供 IT 专业人士使用的域名冲突识别与缓解指南

2013 年 12 月 5 日
1.0 版

目录

1. 简介

新顶级域名引入全球 DNS 根以后组织可能会发现某些其网络专用的“内部”域名解析查询返回不同值，即向用户和程序提供不同的结果。这里涉及两个基本问题：一是“内部”域名泄露到全球互联网，二是专用命名空间的定义与全球 DNS 命名空间冲突。

造成这种不同结果的原因是，网络管理员原本希望使用内部命名空间在本地解析 DNS 查询，但是现在却使用全球 DNS 中的新顶级域名数据进行解析。在这种情况下，未曾料想会离开内部互联网的查询现在却在全球 DNS 中获取结果，因此得到的结果会有所不同。导致不同结果的泄露域名至少会给用户带来困扰（例如，可能造成网页访问延时）。还可能造成安全问题（例如，向错误的收件人发送电子邮件）。

本文档包含组织使用的最常见的专用命名空间类型的冲突缓解与预防策略。还描述了当内部域名泄露到全球 DNS 时组织可能遇到的情况，并详细说明了建议的缓解措施。文中提供的说明和建议针对 IT 专业人员（网络管理员、系统管理员和 IT 部门员工），这些人员一般都了解 DNS 和他们自己的内部域名系统是如何工作的。如欲了解更多背景信息，请参阅本文件的附录 A。如欲了解与安全有关的信息，请直接查看 ICANN 安全与稳定咨询委员会 (SSAC) 的相关报告。

ICANN 是全球 DNS 根目录的管理组织，与命名空间主题专家进行协商后编写了本文档，以帮助专用命名空间可能与全球 DNS 根存在冲突的组织。ICANN 已发布介绍全球 DNS 的组织方式以及新域名加入 DNS 根的方式等内容的其他文档。本文档的附录 A 列出了多个主题的参考信息，以供详细阅读。

请注意，虽然本文档阐述了域名冲突的缓解措施，但是它仅讨论组织在解析域名时可能遇到的问题，而不涉及其他与全球 DNS 自身运营有关的问题。例如，全球 DNS 根域名服务器总是充斥着各种从未打算被全球 DNS 处理的查询（参见附录 A 中的“*SAC 045*”），但是根域名服务器经过良好配置，足以处理这些大量的查询。本文档不涉及与根域名服务器有关的相关问题，仅讨论意外泄露到公共 DNS 根域名服务器的查询引起的后果。

ICANN 开发了一个包含域名冲突相关信息材料的网页，请访问 http://www.icann.org/en/help/name-collision。该网页还提供报告新通用定级域名 (gTLD) 引起的域名冲突导致的显著严重后果的流程。

1.1 域名冲突

全球 DNS 是一个分层命名空间，DNS 中的域名由构成完整域名的一个或多个标签组成。位于顶层的是 DNS 根区域，含有 com、ru、asia 等一系列域名；这些是全球 TLD（顶级域名），通常简称为“TLD”。完整域名（通常称为*完全限定域名*或 *FQDN*）则类似 www.ourcompany.com。

几乎所有专用命名空间都采用分层结构。专用命名空间分为三大类：

- **全球 DNS 的分支命名空间** – 从全球 DNS 分出来的专用命名空间植根于可在全球 DNS 中解析的域名下，但是该域名下的整个目录结构使用全球 DNS 中不会让 IT 管理员看到的域名在本地管理。以植根于 winserve.ourcompany.com 的专用命名空间为例：专用命名空间 (winserve) 中的域名由专用域名服务器管理，这些域名在全球 DNS 中均不可见。

- **使用自身带有专用 TLD 的根的命名空间** – 专用命名空间的根是一个标签，而非全球 TLD 。包括专用 TLD 结构在内的整个目录结构均由在全球 DNS 中不可见的专用命名服务器管理。例如，如果专用命名空间植根于 ourcompany，那么专用域名服务器还负责 www.ourcompany、

region1.ourcompany、www.region1.ourcompany 等。有许多不同类型的命名空间都使用自身含有专用 TLD 的根。例如，微软的 Active Directory（在一些配置中）、多播 DNS (RFC 6762) 和目前在互联网的某些角落仍在使用的较老的 LAN 目录服务。

- **使用搜索列表创建的命名空间** — 搜索列表是本地域名解析器的一项功能（用于专用命名空间或全球 DNS 的递归解析器）。为方便起见，用户通过搜索列表可输入较短的域名；在解析时，域名服务器会在查询中的名称右侧添加配置的域名。（这些配置是域名又称*前缀*。）

从全球 DNS 分出来的命名空间仅在与搜索列表配合使用时会引起域名冲突。根据定义，与来自全球 DNS 的 FQDN 有关的任何查询绝不会与全球 DNS 中的不同域名产生域名冲突。此类查询仅在使用搜索列表无意创建时才会引起域名冲突。

“专用命名空间”的概念使很多基本熟悉一般互联网操作的人都会产生疑惑，这些人只知道全球 DNS 命名规则，而当他们了解到一些域名解析请求不会或不能生成全球 DNS 查询时，就会感到非常诧异。要是知道一些域名查询会特意从专用命名空间开始，却又在全球 DNS 中结束，他们可能会更加诧异。出现域名冲突的一个原因是，原本计划在专用命名空间的域名服务器中开始的查询错误地在全球 DNS 中开始了。

1.2 专用 TLD 引起的域名冲突

出现域名冲突有以下两个原因。第一个原因，对植根于专用 TLD 的完全限定域名的查询从专用网络泄露到了全球 DNS 中。第二个原因，专用 TLD 的专用网络中存在与在全球 DNS 中的查询完全一致的域名。

出现此类域名冲突的共同原因是，在配置系统时，在诸如微软的 Active Directory 等系统中使用的域名不是全球 DNS 中的 TLD，但是后来又被添加到了全球 DNS 中。此前，这类域名冲突已经出现过很多次，而且预计在将新 TLD 引入全球 DNS 以后还会继续出现（参见附录 A 中的“*新 gTLD 计划简介*”）。

1.3 搜索列表引起的域名冲突

引起域名冲突的另一个原因是搜索列表处理。如果某个查询不是 FQDN，那么就是*简短非限定域名*。搜索列表包含一个或多个前缀。前缀叠加到查询的右侧。当解析器无法解析简短非限定域名时，就会附加列表中的前缀，因为它要尝试解析域名，直至找到匹配的域名。搜索列表是一项有用的功能；但是，搜索列表处理会占用简短非限定域名（非 FQDN），这样无意中就会创建并非植根于全球 DNS 中的命名空间。在这种情况下，当用户计划用作简短非限定域名的字符串被搜索列表补充完整并作为 FQDN 解析时，就会出现域名冲突。

例如，假设域名解析器有一个包含前缀 ourcompany.com 和 marketing.ourcompany.com 的搜索列表。再假设用户在使用该解析器的程序中输入 www。这样，解析器可能会先查询 www，如未返回结果，然后就会查询 www.ourcompany.com 和 www.marketing.ourcompany.com。

请注意，本示例描述中使用了“可能”一词。在执行域名解析时，不同操作系统或应用程序的搜索列表应用规则各不相同。有些系统可能总是会在专用命名空间或全球 DNS 中解析域名，然后才应用搜索列表。但是，如果被搜索的字符串不包含“.”字符，有些系统将首先使用搜索列表。如果被搜索的字符串以“.”字符结尾，有些系统还是会使用搜索列表。有些操作系统和应用程序（例如 Web 浏览器）对其搜索列表规则进行过多次更改。因此，要想预测在什么情况下使用或不使用搜索列表、哪些属于或不属于简短非限定域名以及简短非限定域名是否有可能泄露到全球 DNS 是不切实际的。关于搜索列表处理多样性的更多详细信息，请参阅附录 A 中的“*新 gTLD 担忧：无点域名和域名冲突*”。

对搜索列表的这些说明可能会令一些人感到诧异，因为在乍看不会创建“专用命名空间”的地方，搜索列表非常常见。搜索列表中的每个前缀都定义了在域名解析过程中可能查询的另一个命名空间。这样会创建一个只有当客户端在特定解析器上查询时才会可靠运行的专用命名空间。根据搜索列表的执行情况，一些域名解析器甚至可能先尝试查询用户输入或软件配置的简短非限定域名，然后再附加搜索列表中的任何域名。例如，在互联网上的某个位置输入 www.hr，DNS 解析器可能得到一个结果，但是如果在不同位置输入，就可能得到不同的结果。如果出现这种情况，其中一个命名空间相对于其他命名空间就具有“专用”性。

使用搜索列表代替通过全球 DNS 解析 FQDN 有助于降低域名解析的不确定性。由于搜索列表非常常见，因此很难预测搜索列表引起的域名冲突。在许多操作系统、网络设备、服务器等环境中，它们已经成为域名解析器软件的组成部分。在不同操作系统以及同一操作系统的不同版本之间，解析器软件都有不同的工作方式，甚至可以作为操作系统或应用程序判断网络请求来源的工具。部署仅使用全球 DNS 解析域名的域名解析服务可以很好地避免此类不确定性和不可预测的结果。

2. 域名冲突引起的问题

由从专用网络泄露到全球 DNS 中的查询引起的域名冲突会引起很多意想不到的后果。如果查询得到了肯定的响应，但结果却是来自全球 DNS 而非预期的专用命名空间，执行查询的应用程序就会尝试连接到不属于专用网络的系统，连接可能成功，但也可能带来不便（造成域名解析延迟）。事实表明，它还可能带来安全问题，即产生易被恶意利用的漏洞，具体危害视应用程序在连接后执行的操作而定。

2.1 定向到意外网站

假设用户使用专用网络时在其 web 浏览器中输入 https://finance.ourcompany，那么该网络就会有一个专用 TLD 为 ourcompany 的命名空间。如果浏览器查询域名 finance.ourcompany 时能够正常解析，则说明该浏览器获取了财务部门内部 web 服务器的 IP 地址。试想，虽然 TLD ourcompany 也包含在全球 DNS 中，但该 TLD 还含有一个二级域名 (SLD) finance。如果查询泄露，它将解析得到与在专用命名空间解析查询时得到的 IP 地址不同的地址。现在，假设这个不同的 IP 地址配置到 web 服务器。浏览器就会尝试连接到公共网络而非专用网络的 web 服务器。

如前所述，即使在没有专用 TLD 但使用了搜素列表的网络中也可能出现同样的问题。如果某个浏览器在用户拥有搜索列表（包含域名 ourcompany.com）的网络中可以正常使用，那么用户为了访问主机 www.finance.ourcompany.com 就会输入域名 www.finance。现在，假设一家咖啡店的员工正在移动设备上使用该浏览器。如果该查询泄露到互联网，而且互联网上恰好有名为 finance 的 TLD，那么查询就可能解析得到不同的 IP 地址，例如，域名在全球 DNS 中的完全不同的主机地址 www.finance。该查询可能导致浏览器尝试连接到与在专用网络解析器查询完全不同的公共网络 web 服务器。

这种情况下，普通用户往往会认为这是错误网站并立即离开。但是，如果浏览器因为 web 服务器含有与其先前访问的地址完全相同的域名而“信任”该 web 服务器，那么该浏览器就会向其泄露大量信息。浏览器可能会自动输入登录信息或其他敏感数据，从而导致信息被组织以外的人员捕获或分析。其他情况下（例如，对该组织的蓄意攻击），浏览器可能会连接到配置有恶意代码的网站，从而在计算机上安装危险程序。

请注意，使用 TLS 和数字证书可能不能帮您防止域名冲突带来的损害；实际上，由于这种做法会给用户一种安全的错觉，反而危害更大。为全球 DNS 中的域名颁发证书的很多证书颁发机构 (CA) 还会为专用地址空间中的简短非限定域名颁发证书，因此，定向至错误网站的用户仍有可能看到有效证书。有关专用命名空间域名证书的更多详细信息，请参阅附录 A 中的“*SAC 057*”。

2.2 电子邮件定向至错误的收件人

域名冲突可能引起的后果不仅表现在 web 浏览器上。如果收件人地址的主机名相同，本来打算发送给某位收件人的电子邮件可能会被发送给其他收件人；例如，如果 ourcompany 是全球 DNS 中的 TLD，发送给 chris@support.ourcompany 的电子邮件可能会被发送给完全不同的用户账户。即使邮件未被成功发送给特定的电子邮件用户，也可能存在发送尝试，此类尝试可能导致电子邮件内容被组织以外的人员捕获或分析。

很多网络设备（如防火墙、路由器，甚至打印机）可能被配置为通过电子邮件发送通知或日志数据。如果输入的电子邮件通知收件人名称在全球 DNS 中出现域名冲突的情况，那么通知可能会被发送给完全意想不到的收件人。邮件正文中可能透露网络配置和主机行为的事件或日志数据可能泄露给意外收件人。如果该数据的指定收件人未收到日志数据或触发通知的事件无法得到调查或缓解，IT 工作人员的常规网络性能或流量分析就可能中断。

2.3 安全性降低

未得到缓解的域名冲突可能导致专用网络中的系统面临意外行为或危险。依靠域名解析进行正确操作和执行安全功能的系统使用 FQDN 从全球 DNS 解析时*可以*可靠地执行操作。

例如，在防火墙中，安全规则通常基于数据包流的来源或目标。数据包的来源和目标是 IPv4 或 IPv6 地址，但是很多防火墙也会让其作为域名输入。如果使用了简短非限定域名，且未正常执行域名解析，那么规则可能无法按照管理员的期望阻止或允许通讯流量。同样，防火墙日志经常使用域名，而且使用以不可预测的方式进行解析的简短非限定域名会影响事件监控、分析或响应。例如，由于日志中的简短非限定域名会根据创建日志的地址识别不同的主机（即在日志中，同一简短非限定域名可能关联两个或以上不同的 IP 地址），因此导致审核日志的 IT 工作人员可能会误解事件的严重性。这一问题可能很复杂，因为大多数防火墙都可以作为自己的 DNS 解析器或允许管理员使用或配置搜索列表。

2.4 受域名冲突影响的系统

应检查所有联网系统是否使用了植根于专用 TLD 的主机名或基于搜索列表的主机名。所有这些“使用”实例均需要进行更新，以使用全球 DNS 中的 FQDN。要检查的系统或应用程序列表大概包括：

- **浏览器** － 用户可在 Web 浏览器上指定 HTTP 代理的位置，通常针对专用网络。检查用户或 IT 工作人员是否设置了自定义主页、书签或搜索引擎：这些内容会链接到专用网络上的服务器。有些浏览器还提供配置选项，通过这些选项可获取有关指向专用网络上的主机名的 SSL/TLS 证书的撤销信息。

- **Web 服务器** － Web 服务器提供包含嵌入主机名的链接和元数据的 HTML 内容。检查专用网络上的 web 服务器是否含有带简短非限定域名的内容。检查 web 服务器的配置文件是否含有专用网络上其他主机的简短非限定域名。

- **电子邮件用户代理** － 诸如 Outlook 和 Thunderbird 之类的电子邮件客户端均提供配置选项，通过这些选项可使用 POP 或 IMAP 协议接收电子邮件，并基于 SUBMIT 协议发送电子邮件；所有这些都可能使用专用网络上的主机名。检查这些应用程序是否配置为可从分配了简短非限定域名的主机获取有关 SSL/TLS 证书的撤销信息。

- **电子邮件服务器** － 检查电子邮件服务器是否具有列出其他本地主机的简短非限定域名的配置，例如备份电子邮件网关、离线存储服务器等。

- **证书** － 检查使用 X.509 证书的应用程序（如电话和即时消息程序）是否具有使用简短非限定域名识别获取有关 SSL/TLS 证书的撤销信息位置的配置数据。

- **其他应用程序** － 自定义应用程序可能含有储存主机名的多个配置参数。最明显的空间可在配置文件中，但是主机名可能出现在多种应用程序数据、社交媒体或维客网站链接中，甚至还可能硬编码在源代码中。检查这些配置数据是否使用简短非限定域名。

- **网络设备** － 检查网络基础设施设备（防火墙、安全信息与事件管理 [SIEM] 系统、路由器、交换器、网络监控设备、入侵检测或预防系统、VPN 服务器、DNS 服务器、DHCP 服务器、日志服务器），以确定这些设备是否使用专用网络上其他设备的简短非限定域名进行配置。

- **客户端管理** － 检查诸如配置组织工作站和网络设备之类的集中式客户端管理工具，在由系统控制和重置的配置（尤其是搜索列表）中是否含有简短非限定域名。

- **移动设备** － 消费类电子设备，如电话和平板电脑，可能与上述一些应用程序具有类似的配置选项，因此可能有包含来自本地网络的简短非限定域名的配置选择。

应检查所有这些系统中储存简短非限定域名的配置数据，以确保当专用命名空间的根更改或不再使用搜索列表时，此类域名能得到更改。

3. 何时需要缓解域名冲突

域名有时会被添加到全球 DNS 根区域，例如当国家或地区名称更改时，或 ICANN 授权新 TLD 时。二十多年来，几乎每年都会新增这两种类型的顶级域名。今年（2013 年）也有新增域名，预计 2014 年及以后将新增更多域名。

历史记录显示，当 DNS 中新增 TLD 时，有时会出现域名冲突。记录还显示，专用命名空间的域名多年来都有发生泄露，在某些情况下，泄漏频率非常高；更多详细信息请参阅附录 A 中的“*SAC 045*”。历史告诉我们，适用于专用网络的命名空间和域名解析从未像管理员认为的那样彻底实现独立，管理员想要通过内部域名服务器解析的域名查询有时会发送到全球 DNS 中的解析器。

网络管理员有时根据全球 DNS 根中的域名列表不可变的假设选择域名，但是实际上，列表会随时间不断发生变化。例如，大约 25 年前，在为捷克斯洛伐克增加 cs TLD 后，很多大学都使用允许用户输入以 cs 结尾的域名查询计算机科学系的搜索列表，该列表使用大学的域名完全限定，但是由于这些以 cs 结尾的域名当时是全球 DNS 中的 FQDN，所以当新 TLD 加入根区域时，这些决定导致域名解析出现不确定性。即使目前全球 DNS 根域名经常与专用命名空间（专用 TLD 或搜索列表）中的域名重叠，但是网络管理员也经常忘记更新全球 DNS 根中的域名。

建议 IT 部门尽快展开缓解工作。虽然采取“我们将把防火墙做得更好”的立场可以减少一些冲突，但是绝不可能避免所有冲突。同样，虽然“我们将确保用户放心使用我们的域名服务器”或者“我们将让远程工作者使用 VPN”的做法可能会减少一些冲突，但是这也会让其他冲突变得更加难以判断。

不管域名中使用哪些字符都会出现域名冲突；但是，在专用 TLD 中使用非 ASCII 字符（如 ä、中和 й）会使冲突分析变得复杂。解析器可能会以难以预料的方式发出对这些域名的查询，而且可能不符合互联网标准，因此判断何时会发生域名冲突就变得更加困难。

虽然全球 DNS 根终究会随着时间的推移不断扩大，但是向根中增加域名实属常见。新增的各 TLD 都有可能与意外泄露到互联网的专用命名空间存在域名冲突。多年来，各组织一直使用域名并承担着域名冲突的风险。

请注意，向 DNS 根增加新域名不会也绝不会对已使用全球 DNS 中的 FQDN 的组织造成影响。这些组织在使用 DNS 域名时不会觉察到任何变化，因为不存在域名冲突。只有使用专用 TLD 的组织或使用允许输入简短非限定域名搜索列表的组织才会遇到域名冲突的问题，因为简短域名本身可能是全球 DNS 中的有效域名。

3.1 确定出现冲突的可能性

为了便于您确定您所在组织的专用命名空间是否存在域名冲突，您需要确定组织使用的所有专用命名空间和 DNS 搜索列表并对其进行分类，然后基于其来源编制顶级域名列表。对于大多数组织而言，一个命名空间通常只有一个顶级域名，但是某些组织也有多个专用顶级域名，尤其是与其他同样使用专用命名空间的组织兼并的组织（例如，由于企业兼并或收购）。

接下来，您需要确定全球 DNS 区域的当前和预期内容。有关全球 DNS 当前根区域的域名，请访问 http://data.iana.org/TLD/tlds-alpha-by-domain.txt。如需确定专用命名空间的域名是否被考虑通过 2013 年启动的新 gTLD 计划进行分配：

1. 请转至 https://gtldresult.icann.org/application-result/applicationstatus
2. 单击“字符串”栏中的箭头
3. 滚动页面，直至找到包含您的专用命名空间域名的内容

如果您刚刚编写的专用 TLD 列表与 DNS 区域的域名列表有重叠，则可能会造成域名冲突，因此需要马上采取缓解措施。

请注意，将当前轮次的新 TLD 输入根区域以后，可能会出现更多类似提案；特别是新 TLD 列表会出现变化，专用命名空间和未来的新 TLD 之间可能会出现域名冲突。此外，拥有由两个字母（例如 ab）组成的专用 TLD 的组织应该知道，两个字母的顶级域名会被留作国家代码，并且这些域名会通过完全不同的程序添加到根区域中。

4. 缓解专用 TLD 相关问题的步骤

数十年来，一直都不建议将使用专用 TLD 作为最佳实践。事实上，多年以来，微软的 Active Directory 和服务器产品随附的说明中已明确地表示不建议使用专用 TLD。对于因使用以泄漏到全球 DNS 的专用 TLD 结尾的域名而产生的域名冲突，最有效的缓解办法是从使用专用 TLD 转变为使用植根于全球 DNS 的 TLD。

本节中的步骤适用于存在以下情况的任何网络：因其各自的原因不得不选择使用专用 TLD 作为其根，并使用搜索列表解析简短非限定域名，而没有其将命名空间植根于全球 DNS 中，也没有通过查询全球 DNS 解析 FQDN。本节适用于任何使用专用 TLD 的组织，不仅仅是那些已将域名查询泄露到全球互联网的组织。如果您的组织使用的是您认为“安全”的专用 TLD，即未经申请或未经批准授权加入全球 DNS 根的域名，那么您仍然应该慎重考虑转变为使用植根于全球 DNS 的域名。如果您所工作的大型组织拥有多个专用 TLD（比如与另一家公司合并但并没有合并两个命名空间的公司），那么必须针对每个专用 TLD 执行本节中的步骤。

有可能当组织选择使用专用 TLD 后，会在使用时注意采用特定的命名规范。此处的步骤可能会与最初的模式冲突。为了切实缓解与因专用 TLD 导致的域名冲突相关的问题，用户和系统都需要更改其使用域名的方式，并且还需要采用有些用户可能觉得不方便的方式对域名服务器进行重新配置。还应对会影响您组织的意外或不良后果进行解释，以便提高您的用户机构群体的认知度并巩固他们的接受度。

重要提示：在执行本节中的步骤时，您可能还需要缓解因搜索列表导致的域名冲突，与此相关的内容请参阅第 5 节。该节中的很多步骤都与此处的步骤相同，而且可以同时执行。

4.1. 监控对权威域名服务器的请求

要缓解专用 TLD 带来的问题，就要列出请求中使用当前专用 TLD 的所有计算机、网络设备和任何其他系统。当您更改使用的域名时，所有自动使用旧专用域名的设备都需要进行更新。

有三种常用的方法用来执行此系统监控和枚举：

- 权威域名服务器（如 Active Directory）可能有日志记录功能。开启日志记录功能可收集所有专用域名查询的详情。
- 很多现代防火墙都能配置为检测和记录对专用域名的查询。这可能没有通过命名系统本身进行记录那样有效，具体情况取决于您的网络拓扑。例如，如果某个查询没有通过防火墙，防火墙就无法检测到该查询，因此会将其遗漏。
- 如果以上方法都不行，则可以使用数据包捕获程序（如 Wireshark）监控和收集权威域名服务器接收或发送的流量。但是，此方法需要使用某种程序对捕获到的数据进行处理，才能发现对专用域名的查询。

为了增加发现所有请求的机会，有些组织将（并且应该）选择使用以上多种方法。请注意，此步骤产生的结果可能会令人感到困惑。计算机和电话等设备上都有可让用户输入域名的应用程序；这些设备都将作为调查对象，即便没有存储任何旧的专用域名。对于这一步，只需要知道您网络中所有存储旧专用域名的位置以及应用程序所使用的旧专有域名的位置即可。

4.2. 创建自动使用专用 TLD 的各个系统的清单

您需要将在上一步获得日志数据汇总。应在该汇总文件中列出所有设备以及所有被查询的域名，而不是每个进行查询的设备实例。需要列出所有被查询的域名的原因是，有些设备包含多个应用程序，每个应用程序都需要进行修复。因此，汇总文件必须包括所有系统以及各个使用专用 TLD 的系统中的所有应用程序。通过此汇总文件可清楚地看到需要更改的设备。

4.3. 确定您的全球 DNS 域名的管理事宜

您的组织可能已有一个全球 DNS 域名，该域名可用于专用命名空间的根。您需要确定由谁来管理您的 DNS 域名以及使用什么流程在 DNS 中创建和更新域名。此工作可在您的 IT 部门中执行，或者也可以通过服务提供商（通常是为您提供互联网连接服务的公司）执行。

4.4. 将专用命名空间的根更改为使用全球 DNS 中的域名

使用全球 DNS 域名作为专用命名空间的根是比较常见的做法，这样可以从全球 DNS 中授权一个公众可访问的域名，然后再使用现有的权威域名服务器管理该域名之下的所有域名。例如，如果您公司已有的全球域名为 ourcompany.com，则您可以选择 ad1.ourcompany.com 作为根域名。

如果您的组织在全球 DNS 中拥有不止一个域名，那么应该将您的域名植根于组织的 IT 工作人员最容易控制的域名下。在某些情况下，其他域名由其他实体控制，如营销部门。如有可能，最好将您的域名植根于 IT 组织已控制的域名下。

做出这一改变的步骤取决于您使用的专用域名服务器软件、该软件的具体版本、您的专用网络中域名服务器的拓扑以及域名服务器的现有配置。这些详情不在本文档的讨论范围之内，但是应该涵盖在您的供应商为您的当前系统提供的说明中。此外，在很多组织中，这一改变都需要得到某些管理层的授权，尤其是在全球 DNS 域名的管理与专用命名空间的管理不同的情况下。

在此步骤中，对于使用专用命名空间中的域名的任何主机，如果您有证书，则还需要为使用新（完全限定）域名的主机创建证书。获取这些证书的步骤取决于您的 CA，此内容也不在本文档的讨论范围之内。

4.5. 为主机分配 IP 地址（如有需要）

如果您的旧专用 TLD 域名有 TLS 证书，那么您就需要为新域名获取新证书。如果您的 web 服务器不支持允许基于同一个 IP 地址在 TLS 下使用多个域名的 TLS 服务器名称指示 (SNI) 扩展，那么您就需要将 IP 地址添加到主机，以便主机支持原有 IP 地址上的旧专用域名和新 IP 地址上的新域名。或者，您也可以将您的 web 服务器软件更新到能够正确处理 SNI 扩展的版本。

4.6. 创建监控新旧专用域名之间的对等性的系统

将所有专用域名更改为使用新根后，您需要继续为旧专用域名提供地址并记录查询，以便检查没有更新使用 DNS 根域名的系统不在您的清单中。为此，您需要确保新旧专用域名具有相同的 IP 地址值。

有些专用命名空间软件允许您并行使用两个树形结构，但是如果您的软件版本较老或您有多个权威域名服务器，那么可能就必须使用自定义工具监控对等性。这些自定义工具经常需要同时在新旧两个命名空

间中查询所有域名，并且会在出现不匹配的情况时提醒您，以便您判断哪个系统在另一个系统没有同时变更的情况下变更了。

如果由于有 SSL/TLS 证书，您在上一步中需要添加 IP 地址，这种不匹配的情况就需要得到对等性监控软件的允许。

4.7. 培训用户和系统管理员使用新域名

除了更改可在配置中输入域名的系统外，您还需要改变用户的想法，以便让他们从使用旧专用域名转变为使用新专用域名。此培训应该在实施以下步骤前完成，以便用户有机会习惯新域名，但是培训时应该说明更改即将发生，用户应该尽快从新域名的角度开始考虑问题。同时，这也是一个培训用户使用 FQDN 的好机会。还应对会影响您组织的意外或不良后果进行解释，以便提高认知度并巩固接受度。

4.8. 将每个受影响的系统转变为使用新域名

本步骤是让网络中的所有系统（个人计算机、网络设备、打印机等等）从旧专用域名迁移到新专用域名的关键。按系统逐个使用新 DNS 域名替换专用域名。每个旧专用域名的实例都可以在系统的所有软件中找到，并被新 DNS 域名替换。同时，您还应该撤销在搜索列表中使用简短非限定域名的做法。

之前开始的监控在这一步骤中尤其重要。您无法确定所有内嵌有旧专用域名的系统的所有应用程序。但是，在更改各个系统后需要查询监控系统，以了解该系统是否还在请求旧专用域名。

很多系统在首次启动时都会运行一些初始化应用程序。这些应用程序可能内嵌有系统名称，发现所有这些名称可能很困难。在将系统中的所有域名从旧专用域名更改为新 DNS 域名后，即可重启系统并使用监控软件监测域名查找。如果系统正在查找任何旧专用域名，您就需要判断该请求是由哪个软件导致的并将其更改为使用新域名。此过程可能需要数次重启，才能正确地完全配置好一个系统。

4.9. 在域名服务器上开始监控旧专用域名的使用情况

您应该对权威域名服务器进行配置，让其开始监控所有对使用旧根的域名的请求。由于您的用户不得再使用这些域名，此监控步骤创建的日志不会很大；如果是这样，您将需要对您网络上的特定系统重复上述几个步骤。

4.10. 在外围设立长期监控措施监测旧专用域名

在上一步中应该找出了绝大多数使用旧专用域名的情况，但是有些（可能是关键）系统可能仍然在使用旧专用域名，但也许只有很少一部分。检测这些域名查询的一个方法是，将规则添加到您网络边缘的所有防火墙中，以便查找遗漏的任何请求。这些规则应该具有较高的优先级，而且应该配置为能够生成事件通知，以便 IT 工作人员及时获知。您也可以选择在防火墙日志中查找这些事件，但这样做极有可能造成遗漏。通过发生请求时触发的警告，工作人员现在即可检测出这些极少出现的事件。有些防火墙需要支付额外的费用添加额外的功能才能支持此类规则；如果您的防火墙是这样，那么您就需要评估找到遗漏的请求所获得的益处是否值得花费额外的费用。

4.11. 将所有使用旧根的域名更改为指向非功能性地址

用户经过培训后，确保他们停止使用旧专用域名再删除这些域名的最有效的方法是，让所有旧专用域名指向您已配置为不响应任何类型的服务请求的服务器。这样做还有助于排除任何仍在使用旧命名空间但并未在之前的步骤中检测到的系统。

指向的地址应该为确保不会运行任何服务的服务器。这样，所有使用旧专用域名的系统就不会再获得错误的信息，应用程序也不会再报告用户能轻易检测或知晓的错误；在认知培训中，您可以建议用户向 IT 工作人员报告所有此类错误。实施此步骤时，还需要根据这些更改更新负责检查新旧域名之间对等性的监控系统（如上所述）。

一次只能更改一个域名，在每次或每批更改之间可能至少还要间隔数小时。此步骤可能需要召集 IT 部门，所以分批进行更改将有利于平衡召集负担，因为仍在使用中的域名将开始停止工作。

4.12. 撤销为旧专用域名下的任何主机颁发的证书

如果在您组织的使用旧专用域名的网络中，有为其中的任何服务器颁发的 SSL/TLS 证书，那么应该撤销这些证书。如果您的组织充当自己的 CA，那么此任务非常简单。如果您使用商业 CA 为专用命名空间颁发证书，就需要确定 CA 请求撤销的流程，不同的 CA 可能会对此类请求有不同的要求。

4.13. 使用新域名长期运营

请注意，旧专用域名和其下的域名仍可提供服务，而且只要运行域名服务器，其就会继续提供服务。其实并没有必要删除这些域名，而且在很多系统（如 Active Directory）中，系统中配置的首个域名其实很难删除。

事实上，有一个将域名留下的很好理由：这样可以了解您网络的系统中是否还有任何旧专用域名的残留痕迹。只要所有与该专用 TLD 下所有域名相关的地址都指向没有运行任何服务的主机，您就可以使用域名服务器（为了获得额外的益处，还包括记录该服务器接收的所有流量的系统）的日志来判断旧专用域名的删除程度有多彻底。

5. 缓解与搜索列表相关的域名冲突的步骤

为了切实缓解与因搜索列表导致的域名冲突相关的问题，用户和系统都需要更改其使用域名的方式。通过更改通知、认知程序和培训的方式，有助于让用户提前做好准备。

请注意，如果您已采用集中管理，那么这些操作可能会比想象中容易。很多经常使用搜索列表的人都知道，他们在需要时还能输入完整的域名（比如在从组织的专用网络以外访问服务器时），与只知道使用简短非限定域名的人相比，培训这些人将会轻松一些。

5.1. 监控对域名服务器的请求

要缓解搜索列表带来的问题，您就需要了解请求中使用搜索列表的所有计算机、网络设备和任何其他系统。所有自动使用搜索列表的设备都需要进行更新。

有三种常用的方法用来执行此系统监控和枚举：

- 递归域名服务器（如 Active Directory）可能有日志记录功能，您可以开启日志记录功能，以获取所有使用简短非限定域名的查询的详情。
- 很多现代防火墙都能配置为检测和记录对所有域名的查询。这可能没有通过命名系统本身进行记录那样有效，具体情况取决于您的网络拓扑。例如，如果某个查询没有通过防火墙，防火墙就无法检测到该查询，因此会将其遗漏。
- 如果任何方法都不行，则可以使用数据包捕获程序（如 Wireshark）监控域名服务器。但是，此方法需要使用某种程序对捕获到的数据进行处理，才能发现对简短非限定域名的查询。

请注意，此步骤产生的结果可能会令人感到困惑。计算机和电话等设备上都有可让用户输入域名的应用程序；这些设备都将作为调查对象，即便没有存储任何简短非限定域名。对于这一步，只需要知道您网络中所有存储简短非限定域名的位置以及应用程序所使用简短非限定域名的位置即可。

5.2. 创建自动使用简短非限定域名的各个系统的清单

您需要将在上一步获得日志汇总。应在该汇总文件中列出所有设备以及所有被查询的简短非限定域名，而不是每个进行查询的设备实例。需要列出所有被查询的域名的原因是，有些设备包含多个需要进行修复的应用程序。通过此汇总文件可清楚地看到需要更改的设备。

5.3. 培训用户和系统管理员使用 FQDN

除了更改可在任何配置（系统级配置或单个应用程序的配置）中输入简短非限定域名的系统外，您还需要改变用户的想法，以便让他们从使用简短非限定域名转变为完整域名。还应对会影响您组织的意外或不良后果进行解释，以便提高意识并巩固接受度。

5.4. 将每个受影响的系统转变为使用 FQDN

按系统逐个使用同等的 FQDN 替换简短非限定域名。能在系统的所有软件中找到每个简短非限定域名的实例都需要被完全限定域名替换。

之前开始的监控在这一步骤中尤其重要。您无法确定所有被更改且内嵌有简短非限定域名的系统的所有应用程序。但是，在更改各个系统后需要查询监控系统，以了解该系统是否还在请求简短非限定域名。

很多系统在首次启动时都会运行一些初始化应用程序。这些应用程序可能内嵌有依靠搜索列表的系统名称，发现所有这些名称可能很困难。在将系统中的所有域名更改为使用 FQDN 后，即可重启系统并使用监控软件监测域名查找。如果系统正在查找任何简短非限定域名，您就需要判断该请求是由哪个软件导致的并将其更改为使用 FQDN。此过程可能需要数次重启，才能正确地完全配置好一个系统。

5.5. 关闭共享域名解析器上的搜索列表

本步骤是让网络中的所有系统（个人计算机、网络设备、打印机等等）真正实现从简短非限定域名迁移到完整域名的关键。搜索列表可以存在于任何能进行域名解析或能为其他系统提供配置的系统中，如 DHCP 服务器。这些系统通常为独立的域名服务器，但也可能是防火墙或其他网络设备。不管系统类型如何，都需要关闭各个系统的搜索列表，以便防止用户在给定的命名空间中使用简短非限定域名。

5.6. 在域名服务器上开始监控简短非限定域名的使用情况

您应该对域名服务器进行配置，让其开始监控所有对需要使用搜索列表的域名的请求。如果您提供提前通知和培训，您的用户就不得再使用这些域名，此监控步骤创建的日志不会很大；如果是这样，您可能需要对您网络上的特定系统重复上述几个步骤。

5.7. 在外围设立长期监控措施监测简短非限定域名

在上一步中应该找出了绝大多数使用简短非限定域名的情况，但是有些（可能是关键）系统可能仍然在使用简短非限定域名，即便可能只有很少一部分。检测这些域名查询的最佳方法是，将规则添加到您网络边缘的所有防火墙中，以便查找遗漏的任何请求。这些规则应该具有较高的优先级，而且应该配置为能够生成事件通知，以便 IT 工作人员及时获知。您也可以选择在防火墙日志中查找这些事件，但这样做极有可能造成遗漏。通过发生请求时触发的警告，工作人员现在即可检测出这些极少出现的事件。有些防火墙需要支付额外的费用添加额外的功能才能支持此类规则；如果您的防火墙是这样，那么您就需要评估找到遗漏的请求所获得的益处是否值得花费额外的费用。

6. 摘要

域名冲突可能会对使用专用命名空间的组织造成意想不到的结果。本文档列出了一些可能的结果，还详细说明了改变组织内专用命名空间使用方式的最佳实践。

对于使用正在（或已经）变成全球 DNS 中 TLD 的专用 TLD 的命名空间，最好通过将命名空间迁移到植根于全球 DNS 中的命名空间的方式来缓解问题。对于使用搜索列表中简短域名的命名空间，只能通过取消使用搜索列表缓解问题。实施这些缓解措施的步骤还包括在专用网络中设立长期监控措施，以便确保不再使用任何可能引起冲突的域名实例。

缓解域名冲突问题的综合办法是在使用域名的所有地方都使用 FQDN。在已使用全球 DNS 的网络中，这意味着不得使用搜索列表。在使用专用命名空间的网络中，这意味着专用命名空间应该植根于全球 DNS 中，而且不得使用搜索列表。

附录 A：更多阅读材料

以下文档由 ICANN 内部的各个组织编撰而成。其他组织也提供了一些有用的文档。最重要的是，您的域名服务器软件和/或硬件的供应商在其技术支持网站上可能会提供宝贵的信息。

A.1.新 gTLD 计划简介

本页面介绍了将数百个新 gTLD 添加到全球 DNS 中的计划的历史、实施和进展情况。
http://newgtlds.icann.org/en/about/program

A.2.DNS 中的域名冲突

ICANN 委任 Interisle Consulting Group, LLC 撰写此关于潜在域名冲突的深度报告。报告中简单介绍了域名冲突，列出了当前在根服务器中查询的不存在的 TLD 的数据，还提供了大量有关域名冲突可能产生的问题的背景信息。
http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

A.3.新 gTLD 冲突事件管理计划

该计划已被 ICANN 采纳，用于管理新 gTLD 和专用命名空间之间发生的域名冲突事件。其中还包括很多对 ICANN 收到的早期关于根区域中域名冲突相关提案的意见的回应。
http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

A.4.新 gTLD 问题：无点域名和域名冲突

根据被查询的简短非限定域名中内容，不同系统上的搜索列表可以产生千差万别的结果。本文章虽然重点探讨无点域名（顶点上有地址记录的 TLD）的搜索列表，但在很多其他内容中也提供了有关搜索列表处理的宝贵信息。
https://labs.ripe.net/Members/gih/dotless-names

A.5.SAC 045：根级域名系统中的无效顶级域名查询

本 ICANN SSAC 报告描述了在撰写时根服务器中出现的 TLD 查询的类型。
http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

A.6.SAC 057：SSAC 关于内部域名证书的咨询报告

本 ICANN SSAC 报告描述了包含专用（内部）域名的证书的安全性和稳定性含义。报告中指出了 CA 的一种做法，这种做法可能会出现被攻击者利用并对安全互联网通信的隐私和完整性造成严重影响的情况。
http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf