白皮书

为什么选择 Infoblox for DDI

从 *BIND* 和 *Microsoft* 迁移的时机已到

目录

在许多组织中，实现可靠连接和访问互联网的核心服务都是基于免费或看似免费的产品。虽然价格可能很诱人，但这些产品往往带来功能限制和管理效率低下的隐性成本。在规划当今网络中不可避免的增长和变化时，必须考虑“免费”的天然局限性，以及如何通过核心服务将网络提升到新的水平。

DNS、DHCP 和 IPAM：简史

DNS 在诞生之初是访问网站和应用程序的便捷方法，而 DHCP 则几乎闻所未闻。它们通常由了解它们的人来管理，并依赖于“免费”系统，例如 BIND/DHCPD 和 Microsoft DNS/DHCP。有时，电子表格是维护基本协议服务的基础（即DNS 和 DHCP）。这些系统通常是由一个小型专家团队维护的一系列“自助”工具集合演变而来的。当这些专家被调往其他岗位或其他组织时，就会妨碍业务和规划决策。

IP 地址管理 (IPAM) 是后来的增强功能，有时与管理 DNS 和 DHCP 的人员脱节。分配资源和定义网络的团队并不是管理和定义域名和地址的人员。

在总体 IT 战略中，这些系统的业务影响或可靠性往往被忽视，而且对于由哪个部门（运营、系统或网络）负责系统维护也很少有统一的规定。直到最近，DNS、DHCP 和 IPAM 相结合（“DDI”）的概念才被采用。

现代网络中的 DDI

在过去 20 年里，随着网络和移动性的惊人增长、人们对其的依赖，以及移动设备使用量的激增，人们现在希望 DNS 成为一种“拨号音”服务，能够一直正常工作。

访问身份验证、数据库和其他后端资源、IPv6、物联网以及几乎所有其他技术的迫切需求，现在都将 DDI 置于网络的核心。这就增加了对极端可靠性、集成性和保管责任的额外要求。在最初的设计模型中，从未充分考虑过这些问题。

尽管免费或开源解决方案可以提供必要的服务，但它们可能需要大量维护，并且缺乏在当今现代网络中被视为“企业级”的稳健性。

企业也在向更加自动化的环境转变，尤其是在云和虚拟空间中。然而，这些现有的解决方案要想适应预期的自动化水平，就需要进行更多的定制。随着 IPv6 的普及，这种困难将进一步增加，因为通过电话读出 IP 地址的时代早已一去不复返了。要妥善管理这些日益复杂的环境，必须有一个可支持、可扩展、集中管理的 DDI 解决方案。

简而言之，如果 DDI 服务瘫痪，或实施更改耗时过长，业务功能就会受到负面影响，最终导致生产力和利润损失。

高管的优先级

毕马威 (KPMG) 会计师事务所最近的一份报告列出了首席信息官的五个执行战略重点：

- 更快进入市场
- 业务数字化
- 更加以数据为导向
- 建立公众信任
- 实施颠覆性技术

在 DDI 领域，这些策略可以理解为“保障业务”、“提高业务速度”或“保护公司声誉”等举措。

在重新设计 DDI 基础设施以解决此类问题时，我们不需要花费太多精力就能将这些问题联系起来，并发现传统解决方案与现代集成解决方案之间的局限性。

只有充分保护和减少针对数据的所有可能攻击载体，才能确保业务安全，而 DNS 现在是 78% 的应用层攻击 (DDoS) 和 91% 的恶意软件分发、命令与控制和数据泄露的主要渠道。

只有当网络核心服务所使用的系统能够保护基础架构并满足合规性要求、缓解恶意软件以及提供集中式的遏制威胁和运营的模式，才能够保障公司的声誉的同时，实现向数据驱动型业务发展。

只有当 DDI 自动化程度达到能够满足基于云的基础设施所要求的那种快速和可延展时，业务的速度才变得可行。

实现下一代数据中心承诺的道路可能很艰难。传统的 DNS 基础设施和电子表格中的 IP 地址管理无法提供工作负载调度所需的效率、可视性或自动化，这让 IT 部门只能采用耗时的手动流程来配置核心网络服务。真正的数据中心转型不仅仅是存储和计算自动化，组织还需要网络自动化，以实现灵活、集中管理和高度可扩展的数据中心。

您需要知道所有设备在哪里、它们在做什么、它们在与谁通话、它们随着时间的推移发生了哪些变化，以及根据手头有限的资源，应将工作重点放在哪里。

理想的系统

在当今的环境中，DDI 必须满足许多重要标准：

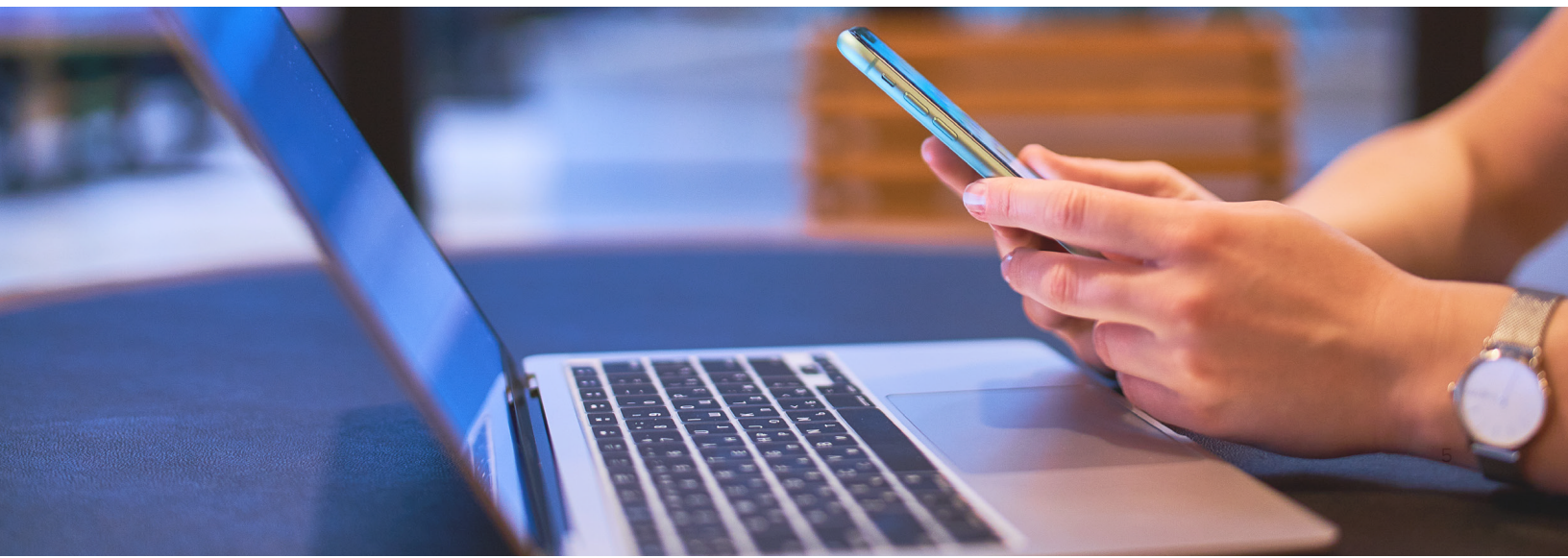
- 可靠的正常运行时间
- 易于更改
- 实时端点和拓扑可视性
- 与自动化系统集成
- 冗余和/或快速恢复时间

因此，理想的系统应该是集中管理的，需要最少的资源来维护，易于部署和扩展。它还应该稳定、安全并支持各种不同的需求，如高级管理员、站点/桌面支持、自动化任务、网络规划和安全取证。

对于规划和取证来说，“单一可信来源”是关键。系统必须能提供一个查找任何设备或网络信息的地方，而不是搜索多个可能相互冲突或不同步的系统。

这包括历史增长模式、DNS 使用情况和趋势的可视性、DHCP 租约历史记录和设备历史记录。所有这些都是快速应对安全事件、解决网络故障和进行总体容量规划的关键。

理想的解决方案还能作为更大生态系统的一部分与其他系统互动，并动态地相互通信以交换信息。现在，自动化是必备条件。



这方面的例子包括：

- 对已被标记为潜在恶意的 DNS 记录的查询，DNS 可以通过响应策略区域（RPZ）“捕获”此记录。然后，可将匹配结果传送给设备管理系统，以自动扫描相关系统，查找可能存在的问题，并在必要时发出警报，隔离相关系统。
- DHCP 租约日志可发送到第三方日志系统，以跟踪使用趋势和事件关联
- 为新创建的虚拟机分配和回收 IP 的自动化系统可将配置时间从几小时或几天缩短到几分钟。
- 端点安全系统标记出恶意端点后，可自动将此信息推送到安全策略中，防止客户端与所述端点联系。

系统间的自动交互可以实现轻松的策略变更、实时端点和拓扑可视性以及与自动化系统的集成，上面只是众多例子中的一小部分。

Infoblox 的优势

传统系统无法扩展

尽管 BIND 已成为 DNS 和 Internet 方面的行业标准，但它需要高水平的知识和技能才能正确实施和操作。要正确完成简单的任务（例如，在添加/修改/删除记录时，区域的序列号必须递增），需要经过多个手动步骤。在实施更复杂的配置和功能（如 DNSSEC）时，存在一些隐患，可能导致性能不可预测，甚至可能导致 DNS 完全中断。

此外，虽然 BIND 支持 DNS，但它不提供内置报表来进行性能监控和管理，也没有与 IP 地址管理集成，这导致本地 DNS 记录与 IPAM 中可能出现的内容不一致。BIND 在开发时从未考虑过自动化问题，因此它不包含用于更改 DNS 记录的强大 API，而这正是出色的 DDI 系统所能提供的。

将 IPAM 与 DNS 集成

将 IPAM 与 DNS 集成对于保持两个系统的准确性和同步性至关重要。当网络上部署新设备时，首先会分配 IP 地址，然后通常会立即请求将主机添加到 DNS。通过集成 DNS 和 IPAM，此过程只需一个步骤 - 在分配 IP 的同时创建 DNS 记录。这不仅能提高效率，还能减少出错的可能性，因为数据无需转录或转发。随着 IPv6 的不断普及，对集成 IPAM 和 DNS 的需求也会不断增加。

为了进一步提高 DNS 和 IPAM 的准确性，可以添加发现组件。将发现组件集成到 IPAM 中，可将其从一个几乎完全依赖人工操作的系统转变为“权威 IPAM”，让网络管理员和安全操作员随时随地都能实时了解网络上的情况。如果与报表方案相结合，就可以时刻跟踪 IP 地址的历史，这对正确分析安全事件至关重要。

使用 Infoblox DDI，您就拥有了一个现代化的 DNS 服务系统，可以通过以下方式解决许多此类问题：

- 将 DNS、DHCP、IP 地址管理和其他核心网络服务整合到一个平台中，并通过一个通用控制台进行管理
- 通过混合云、公有云、虚拟化和私有云环境的集成功能，跨不同基础设施集中协调 DDI 功能
- 获取丰富的整合报告和分析功能，以进行容量规划、资产管理、合规控制和审计
- 通过 RESTful API 与其他 IT 系统无缝集成，结合 Infoblox 网格提高 IT 效率和自动化水平

Infoblox for DNS 与 Microsoft DNS

在选择与 Microsoft Active Directory 一起使用的 DNS 解决方案时，许多管理员只是选择“Windows Server 中的DNS”。但也有必要使用非 Microsoft DNS。

- **安全**：各组织要求为其暴露于互联网攻击的外部 DNS 提供最佳解决方案。第三方 DNS 解决方案从设计和构建之初就考虑到了安全性。组织的内部 DNS 结构同样会受到恶意威胁、恶意软件、网络钓鱼和数据泄露的影响。
- **可视性和单一视图**：大多数组织都拥有各种不同的技术。准确的一站式可视性对于高效合规和控制至关重要。
- **运营效率**：利用自动化和工作流比起手动电子表格管理，更能够优化运营支出（OPEX）。
- **智能服务**：与 DNS 集成的流量控制、网络负载平衡和服务监控为组织增添了巨大价值。Microsoft IPAM 中的不一致会造成当前网络拓扑状态与 Microsoft Active Directory (AD) 中的信息不一致。这可能导致用户身份验证和文件可用性等基本服务彻底中断。

Infoblox IPAM 还能与 Microsoft AD 站点和服务无缝集成，为 AD 和网络管理员填补了这一空白。此外，Infoblox 跨越 Microsoft Forests，将整个 Microsoft 环境纳入集中管理的 GUI 中，提供前所未有的可视性、运营效率和服务正常运行时间。

有关详细信息，请参阅组策略 MVP Jeremy Moskowitz 撰写的“Microsoft vs Non-Microsoft DNS: Facts vs Fiction”（Microsoft 与非 Microsoft DNS：事实与虚构）。

Infoblox 与其他生态系统中的产品集成

Infoblox 还提供与领先安全和管理技术的无缝集成。我们通过开放 API 实现智能自动化，并支持跨云和本地环境的工作负载。我们的产品包括具有高级威胁情报和生态系统集成的情境感知安全功能。

作为更大的安全生态系统的一部分，Infoblox 还支持 REST 和 PERL API，以及基于事件的对外 API，可与安全基础设施中的其他系统交互，以便在网络终端添加到 IPAM 时对其进行扫描，在终端设备发送的DNS查询与 RPZ 规则（包括威胁洞察）相匹配时触发设备扫描和/或隔离等。此外，Infoblox 还与 Cisco ISE、McAfee 等 100 多家公司集成，而且这一数字还在不断增长。

结论

您应该做什么

“免费”系统，例如 BIND/DHCPD、Microsoft DNS/DHCP 和电子表格，并不能充分满足现代网络的需求。花时间检查您的核心网络服务中的弱点并制定一项计划，迁移到统一的 IPAM 系统。

确定您现有的工作流程和 IPAM 流程，并找出可以改进的地方：

- 可靠的正常运行时间
- 易于更改
- 实时端点和拓扑可视性
- 与自动化系统集成
- 冗余和/或快速恢复时间

此外，作为市场领导者，Infoblox 拥有超过 50% 的市场份额和 13,000 多个客户，其口碑也是有目共睹的。我们有许多资源可帮助您做出决定：https://www.infoblox.com/resources/?category=Whitepaprs

接下来的步骤

请联系您的 Infoblox 销售团队，讨论建议的部署架构。

公司总部
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com