阿里云
域名

域名安全

文档版本：20190218

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 域名安全最佳实践

域名越来越稀少，好域名越来越贵，域名一旦被盗则令人费心费力，还不一定能够找回。因此，做好域名防盗工作很有必要。作为域名持有者，您完全可以事先做好多方面防盗措施。

开启注册局安全锁

注册局安全锁是目前最高等级的域名安全保护措施，由注册局在根服务器层面操作，禁止域名被恶意转移、篡改及删除。目前该服务支持*.com*、*.cn*、*.net*、*.cc*、*.tv*、*.name*、.中国、*.gov.cn*等后缀。开启注册局安全锁后，域名将被置为三种锁定状态：

- 注册局设置禁止删除（serverDeleteProhibited）
- 注册局设置禁止转移（serverTransferProhibited）
- 注册局设置禁止更新（serverUpdateProhibited）

如需对域名做任何状态及信息更改，需优先解除该锁定状态。

开启域名禁止转出阿里云

注册商是阿里云的域名，可以免费使用该服务。在开启域名禁止转出阿里云功能后，域名将被置为注册商禁止转移状态（clientTransferProhibited），避免您的域名被恶意转出阿里云。

如需索取域名转移密码，需要先取消该功能。

域名禁止转出阿里云详细信息，请参见禁止域名转出万网。

开启域名禁止更新锁

注册商是阿里云的域名，可以免费使用该服务。开启禁止更新锁后，可防止您的域名注册信息（域名联系人、电话、地址、传真、电子邮箱）、域名 DNS 服务器被恶意篡改。目前该服务支持*.com*、*.net*、*.org*、*.info*、*.biz*、*.mobi*、*.asia*、*.me*、*.so*、*.cc*、*.tv*、*.name*、*.tel*、*.cn*、.中国、.公司、.网络 等后缀。

禁止更新锁详细信息，请参见禁止更新锁。

填写真实的所有者信息

当域名发生归属权纠纷问题时，域名管理机构需要根据域名注册信息中的所有者信息认定归属权。所以，在填写域名注册信息时，需要认真填写与您本人（或本企业）的真实信息相匹配的信息。万一域名被盗，也可以提供相应的证明材料，有利于域名找回。

还可以在域名 基本管理 页面上传域名持有者的实名制资料加以保护。

如果您担心因为留存真实信息而被垃圾短信、垃圾邮件骚扰，可以开启域名隐私保护服务。

域名隐私保护服务详细信息，请参见域名隐私保护服务。

维护更新电子邮箱和手机号码

确保留存的会员账号、域名信息中的电子邮箱、手机号码都是您自己的并且可用。当电子邮箱、手机号码变更或注销时，记得及时更新。

确保域名信息中留存的邮箱是安全的。如果邮箱密码设置过于简单，往往会被轻易破解，从而丢失账号、丢失域名。所以，要尽量设置复杂的邮箱密码，比如大小写、标点符号、数字混用等方式，可提高密码的安全性。

严禁泄露会员账号、密码

不要将您的会员账号和密码告知任何人。如果您有专人代为管理域名，比如制作网站、设置解析等，那么您可以先开启域名禁止转出阿里云功能，然后启用域名密码。这样，域名管理员可以使用域名和域名密码登录单域名控制台，操作解析、DNS 修改等操作，但不能够进行域名持有者变更（过户）、转出阿里云、转移账号等操作。

域名密码详细信息，请参见修改域名管理密码。

2 使用禁止转出锁

禁止域名转出阿里云，保护您的域名不被恶意转出。如果您的域名注册商是阿里云，您可以随时在线自助设置 域名禁止转出阿里云。

域名状态，请单击 此处 查询。

设置禁止域名转出阿里云

1. 登录 阿里云域名控制台，在相应域名后面单击管理。
2. 单击上方的安全 > 安全设置 。在禁止域名转出阿里云后面的操作 开启/关闭禁止域名转出阿里云。
3. 选择验证方式：手机认证、阿里云 App 一键认证。

   以手机认证为例：单击获取验证码，输入刚刚发送到绑定手机号的验证码，单击确认。

设置项禁止域名转出阿里云成功开启后，右侧操作列下方状态显示为绿色。设置项禁止域名转出阿里云成功关闭后，右侧操作列下方状态显示为灰色。

3 使用注册局安全锁

注册局安全锁是目前最高等级的域名安全保护措施。

什么是注册局安全锁?

注册局安全锁是目前最高等级的域名安全保护措施，由注册局在根服务器层面操作，禁止域名被恶意转移、篡改及删除。注册局安全锁解锁需经过人工授权认证，确保域名的任何操作均通过授权认证人同意。

注册局安全锁与禁止转出锁有什么区别?

域名的安全保护分两个层级，注册局层级及注册商层级，域名禁止转出及禁止修改锁是阿里云为用户提供的注册商层面免费服务，能够在一定程度上保护域名安全，但是无法避免由于阿里云平台以外因素对域名安全造成的威胁。注册局安全锁从根服务器端加锁，由域名注册局提供，是更高层级的安全保障。

什么样的客户需要注册局安全锁?

建议运营以下网站的客户使用注册局安全锁：

- 重要程度较高的网站（如用于承接企业重要业务的网站、访问量大的网站、信息影响力大的网站）
- 对安全要求较高的网站（如银行、金融产品相关网站）
- 直接影响品牌形象的网站

注册局安全锁可用于哪些域名?

目前 Verisign 及 CNNIC 两个注册局可为旗下域名提供安全锁服务，涵盖域名后缀*.com*、*.net*、*.cc*、*.name*、*.tv*、*.cn*（含*.gov.cn*）和.中国。

如何购买注册局安全锁?

请确保满足以下购买条件：

- 注册局安全锁按年服务，加锁域名有效期应长于安全锁服务期。
- 按照 CNNIC 注册局要求，*.cn*和.中国域名需要在注册 5 天后方可加锁，且必须完成实名认证。
- 购买安全锁账号需要与域名账号相同。

您可以访问注册局安全锁产品页直接进行购买，或登录阿里云域名控制台在域名列表对应域名后选择购买。

注册局安全锁如何进行授权认证?

注册局安全锁的授权认证主要用于解锁指令验证，是保护您域名安全的一道重要防线，建议您在首次加锁成功后尽快完成授权认证。授权认证具体操作步骤如下：

1. 准备授权认证资料

   - 如果域名持有人为企业，您需要提供企业营业执照复印件、授权认证书以及被授权人身份证复印件，以上资料均需加盖企业公章。请点击下载授权委托书模板（企业域名）。
   - 如果域名持有人为个人，您需要提域名持有人身份证复印件、授权认证书以及被授权人身份证复印件，以上资料需域名持有人签字。请点击下载授权委托书模板（个人域名）。
   - 特殊情况：如果域名持有人本人作为安全锁解锁指令的操作者，则仅需提供身份证复印件，我们将默认您的域名信息邮箱为指令邮箱。

2. 上传授权资料

   请用加锁域名所属管理账号登录阿里云管理控制台，依次选择工单 > 提交工单 > 域名 > 注册局安全锁相关问题，然后创建工单，并以附件形式上传您的授权认证资料，完成后提交即可。我们将通过工单方式向您反馈审核结果。

注册局安全锁加锁及解锁申请

加锁及解锁的说明如下：

- 首次加锁。成功购买安全锁成功后，域名会上锁，无需指令操作。
- 非首次加锁。如果不是首次加锁，您需要通过授权认证书中确认的认证邮箱发送加锁指令至安全锁服务邮箱：saftylock@service.aliyun.com，指令内容示例如下：

  邮件主题：example.com 域名加锁申请

  邮件正文：请将我司如下域名加锁：

  example.com example.com example.cn
- 解除安全锁，您需要通过授权认证书中确认的认证邮箱发送解锁指令至安全锁服务邮箱：saftylock@service.aliyun.com，指令内容示例如下：

  邮件主题：example.com 域名解锁申请

  邮件正文：解锁域名 example.com

  解锁时间：20xx年xx月xx日

  恢复时间：20xx年xx月xx日

   说明:

- 安全锁走人工操作流程，预计需要2-3个工作日，请确保您的指令时间与解锁时间留出对应间隔，以免影响您的下一步操作。
- 解锁后域名处于无保护状态，为了保护您的域名，建议您解锁时告知我们恢复锁定时间，以免造成不必要的风险。
- 发送解锁指令前，请先确认您的域名已经完成授权认证，否则无法对域名进行解锁，请参阅注册局安全锁如何进行授权认证？。

4 使用阿云检测排查域名问题

自助排查工具阿云检测可以帮助您检测如下域名问题，并提供解决方案。

阿云检测 适用的域名后缀：.com、.net、.asia、.org、.info、.biz、.tel、.mobi、.name、.cc、.tv、.me、.so、.co、.hk、.cn。

目前不支持二级域名检测，主要支持顶级域名检测。

检测内容

域名检测

- 域名检测
- 域名输入合法性检测
- 域名服务商检测
- 域名到期日检测
- 域名状态检测

解析检测

- DNS 服务商检测
- DNS 设置检测
- A 记录设置检测
- 本机电脑 DNS 生效检测
- 全国各运营商 DNS 生效检测

网站访问检测

- 主机服务商检测
- HTTP 80 端口检测
- 备案检测

使用方法

进入 阿云检测，输入域名，单击 立即检测。

检测结果会显示以下方面的问题并提供解决方案：

- 解析生效问题

  已生效：代表用户本地电脑/用户当地运营商的访问探测结果。举例：客户在北京，使用自己的电脑访问该域名。如此字段的检测结果为已生效，表明用户本地的运营商的 Local DNS 已生效。

暂不支持：目前该工具不支持非阿里云 DNS 的检测。

暂不生效：代表用户本地的运营商的 Local DNS 未生效，需要等待。

暂无数据：这种报错可能为多种原因导致。代表全国各地运营商的 Local DNS 未能返回任何结果，可能为网络超时，也可能为当地 Local DNS 运营商问题。建议稍后进行检测。

- 全国各地运营商 DNS 生效情况

  单击 查看全国解析生效情况，可以查看到全国各地运营商的 DNS 解析生效情况。对于部分地区未生效的情况，需要联系当地运营商解决。

- HTTP 状态

  如果此字段，出现非错误码为 200 的报错，用户可以单击 查看详情，根据报错码来判断问题源。此部分调试多为客户的服务器、网站程序调试问题。如果是服务器配置问题，可以联系主机服务商。如果是网站程序问题，可以联系自己的建站服务商或者技术人员解决。

5 找回域名

如果在域名解析列表页添加域名时，发现域名已被其他账户添加。您可以通过以下步骤快速找回域名。

1. 登录 阿里云域名控制台，单击上方的 进入域名解析列表 > 添加域名。输入域名后，单击添加。

   下方出现域名已被其他账户添加的提示。单击提示消息中点击这里取回找回域名。
2. 登录域名持有者邮箱，单击验证邮件中的验证链接完成验证（注意检查您的垃圾箱，验证邮件有可能会被误认为垃圾邮件）。验证成功后，域名将自动添加至您的域名列表。

6 找回域名所在账号的登录名

登录阿里云账号后发现找不到域名，很有可能是查找的域名不在该账号下所致。您可参考本文找回域名所在账号的登录名，然后通过此登录名登录控制台，管理维护您的域名。

前提条件

找回域名所在账号的登录名前，您首先需要确认以下信息：

- 域名在有效期内。
- 域名的注册商是在阿里云。
- 域名没有因过期未及时续费，已经被其他人注册。

您可通过 *whois* 来查询域名当前状态。

操作步骤

确认域名状态正常后，找到域名所在账号步骤如下：

1. 进入 找回登录名 页面，选择 域名找回 页签。

   说明：

   找回登录名页面也可从阿里云官网上方的菜单支持与服务 > 帮助文档 > 自助工具中，单击找回账号登录名工具进入。

2. 输入域名，并拖动滑块操作验证。
3. 单击 立即找回。
4. 在弹出的页面中选择验证方式，单击 立即验证：
   - 通过 手机验证码
   - 通过 拍摄脸部
   - 通过 联系客服
5. 根据界面提示完成验证后，找回登录名。

绑定的手机或邮箱会收到阿里云发送的域名所在账号。通过找回的会员账号登录后，进入 阿里云域名控制台，便可找到相应的域名。

7 查看域名解析日志

如果域名解析被异常修改或删除，请通过日志情况判断是否由于账号信息被盗导致，建议您及时修改会员账号密码及域名密码。

查看域名解析被删除或修改的步骤：

1. 登录 阿里云域名控制台，单击相应域名后面的 管理。
2. 单击 域名解析 > 解析日志。在日志中可以查看操作时间、操作行为和操作者 IP。
3. 单击 安全 > 操作记录，在日志中可以查看操作行为、操作结果、操作时间、操作者 IP 和详情。

8 域名系统安全扩展（DNSSEC）配置

域名系统安全扩展（DNS Security Extensions，DNSSEC）是用于确定源域名可靠性的数字签名，通过添加DNSSEC记录到域名，可以增强对DNS域名服务器的身份认证，进而帮助防止DNS缓存污染等攻击。本文介绍如何在阿里云域名服务控制台上添加、同步DNSSEC记录。

DNSSEC设置限制

- 域名后缀类型：

  阿里云还未全面支持所有后缀类型域名的DNSSEC设置，目前支持.com/.net/.cc/.tv/.name/.info/.mobi/.pro/.xin/.biz/.club等域名的DNSESEC设置，不支持DNSSEC设置的域名在其控制台中无DNSSEC设置入口。实际支持情况以控制台左侧菜单显示为准。

- 域名解析渠道：

  使用非阿里云解析服务进行DNS解析的域名，可以按照如下步骤设置和查看DNSSEC。使用阿里云解析服务进行DNS解析的域名暂无法成功的进行DNSSSEC设置操作。

操作步骤

1. 登录 阿里云域名控制台，在相应域名后面单击 管理。
2. 在左侧导航栏的域名列表中，找到待配置的域名，在操作列单击管理。
3. 在弹出的页面中单击DNSSEC设置，进入DNSSEC设置页面。

   说明：
   不支持DNSSEC设置的域名，进入操作列表后，左侧无DNSSEC设置操作入口。

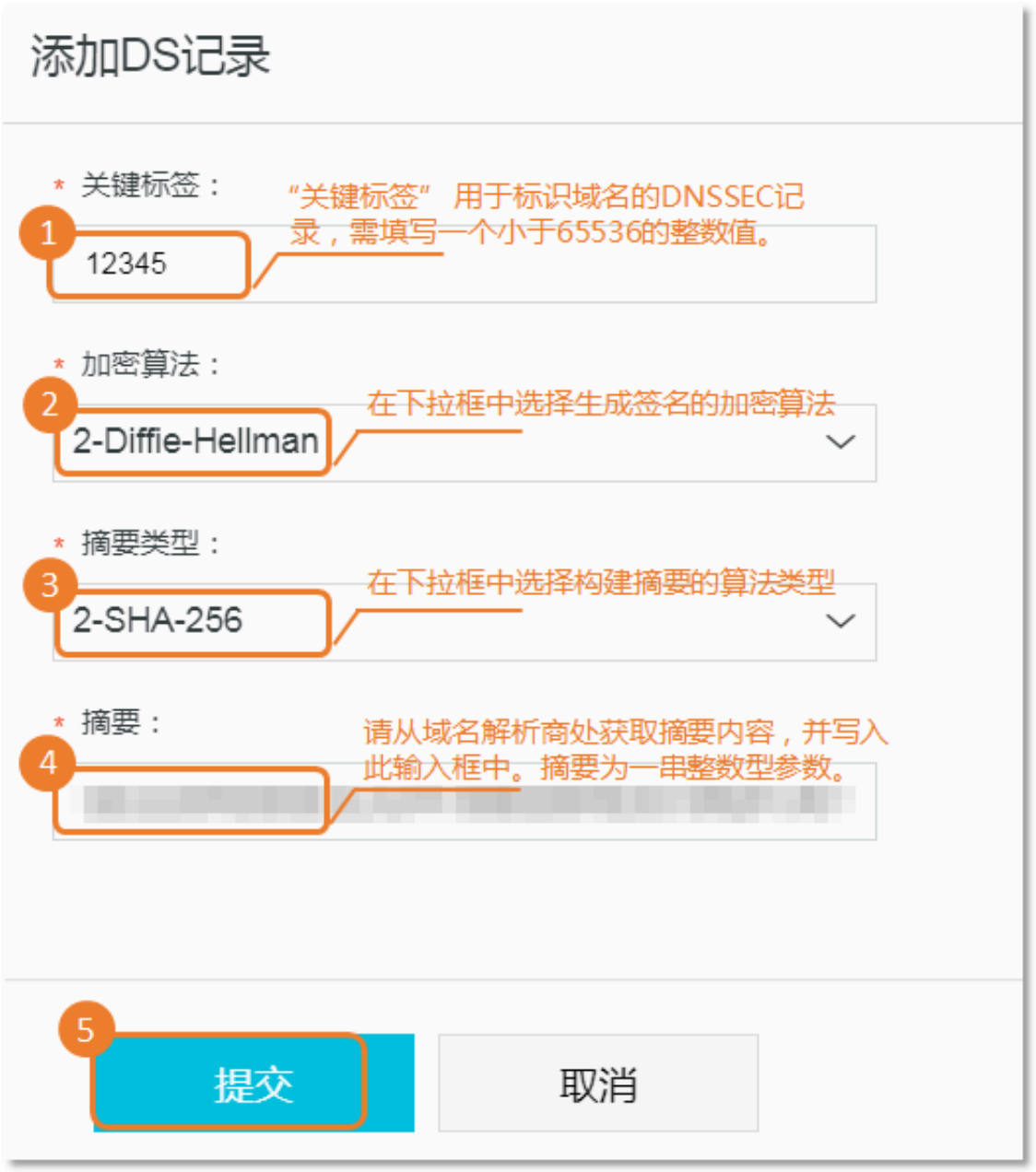
4. （可选）单击同步DS记录。

   如果此域名是从其他域名注册商转入阿里云，且在原注册商处添加过DNSSEC记录，可单击同步DS记录，将之前添加的DNSSEC记录同步至阿里云控制台。

5. 单击添加DS记录添加新的DNSSEC记录。

   说明：
   每个域名最多添加8条DNSSEC记录。

6. 在弹出的页面中填写参数信息，填写完成确认无误后单击提交。



7. 在弹出的窗口中单击获取验证码，收到验证码后填写人输入框中，完成短信的验证码安全验证。