云解析服务

最佳实践

文档版本 01

发布日期 2024-03-15

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 设置 CAA 记录防止错误颁发 HTTPS 证书.....1
2 为云服务器配置内网域名.....9

1 设置 CAA 记录防止错误颁发 HTTPS 证书

方案概述

应用场景

CAA（Certification Authority Authorization，证书颁发机构授权）是一项防止HTTPS证书错误颁发的安全措施，遵从IETF RFC6844。从2017年9月8日起，要求CA（Certification Authority，证书颁发）机构执行CAA强制性检查。

全球约有上百个CA机构有权发放HTTPS证书，证明您网站的身份。假如浏览器将某个CA机构列入黑名单，并宣称不再信任其颁发的HTTPS证书，当您访问到部署了这些HTTPS证书的网站时，会被提示HTTPS证书不受信任，如图1-1所示。

图 1-1 HTTPS 证书错误颁发

CAA标准要求CA机构在为域名签发证书时执行CAA强制性检查：

- 如果检查域名的DNS解析记录，发现未设置CAA字段，则为该域名颁发证书。
  这种情况下，任何CA机构均可为该域名签发证书，存在HTTPS证书错误颁发的风险。
- 如果检查域名的DNS解析记录，在CAA字段发现获得授权，则为该域名颁发证书。
- 如果检查域名的DNS解析记录，在CAA字段发现未获得授权，则拒绝为该域名颁发证书，防止未授权HTTPS证书错误颁发。

公有云的云解析服务支持为公网域名设置CAA记录，您可以通过在管理控制台为域名添加CAA解析记录。

方案优势

为网站的域名添加CAA解析记录可以使网站将指定CA机构列入白名单，仅授权指定CA机构为网站的域名颁发证书，提高网络的安全性。

约束和限制

CAA记录集的格式为：[flag] [tag] [value]，由一个标志字节的[flag]和一个[tag]-[value]（标签-值）对组成。

配置原则：

- flag：认证机构限制标志，定义为0~255无符号整型。常用取值为0。
- tag：仅支持大小写字母和数字0~9，长度1~15，常用取值：
  - issue：授权任何类型的域名证书
  - issuewild：授权通配符域名证书
  - iodef：指定违规申请证书通知策略
- value：域名或用于违规通知的电子邮箱或Web地址。其值取决于[tag]的值，必须加双引号。取值范围：字符串（仅包含字母、数字、空格、-#*?&_~=:;.@+^/!%），最长255字符。

不同应用场景下，设置CAA记录集的规则如**表1-1**所示。

表 1-1 CAA 记录配置规则

目的	样例	描述
设置单域名CAA记录	0 issue "ca.example.com"	该字段表示只有ca.example.com可以为域名domain.com颁发证书，未经授权的第三方CA机构申请域名domain.com的HTTP证书将被拒绝。
	0 issue ";"	该字段表示拒绝任何CA机构为域名domain.com颁发证书。
设置发送警报通知	0 iodef "mailto:admin@domain.com"	该字段用于当第三方尝试为一个未获得授权的域名申请证书时，通知CA机构向网站所有者发送警报邮件。
	0 iodef "http://domain.com/log/" 0 iodef "https://domain.com/log/"	该字段用于记录尝试在其他CA申请HTTPS证书的行为。
设置颁发通配符域名证书	0 issuewild "ca.example.com"	该字段用于将通配符证书的颁发权限指定CA机构ca.example.com。

目的	样例	描述
综合配置样例	0 issue "ca.abc.com" 0 issuewild "ca.def.com" 0 iodef "mailto:admin@domain.com"	该字段表示域名domain.com： • 授权CA机构ca.abc.com颁发不限类型的证书。 • 授权CA机构ca.def.com颁发通配符证书。 • 禁止其他CA机构颁发证书。 • 当有违反设置规则的情况发生，CA机构发送通知邮件到admin@domain.com。

资源成本和规划

本节介绍最佳实践中资源规划情况，包含以下内容：

表 1-2 域名资源规划

资源	公网域名	记录集类型
DNS	domain.com	CAA

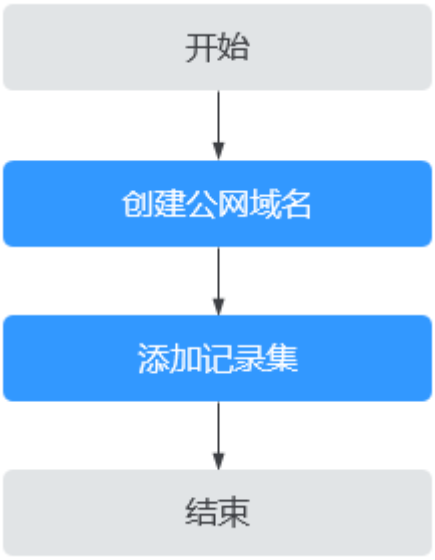
表 1-3 资源和成本规划

资源	资源名称	资源说明	数量	每月费用
域名注册	域名	公网域名：domain.com	1	-
云解析服务	公网域名 解析记录集	• 公网域名：domain.com • 记录集类型：CAA 值： 0 issue "ca.abc.com" 0 iodef "mailto:admin@domain.com"	1	免费

设置公网域名的 CAA 记录流程

为公网域名添加CAA记录集的流程如图1-2所示。

图 1-2 设置公网域名 CAA 记录



实施步骤

步骤1 创建公网域名

1. 进入**公网域名列表页面**。
2. 在公网域名页面，单击“创建公网域名”。
3. 根据界面提示配置相关参数，参数说明如**表1-4**所示。

表 1-4 创建公网域名参数说明

参数	参数说明	取值样例
域名	从域名注册商处获得的授权域名。 支持添加主域名及主域名的子域名，即最多支持添加二级域名，例如： – domain.com的子域名 abc.domain.com – domain.com.cn的子域名 abc.domain.com.cn。 域名的格式请参见**域名格式与级别**。	domain.com
邮箱	可选参数。 管理该公网域名的管理员邮箱。建议用户使用保留邮箱“HOSTMASTER@*域名*”作为此管理员邮箱。 更多关于邮箱的信息，请参见**SOA记录中的Email格式为什么变化了？**。	-

参数	参数说明	取值样例
标签	可选参数。 域名的标识，包括键和值，每个域名可以创建10个标签。 键和值的命名规则请参见表1-5。 **说明** 如您的组织已经设定云解析服务的相关标签策略，则需按照标签策略规则为域名添加标签。标签如果不符合标签策略的规则，则可能会导致域名创建失败，请联系组织管理员了解标签策略详情。	example_key1 example_value1
描述	可选参数。 域名的描述信息。 长度不超过255个字符。	This is a zone example.

表 1-5 标签命名规则

参数	规则	举例
键	- 不能为空。 - 对于同一资源键值唯一。 - 长度不超过36个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”和“/”的所有Unicode字符，且首尾字符不能为空格。	example_key1
值	- 不能为空。 - 长度不超过43个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”和“/”的所有Unicode字符，且首尾字符不能为空格。	example_value1

4. 单击“确定”。

步骤2 添加记录集

1. 在“公网域名”页面的域名列表中，单击待添加CAA记录集的域名domain.com。
   系统进入domain.com的域名解析记录页面。
2. 单击“添加记录集”。
   系统进入“添加记录集”页面。
3. 根据界面提示配置相关参数，参数说明如表1-6所示。

表 1-6 添加 CAA 类型记录集参数说明

参数	参数说明	取值样例
主机记录	解析域名的前缀。 例如创建的域名为“domain.com”，其“主机记录”设置包括： – www：用于网站解析，表示解析的域名为“www.domain.com”。 – 空：用于网站解析，表示解析的域名为“domain.com”。 主机记录置为空，还可用于为空头域名“@”添加解析。 – abc：用于子域名解析，表示解析的域名为“domain.com”的子域名“abc.domain.com”。 – mail：用于邮箱解析，表示解析的域名为“mail.domain.com”。 – *：用于泛解析，表示解析的域名为“*.domain.com”，匹配“domain.com”的所有子域名。	置空
类型	记录集的类型，此处为CAA类型。 添加记录集时，如果提示解析记录集已经存在，说明待添加的记录集与已有的记录集存在限制关系或者冲突。 详细内容请参见**为什么会提示解析记录集已经存在？**。	CAA – CA证书颁发机构授权校验
线路类型	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 仅支持为公网域名的记录集配置此参数。 – 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。 – 运营商线路解析：根据访问者所在运营商，设置解析线路。 – 地域解析：根据访问者所在地域，设置解析线路。	全网默认

参数	参数说明	取值样例
TTL(秒)	解析记录在本地DNS服务器的缓存时间，以秒为单位。 默认值为“300秒”。取值范围为：1~2147483647 如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。 更多TTL相关内容请参见**什么是TTL值?** 。	5分钟，即300s。
值	指定要授权的证书颁发机构，使其可以给域名或者子域名颁发证书。 最多可以输入50个不重复记录，多个记录之间以换行符分隔。 填写格式：[flag] [tag] [value] 配置规则： – flag：认证机构限制标志，定义为0~255无符号整型。常用取值为0。 – tag：仅支持大小写字母和数字0~9，长度1~15，常用取值： ▪ issue：授权任何类型的域名证书 ▪ issuewild：授权通配符域名证书 ▪ iodef：指定违规申请证书通知策略 – value：域名或用于违规通知的电子邮箱或Web地址。其值取决于[tag]的值，必须加双引号。取值范围：字符串（仅包含字母、数字、空格、-#*?&_~=:;.@+^/!%），最长255字符。	0 issue "ca.abc.com" 0 iodef "mailto:admin@domain.com"
权重	可选参数，返回解析记录的权重比例。默认值为1，取值范围：0~1000。 仅支持为公网域名的记录集配置此参数。 当域名在同一解析线路中有多条相同类型的解析记录时，可以通过“权重”设置解析记录的响应比例。。	1

参数	参数说明	取值样例
标签	可选参数，记录集的标识，包括键和值，每个记录集可以创建10个标签。 键和值的命名规则请参见表1-7。 **说明** 如您的组织已经设定云解析服务的相关标签策略，则需按照标签策略规则为记录集添加标签。标签如果不符合标签策略的规则，则可能会导致记录集创建失败，请联系组织管理员了解标签策略详情。	example_key1 example_value1
描述	可选参数，对域名的描述。 长度不超过255个字符。	The description of the hostname.

表 1-7 标签命名规则

参数	规则	举例
键	- 不能为空。 - 对于同一资源键值唯一。 - 长度不超过36个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”和“/”的所有Unicode字符，且首尾字符不能为空格。	example_key1
值	- 不能为空。 - 长度不超过43个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”和“/”的所有Unicode字符，且首尾字符不能为空格。	example_value1

4. 单击“确定”，完成CAA类型记录集的添加。

----结束

验证 CAA 解析记录是否生效?

CAA解析记录可以通过dig+trace命令查看域名是否生效以及具体的解析过程。如果操作系统没有自带dig命令，需要手动安装后才能使用。

命令格式为：dig [类型] [域名] +trace。

示例如下：

dig caa www.domain.com +trace

2 为云服务器配置内网域名

方案概述

应用场景

网站在运行过程中，当某一台ECS故障，需要将业务切换到备份的云服务器时，如果云服务器没有配置内网域名，则需要通过修改主业务节点ECS的代码来重新设置云服务器的内网IP地址，该操作需要中断业务并重新发布网站，耗时耗力。

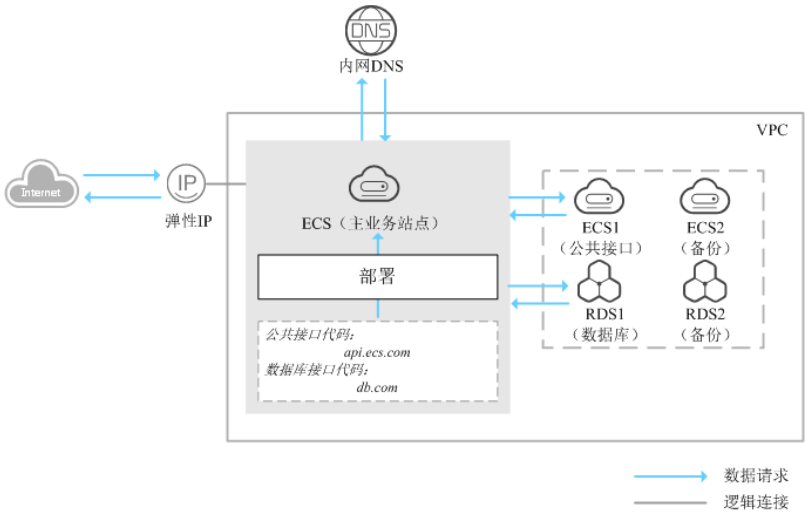
内网域名功能支持为VPC内每个云服务器创建一个内网域名，在部署该网站时，我们为云服务器申请了内网域名，且代码中设置的是云服务器的内网域名，则仅需要通过修改内网域名解析记录即可实现云服务器的切换，无需中断业务，也不需要重新发布网站。

方案架构

图2-1展示了某网站的逻辑组网，在一个VPC内，部署了ECS和RDS。其中：

- ECS：作为主业务站点和业务入口。
- ECS1：作为公共接口。
- RDS1：作为数据库，存储业务数据。
- ECS2和RDS2：作为备份服务器和数据库。

图 2-1 逻辑组网图



方案优势

- 通过内网域名访问VPC内的云服务器，无需经过Internet，访问速度更快、安全性更高。
- 在代码中使用内网域名代替内网IP。当需要进行云服务器切换时，只需通过修改内网域名解析记录即可，无需修改代码。

资源成本和规划

本节介绍最佳实践中资源规划情况，包含以下内容：

表 2-1 内网域名资源规划

资源	内网域名	关联VPC	内网IP	记录集类型	说明
ECS1	api.ecs.com	VPC_001	192.168.2.8	A	公共接口ECS。
ECS2	api.ecs.com	VPC_001	192.168.3.8	A	备份公共接口ECS。
RDS1	db.com	VPC_001	192.168.2.5	A	数据库，用于存储业务数据。
RDS2	db.com	VPC_001	192.168.3.5	A	备份数据库。

表 2-2 资源和成本规划

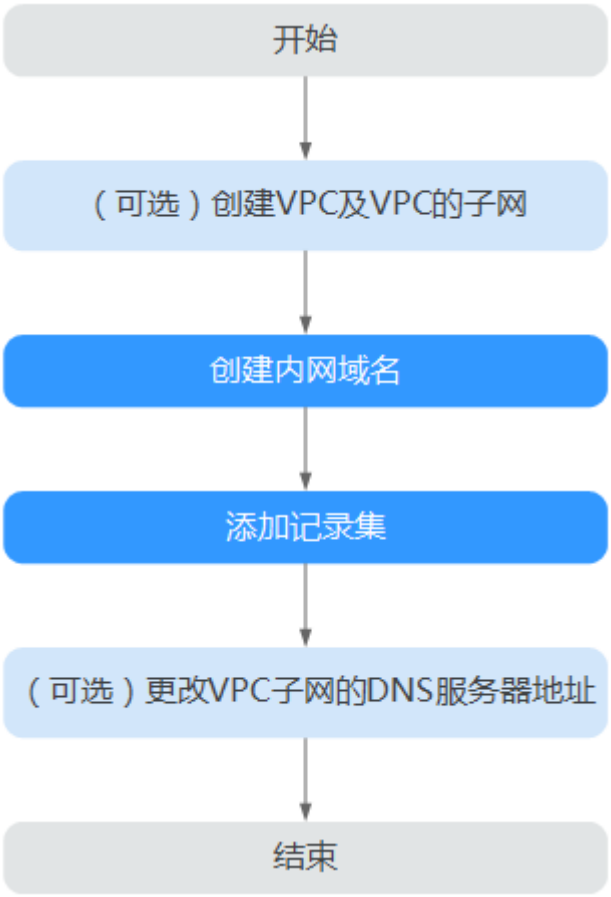
区域	资源	资源名称	资源说明	数量	每月费用（元）
中国-香港	虚拟私有云VPC	VPC_001	设置DNS服务器地址与华为云的内网DNS地址保持一致。 详细请参见**华为云提供的内网DNS地址是多少?**	1	免费
	弹性云服务器ECS	ECS ECS1 ECS2	• 内网域名：api.ecs.com • 关联VPC：VPC_001 • ECS1：公共接口ECS，内网IP：192.168.2.8 • ECS2：备份公共接口ECS，内网IP：192.168.3.8	3	详细请参见**弹性云服务器产品价格详情**。

区域	资源	资源名称	资源说明	数量	每月费用（元）
	云数据库 RDS	RDS1 RDS2	• 内网域名：db.com • 关联VPC：VPC_001 • RDS1：数据库，用于存储业务数据，内网IP：192.168.2.5 • RDS2：备份数据库，内网IP：192.168.3.5	2	详细请参见**云数据库产品价格详情**。
	云解析服务	api.ces.com db.com	• api.ces.com： 关联VPC：VPC_001 记录集类型：A，值：192.168.2.8 • db.com 关联VPC：VPC_001 记录集类型：A，值：192.168.2.5	2	免费

为云服务器配置内网域名总流程

为云服务器配置内网域名的流程如**图2-2**所示。

图 2-2 内网域名配置流程



配置流程说明：

1. “（可选）创建VPC及VPC子网”：在管理控制台虚拟私有云服务页面完成配置，仅当您在网站部署阶段为云服务器配置内网域名时，执行本操作。
2. “创建内网域名”和“创建记录集”：在管理控制台云解析服务页面完成相关配置。
3. “（可选）更改VPC子网的DNS”：在管理控制台虚拟私有云服务页面完成配置，仅当您为已运行网站的云服务器配置内网域名时，执行本操作。

实施步骤

步骤1 （可选）创建VPC及VPC的子网

当您在网站部署阶段为云服务器配置内网域名时，需要首先完成VPC及其子网的创建。

1. 进入**创建虚拟私有云页面**。
2. 根据界面提示配置参数，关键参数的配置说明如**表2-3**所示。

表 2-3 虚拟私有云关键参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	中国-香港
名称	VPC名称。	VPC_001
网段	VPC的地址范围，VPC内的子网地址必须在VPC的地址范围内。 目前支持网段范围： – 10.0.0.0/8~24 – 172.16.0.0/12~24 – 192.168.0.0/16~24	192.168.0.0/16
子网名称	子网的名称。	Subnet
子网网段	子网的地址范围，需要在VPC的地址范围内。	192.168.0.0/24
网关	子网的网关。	192.168.0.1
DNS服务器地址	若要为VPC内的云服务器配置内网域名，需要设置DNS服务器地址与华为云的内网DNS地址保持一致。	100.125.1.250 100.125.3.250

3. 单击“立即创建”，完成VPC以及VPC默认子网的设置。

步骤2 创建内网域名

为云服务器ECS1和数据库RDS1创建内网域名。

1. 进入**内网域名列表页面**。
2. 单击“创建内网域名”，开始创建内网域名。
3. 根据界面提示配置参数，参数说明如**表2-4**所示。

表 2-4 创建内网域名参数说明

参数	参数说明	取值样例
域名	域名。可以自定义，支持创建顶级域，但需符合域名命名规范。	api.ecs.com
VPC	内网域名要关联的VPC。	VPC_001

参数	参数说明	取值样例
邮箱	可选参数。管理该内网域名的管理员邮箱。建议用户使用保留邮箱“HOSTMASTER@*域名*”作为此管理员邮箱。 更多关于Email的信息，请参见**SOA记录中的Email格式为什么变化了？** 。	HOSTMASTER@ecs1.com
标签	可选参数。由键和值组成，用于搜索域名或为域名资源分组。当系统中配置多个域名时，可以选择配置此参数。 键和值的命名规则请参见**表2-5**。 **说明** 如您的组织已经设定云解析服务的相关标签策略，则需按照标签策略规则为域名添加标签。标签如果不符合标签策略的规则，则可能会导致域名创建失败，请联系组织管理员了解标签策略详情。	-
描述	可选参数。域名的描述信息。长度不超过255个字符。	This is a zone example.

表 2-5 标签命名规则

参数	规则	举例
键	- 不能为空。 - 对于同一资源键值唯一。 - 长度不超过36个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”和“/”的所有Unicode字符，且首尾字符不能为空格。	example_key1
值	- 不能为空。 - 长度不超过43个字符。 - 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”和“/”的所有Unicode字符，且首尾字符不能为空格。	example_value1

4. 单击“确定”，完成内网域名api.ecs.com的创建。
   创建完成后，您可以在“内网域名”页面查看新创建的域名信息。

说明

单击“名称”列的域名名称，可以看到系统已经为您创建了SOA类型和NS类型的记录集。其中，

- SOA类型的记录集标识了对此域名具有最终解释权的主权威服务器。
- NS类型的记录集标识了此域名的权威服务器。

5. 重复执行3~5，完成内网域名db.com的创建。
   内网域名规划请参见表2-1。

步骤3 创建记录集

为云服务器ECS1和数据库RDS1的内网域名添加到对应内网IP的解析记录。

1. 在“内网域名”页面的域名列表中，单击新创建域名的名称。
   系统进入域名解析记录页面。
2. 单击“添加记录集”。
3. 根据界面提示填写参数配置，参数说明如表2-6所示。

表 2-6 添加 A 类型记录集参数说明

参数	参数说明	取值样例
主机记录	域名前缀。 此处参数设置为空，表示解析的域名是api.ecs.com。	-
类型	记录集的类型，此处为A类型。	A – 将域名指向IPv4地址
TTL(秒)	解析记录在DNS服务器的缓存时间，以秒为单位。 如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。	默认为“5min”，即300s。
值	域名对应的IPv4地址。多个IPv4地址以换行符分隔。 此处设置为云服务器的内网IP。	192.168.2.8
标签	可选参数，由键和值组成，用于搜索记录集或为记录集资源分组。当系统中配置多个记录集时，可以选择配置此参数。 键和值的命名规则请参见表2-5。 **说明** 如您的组织已经设定云解析服务的相关标签策略，则需按照标签策略规则为记录集添加标签。标签如果不符合标签策略的规则，则可能会导致记录集创建失败，请联系组织管理员了解标签策略详情。	-
描述	可选配置，对域名的描述。	-

4. 单击“确定”，完成为内网域名api.ecs.com添加A类型记录集。
5. 重复执行1~4，为内网域名db.com添加A类型的记录集。
   域名db.com对应记录集的“值”设置为“192.168.2.5”。
   记录集的详细数据规划请参见表2-2。

步骤4 （可选）更改VPC子网的DNS

当您为已运行网站的云服务器配置内网域名时，需要更改VPC子网的DNS。

为实现内网域名在VPC内的正常解析，您需要把VPC子网的DNS改成云解析服务提供的内网DNS。

更改VPC子网的DNS的操作请参见怎样切换内网DNS？。

步骤5 切换ECS

当ECS1发生故障，需要将业务切换到备份的云服务器ECS2上。此时，可以通过修改内网域名api.ecs.com的解析记录实现业务切换。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择“中国-香港”。
3. 选择“网络 > 云解析服务”。
   进入云解析服务页面。
4. 在左侧树状导航栏，选择“内网域名”。
5. 在“内网域名”页面域名列表中，单击“名称”列的域名“api.ecs.com”进入域名解析记录页面。
6. 在A类型记录集中，单击“操作”列的“修改”。
7. 将“值”修改为“192.168.3.8”。
8. 单击“确定”，完成解析记录的修改。

此时，ECS到公共接口ECS1的访问会通过内网DNS解析到ECS2上，实现了ECS的切换。

----结束

