适用于政府采购官员的 DNS 采购指南

ICANN 首席技术官办公室

大卫 • 休伯曼 (David Huberman)
OCTO-013
2020 年 7 月 24 日

ICANN

目录

本文档是首席技术官办公室 (OCTO) 文档系列的一部分。请参阅 OCTO 文档页面，以了解该系列的文档列表。关于这些文档，如果您有任何问题或建议，请将您的反馈发送至 octo@icann.org。

1 简介

本指南旨在帮助政府采购官员做出明智的域名及域名系统 (DNS) 采购选择，进而确保政府网络中各项服务和主机的命名安全、稳定，且富有弹性。使用本指南并不要求您具备 DNS 方面的专业知识。为了便于您与您的信息技术 (IT) 部门以及供应商合作，本指南采用易于理解的语言编写。

本文档由互联网名称与数字地址分配机构 (Internet Corporation for Assigned Names and Numbers, ICANN) 负责发布。ICANN 是一个代表互联网社群的非营利公益型组织，负责监督互联网顶级 DNS 的技术协调，以此来保证 DNS 的安全、稳定与弹性。

本指南提出了一些不错的运营技术和做法建议。尽管并非所有供应商都提供我们列出的每项服务或技术，但是为了有助于您在充分知情的基础上制定采购决策，您应当清楚在我们推荐的技术中，供应商支持和不支持哪些技术。

本指南重点介绍获取域名并将之投入运营的三个阶段：

- 选取域名
- 注册域名
- DNS 运营：托管您的域名

2 选取域名

域名以后缀作为结尾。有关这些后缀的示例包括：*.com*、*.gov*、*.uk* 和 *.asia*。DNS 中有 1300 多个这样的后缀，它们被称为“顶级域”（也就是 *TLD*）。选取域名时，您应当首先确定要使用的 TLD：选择一个称为通用顶级域 (*gTLD*) 的通用名称（类似“.com”或“.asia”这样具有通用含义的后缀），或者选择由代表公认的地区的两个字母构成的国家和地区顶级域（称为 *ccTLD*，类似这样的后缀包括：*.fr* 代表法国，*.za* 代表南非，这里的每个后缀都与 ISO-3166-2 标准中列出的地区代码相对应）。[1]

在许多情况下，为了遵循既定的当地规则和政策，政府机构可能需要在其国家的 ccTLD 基础上使用域名（例如，*go.jp* 代表日本的政府机构）。不同政府会采用不同方式来运营其 ccTLD。我们建议您与政府的域名服务运营商沟通，询问有关政策并核实每项政策的功能、安全特性和业务连续性计划（如下所述），以便您可以将这些政策与任何其他适用的 TLD 方案进行比较。每个 TLD（包括每个 ccTLD）经理的联系信息，均发布在位于 https://www.iana.org/domains/root/db 的目录中（要获得联系信息，您需要点击相应 TLD 的链接）。

ICANN 与每个 gTLD 的运营商都签署了一份合同，其中明确列出了多项规则。具体来说，gTLD 运营商必须遵守与 ICANN 签署的注册管理机构协议中规定的条款和条件。[2]这些条款和条件对

[1] 有关 ISO-3166-2 标准的更多信息，请参阅 https://www.iso.org/iso-3166-country-codes.html。ICANN 不负责分配 ISO-3166 代码；分配代码是 ISO-3166 维护机构的职责。

[2] ICANN 有多个版本的注册管理机构协议，不同的 TLD 需签署不同版本的协议。最新版本为“2017 年注册管理机构基本协议”，您可在以下地址找到该协议：
https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html

gTLD 经理提出了具体的技术和政策要求，以期改善 DNS 生态系统的健康状况并保护域名持有人。相比之下，ccTLD 运营商没有与 ICANN 签署协议。域名持有人可能需要的任何法律补救措施可能取决于 ccTLD 注册管理机构所属的法律管辖区。

无论您是注册 ccTLD 还是 gTLD，TLD 都应该具备四项重要特征：支持 DNSSEC，支持 IPv6，实施某种形式的注册管理机构锁定，以及 TLD 具有良好的信誉。

2.1 DNSSEC 支持

如果域名所有者（即，您的组织）对域名采取了加密签名处理，那么用户将会因此而获得更好的保护。您的组织可通过称作“域名系统安全扩展”(Domain Name System Security Extensions, DNSSEC) 的技术对域名实施数字签名。有关 DNSSEC 为何如此重要的更多信息，请参阅 ICANN 的文档“DNSSEC：保护 DNS 的安全”。[3]

要对域名进行签名，您选取的 TLD 需支持 *DNSSEC 签名*。值得庆幸的是，大多数 TLD（包括所有 gTLD）都支持 DNSSEC。但是，如果您选择的 TLD 运营商不具备 DNSSEC 支持选项，那么您应该询问他们当前或未来的支持计划。诚然，了解 TLD 对 DNSSEC 的支持情况并不总是那么简单。有些 TLD 运营商会在他们的网站上发布相关信息；有些则不会发布。您或许可以通过在网上搜索来查找相关信息，或者，您甚至需要发送电子邮件或打电话来咨询相关事宜。

2.2 IPv6 支持

互联网上的计算机使用互联网协议 (IP) 地址来彼此识别。目前有两种类型的 IP 地址：IPv4 和 IPv6。IPv4 地址是最常见的 IP 地址类型。IPv6 是一种新型 IP 地址，旨在随着越来越多的计算机不断加入网络而帮助互联网继续扩展。

由于有些政府要求互联网基础设施同时支持 IPv4 和 IPv6 寻址功能，为此，请与 TLD 运营商核实，以确保您的 DNS 服务器同时支持 IPv4 和 IPv6 地址。具体来说，TLD 运营商需要支持您构建具备 IPv6 地址功能的权威域名服务器。如果在这种情况下您的 TLD 运营商不支持 IPv6，那么您域中的站点就如同信息孤岛，失去了与世界互连的机会。

2.3 注册管理机构锁定

选取 TLD 时，另一个值得重点考虑的因素是询问 TLD 运营商是否支持所谓的*注册管理机构锁定*功能。

TLD 运营商管理着“注册管理机构”，该机构包含 TLD 中的所有二级域（例如，example.tld）。[4]注册管理机构锁定允许域名所有者（即“注册人”）让 TLD 运营商“锁定”域名，就像锁上车门一样。您的域名被锁定后，任何人都不能对该域名进行更改、删除，或将其转让给其他注册人，除非您已经与 TLD 运营商确定了某种授权流程。但是请注意，关于具体怎样实

[3] 请参阅 https://www.icann.org/en/system/files/files/octo-006-en.pdf
[4] 令人困惑的是，TLD 运营商也可以称为注册管理机构

施注册管理机构锁定，业内尚无标准，所以您应该询问 TLD 运营商是否提供注册管理机构锁定服务，如果提供，如何运作。

总之，我们认为处理授权变更的最佳办法是“带外”授权，这种授权方法要求所有各方均不依赖以互联网为中心的通信方式，而是依靠电话或其他令攻击者难以侵入的方式沟通。由于只有在极少数情况下才需要变更域名的基本特征，所以采用类似“带外”授权这种较慢的处理方法，应该是可以接受的。但是与此同时，一种明智的做法是，确保让您的 TLD 运营商提供一份内容清晰的书面升级流程，以防在紧急情况下某些 DNS 数据需要更改（尽管这种情况比较少见）。

我们强烈鼓励所有注册人都使用支持注册管理机构锁定的 TLD，因为这样可以防止那些危及整个域的已知攻击。

2.4 信誉

最后，在您选取 TLD 之前，应考虑对它的信誉进行调查。根据反滥用公司 Spamhaus [5]的经验，如果在一个 TLD 中注册的许多域名都与垃圾邮件和恶意软件传播等活动有关，那么这个 TLD 的信誉就会很差。尽管每个 TLD 中都难免会注册一些恶意域名，但是像 Spamhaus 这样的公司会衡量整个 TLD 域名组合的情况，以此来判断 TLD 的信誉是否良好。

选取一个没有大量恶意注册域名的 TLD 至关重要。如果某个 TLD 在技术社群中信誉不佳，可能会被互联网服务提供商 (ISP) 和企业网络运营商拦截。例如，如果您使用的 TLD 信誉不佳，您可能无法使用您的域发送电子邮件，因为许多邮件服务器会自动配置为拦截来自拦截清单上的域的电子邮件。

许多反滥用公司（包括 Spamhaus 和 SURBL）会公布 TLD 信誉排名。[6]

3 选取域名注册服务机构

您在为机构选取 TLD 之后，接下来就要在其中注册域名。您可以直接通过 TLD 运营商在一些 ccTLD 中注册域名。然而，对于许多 ccTLD 和大多数 gTLD 来说，您需要通过一个域名“注册服务机构”[7]来注册域名。在这一部分中，我们列出了一些标准，建议您在选择可能的域名注册服务机构时参考这些标准。

5 请参阅 https://www.spamhaus.org/
6 请访问 http://www.surbl.org/
7 您可以将注册管理机构/注册服务机构之间的关系看作类似于批发/零售之间的关系，也就是说，就像人们从零售商那里购买商品，而零售商又从批发商那里进货一样；注册人从注册服务机构那里购买域名，而注册服务机构又从注册管理机构那里获取存货。

3.1 认证

ICANN 可以为注册服务机构提供官方认证。如果成功获得并保持认证，则意味着该注册服务机构已证明其符合从事注册服务机构业务所需满足的各项技术、运营和财务标准要求。[8]重要的是，注册服务机构必须遵守《注册服务机构认证协议》[9]中列出的条款和条件，其中包括对域名注册人的多项保护措施。

如果您要在 gTLD 中注册域名，请确保选取 ICANN 认证注册服务机构。ICANN 网站上列出了经过认证的注册服务机构名单。[10]此外，根据注册服务机构与 ICANN 签署的协议，还允许注册服务机构与“分销商”合作，“分销商”是代表注册服务机构提供域名注册服务的第三方公司。但是，对于高价值域名，我们建议在可能的情况下直接与经过认证的注册服务机构合作，因为如果需要解决紧急问题，这样可以减少相关方的数量。

如果您要在 ccTLD 中注册域名，请确保您选用的是 ccTLD 注册管理机构授权的注册服务机构或分销商。

3.2 基本安全功能

您选择的任何域名注册服务机构都应该支持强密码（通常是一个长字符串，由一个大写字母、一个小写字母和至少一个符号组合而成），并且应该为登录其帐户门户的用户提供多重要素验证（即，要求输入密码，外加使用某种安全令牌，通常是发送到手机上的短信 (SMS) 代码）。

另外，您还应该向您即将选用的注册服务机构或分销商核实，客户帐户门户是运行在使用 HTTPS 协议进行通信加密的网站上。这有助于确保您的 IT 人员与注册服务机构/分销商之间的电子通信具有保密性。

3.3 DNSSEC 支持

如果您已经着手要确保您的注册管理机构支持 DNSSEC，那么选取一个允许您提供必要 DNSSEC 相关信息的注册服务机构至关重要，如果您不是直接管理您的区域，请对您的区域进行 DNSSEC 签名。通常，注册服务机构应该在其网站上公布他们支持的 DNSSEC 服务。您可能还需要让您的技术人员与注册服务机构讨论应提供的 DNSSEC 支持级别，以确保满足您的技术要求。

3.4 IPv6 支持

域名注册服务机构必须支持同时使用 IPv4 和 IPv6 地址，也就是说，允许您管理要在域名中命名的所有设备的地址（“A”和“AAAA”）资源记录。

8 您可在以下位置找到有关认证资格的说明：https://www.icann.org/resources/pages/policy-statement-2012-02-25-zh#IIA
9 最新版《注册服务机构认证协议》位于以下位置：https://www.icann.org/resources/pages/registrars/registrars-en
10 请参阅 https://www.icann.org/registrar-reports/accreditation-qualified-list.html

3.5 导出数据

从长远考虑，您并不希望永远都使用一家域名注册服务机构。您的技术需求可能会变化，或者注册服务机构的服务质量可能会下降，亦或是将来可能会发生其他情况，这些因素都会促使您将域名转移到不同的注册服务机构。为此，如果注册服务机构允许您“导出您的区域数据”，也就是说，允许您下载与您的域名关联的所有 DNS 数据，这将会非常有帮助。这样您就可以控制您的域名的 DNS 数据，并允许 IT 人员快速将服务转移到新的注册服务机构。

3.6 信誉

您选择的任何域名注册服务机构都应具备良好的反滥用信誉，并且具有可靠的跟踪记录，能够证明在接到 DNS 滥用举报时，可以配合国家和国际执法机构的工作。例如，您应该确保注册服务机构正在运行一个功能强大的反欺诈程序，可以检测并阻止那些涉及使用被盗信用卡信息的域名注册。

4 DNS 运营：第三方托管您的域名

注册域名后，您需要将域名托管在某个位置。域名可以由您的政府 IT 部门托管，或者，您甚至有必要选择第三方供应商，以便将域名托管到他们的数据中心。当您从 IT 提供商处购买一揽子服务时，其中可能包含托管服务。这部分重点介绍如何帮助您选择第三方供应商，并围绕我们认为重要的一些方面为您提出相关建议。

4.1 域名管理

能够快速、轻松地创建子域，这是非常重要的。子域是一种看起来像 *mail.department.za* 或 *elections.government.co.jp* 或类似名称的域名。您应该向第三方供应商询问创建、修改以及删除子域的难易程度，尤其是针对批量处理的情况。同样重要的是，您应当能够创建现代类型的 DNS 记录，例如，传输层安全协议验证 (TLSA) 记录类型，这是一项名为“基于 DNS 的名称实体验证”(DANE) 的安全技术使用的记录类型。

4.2 运营安全

购买 DNS 服务时，安全是考虑事项的重中之重。您的组织必须始终*保持*对所有托管域名及服务的*控制*，这一点至关重要。保持这种控制的最佳方法是始终与各种供应商合作 - 上至域名注册服务机构，下至所有的 IT 提供商 - 他们拥有深厚的安全文化底蕴，致力于安全事业。如果您失去对 DNS 技术中任何一部分的控制，那么攻击很快就会趁虚而入，并且可能会发生数据外泄。

对于第三方托管提供商，我们注意到以下三个安全要素是确保高度安全的关键所在：

- 他们必须在帐户登录环节设置多重要素验证。如果只通过提供一个要素（例如，密码）就可以访问相关技术，这样的验证机制势必不安全。

- 提供商应采取已公布的综合性安全惯例和政策。
- 此外，提供商还应对基础设施要素和 DNS 数据实施周密的安全监控。这种监控应定期执行，以确保能够快速发现攻击者实施的任何更改。检测到异常活动时，提供商应该有一套现行的升级警报体系来通知技术人员。

常规做法是，还要询问针对 *BCP 38*[11] 的支持情况。“BCP 38”是一份文档，其中规定了为减少互联网上网络路由欺诈的数量，提供商应遵循的运营惯例。所有网络提供商都应支持 BCP 38。有些例外情况可能会造成无法遵循 BCP 38，但是在典型的域名托管组织环境中，这种情况很少见，如果出现这种情况，您应要求提供详细的理由依据。

4.3 权威域名服务

权威域名服务指的是您告知世界：您的域名如何解析为特定的 IP 地址，您选用哪个邮件服务器来接收邮件，您的组织如何布局命名空间等等。无论您是要设立自己的权威域名服务器，还是付费请第三方供应商代表您托管权威域名服务器，以下注意事项需要牢记心间：

- 最佳做法是：在不同地域且选用不同网络拓扑结构的网络上，分别设立多个不同的权威域名服务器。
- 确保托管服务的所有域名服务器完全支持 DNSSEC，包括将 DNSKEY 和/或签署授权 (DS) 记录上传到您的域名注册服务机构。
- 确保能够较好地支持大规模添加、修改或删除 DNS 数据（包括资源记录和子域）。
- 了解用来防范分布式拒绝服务攻击的措施，无论您是决定自行运营域名服务器，还是与第三方提供商共同设置域名服务器。

4.4 IPv6 支持

第三方托管供应商应当在其软件和服务中支持 IPv6，这一点正变得日益关键。地区互联网注册管理机构 (RIR) 是 IP 地址的顶级分配机构，他们制作了大量资料，面对各种利用 IP 地址的服务，这些资料可帮助您制定出明智的采购决策。这些 RIR 机构包括：

- 非洲网络信息中心 (AFRINIC)，这是面向非洲设立的 RIR，该机构为政府提供了 IPv6 指南手册。[12]
- 美洲互联网号码注册管理机构 (ARIN)，这是面向北美和加勒比海部分地区设立的 RIR，该机构制作了一个 6 分钟的视频，阐述了 IPv6 的概念以及 IPv6 之所以重要的原因。[13]
- 拉丁美洲和加勒比海地区互联网地址注册管理机构 (LACNIC)，这是面向拉丁美洲设立的 RIR，该机构为政府和企业发布了一个包含 12 项步骤的 IPv6 部署指南。[14]
- 欧洲网络协调中心 (RIPE NCC)，这是面向欧洲和西亚部分地区设立的 RIR，该机构发布了一份关于信息和通信技术 (ICT) 设备的 IPv6 要求指南。[15]

11 请参阅 https://datatracker.ietf.org/doc/bcp38/
12 请参阅 https://afrinic.net/guidebook-gov-ipv6
13 请参阅 https://youtu.be/bkLs5_geTM4
14 请参阅 https://www.lacnic.net/innovaportal/file/3635/1/10-12-steps-government-ipv6-v3.pdf
15 请参阅 https://www.ripe.net/publications/docs/ripe-554

5 总结

我们在本指南中涵盖了大量资料。再次重申一下，我们在此列出的所有我们认为重要的服务，并非所有供应商都能提供。但是，我们希望传达的最重要信息是：

- 安全是重中之重，它不仅仅是一个精心选择的密码。
- 支持 DNSSEC 并且支持 IPv6 应该是一项基本要求。
- 与您合作的公司应当致力于在减少滥用和处理滥用投诉方面，维护良好的信誉。

附录：采购检查清单

选取 TLD 注册管理机构

- ❑ 支持 DNSSEC
  在这个 TLD 中注册的域名可以经过 DNSSEC 签名
- ❑ 支持 IPv4 和 IPv6
  TLD 的域名服务器记录可同时使用 IPv4 和 IPv6 地址发出
- ❑ 提供注册管理机构锁定
  拥有锁定记录的流程，且要求采用“带外”授权才能对锁定的记录进行更改
- ❑ 信誉良好
  TLD 积极抵制滥用在 TLD 中注册的域名的行为

选取域名注册服务机构

- ❑ 是经过认证或授权的注册服务机构
  如果是 gTLD，则需要获得 ICANN 的认证；如果是 ccTLD，则需要获得提供域名的授权
- ❑ 践行良好的网络卫生
  要求针对用户帐户登录采用多重要素验证，并且要求网页使用 HTTPS 协议
- ❑ 支持 DNSSEC
  域名可以经过 DNSSEC 签名
- ❑ 允许第三方托管域名
  仅支持域名注册，但不强制您将域名托管在他们的网络服务器上
- ❑ 允许导出数据
  您的 IT 人员可以导出 DNS 数据，以便您能够轻松地将域名转移到新的注册服务机构
- ❑ 支持 IPv4 地址和 IPv6 地址
  域名服务器记录可同时使用 IPv4 和 IPv6 地址发出
- ❑ 信誉良好
  积极预防、检测并减少滥用，并对投诉做出回应

选取第三方托管提供商

- ❑ 支持批量子域管理和现代的 DNS 记录类型
  可以批量添加、修改或删除子域，并且可以添加像 TLSA 这样的资源记录
- ❑ 实施安全运营
  针对用户登录环节实施多重要素验证、发布安全惯例和政策、主动监控 DNS 数据，并且支持 BCP 38
- ❑ 支持权威的 DNS 服务
  在不同的地理位置部署域名服务器，采取良好的防控攻击措施等
- ❑ 支持 IPv4 地址和 IPv6 地址
  访问提供商的服务器和域名服务器更新时，同时支持 IPv4 地址和 IPv6 地址