ALIBABA CLOUD

Alibaba Cloud

企业级分布式应用服务 EDAS

最佳实践

文档版本：20200831

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.如何自动为ECS实例添加访问ACM所需的RAM角色

借助ECS实例RAM角色，可实现无需配置AccessKey（AK）即可访问ACM，从而提高安全性。本文介绍了借助EDAS应用的挂载脚本能力，在扩容ECS实例到应用中时，自动为ECS实例添加访问ACM所需的RAM角色。

权限访问权限控制RAM挂载脚本

背景信息

以往，如果部署在ECS实例中的应用程序需要访问ACM，则必须将AccessKey以配置文件或其他形式保存在ECS实例中，这在一定程度上增加了AK管理的复杂性，并且降低了AK的保密性。AccessKey详情请参见创建AccessKey。

现在，借助ECS实例RAM角色，您可以将RAM角色和ECS实例关联起来，然后将RAM角色名称告知ACM SDK（版本1.0.8及以上），此后无需配置AK即可访问ACM。另外，借助RAM（访问控制），您可以通过角色和授权策略实现不同实例对ACM具有不同访问权限的目的。例如，如果配置只读策略，关联了该角色的ECS就只能读取ACM的配置，而无法新增或修改ACM配置。

前提条件

已开通访问控制（RAM），相关操作请参见：计费方法。

步骤一：创建RAM角色并配置授权策略

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 单击**创建RAM角色**，选择可信实体类型为**阿里云服务**，单击**下一步**。
4. 选择**角色类型**，输入**角色名称**和**备注**，选择受信服务为**云服务器**，然后单击**完成**。
5. 在**RAM角色名称**列，找到刚创建的RAM角色。
6. 在**操作**列单击**添加权限**。
7. 在**添加权限**对话框中，通过关键词搜索授权策略`AliyunACMFullAccess`，并单击该授权策略将其添加至右侧的**已选授列表**，然后单击**确定**。

   > **说明** 如果需要用到加解密配置功能，则还要添加`AliyunKMSCryptoAdminAccess`授权策略。

   此时，该角色已具备ACM的所有操作权限。

步骤二：创建权限策略

1. 在左侧导航栏的**权限管理**菜单下，单击**权限策略管理**。
2. 单击**创建权限策略**。
3. 填写**策略名称**为AttachACMRamRoleToECSPolicy，并填写**备注**。
4. **配置模式**选择**脚本配置**，在**策略内容**文本框内输入以下内容：

```
{
"Statement": [
{
"Effect": "Allow",
"Action": "ecs:AttachInstanceRamRole",
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "ecs:DescribeInstanceRamRole",
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "ram:*",
"Resource": "acs:ram:*:<替换成您的主账号ID>:role/<替换成中创建的角色名称>"
}
],
"Version": "1"
}
```

5. 单击**确定**。

步骤三：创建RAM用户并添加授权

1. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
2. 单击**创建用户**。

   > **说明** 单击**添加用户**，可一次性创建多个RAM用户。

3. 输入**登录名称**和**显示名称**。
4. 在**访问方式**区域下，选择**编程访问**，然后单击**确定**。
   在**用户信息**页面会显示创建用户的**AccessKey ID**和**AccessKeySecret**，请记录下来供后续步骤使用并妥善保管。
5. 在**用户登录名称/显示名称**列表下，找到目标RAM用户。
6. 单击**添加权限**，被授权主体会自动填入。
7. 在**权限策略名称**右侧的输入框内，输入步骤二：创建权限策略中生成的策略名称。
8. 单击**确定**，然后关闭右侧面板。

步骤四：通过挂载脚本为ECS实例授予RAM角色

1. 登录EDAS控制台。
2. 在左侧导航栏中选择**应用管理 > 应用列表**，在顶部菜单栏选择地域并在页面上方选择命名空间，然后在**应用列表**页面单击具体的应用名称。
3. 在应用的**基本信息**页签的**应用设置**区域单击**编辑**，然后在下拉列表中单击**挂载脚本**。
4. 在**挂载脚本**对话框中单击展开**准备实例脚本**
5. 在文本框中输入以下脚本，然后单击**修改**。

   > **注意** 以下脚本含有您在步骤三：创建RAM用户并添加授权中创建的子账号的访问密钥，请妥善保管。

   ```
   #!/bin/sh
   fileURL='https://edas-public.oss-cn-hangzhou.aliyuncs.com/samples/acm/attachAcmRamRole.sh'
   file=/tmp/attachAcmRamRoleToEcs.sh
   wget "$fileURL" -O "$file" &>/dev/null
   chmod +x "$file"
   #<accessKeyId>替换成子账号对应的accessKeyId
   #<accessSecret>替换成子账号对应的accessSecret
   #<ecsRamRoleForACM>替换成中所创建的角色名称。bash "$file" <accessKeyId> <accessSecret> <ecsRamRoleForACM>
   ```

   该脚本执行后会将 <ecsRamRoleForACM> 绑定到扩容的ECS实例上。

更多信息

- 创建AccessKey
- RAM（访问控制）
- 创建可信实体为阿里云服务的RAM角色
- 使用实例RAM角色访问其他云产品
- ACM Java Native SDK 概述

2.实现容器服务 Kubernetes 集群中应用的数据加密传输

您可以为在 EDAS 容器服务 Kubernetes 集群中部署的应用添加 SSL 证书，为应用提供 HTTPS 保护，将所有 Web 流量加密以防数据遭到窃取和篡改，从而保证应用的安全性。本文将以一个示例介绍如何实现应用的数据加密传输。

前提条件

已获取由证书颁发机构 （CA）签署的 SSL 证书。推荐您使用阿里云 SSL 证书，也可以从第三方证书颁发机构获取证书。

示例场景

本示例将以一个 hello-edas 的 Web 应用为例介绍如何通过使用阿里云 SSL 域名证书实现应用的数据加密传输。

hello-edas 应用部署在 EDAS 容器服务 Kubernetes 集群中，通过负载均衡 SLB 提供服务，服务域名为 edas.site。您购买了阿里云 SSL 域名证书， 准备将该证书添加到 hello-edas 应用中，实现应用的数据传输加密，以保证应用的安全性。您需要完成以下操作步骤：

1. 在负载均衡 SLB 中创建证书。
2. 在容器服务 Kubernetes 版中为应用创建服务（Dashboard）。
3. 在云解析 DNS 中添加域名和域名解析。

在负载均衡 SLB 中创建证书

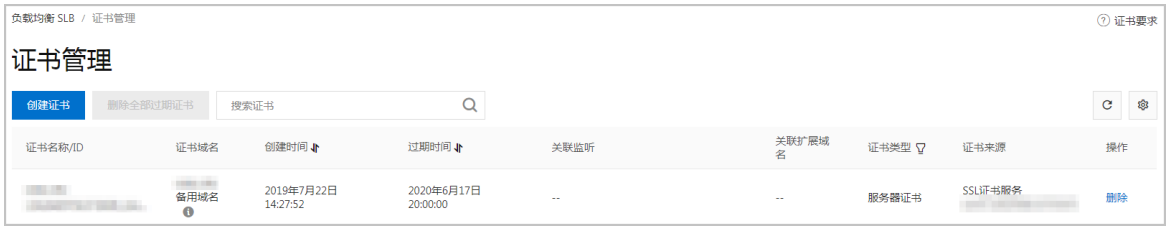
1. 登录负载均衡管理控制台。
2. 在左侧导航栏单击**证书管理**。
3. 在**证书管理**页面单击**创建证书**。
4. 在**创建证书**对话框中选择**阿里云签发证书**，并设置相关参数，然后单击**创建**。

   选择阿里云签发证书参数说明：

参数	说明
证书部署地域	选择您要实现身份验证和数据加密传输的应用所在的地域。本示例为华为 2（北京）。
所属资源组	选择默认资源组即可。
证书列表	在下拉列表中选择您在阿里云 SSL 证书中购买并签发的证书。如果没有可在 SSL 证书中购买，详情请参见新手入门。

> **说明** 如果您要使用第三方签发证书，创建证书的操作步骤请参见上传第三方签发证书。

创建完成后，返回**证书管理**页面，查看证书。



> **说明** 保存证书 ID，在创建服务时会用到。

在容器服务 Kubernetes 版中为应用创建服务（Dashboard）

> **说明** 容器服务 Kubernetes 版控制台和 Dashboard 的功能有些差别，推荐您使用 Dashboard 创建服务。

1. 登录容器服务控制台。
2. 在左侧导航栏选择**集群 > 集群**。
3. 在**集群列表**找到您导入 EDAS 并创建应用的集群，在**操作**列单击**控制台**。

   > **说明** 当您选择集群后，也就选择了该集群所在的地域和 K8s Namespace。

4. 在该集群 Dashboard 的左侧导航栏选择**服务发现与负载均衡 > 服务**。
5. 在**服务**页面右上角单击**创建**。
6. 在**创建资源**页面的**使用文本创建**页签中输入 YAML 或 JSON 格式定义的资源，部署在当前所选的 K8s Namespace 内，然后单击**上传**。

配置 SLB 时，需要注意以下限制：

- 使用已有 SLB 会强制覆盖已有监听。
- 创建服务时新建的 SLB 不能复用（会导致 SLB 被意外删除）。
- 复用同一个 SLB 的多个服务不能设置相同的服务端口，否则会造成端口冲突。
- 不支持跨集群复用 SLB。

如果您想了解或使用更多通过 SLB 访问 Kubernetes 服务的参数，请参见通过SLB访问服务。

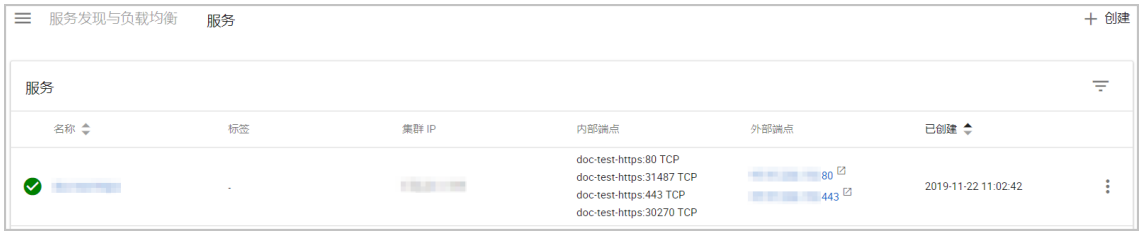
- 已有公网 SLB，可以基于以下 YAML 示例修改配置。

```
apiVersion: v1
kind: Service
metadata:
annotations:
service.beta.kubernetes.io/alibaba-cloud-loadbalancer-cert-id: xxxxxxxxxxxxxxxxxxxxxxxxxxxx
# 负载均衡创建的证书ID
service.beta.kubernetes.io/alibaba-cloud-loadbalancer-protocol-port: http:80,https:443
service.beta.kubernetes.io/alicloud-loadbalancer-address-type: internet # 公网SLB
service.beta.kubernetes.io/alicloud-loadbalancer-id: xxxxxx # 已有SLB的ID
service.beta.kubernetes.io/alicloud-loadbalancer-force-override-listeners: true
name: app-test-https # 任意命名，例如internet-{{应用名}}-{{随机字符串}}
namespace: default
spec:
ports:
- name: http-80
port: 80
protocol: TCP
targetPort: 8080
- name: https-443
port: 443
protocol: TCP
targetPort: 8080
selector:
edas.appid: xxxxx-xxxx-xxxxx-xxxxxxxx # EDAS容器服务Kubernetes集群中部署的应用的ID
sessionAffinity: None
type: LoadBalancer
```

- 新建 SLB 的需要在 YAML 示例中删除以下 3 个参数配置。

```
service.beta.kubernetes.io/alicloud-loadbalancer-address-type: internet # 公网SLB
service.beta.kubernetes.io/alicloud-loadbalancer-id: xxxxxx # 已有SLB的ID
service.beta.kubernetes.io/alicloud-loadbalancer-force-override-listeners: true
```

返回服务页面，等待服务创建成功。服务创建成功后，可以看到服务的外部端点显示 `<SLB IP>:<配置的 port>`，并且包含 HTTPS 的 443 端口信息。则说明该服务创建成功，如下图所示。



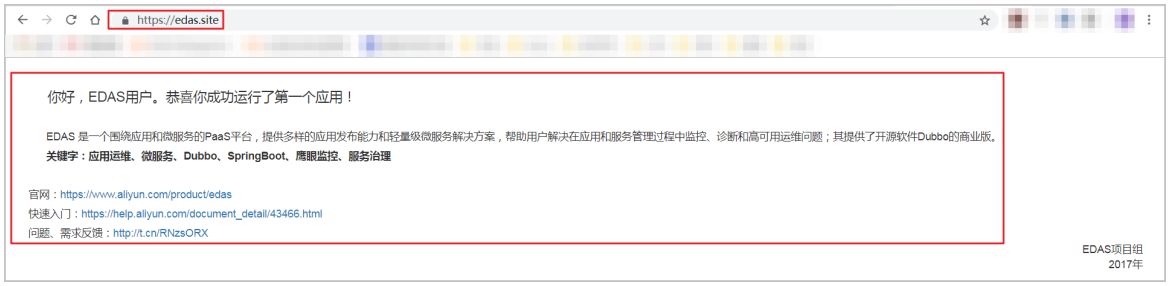
在云解析 DNS 中添加域名和域名解析

您需要在云解析 DNS中添加域名和域名解析，以便您提供服务的域名可以通过 HTTPS 访问。详情请参见域名管理和添加解析记录。

结果验证

操作完成后，检查是否可以通过 HTTPS 安全访问服务域名。

1. 打开浏览器，访问 *https://edas.site*。
2. 查看服务是否可以正常访问，且地址栏显示访问是安全的。



3.构建开发环境

您可以根据实际需求决定在本地或者云上构建开发环境，以便开发和调试应用。

开发环境 构建环境 开发 调试

构建方案简介

EDAS为您提供三种可选方案，下面将介绍这三种方案构建开发环境的特点。

构建环境	方案	说明
本地	在本地搭建轻量配置中心实现服务注册和发现，在本地开发、调试。	轻量配置中心不具有生产环境的性能水平，当注册上来的服务较多的时候可能会有性能问题。因为是本地环境，也无法使用EDAS中的服务治理、监控和发布等功能。完全为您的自建环境。
阿里云	在云上创建开发环境，开发人员通过端云联调插件连接云端应用，进行开发、调试。	可以使用EDAS的全部能力。因为使用云上资源，成本比较高。
混合云	在混合云中创建开发环境，开发人员可以直接在本地进行开发、调试。	可以使用EDAS的全部能力。需要通过VPN或专线连通本地网络和阿里云VPC。注意：需要开通EDAS专业版或铂金版。

在本地构建开发环境

1. 在本地搭建轻量配置中心，详情请参见搭建轻量配置中心。
2. 在本地开发、调试应用。

在阿里云构建开发环境

1. 开通EDAS。
2. 创建资源。 命名空间用于服务和配置隔离，您可以为开发、测试环境分别创建命名空间。
3. 将应用部署到开发环境，即对应的命名空间中。详情请参见应用部署概述（ECS集群）和应用部署概述（K8s集群）。
4. 使用端云互联插件开发和调试应用。

在混合云中构建开发环境

> 注意 EDAS专业版或铂金版才支持混合云。

1. 开通EDAS。
2. 创建资源。
   - 命名空间用于服务和配置隔离，您可以为开发、测试环境分别创建命名空间。
   - 您需要创建混合云（非阿里云）集群。
3. 将应用部署到混合云的开发环境，即对应的命名空间中。详情请参见在混合云中部署应用。

   > 说明 您需要为阿里云ECS实例和非阿里云的机器开通所需端口。

4. 在本地开发和调试应用。