

第1章 如何申请 AWS 免费 ACM

1.1 打开 ACM 控制台

登录 AWS 管理控制台，并通过以下网址打开 ACM 控制台：<https://console.aws.amazon.com/acm/home>

选择导入证书以导入现有证书而非请求新证书。[了解更多。](#)

导入证书

请求证书

选择您需要的证书类型，然后单击**请求证书**

- ☒ 请求公有证书

- 向 Amazon 请求公有证书。默认情况下，公有证书受到浏览器和操作系统信任。[了解更多](#)
- ☐ 请求私有证书

- 向贵组织的证书颁发机构请求私有证书。[了解更多](#)

1.2 选择请求公有证书

键入要使用 SSL/TLS 证书保护的站点的完全限定域名
(例如，`www.example.com`)。使用星号 (*) 创建通配符证书以保护同一域中的若干站点。
例如，`*example.com` 可保护 `www.example.com`、`site.example.com` 和 `images.example.com`。

请求证书

- 步骤 1：添加域名
- 步骤 2：选择验证方法
- 步骤 3：审核并请求
- 步骤 4：验证

当续订证书时，AWS Certificate Manager 将您证书中的域名记录到公有证书透明度 (CT) 日志中。您可以选择不记录 CT 日志。[了解更多](#)

您可以将 AWS Certificate Manager 证书与其他 [AWS 服务](#) 配合使用。

添加域名

键入要使用 SSL/TLS 证书保护的站点的完全限定域名 (例如，www.example.com)。使用星号 (*) 创建通配符证书以保护同一域中的若干站点。例如，*example.com 可

域名*

删除

com

com

✖

向此证书添加另一个名称

您可向此证书添加更多名称。例如，如果您为“www.example.com”请求证书，您可能需要添加名称“example.com”，以便让客户通过任一名称访问您的站点。[了解更多](#)。

*必须提供至少一个域名

1.3 选择验证方法

使用 DNS 验证比较方便，而且后期续订也方便

请求证书

- 步骤 1：添加域名
- 步骤 2：选择验证方法
- 步骤 3：审核并请求
- 步骤 4：验证

选择验证方法

选择 AWS Certificate Manager (ACM) 应如何验证您的证书请求。在颁发您的证书前，我们需要验证您对请求证书的域具有所有权或控制权。ACM 可以使用 DNS 验证所

☒ DNS 验证

对于您请求证书的域，如果您拥有修改 DNS 配置的权限，或能够获得此权限，请选择此选项。[了解更多](#)。

☐ 电子邮件验证

对于您请求证书的域，如果您没有修改 DNS 配置的权限，也无法获得此权限，请选择此选项。[了解更多](#)。

请求证书

步骤 1：添加域名

步骤 2：选择验证方法

步骤 3：审核并请求

步骤 4：验证

审核

在您请求证书后，将会向以下每个域名注册的所有者发送电子邮件。域所有者或授权代表可按照电子邮件正文中的说明进行操作，以验证域的控制和审批证书。验证完成后，证书将颁发给您的域名。

域名

要使用 SSL/TLS 证书保护的名称。

域名

其它域名

验证方法

AWS 为了验证您的证书请求所用的方法。

验证方法

DNS

点击 在 route53 中创建记录，就会自动配置到 route53 中

请求证书

步骤 1：添加域名

步骤 2：选择验证方法

步骤 3：审核并请求

步骤 4：验证

请求正在处理中

状态为“等待验证”的证书请求已创建。需要执行其它操作来完成证书的验证和审批。

验证

对于下列每个域，在 DNS 配置中创建一条 CNAME 记录。您必须先完成此步骤，AWS Certificate Manager (ACM) 才可以颁发证书，但您可以通过单击继续暂时跳过此步骤。

域

krn-mart.com

将以下 CNAME 记录添加到域的 DNS 配置中。添加 CNAME 记录的过程取决于您的 DNS 服务提供商。[了解更多。](#)

名称	类型	值
_b8ef	CNAME	

注意：更改 DNS 配置后，ACM 会对存在此 DNS 记录的域颁发证书。只要删除这条记录，您即可随时撤销权限。[了解更多。](#)

在 Route 53 中创建记录

Amazon Route 53 DNS 客户 ACM 可为您更新 DNS 配置。[了解更多。](#)

*.krn-mart.com

将以下 CNAME 记录添加到域的 DNS 配置中。添加 CNAME 记录的过程取决于您的 DNS 服务提供商。[了解更多。](#)

名称	类型	值
_b8ef	CNAME	

注意：更改 DNS 配置后，ACM 会对存在此 DNS 记录的域颁发证书。只要删除这条记录，您即可随时撤销权限。[了解更多。](#)

在 Route 53 中创建记录

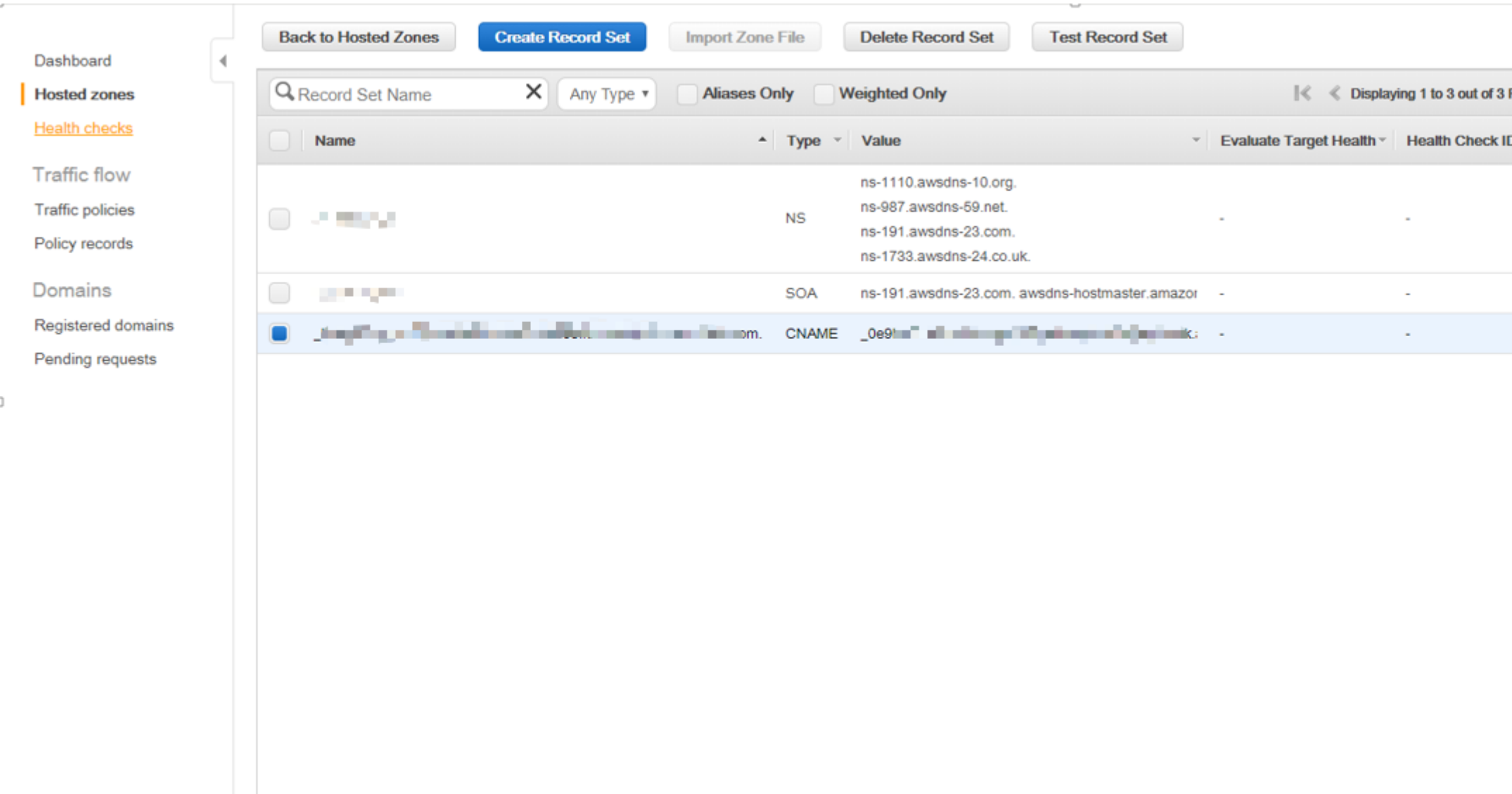
Amazon Route 53 DNS 客户 ACM 可为您更新 DNS 配置。[了解更多。](#)

将 DNS 配置导出为文件

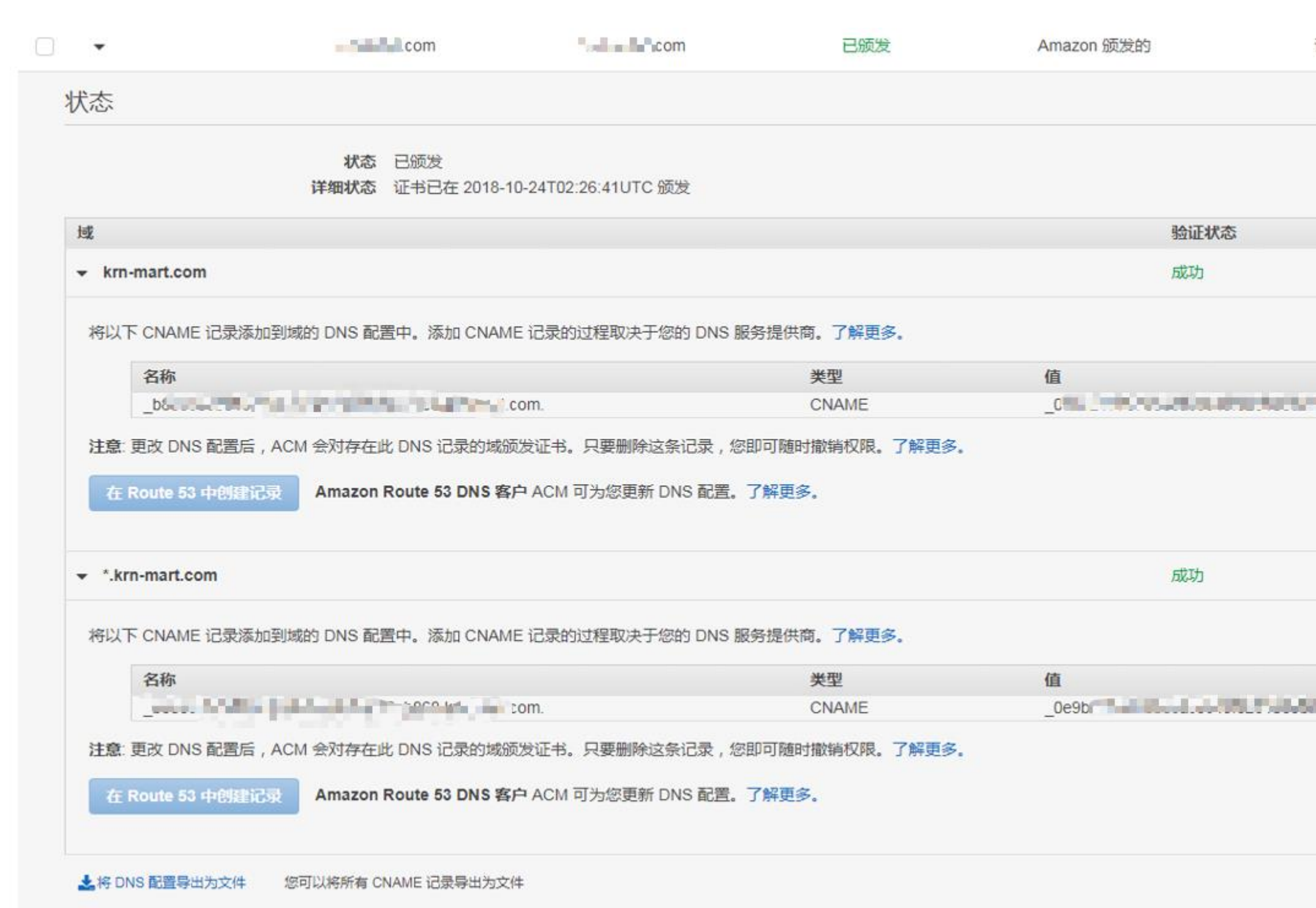
您可以将所有 CNAME 记录导出为文件

1.5 DNS 验证

配置后如下图显示



1.6 成功



<

侦听器

添加新侦听器。 每个 侦听器 必须包含一个该类型的操作转发, 重定向, 固定响应。

 talb | 添加侦听器

属于 Application Load Balancer 的侦听器将使用您配置的协议和端口检查连接请求。每个侦听器均必须包含一个默认操作以确保所有请求均被路由。理其他路由规则。 [了解更多信息](#)

协议:端口

选择用于从客户端到负载均衡器连接的协议，然后输入要从其中监听流量的端口号。

HTTPS

:

443

默认操作

指示此侦听器路由流量(未由其他规则路由)的方式。

1. 转发至...

server

+

添加操作

安全策略

ELBSecurityPolicy-TLS-1-2-Ext-2018-06

默认 SSL 证书

从 ACM 中(推荐)

17c0...59b40

[请求新的 ACM 证书](#)

侦听器使用它的配置协议和端口来检查连接请求，而负载均衡器使用侦听器规则，将请求路由到目标。您可以添加，移除或更新侦听器

添加侦听器

编辑

删除

	侦听器 ID	安全策略	SSL 证书
<input type="checkbox"/>	HTTP : 80 arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/amzn-elb-us-east-1-123456789012	不适用	不适用
<input type="checkbox"/>	HTTPS : 443 arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/amzn-elb-us-east-1-123456789012	ELBSecurityPolicy-TLS-1-2-Ext-2018-06	默认: 17c04e2c-...74d59b40 (A 查看/编辑证书

