注：本内容的英文原始版本源自 icann.org，现已被翻译成中文。刊登在 icann.org 上的英文版应被视为权威版本。

RSSAC 常见问题解答

本文包含关于根服务器系统咨询委员会 (RSSAC) 的许多最常见问题和解答。本文内容将随着答案的变化或新问题的频繁出现而更新。

如果您的问题下面没有列出，或者需要进一步的信息或澄清，可以直接发送邮件至 ask-rssac@icann.org。如果您希望引用此常见问题解答中的某个问题，请在电子邮件中注明问题的编号和主题。

主题列表

1.运营商数量

1.1 为什么有 13 个根服务器标识符？

1985 年，有四个根服务器。从 1987 年到 1991 年，有七个根服务器，全部位于美国。到 1993 年，有八个根服务器。此时，遇到了一个问题。RFC 1035 规定“通过用户数据包协议 (UDP) 传输的 [DNS] 消息不得超过 512 字节。”添加更多的根名称服务器将导致启动响应超过 512 字节。RFC 1035 没有提供 512 字节限制的理由，但同样值得注意的是，当时有一个通用的要求，即，通过互联网传输的 IP 数据包不得超过 576 字节。

根服务器运营商意识到，如果他们能够利用域名系统 (DNS) 名称压缩，则可以添加更多的域名服务器。因此，提出了在 root-servers.net 区域中提供根服务器名称的建议。到 1995 年，现有的九个根服务器已重命名为“a.root-servers.net”、“b.root-servers.net”等。1997 年，又增加了 4 个根服务器，使根服务器标识符 (RSI) 总数达到 13 个。

直到 1998 年，当时的互联网号码分配机构 (IANA) 主管强 • 珀斯特尔 (Jon Postel) 博士一直负责指定根服务器运营商。在他于 1998 年去世后，尽管多年来有一小部分运营商已经易手，但是运营商的数量并没有变化。

自 1998 年以来，根服务器领域在多个方面发生了变化。每个根服务器都添加了自己的 IPv6 地址，并且 ICANN 使用域名系统安全扩展 (DNSSEC) 对该区域进行了签名。此外，通过 UDP 传输的消息大小，已经使用域名系统扩展机制 (EDNS) 协议扩展进行了扩展。所有这些变化使得 512 字节的 UDP 限制和 13 个 RSI 限制变得不那么重要了。

2002 年，互联网软件联盟（ISC，现在的“互联网系统联盟”）成为第一个部署 IP 任播的根服务器运营商，尽管 WIDE 项目早些时候已经对这项技术进行了试验。多年来，其他根服务器运营商也紧随其后部署了 IP 任播。任播允许每个运营商从多个不同的节点提供服务。虽然当今 RSI 数量仍然是 13 个，但事实上，全世界范围内运营超过 1000 个任播节点。

要更好地了解根服务器系统 (RSS) 的发展历史，请参阅 RSSAC023：根服务器系统发展史。如果您对 RSS 的持续发展感兴趣，请阅读 RSSAC037：DNS 根服务器系统治理模型提案。

1.2 13 个根服务器标识符限制背后的数学原理是什么？

1997 年，当时的根服务器还充当 .COM、.NET 和 .ORG 区域的权威服务器，并且增加的这项功能对可以存在的 RSI 数量设置了重要限制。与根区的启动查询一样，对 .COM、.NET 和 .ORG 区域的 NS RRSET 查询也不能超过 512 字节，并且由于相同的服务器为这些区域提供服务，因此所有这些区域也都具有相同的限制。

DNS 响应数据包中还包含“问题”部分中提出的完整问题。对根启动查询的响应，“问题”部分将始终使用 5 字节。限定名称占用 1 字节，限定类型和限定分类各占用 2 字节，总共 5 字节。然而，对于一个 .COM 启动查询，“问题”部分可能会大得多。

用途	字节数
DNS 抬头	12
首个 NS 记录	31
12 个压缩的 NS 记录	(12 * 15) 180
13 个 A 记录	(13 * 16) 208
“问题”部分的限定类型和限定分类	4
“问题”部分的限定名称	?
	=

	435

表 1：根启动响应中使用的字节数说明

由于已使用 435 字节，因此，“问题”部分的限定名称还剩 77 字节可用。当时认为 64 字节足以处理针对 .COM、.NET 和 .ORG 的大部分查询。添加另一台服务器将需要 25 字节，由于 435 + 64 + 25 > 512，因此当时决定不另外添加服务器。

2.任播

2.1 为什么有些运营商有许多任播节点，而其他运营商却只有几个？

根服务器运营商 (RSO) 是拥有不同使命、不同运营模型和不同资金来源的独立组织。这些差异可能会影响任播节点的数量，以及其他运营选择。根服务器运营商在如何部署网络方面拥有高度的独立性，请参阅 RSSAC042：RSSAC 针对根服务器运营商独立性的声明。所有 RSO 都致力于提供高质量的根 DNS 服务。

2.2 如何确保正确复制根区？根区文件是否可能会被任何攻击或恶意软件破坏？

根区文件通过 DNS 区域传输协议（RFC 5936 中的 AXFR 和 RFC 1995 中的 IXFR）从根区维护人 (RZM) 传输到单个 RSO。如 RFC 2845 中所述，使用交易签名 (TSIG) 资源记录对这些区域传输消息进行安全保护。这是一个可靠的协议，没有发生过已知的数据损坏事件。而且，由于会对根区进行签名，因此，DNSSEC 验证器可以检测到不正确或伪造的答案。RSSAC 鼓励在可能的情况下使用 DNSSEC 验证。

2.3 任播节点的数量是不受限制，还是具有一定的数量限制？

RFC 4786“任播服务运营”和 RFC 7094“IP 任播架构考量因素”中对任播运营进行了定义和描述。任播服务中的节点数量没有任何固有的限制。

2.4 根服务器会复制权威根区并重新发布，然后任播节点会重新发布源自这些根区的数据。这两种类型的重新发布有什么区别？

RSO 从根区维护人 (RZM) 接收权威根区数据。然后，每个 RSO 使用其自己的内部分发系统将根区数据传送到其所有站点和任播节点。

2.5 我们在地方城市托管了一个根服务器任播节点。我们看到该任播节点在答复来自全球各地的查询。我如何将其设置为仅答复来自本地的查询？

这实际上是一个关于 IP 路由和 RSO 如何运营其任播服务的问题。一些 RSO 会对其路由器和对等会话进行配置，使任播节点只接收本地流量。其他 RSO 则会将其路由器和对等会话配置为接

收全球流量，依靠路由系统选择网络中的最佳传输路径。如果您发现托管服务器有不正常行为，应与提供此服务的 RSO 进行讨论。

2.6 2016 年，Dyn 曾遭到大规模攻击。同样的事件是否会发生在所有根服务器任播节点上？

会，至少理论上是这样。这是 RSS 拥有许多运营商和许多根服务器节点的原因之一。大量的任播节点增加了 RSS 的容量，在遭受攻击的情况下肯定会有所帮助。

2.7 如何为我的组织请求根服务器任播节点？

请使用以下联系信息直接联系根服务器运营商。与问题 3.4 相似，您还可以考虑运行根区的本地副本（如 RFC 7706 中所述），而不是在形式上作为根服务器任播系统的一部分。

Cogent 通信公司 (Cogent Communications)	
美国国防部 (NIC)	
ICANN	https://www.dns.icann.org/imrs/host/
Internet Systems Consortium, Inc.	https://www.isc.org/f-root/hosting-an-f-root-node/
美国国家航空航天局（艾姆斯研究中心）	
Netnod	https://www.netnod.se/i-root/i.root-servers.net
欧洲网络协调中心 (RIPE NCC)	https://www.ripe.net/analyse/dns/k-root/hosting-a-k-root-node
马里兰大学	
南加利福尼亚大学， 信息科学研究所	https://b.root-servers.org/
美国陆军（研究实验室）	
Verisign, Inc.	https://www.verisign.com/rirs
WIDE 项目	

3.DNS 与网络

3.1 递归服务器如何选择查询哪个根服务器？我的递归服务器应优先选择哪个根服务器标识符？

这称为“服务器选择算法”。DNS 协议没有指定递归名称服务器应该如何从一组特定查询中进行选择。因此，每个递归软件供应商都可以确定他们自己的服务器选择算法。某些解析器实施会“锁定”到延迟最短的服务器，或具有与最快速服务器相似延迟的某个服务器。有些解析器实施每次会随机选择服务器，有些则会根据复杂的公式来分发查询。一篇 2012 年的文章介绍了当时流行的实施算法。

让您的递归软件执行其本职功能可能是更可靠的做法，而不要试图影响它如何优先选择或避免选择特定的服务器。

3.2 我们知道 DNS 使用 UDP 端口 53，能否说明一下什么情况下 DNS 使用 TCP 端口 53？

默认情况下，几乎所有的 DNS 客户端都使用 UDP 传输进行查询。但是，在某些情况下，需要改用 TCP。

当 UDP 响应被截断时，通常会使用 TCP。当服务器的响应太大而无法包含在单个 UDP 消息中时，就会发生这种截断。这取决于客户端发布的 UDP 缓冲区大小，以及服务器可能对自身设置的响应大小限制。当客户端接收到设置了截断位的响应时，DNS 协议会指示必须通过 TCP 重试查询才能获取完整响应。

另一个对 DNS 使用 TCP 的情况是区域传输。由于整个区域通常比单个 UDP 消息大得多，无法包含在单个消息中，因此，通过 TCP 执行这些传输是合情合理的。

当服务器发现自己遭受攻击时，TCP 也会发挥作用。服务器可能会向客户端发送截断响应，以此来确定消息源是否可靠。可以将建立 TCP 连接的客户端列入白名单，作为可靠信息源。此外，一种名为响应速率限制 (RRL) 的技术偶尔也会发送截断的响应，以便合法的客户端有机会通过 TCP 接收响应，而攻击流量将无法重试发起攻击。

必须通过 TCP 使用 DNS 才能在 DNS 软件中实施。有关更多信息，请参阅 RFC 7766。

3.3 如何减少我运行的递归服务器与根服务器之间的延迟？

首先，您应该仔细考虑靠近（更多）根服务器是否有任何实质性的优势。对离开您的递归名称服务器，以处理发送到根名称服务器的查询流量进行分析。如果您看到的流量超出预期，也许可以修复您的应用程序或网络配置，以便这些流量无需经常查询根服务器。使用类似“dig”实用工具的程序来测量实际延迟。如果至少两个根服务器的延迟在 100 毫秒以内，这通常就足够了。

使用“traceroute”等工具探索递归服务器与递归名称服务器使用的根服务器之间的网络路径。如果您发现一些没有意义的路径（例如，通过较远位置的路由），可以询问您的 ISP 是否可以调整路由。

为获取有关 DNS 服务质量度量的更多信息，欧洲网协 (RIPE) Atlas 项目组通过其 DNSMON 项目对根服务的服务质量进行了监控。数百个 RIPE Atlas 锚点的测量结果显示，大多数服务器的延迟低于 60 毫秒。

如果附近没有合适的根服务器，那么您可以尝试确定根服务器所在位置附近的一个交换点或数据中心。询问一个或多个根服务器运营商是否可以在那个位置放置服务器。但是，请注意，如果某个位置已有一个根服务器，那么运营商通常不希望在该处放置另一个服务器。通过访问 http://www.root-servers.org，并在页面底部的“根服务器”部分中找到“Contact Email”（联系电子邮件）按钮，您可以找到运营商联系信息。

3.4 您可以通过下载根区文件并自行验证签名来设置根服务器吗？

RFC 7706 介绍了如何通过此方法设置根服务器，并列出了关于这样做可能带来的负面影响的多项警告意见。请注意，这需要进行 DNSSEC 验证。另请参阅 LocalRoot 项目。

3.5 递归服务器会将信息缓存多长时间？

每个 DNS 记录都有一个由区域运营商指定的存活时间 (TTL) 值。此值决定递归名称服务器或其他客户端应将数据缓存以供重复使用的时间长度。超过此时间之后，递归名称服务器需要再次联系权威服务器以获取新数据。

对于根区，某些记录的 TTL 为 24 小时，其他记录的 TTL 为 48 小时。有些解析器的最长缓存生存期通常为 24 小时。

3.6 由于过期后的缓存会提供错误信息，如何更新解析器，使其提供正确的 DNS 信息？

如果您怀疑递归名称服务器缓存中的数据已过时，可以刷新缓存或重新启动服务器进程。

3.7 什么是 DNS 启动查询和响应？

在开始答复常规查询之前，DNS 递归解析器需要使用源自根区的特定数据来启动缓存。RFC 8109 介绍了递归解析器会发送哪些查询，以及它们期望从根服务器得到怎样的响应。

4.DNSSEC

4.1 DNSSEC 能否抵御快速通量攻击？

不能。实施 DNSSEC 旨在防止篡改数据，但不能抵御快速通量攻击。

4.2 DNSSEC 是否使在本地提供根区副本变得更加困难？

否，提供本地根区副本仅仅意味着提供根区的最新副本而不做任何更改。根区经理 (RZM) 提供的根区具备所有必要的 DNSSEC 签名。

有关如何提供本地根区的更多信息，请参阅问题 3.4 和 RFC 7706。

4.3 好像通过 UDP 传输的 DNS 不得超过 512 字节，通过 TCP 传输的 DNS 不得超过 4096 字节。如果我签名的根区超过了 MTU，会被防火墙拦截吗？

通过 UDP 传输的 DNS 不再仅限于 512 字节。RFC 2671 中介绍且后来在 RFC 6891 中更新的域名系统扩展机制 (EDNS) 说明了客户端和服务器如何指示对超过 512 字节的消息提供支持。

TCP 从未有过 4096 字节的限制。TCP 设计用来传输任意大小的数据。

有一些对签名响应的大小的担忧是合理的。如果通过 UDP 传输的 DNS 响应超过了网络 MTU 大小，它将被分段。这种情况已被确定为存在缓存投毒攻击安全风险。某些防火墙会拦截这些分段。为此，现代递归解析器设计为使用较小的 EDNS 缓冲区大小，并使用较小的缓冲区大小重试查询。当缓冲区变得足够小时，递归名称服务器将接收到一个未分段响应，或者设置了截断位的响应，指示它应该通过 TCP 重试。

5.RSSAC

5.1 RSSAC 与 RZERC 之间有什么关系？RZERC 是 RSSAC 的一个机构吗？

根服务器系统咨询委员会 (RSSAC) 与根区发展审核委员会 (RZERC) 是 ICANN 内的两个独立委员会，尽管两者之间有联络人，个人可以在这两个委员会中任职。

《RSSAC 章程》规定：
“RSSAC 负责针对有关根服务器系统的运营、管理、安全性和完整性事宜，向 ICANN 董事会和社群提供建议。”有关 RSSAC 的角色的更多信息，请参阅 RSSAC033：RSSAC 针对 RSSAC 与根服务器运营商之间不同之处的声明。

《RZERC 章程》规定：

“RZERC 负责审核以下内容：针对 DNS 根区内容的建议架构调整、执行 DNS 根区调整过程中使用的系统（包括硬件和软件元素）以及使用的 DNS 根区分布机制。”

下图对每个组织的角色进行了阐述。

<此图位于：https://www.icann.org/groups/rssac/faq>

5.2 关于我们何时可以知道 RSSAC 希望设置的根服务器数量，是否有一个时间表？何时会进行评估以决定字母的数量？

RSSAC 对根服务器的数量或者应该有多少个 RSO 没有先入之见。目前对运营商数量的限制是技术层面的，而不是行政性的。

6.RSSAC 决策委员会

6.1 RSSAC 决策委员会成员的数量是否有限制？

没有。

6.2 对 RSSAC 决策委员会成员有哪些时间方面的要求？

RSSAC 决策委员会成员需要参加工作会议，并加入 RSSAC 决策委员会电子邮件清单。部分成员需要能够投入比其他成员更多的时间，而且某些工作会议和文档审核需要占用更多的时间。不过，一般情况下，RSSAC 希望成员每月至少抽出 4 个小时参加决策委员会活动。

7.常见误解

要了解 DNS 的工作原理，请参阅丹尼尔 • 凯伦博格 (Daniel Karrenberg) 撰写的面向非专业人士的互联网域名系统阐述。

7.1 根服务器是否控制互联网流量的流向？

否，路由器和 BGP 协议决定数据包从源到目的地的网络传输路径。DNS 提供了一个从面向人类的名称到 IP 地址的映射，路由器最终使用这些 IP 地址来决定数据包的流向。

7.2 大多数 DNS 查询都由根服务器处理吗？

不是，大多数查询都由递归解析器处理，不与根服务器缓存中已有的数据进行任何交互。如果递归解析器的缓存中不包含关于顶级域或根本身的未过期信息，则它只能与根服务器进行交互。根服务器接收到的几乎所有查询都会产生一个引荐响应，告诉递归名称服务器接下来向哪里提出问题。

7.3 根服务器标识符是否具有特殊含义？

根服务器标识符都没有特殊的含义。

7.4 是否只有 13 个根服务器？

虽然全球范围内的服务器数量超过 1000 个，但只有 13 个根服务器标识符 (RSI)，每个 RSI 使用一个 IPv4 地址和一个 IPv6 地址以及任播路由。

7.5 根服务器运营商是否独立运营？

尽管 RSO 确实是各自独立运营，但也通过 RSSAC 和其他论坛开展密切协作。如需了解更多信息，请参阅“RSSAC042：RSSAC 针对根服务器运营商独立性的声明”。

7.6 根服务器是否只接收 DNS 查询的 TLD 部分？

目前，根服务器（实际上是所有的 DNS 服务器）通常会接收 DNS 请求中的整个查询名称。但是，正在开展新的工作，以便在必要情况下仅将域名的 TLD 部分发送到根服务器。

2016 年，互联网工程任务组 (IETF) 发布了 RFC 7816，其中介绍了递归 DNS 服务器如何只发送查询名称中的最小必要部分。这种做法称为限定名称最小化 (QMIN)。限定名称最小化的工作原理是，让递归 DNS 服务器仅将域名的必要部分发送到它们查询的服务器。利用限定名称最小化的递归 DNS 服务器应该仅发送根服务器查询的 TLD 部分。这样可以最大限度地减少网络上的信息量，从而加强查询 DNS 的用户的隐私性。截至 2020 年，限定名称最小化这种方法仍然相对较新，尚未广泛部署。