

数据表

NS1 优势

- 通过集成 DNS 与 DHCP 服务，将管理视图与任务自动化相结合
- 一键式软件升级，轻松添加新功能并保障安全使用
- 高可用性、快速的网络故障转移和数据库同步
- 安全性增强，具备 DNS 攻击检测与缓解功能
- 保障安全管理，使用基于安全套接层的 VPN，可在任意地点透过任何防火墙运行
- Infoblox 视图是 BIND 视图的增强版，提供虚拟 DNS 服务，并使单个 Infoblox 设备可以根据查询源的不同，对 DNS 查询做出不同的响应
- 内置式 TFTP、FTP 和 HTTP 服务器，可以为网络设备分配固件和配置文件，例如在启动过程中分配因特网语音协议 (VoIP) 电话和无线接入点

NS1 软件包特点和优势

NS1 软件包能够交付可信赖、可管理和可扩展的服务，并能有效保障核心网络服务，与服务器软件相比成本更低、安全性更高，并拥有比其他解决方案更为强大的网络可用性。NS1 软件包所提供的服务包括：

- 通过域名系统 (DNS) 提供域名服务；
- 通过动态主机配置协议 (DHCP) 提供地址服务；
- 通过 IP 地址管理 (IPAM) 提供网络可视性并进行控制；
- 通过简单文件传输协议 (FTP、HTTP 和 TFTP) 提供文件交付服务；
- 通过网络时间协议 (NTP) 提供时间同步服务；

其他优势

高可用性服务：NS1 软件包在可靠的 Infoblox 设备平台上运行，这些平台能够在高性能网络中进行连续操作。高可用性 (HA) 服务以两种关键技术为依托，一种是 bloxHA™ 技术（该技术采用了行业标准的虚拟路由器冗余协议 (VRRP)，实现了 5 秒内网络故障转移），一种是 bloxSYNC™ 技术，从而确保了实时数据库同步时不会遗漏或重复数据。综合运用这两项技术，使得关键名称服务器和动态主机配置协议 (DHCP) 服务总能及时响应并不断更新，并消除了发布重复的 IP 地址等常见而又棘手的问题。

集成的零管理数据库：NS1 软件包将所有 DNS 和 DHCP 数据储存在集成 bloxSDB™ 数据库中，该数据库内置于所有 Infoblox 设备的 Infoblox NIOS™ 操作系统软件中。bloxSDB 数据库专为支持集成核心网络服务而设计，并在不损害性能的前提下，为服务和基于 IP 地址的网络服务数据管理视图之间提供了无与伦比的一致性。

集成 Web GUI：凭借 Infoblox Web GUI，管理员只需轻点几下鼠标，就能够部署并管理整个 DNS、DHCP 和 IPAM 基础架构。基于网络的 Infoblox GUI 功能强大，是唯一一款无需借助客户端架构或命令行接口，就能够全面管理所有基础架构和数据的解决方案（包括软件更新与升级、备份与恢复、灾难恢复，以及所有服务和数据管理）。

• Infoblox Web UI 能够管理产品的各个方面，包括 DNS、DNS 安全扩展 (DNSSEC)、DHCP、IPAM 和网络管理、监控和报告。向导和图形化工具可以保证配置和管理没有误差。

集成管理：NS1 软件包可以提供实际的操作效能，降低总体拥有成本。例如，创建 DHCP 范围时将自动创建一份关联的 DNS 记录，减少网络管理员需要完成的工作数量。



Infoblox NS1 软件包可以在所有 Infoblox 设备平台上获得。

数据表

粒度，基于角色的管理：基于角色的管理是一种功能强大的方法，可以确保管理员只能获得特定的权限，从而只能查看和修改与其组织和职能角色相符的特定核心网络服务。例如，某位高级 DNS 管理员可以定义新域并向网格中添加新设备，而某位服务台管理员可能只能查看特定子网，并从预定义的列表中选择向新设备发布的 IP 地址。Infoblox 创建了一个可扩展性很强，且粒度很大的基于角色的管理框架。该框架使客户在授予下方目标级管理权限的同时，又能够维持复杂的大型管理模型的权限。详细情况如下：

- 简化管理权限的流程。管理员可以右键点击任何目标，在权限列表中设置权限。与转到单独的管理面板相比，这种方法要简单许多。此外，它还提供了一个详尽的列表，注明了已授予各个管理组的权限。
- 使用角色也让管理更为轻松。可以将角色映射到某个组织或工作中（例如打印机管理员、DNS 管理员），然后将角色分配给管理组。这种抽象模型可以在所有与角色关联的组继承角色的更改后，对一系列权限进行定义。

安全性增强：Infoblox NIOS™ 软件能够在要求最为严苛的政府和军事组织中，加强安全扫描并持续对抗攻击。NS1 软件包中提供的 DNS 和 DHCP 服务能够轻松升级，以支持最新版的伯克利互联网域名 (BIND) 和 DHCP，确保将安全风险降到最小。一旦发现某个新的利用漏洞，强大的 Infoblox NIOS 软件就可以在几分钟内通过一项简单的操作完成升级，相比于带有已知漏洞的通用操作系统来说更为安全。此外，该软件还利用安全套接层 (SSL) 加密 VPN 来保障管理通信，以免破坏管理水平。

DNS 攻击检测与缓解：Infoblox 可以检测、提醒并缓解针对配置为递归 DNS 服务器的成员的攻击。NIOS 软件将对两大标志攻击的参数进行监控：匹配错误的 DNS 消息 ID 和 DNS 响应中匹配错误的用户数据报协议 (UDP) 端口。当某个攻击者猜测这些参数，使用有毒数据“欺骗”某个响应时，即会出现这种情况。管理员可以对两个参数设置临界值，当其中任何一个参数超过临界值时，系统就会发送电子邮件提醒和/或 SNMP 陷阱（根据系统配置决定）。这一功能可以及时提醒管理员某个服务器正受到攻击。

此外，Infoblox NIOS 可以执行查询速率限制以缓解攻击。管理员可以在某个特定 IP 或网络中执行过滤，以限制或截止所有流量。这样可以减缓或阻止攻击，这种做法能否成功取决于攻击者的能力，看他能否在合法的 DNS 服务器做出响应之前，尝试尽可能多的响应“猜测”。

一键式 DNSSEC：Infoblox 拥有“一键式 DNSSEC”解决方案，可以自动处理签名流程并维护签名区域，从而消除数十项容易出错的手动操作，并消除编写和维护自定义脚本的需要。此外，可以使用网格或区域级中指定的 DNSSEC 属性自动生成密钥；资源记录签名也可以得到维护；而且，根据国家标准和技术研究所推荐的最佳实践 (NIST-800-81) 以及 RFC 4641 标准，可以自动、持续地进行区域签名密钥轮换。

可扩展的集成管理

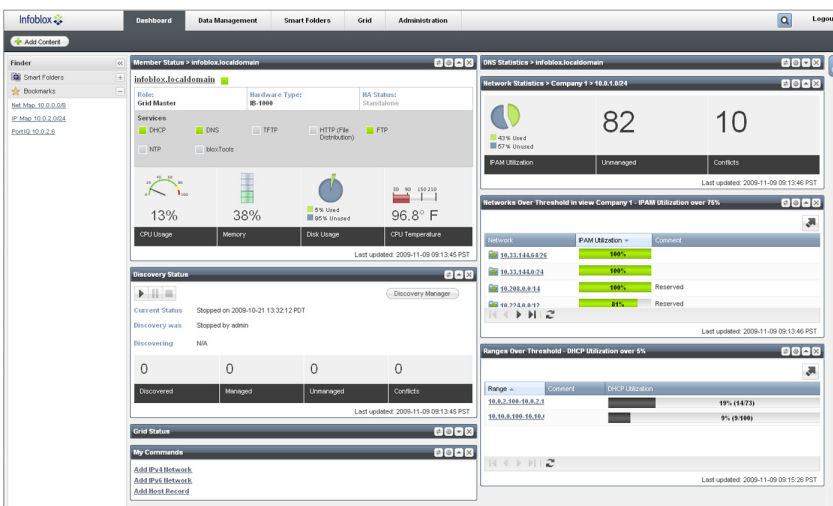
灵活的 Infoblox Device Manager 用户界面提供了动态 IP 网络中管理所有核心网络服务所需的可视性和控制力。Infoblox Device Manager 简化了设备、服务和数据的管理 — 轻轻一点击，即可查看概要和细分视图。凭借基于角色的粒度管理功能，管理员得以授权初级人员或部门工作人员管理特定的网络、范围、主机和设备。Infoblox Device Manager 使我们能够轻松应对复杂多变的网络，而且，由于所有数据都储存在 Infoblox 设备数据库中，Infoblox Device Manager 中显示的设备和服务状态总能反映出真实、实时的网络状态。

关键网络解决方案的不间断运行基础架构

Infoblox 网络服务设备包括众多特殊功能，可以服务于关键网络应用：

IP 语音

用户要求语音通信具备拨号音可靠性。要在 IP 环境中达到这种可靠性级别，需要运用连续的 DHCP 服务向 IP 语音听筒和 IP 软件电话分配 IP 地址，同时还要提供更新电话固件和配置的服务。NS1 软件包拥有众多组合服务，可以为 IP 语音设备提供易于管理、高可用性的解决方案：



使用 Infoblox Device Manager 管理设备、服务和数据。

高可用性 DHCP

Infoblox 支持行业标准 DHCP 故障转移协议，可以部署在分布式广域网 (WAN) 中。此外，可以在“HA 模式”中轻松配置成对的 Infoblox 设备，从而在不降低 IP 地址分配效率的情况下，提供快速故障转移和实时数据同步。

内置式 TFTP、FTP 和 HTTP

过去，TFTP 是由单独管理的孤立服务器提供的，这些服务器位于不同的位置，没有实现集中控制，而且缺乏高可用性。NS1 软件包通过提供可靠且易于管理的 TFTP 服务来管理 IP 电话技术，从而扩大了网络服务设备的优势。

固件和配置文件均上传到设备中，并在启动时为 IP 电话提供服务。此外，在电话环境中还可以利用一对 HA 设备来增强可靠性，从而提供可靠的 TFTP 服务。

数据表



可靠的 Microsoft 活动目录 (AD) DNS 基础架构

Infoblox 是微软金牌认证合作伙伴，Infoblox NS1 软件包为轻松集成微软 AD 环境提供了特别支持。凭借这一功能，企业可以确保其微软或非微软设备所需要的关键 DNS 服务始终安全可用。

性能与功能规格						
	Infoblox-250-A	Infoblox-550-A	Infoblox-1050-A	Infoblox-1550/2-A	Infoblox-1852-A	Infoblox-2000
DNS 每秒查询数	3,000	12,000	24,000	36,000	110,000	75,000
DHCP 租约/秒	25	75	150	225	225	750

DNS 技术规格	
支持 RFC	1034 和 1035 动态更新, RFC 2136 增量区域传输, RFC 1995 区域变更通知, RFC 1996 密钥事务验证 (TSIG), RFC 2845 无类别 IN-ADDR.ARPA 授权, RFC 2317
协议引擎	BIND 9.6.1
额外功能	<ul style="list-style-type: none"> 使用事务数字签名 (TSIG) 进行安全的动态 DNS 更新 条件转发器 Microsoft 活动目录支持 Infoblox 视图 基于 IP 地址的查询、区域传输和动态更新访问列表 区域导入工具 自定义生存期 (TTL) 设置

DHCP 技术规格	
支持 RFC	请求注解 (RFC) 3046、2131 和 1531 BOOTP、RFC 1534、2132, 和 RFC 4388
协议引擎	DHCPD 3.1
额外功能	<ul style="list-style-type: none"> 支持可变长度子网掩码 (VLSM) 支持无类别域间选路 (CIDR) 每个分段中多个子网 (超网) 基于 MAC 地址的“静态租约” (手动分配) 基于 MAC 地址的过滤 分派前执行地址可用性检查 DHCP 中继代理/支持 Option 82 DHCP 供应商类别标识符/支持 Option 60 发布租约时对 DHCP-DNS 集成进行安全更新 增强版 DHCP 选项编辑器 Windows、Unix 和 Mac OS 兼容性 支持外部系统日志服务器

Infoblox 产品保修与服务

标准硬件保修期为一年。系统软件保修期为 90 天，按照公布的规范执行。用户也可以选择各种服务产品，以延长硬件和软件的保修期。我们建议您选择这些产品，以确保设备及时获得最新的软件增强功能，并确保系统的安全性与可用性。Infoblox 还提供各种专业服务和培训课程。本文内容如有更改，恕不另行通知。Infoblox Inc. 对本文中出现的错误不承担任何责任。