2013 年 10 月 21 日

集中化域资料服务 (CZDS)

常见问题解答

在 ICANN 第 47 届德班会议期间，工作人员就集中化域资料服务（当时被称为 CZDAP）发表了演讲，该服务是数百个新通用顶级域被添加到互联网时 ICANN 为调整域资料提供方式而制定的解决方案。我们在会议期间收到了一些问题，但鉴于时间有限未能当场给予解答。下文将为您提供这些问题以及其他各种与 CZDS 相关问题的解答。若要了解其他问题与解答，请访问帮助页面：https://czds.icann.org/en/help。

最终用户

问：用户可以更改用于访问的 IP 地址吗？

答：可以，您可在用户配置文件中找到一个或多个用于访问 SFTP 服务器的 IP 地址。

问：如果一名最终用户拥有多个 TLD（如 1400 个）的访问权限，那么该用户需要单独下载每个数据文件吗？

答：不需要，我们创建了 CZDS API，这是一个基于令牌的系统，允许批量下载 SFTP 凭据。该令牌可为用户提供自动访问功能，用户无需手动登录即可获取新的域资料。如果检测到滥用情况，令牌将作废（由 CZDS 管理员操作，或由注册管理运行机构自行操作），那么所有脚本均将无法再执行下载，直至为脚本配置新的、有效的用户令牌。

我们创建了用于批量下载 SFTP 凭据的工具。有关此工具的所有信息，请访问以下公开资源库：

https://github.com/fourkitchens/CZDS-tools

问：最好能有一个综合下载页面，上面显示我们具有访问权限的所有文件，而无需逐个访问单个页面。最好能有一个页面，上面列出我们具有访问权限的所有 TLD，并随附相关元数据。例如，可在 FTP 上显示注册管理机构上次更新信息的时间以及其他信息。最好能设置一个我们可以看到所有相关信息的 FTP 帐户。

答：目前还未提供该功能。

问：是否可提供某些历史数据（例如，上周或前四周的数据）？

答：此系统不提供该功能。

问：我可以对注册管理机构的否决决定提出投诉吗？

答：《注册管理机构协议》规定，通用顶级域注册管理机构应免费为数据消费者提供域资料。如果最终用户认为注册管理机构不公正地拒绝了其访问请求或一直未获得机构的回应，则该用户可以向 ICANN 合规部门投诉，我们将派人联系该机构并展开调查。

注册管理运行机构

问：新通用顶级域注册管理机构应在何时开始提供其域资料？是在合同签署时、技术授权时，还是尚未明确该时间？

答：按规定，新通用顶级域注册管理机构应在技术授权时提供域资料。

问：注册管理机构如何将域资料传输至 CZDS 系统？通过 FTP 上传还是域传输？

答：有两个选择 — 注册管理运行机构可以保留资料控制权，仅批准用户访问并为其（通过 CZDS）提供 SFTP 服务器的访问凭据；或者注册管理运行机构可以让 ICANN 进行定期的域传输 (AXFR) 并代其配置资料，这样用户便可直接通过 CZDS 系统下载。

问：如果注册管理运行机构不希望用户通过集中化域资料服务系统直接下载，而选择通过自己的系统为用户提供域访问权限，流程应如何？

答：注册管理运行机构必须选择“SFTP 凭据”作为其下载方式。最终用户提出请求后，注册管理运行机构将批准请求并为该用户提供其 SFTP 服务器名称和登录凭据。然后，最终用户必须在 CZDS 中输入机构为其提供的用户名和密码，方可通过指定的主机获取资料。

存储凭据前，CZDS 网站将使用每位用户的公共密钥对凭据进行加密。

问：注册管理运行机构如何将域文件传输至 CZDS？文件是否应以未压缩的形式通过 API 发送？

答：注册管理运行机构应向 CZDS 管理员提供其 TSIG 密钥和服务器地址，和/或允许从指定的 ICANN IP 地址列表进行传输 (AXFR)。ICANN 将执行传输并将资料转换为指定格式，以便最终用户通过 CZDS 直接下载。

问：新通用顶级域注册管理机构必须向系统提供域资料吗？

答：是的。根据通用顶级域《注册管理机构协议》第 2 节规定 4，新通用顶级域注册管理机构必须向提出请求的最终用户提供域资料。按规定，其也必须使用 CZDS。要符合上述要求，有两种方法可供选择：让 ICANN 进行域资料传输；或者提供其 SFTP 服务器名称和凭据，以便最终用户从 CZDS 以外的系统获取资料。

问：作为未来的注册管理机构，我可以自动批准全部请求吗？

答：选择所有请求，然后单击批准即可一次性批量批准全部请求，但现在您还无法默认“预批准”全部请求。ICANN 将考虑在之后的版本中添加此自动批准功能。

问：注册管理运行机构如何知道有待批准或否决的请求？

答：注册管理运行机构可打开或关闭电子邮件通知功能。打开此功能即可在每次有新请求时收到通知；但如果通知量过大，也可关闭此功能。关闭此功能后，注册管理运行机构则需要定期登录系统查看是否有新请求。

问：如果注册管理运行机构必须在签署《注册管理机构协议》前发布域文件，那么默认使用“批准”功能不是更好吗？

答：确切地说，新的注册管理运行机构不能在签订《注册管理机构协议》*前*提供域资料，而必须在签订*后*、技术授权时才可提供。现在尚不支持自动预批准功能。

问：我不想每天登录进行批准，最好能预批准或自动批准全部请求。

答：注册管理运行机构不必每天登录进行批准，但是有责任验证最终用户的的请求。24 小时规则是指注册管理运行机构必须每 24 小时上传一次域资料，此操作可自动执行。

问：对于响应请求的时间是否有规定？ICANN 合规部门会就此进行检查吗？

答：我们并未明确规定响应时间，但希望注册管理机构能够在合理的时间内给予响应。ICANN 合同合规部门将进行监管，以便为用户提供域资料访问权限。

问：注册管理运行机构必须批准每个域资料访问请求吗？例如，如果 .veryprivate 并未同意分享此资料，那么它能默认否决所有请求吗？

答：新通用顶级域《注册管理机构协议》要求注册管理机构为用户提供其域文件的访问权限。在某些情况下他们可以否决请求。若要了解注册管理运行机构在哪些情况下可否决域文件访问请求，请参考《注册管理机构协议》。

问：如果最终用户多次请求访问资料，且注册管理运行机构已对这些请求进行过一次或多次审查和批准，那么注册管理运行机构是否可以批量批准该用户的所有其他请求？

答：注册管理运行机构必须对用户的每个 TLD 请求进行批准。每次批准至少 90 天内有效，注册管理机构也可选择更长时间。

问：如果*未*对域资料的访问请求进行批准，是否会受到任何惩罚？

答：请参考您的《注册管理机构协议》获取相关信息。

问：如果注册管理运行机构管理多个 TLD，需要多少个帐户（拥有一些列登录凭据）才能管理针对所有 TLD 的域资料访问请求？

答：在我们出台其他政策前，CZDS 上的帐户仅能代表一家注册管理运行机构。一个帐户可以管理多个 TLD。CZDS 可授权注册管理运行机构用户和超级管理员，让其代表所有与分配的注册管理机构相关联的 TLD 签署条款和条件。每个“超级管理员”的具体权限取决于每家注册管理机构的业务决策。例如，一家注册管理运行机构可以根据 TLD 数量的多少，分配一名或多名注册管理运行机构用户管理多个 TLD 的域资料访问权限。

问：注册管理运行机构的联系人可以不止一个吗？

答：可以，超级管理员功能允许注册管理运行机构指定/添加其他注册管理运行机构用户来管理其 TLD。超级管理员必须确认所有被指定的注册管理运行机构都有权代表注册管理机构签署相关条款和条件。

问：如果有多家注册管理机构，一个注册管理运行机构是否可登录并查看随附的所有信息，还是将有多个登录名？

答：一个注册管理运行机构用户与一个注册管理机构相关联后，使用一个登录名即可查看其管理的全部 TLD 请求。

问：如果我指定某人为超级管理员，那我如何审查他们的操作？例如，我有 5 家注册管理机构，我登录后指定我的管理员担任这 5 家注册管理机构的超级管理员角色，如果他们点击“全部批准”后离职了，我该怎么办？

答：如果指定的注册管理运行机构用户离开了公司，则超级管理员可将其降级为最终用户，而不是注册管理运行机构用户。他们不能再批准任何请求，但是他们此前批准的所有事项在条款和条件过期前均有效。如果您不希望批准所有请求，则可以撤销一条或多条甚至所有请求，这样最终用户必须登录重新请求访问权限。

问：是否计划构建沙盒 — 兼具 SFTP 版本以及 HTTP 版本？

答：暂无构建沙盒的计划。注册管理机构可在 CZDS 管理员的配合下正确进行系统设置，并测试其域文件传输。注册管理运行机构开始批准最终用户请求前，ICANN 将帮助确保一切正常运行。

问：条款和条件会否取代域文件访问协议？

答：是的，条款和条件的内容实际上直接取自当前域文件协议。

问：我们可以向注册管理机构一样创建我们自己的条款和条件吗？如果可以，我们是否需要针对每一个 TLD 创建不同版本的条款和条件？

答：根据新通用顶级域《注册管理机构协议》第 2.1.1 节规定 4，域文件访问协议“将由集中化域资料访问提供商制定标准、推动执行和进行管理。”

问：如果注册管理机构检测到用户滥用，将会以何种流程通知 ICANN？

答：如果用户违反了其与注册管理运行机构之间的访问协议，则注册管理运行机构可撤销用户的访问权限。有关 CZDS 系统的任何疑问或反馈，请发送电子邮件至 CZDS@icann.org。

安全性

问：“CZDS 如何使用公共密钥加密？”初始下载密钥有何用处？该资料采用 ASCII 编码且可读，为什么还需要解密？为什么不使用其他方式，如 HTTPS？

答：HTTPS 可有效保护信息的机密性，若使用这种方式，访问凭据传输至域文件服务器，即从服务器到客户端，仅涉及两方。但 CZDS 涉及三方：注册管理运行机构、域文件用户和作为中间方的 CZDS 运营商。使用 HTTPS 只能保护两方之间传递的信息，并非涉及中间方的整个通信链。通过使用公共密钥加密，我们可以确保信息从注册管理运行机构传输至域文件用户的私密性。CZDS 运营商（中间方）将无法访问凭据。

CZDS 网站将生成一对 2048 位 RSA 密钥（非 PGP）。私人密钥和公共密钥均由 CZDS 网站服务器生成。私人密钥使用 HTTPS 通过网络线缆传输，因此用户可以进行下载，密钥随后将被销毁，不会写入磁盘、浏览器会话或任何可以存储数据的机制。公共密钥与其他配置文件数据共同存储于 CZDS 网站。解密 SFTP 凭据必须使用这对密钥（私人密钥由每位用户自行保存，公共密钥则存储于 CZDS 网站）。我们不使用 HTTPS 是为了防止凭据泄露给第三方。

CZDS 将生成一对私人/公共密钥。*公共*密钥留在服务器中（类似于服务器中的 SSH 密钥），并且我们不打算公开此公共密钥，但即使被公诸于世，对安全性的影响也不大。因此我们将其存储于数据库中。同时，在这对密钥生成后，*私人*密钥将一次性被发送给用户（与包含密钥下载说明的网页一起发送）。用户应下载此私人密钥并妥善保存。当用户浏览包含密钥的网页时，我们将在网页上用非常显眼的信息提示用户妥善保存密钥。

如果用户未下载密钥便离开了此网页，那么其将无法解密凭据。这时，他们需要生成一对新的私人/公共密钥，生成操作在 CZDS 界面即可轻松完成。假如用户想要生成新密钥且公共密钥已存储于其帐户，那么在新密钥覆盖现有公共密钥前，界面会发出警告（以防意外覆盖有效密钥）。

在解密时，用户需向包含加密凭据的网页提供其*私人*密钥，然后这些加密凭据将通过所有网页浏览器的客户端编程语言 JavaScript 来解密。此操作中，私人密钥将不会被发送至服务器。每位用户的计算机均需要解密。

系统会提供一个与加密/解密密钥*完全无关*的单独令牌（用于访问 API）。API 令牌允许用户批量下载 SFTP 凭据，其完全不参与解密流程。API 令牌是 CZDS 的选用功能，有些用户甚至不会去创建。

问：如果使用 RSA 私人密钥解密 SFTP 凭据，但同时此 API 密钥提供 SFTP 凭据的批量访问权限。那么 API 系统是否会绕开凭据的 RSA 加密流程？还是这些凭据需要带外解密？

不会，API 不会绕开解密流程。系统的每一部分都不会绕开解密流程，因为凭据绝不会存储在纯文本中，并且解密所需的密钥也不会存储在服务器中。

其他

问：如果条款和条件发生变化，将以什么方式通知最终用户？如果最终用户不承认条款变化，比如拒绝数据，会有什么后果吗？

答：一旦条款和条件变化或更新，注册管理运行机构可以选择撤销当前所有用户的访问权限；这样，他们必须在新条款下登录并重新请求域文件访问权限。否则，最终用户仍只需遵守其之前签署的 TLD 条款和条件中的义务。需要注意的是，撤销 CZDS 系统内的访问权限不会自动取消最终用户通过 SFTP 访问域资料的权限。若要在 CZDS 以外为被取消或终止系统访问权限的用户更改凭据，则由注册管理运行机构管控。

问：你们在 CZDS 中提供哪些数据元素？

答：TLD 域文件包括在指定的注册管理机构中注册并表现活跃的域名列表。还包含注册管理机构基于其提供的服务而使用的其他 DNS 记录。RFC 1035 和随后的 RFC 中定义了域文件的格式。正如域文件访问咨询小组在策略提案第 9 页第 5.1.7 节，以及《注册管理机构协议》规定 4 所述，CZDS 分发的域文件的所需格式实际是这些 RFC 子集。

问：你们将访问哪些人的 IP 地址？是否通过 DNS 获取？这些 IP 地址如何显示？你们如何操作？你们怎么知道这些地址对应的是哪些用户？

答：最终用户的 IP 地址由用户在创建其用户配置文件时提供，并传输至注册管理运行机构。

问：如果用户下载注册管理机构的数据，该机构是否会留下用户历史记录？

答：注册管理运行机构拥有每位用户的请求历史记录，但没有用户的下载历史记录。
记录 CZDS 系统中的直接下载操作并非不可行，但系统目前尚未提供此功能。

问：是按下载请求批准，还是按 TLD 访问批准？

答：按 TLD。一旦授予访问权限，便可在条款和条件有效期内获取 TLD 域资料 — 有效期至少 90 天，或由注册管理机构选择。条款和条件到期后，用户必须再次请求访问权限。

问：我们需要主题问题专家来帮助我们实现区域调整的全自动化。有何规定？多久可以下载一次？最好能设置一键访问功能。

答：条款和条件规定：最终用户在 24 小时内仅可访问域文件一次。文件每 24 小时上传一次，所以即使最终用户在一天内下载多次，他们也获取不到任何新信息。另外，用户不可在 24 小时内通过 CZDS 直接下载 TLD 文件超过三次。若超过三次，其将收到一条错误信息。