行更新操作。

```
{
 "Statement": [
  {
   "Action": [
    "ros:UpdateStack"
   ],
   "Effect": "Allow",
   "Resource": "acs:ros:cn-beijing:12345****:stack/myStack/94dd5431-2df6-4415-81ca-732a7082****"
  }
 ],
 "Version": "1"
}
```

- 当ROS进行临时授权访问时，ROS支持带 `acs:SourceIp` 和SSL信息限制的授权。
  授权策略需满足以下两个条件：
  - RAM用户当前的IP网段为42.120.99.0/24。
  - RAM用户正在使用HTTPS访问阿里云控制台或OpenAPI。

  当ROS通过阿里云STS（Security Token Service）进行临时授权访问时：
  - 以下授权策略可以访问ROS所有功能和资源，但不能访问其他服务。因为STS场景下无法透传acs:SourceIp和acs:SecureTransport。

```
{
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ros:*",
   "Resource": "*",
   "Condition": {
    "IpAddress": {
     "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
     "acs:SecureTransport": "true"
    }
   }
  }
 ],
 "Version": "1"
}
```

- 以下授权策略可以访问ROS所有功能和资源，但不能访问包括ECS在内的其他服务。

```
{
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ros:*",
    "ecs:*"
   ],
   "Resource": "*",
   "Condition": {
    "IpAddress": {
     "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
     "acs:SecureTransport": "true"
    }
   }
  }
 ],
 "Version": "1"
}
```

当ROS不通过阿里云STS（Security Token Service）进行临时授权访问时：

- 以下授权策略可以访问ROS所有功能和资源，但不能访问其他服务。

```
{
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ros:*",
   "Resource": "*",
   "Condition": {
    "IpAddress": {
     "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
     "acs:SecureTransport": "true"
    }
   }
  }
 ],
 "Version": "1"
}
```

- 以下授权策略可以访问ROS、ECS所有功能和资源，但不能访问其他云服务。

```
{
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ros:*",
    "ecs:*"
   ],
   "Resource": "*",
   "Condition": {
    "IpAddress": {
     "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
     "acs:SecureTransport": "true"
    }
   }
  }
 ],
 "Version": "1"
}
```

> **说明**
>
> - 关于阿里云STS的更多信息，请参见什么是STS。
> - 关于 `acs:SourceIp` 的更多信息，请参见通过指定的IP地址访问阿里云。
> - 关于 `acs:SecureTransport` 的更多信息，请参见通过指定的访问方式访问阿里云。
> - 关于阿里云SSL的更多信息，请参见什么是SSL证书服务。

3.创建更改集

您可以通过更改集功能更新资源栈的模板及模板参数。本文为您介绍如何创建更改集。

前提条件

请确保您已创建资源栈，操作方法请参见创建资源栈。

使用限制

只有以下状态的资源栈支持创建更改集：

状态	说明
CREATE_COMPLETE	资源栈创建成功。
UPDATE_FAILED	资源栈更新失败。
UPDATE_COMPLETE	资源栈更新完成。
ROLLBACK_COMPLETE	资源栈回滚完成。
ROLLBACK_FAILED	资源栈回滚失败。
IMPORT_CREATE_COMPLETE	通过资源导入创建资源栈成功。
IMPORT_UPDATE_COMPLETE	通过资源导入更新资源栈成功。
IMPORT_UPDATE_FAILED	通过资源导入更新资源栈失败。
IMPORT_UPDATE_ROLLBACK_COMPLETE	通过资源导入更新资源栈失败，回滚成功。
IMPORT_UPDATE_ROLLBACK_FAILED	通过资源导入更新资源栈失败，回滚失败。
CHECK_FAILED	资源栈校验失败。
CHECK_COMPLETE	资源栈校验完成。

创建更改集（控制台）

1. 登录资源编排控制台。
2. 在左侧导航栏，单击**资源栈**。
3. 在页面左上角的地域下拉列表，选择资源栈的所在地域。
4. 在目标资源栈操作列，选择 > **创建更改集**。

   您也可以单击**资源栈名称**下面的资源栈ID，在资源栈管理页面，选择**更改集**页签，然后单击**创建更改集**。
5. 在**选择模板**页面，根据所需选择已有模板或者示例模板，单击**下一步**。
6. 在**配置模板参数**页面，配置**更改集名称**和模板参数，然后单击**下一步**。

> **说明** 模板参数是从模板中解析而来，请您根据控制台提示输入参数信息。

7. 在**配置更改集**页面，配置**资源栈策略**、**失败时回滚**、**超时设置**、**RAM角色**和**是否启用替换更新**，然后单击**下一步**。
8. 在**检查并确认**页面，单击**创建更改集**。

通过阿里云CLI创建更改集

您可以借助阿里云命令行工具 CLI（Alibaba Cloud CLI），通过调用命令**aliyun ros CreateChangeSet**来创建更改集。

您需要指定更改集类型为 `CREATE` ，并指定资源栈名称、模板、参数和更改集名称。例如：为资源栈创建名为 `test-change-set` 的更改集，更改集使用当前资源栈模板（ `oss://ros-templates/test-change-set.json?RegionId=cn-hangzhou` ）。

```
aliyun ros CreateChangeSet --TemplateURL oss://ros-templates/test-change-set.json?RegionId=cn-hangzhou --StackId <stack_id> --ChangeSetName test-change-set --Parameters.1.ParameterKey Count --Parameters.1.ParameterValue 1
```

4.检测资源栈的偏差状态

通过偏差检测，您可以检测资源栈的实际配置是否与其模版配置不同或已经偏差。

前提条件

请确保您已经创建了资源栈。具体操作，请参见创建资源栈。

使用限制

- 只有以下状态的资源栈支持偏差检测。

状态	说明
CREATE_COMPLETE	资源栈创建成功。
UPDATE_FAILED	资源栈更新失败。
UPDATE_COMPLETE	资源栈更新完成。
ROLLBACK_COMPLETE	资源栈回滚完成。
ROLLBACK_FAILED	资源栈回滚失败。
CHECK_COMPLETE	资源栈校验完成。
CHECK_FAILED	资源栈校验失败。

- 目前只支持部分资源的偏差检测。更多信息，请参见支持偏差检测和资源导入的资源类型。

检测偏差（控制台）

1. 登录资源编排控制台。
2. 在左侧导航栏，单击**资源栈**。
3. 在页面左上角的地域下拉列表，选择资源栈的所在地域。
4. 在目标资源栈的操作列，选择 > **检测偏差**。

   您也可以单击**资源栈名称**下面的资源栈ID，在**资源栈信息**页签，单击**检测偏差**。
5. 在**偏差**页签，查看资源栈的**偏差状态**、**上一次偏差检查时间**和**资源偏差状态**。

检测偏差（阿里云CLI）

您可以借助阿里云命令行工具 CLI（Alibaba Cloud CLI），调用偏差检测相关接口检测资源栈偏差。具体如下：

- 调用DetectStackDrift接口对资源栈进行偏差检测。您需要指定资源栈ID，以及用于此次偏差检测操作筛选条件的特定资源名称。
  输入以下命令：

  ```
  aliyun ros DetectStackDrift --StackId bc1a154f-d073-4e77-9ae5-323d3b23****
  ```

  预期输出：

```
{
  "DriftDetectionId": "ad9cf0c7-938e-40b3-9466-ec9f25a1****",
  "RequestId": "B288A0BE-D927-4888-B0F7-B35EF84B6E6F"
}
```

- 调用GetStackDriftDetectionStatus接口查询偏差检测的状态。此接口将获取 DetectStackDrift 返回的资源栈偏差检测ID。
  在以下示例中，我们采用了如上 DetectStackDrift 示例返回的资源栈偏差检测ID，并将其作为参数传递给 GetStackDriftDetectionStatus 。此参数返回操作详细信息，显示偏差检测操作已完成。
  输入以下命令：

  ```
  aliyun ros GetStackDriftDetectionStatus --DriftDetectionId ad9cf0c7-938e-40b3-9466-ec9f25a1****
  ```

  预期输出：

  ```
  {
    "RequestId": "52398D3A-E868-4F95-8B5E-6A2DFB778B16",
    "DriftDetectionTime": "2020-03-17T07:21:17",
    "DriftDetectionStatusReason": "Detect stack drift successfully",
    "DriftedStackResourceCount": 2,
    "DriftDetectionStatus": "DETECTION_COMPLETE",
    "StackDriftStatus": "DRIFTED",
    "DriftDetectionId": "ad9cf0c7-938e-40b3-9466-ec9f25a1****",
    "StackId": "bc1a154f-d073-4e77-9ae5-323d3b23****"
  }
  ```

- 调用ListStackResourceDrifts接口查询资源栈的资源偏差详情。
  输入以下命令：

  ```
  aliyun ros ListStackResourceDrifts --StackId bc1a154f-d073-4e77-9ae5-323d3b23****
  ```

  预期输出：

```
{
 "ResourceDrifts": [
  {
   "ResourceDriftStatus": "MODIFIED",
   "LogicalResourceId": "Vpc1",
   "PropertyDifferences": [
    {
     "ActualValue": "test11",
     "PropertyPath": "/Description",
     "ExpectedValue": "test1",
     "DifferenceType": "NOT_EQUAL"
    }
   ],
   "PhysicalResourceId": "vpc-m5euqfvmzygb7xqmx****",
   "ExpectedProperties": "{\"CidrBlock\": \"192.168.0.0/16\", \"Description\": \"test1\", \"VpcName\": \"tes
t1\"}",
   "DriftDetectionTime": "2020-03-17T07:21:17",
   "ResourceType": "ALIYUN::ECS::VPC",
   "ActualProperties": "{\"CidrBlock\": \"192.168.0.0/16\", \"Description\": \"test11\", \"VpcName\": \"test1
\"}",
   "StackId": "bc1a154f-d073-4e77-9ae5-323d3b23****"
  },
  {
   "ResourceDriftStatus": "DELETED",
   "LogicalResourceId": "Vpc2",
   "PhysicalResourceId": "vpc-m5exf3skxrxtvtkbc****",
   "DriftDetectionTime": "2020-03-17T07:21:17",
   "ResourceType": "ALIYUN::ECS::VPC",
   "StackId": "bc1a154f-d073-4e77-9ae5-323d3b23****"
  }
 ],
 "RequestId": "8E1DE57B-6124-482B-8283-EF5562653308"
}
```