

Utility-Grade Core Network Services



稳定且安全的网络核心服务



Infoblox 网络服务设备是专门为网络核心服务，包含 **DNS**、**DHCP**、**IPAM** 以及 **RADIUS**，提供一个可靠、可扩充、安全的平台。全功能的 Infoblox 结合了硬设备的简易特性，以及先进的分布式数据库技术，提供多功能、强化的网络服务，进而达到可用性、易用性、可见性与控制性，这些是采用传统技术的解决方案所无法媲美。Infoblox 核心基础的 NIOS 软件是一个安全强化、实时的操作系统，内建「零管理」的数据库，用以支持高可靠度的作业，Infoblox 具备多个模块，提供各种网络服务，包含有：

- Domain Name System (DNS) 命名服务 (Naming Services)
- Dynamic Host Configuration Protocol (DHCP) 地址服务 (Addressing Services)
- IP address management (IPAM) 的 IP 地址管理，强化网络的可见性与控制机制
- NAC Foundation 模块与专属网站，提供网络存取控管 (Network Access Control) 服务
- RADIUS 身份识别认证服务
- Trivial File Transfer Protocol (TFTP) 与 HTTP 组态服务 (Configuration Services)
- Network Time Protocol (NTP) 时间同步服务
- Syslog 登录记录服务

Infoblox 设备提供了不间断的网络核心服务，包含：DNS、DHCP、IPAM、RADIUS、TFTP、NTP 等等，这些服务可说是所有 IP 网络运作的关键所在。由于硬设备本质上比一般软件服务器更加稳定、容易管理、可扩展性高与更具安全，因此，不管组织的规模大小，使用硬设备提供此类服务已经成为市场上广受欢迎的实务应用与趋势。对于大型组织而言，分散各地的 Infoblox 设备可以连接在一起而形成一致性的网格（Grid），具有极佳的管理性、控制性、可见性与服务弹性。

Infoblox 基础软件 (NIOS) 采用全新的强化机制与功能，包含：完全地整合 IPv6 双堆栈网络 (IPv6 dual-stack networking) 以支持 DNS over IPv6，提供全新的 IPAM 功能，例如：资源回收文件 (Recycle Bin)、区域阻隔 (Zone Locking) 与强大的稽核纪录，以及新的 NAC Foundation 模块，提供认证型 DHCP、可结合 McAfee ePO 与专属认证 Web 网站。

在每台 Infoblox 设备上的 NIOS 软件均有功能强大的 API 接口，让外部的应用程序藉其连接设备上的服务与应用程序。透过此 API，第三方的应用程序可以汇入既有 DNS 与 DHCP 系统的数据，读取与修改 Infoblox 设备上 bloxDB 数据库，执行管理作业，以及汇出备存与报表所需的数据。

▼ Infoblox 具备的网络服务与通讯协议

PROTOCOL	SERVICES
DNS (Domain Name System)	Naming
DHCP (Dynamic Host Configuration Protocol)	Addressing
IPAM (IP Address Management)	Management
RADIUS (Remote Access Dial-In User Service)	Authentication
TFTP (Trivial File Transfer Protocol)	Configuration
NTP (Network Time Protocol)	Time Sync

功能与效益

高可靠度服务

由 bloxHA™ 技术所建构的高可靠度 (High-availability, HA) 服务，是在主要 (Active) 与备用 (Backup) 设备之间，采用业界标准的 Virtual Router Redundancy Protocol (VRRP)，可以在 5 秒之内完成网络故障复原。而 bloxSYNCTM 技术则是确保数据库的实时同步作业，避免发生数据遗漏或重复。此二技术让重要的 DNS、DHCP、RADIUS、TFTP 与其它服务，均能保持响应能力与最新状态，同时避免诸如 IP 地址重复等一般常见却又棘手的问题。

整合式、零管理的数据库系统

Infoblox NIOS 软件将所有的网络数据，包含：IP 地址、计算机名称、MAC 地址、用户身份认证以及其它数据，储存在一个整合式 bloxSDB 数据库中。此数据库是特地为支持整合式网络服务而设计，可以在 IP 网络数据服务与管理的权衡之下，提供最佳的一致性，且不需担心效能问题。

容易使用的 GUI 接口

Infoblox Grid Manager 可执行于 Windows 2000/XP 或者 Linux PC 上，以数据为中心的使用接口使得复杂、重复的管理操作变得更加简单，让管理者可以专注于资料与服务，而不是装置机器与通讯协议。而新增的功能，则进阶地提升其使用能力，包含：透过 DNS 区域锁定提供细密严谨的异动管理，以及利用资源回收筒 (Recycle Bin)，当意外删除大型 DNS 区域和 DHCP 网络时，可以提供“undo”功能，以减少管理时间，同时避免一般常见的数据输入错误。

整合式管理

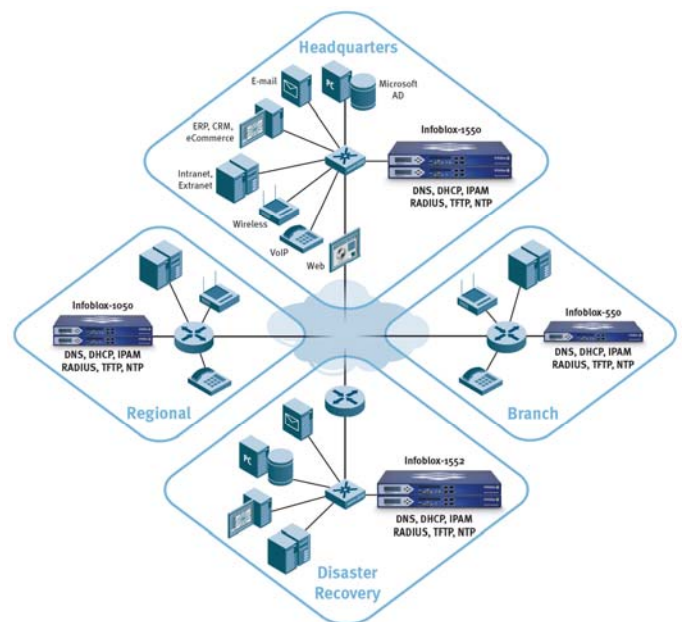
Infoblox 具有极佳的运作效能，可以降低系统建置的总成本。例如：自动建立 DHCP 范围会产生一个关连的 DNS 纪录，而减少多个需要倚赖网络管理者的工作；自动将用户凭证分派到 Grid 网格中提供 RADIUS 服务的设备，使一个身份凭证即可让所有提供 RADIUS 服务的设备一起共享；再者，可以上传档案到 Grid Master，并且透过 TFTP 与 HTTP 自动分派到所有提供档案服务的设备上。这些功能不仅可以节省时间，同时亦能提升服务质量。

个别、角色导向的分权管理

管理者可以指派个别的区域、网络、装置甚至特定资源纪录类别给其它管理者，也可以产生“只读”的组态档案给受指派的管理者。因此，即可将部份的网络资源，配合严谨的稽核纪录，而授权给组织管理上不同单位的个人。

强化的安全性

Infoblox NIOS 软件是经过安全强化，且通过安全扫描与攻击的测试与考验。一旦发表新的版本，底层的 Infoblox NIOS 软件可以在几分钟内，经由单一、简便的操作即可完成升级，相较于一般具有已知漏洞的操作系统，此将使其更难渗透。另外，为了控管管理上的损失，管理通讯都是使用加密的 SSL 来进行安全防护。



▲ Infoblox Grid 确保通讯协议、数据与档案的数据完整性

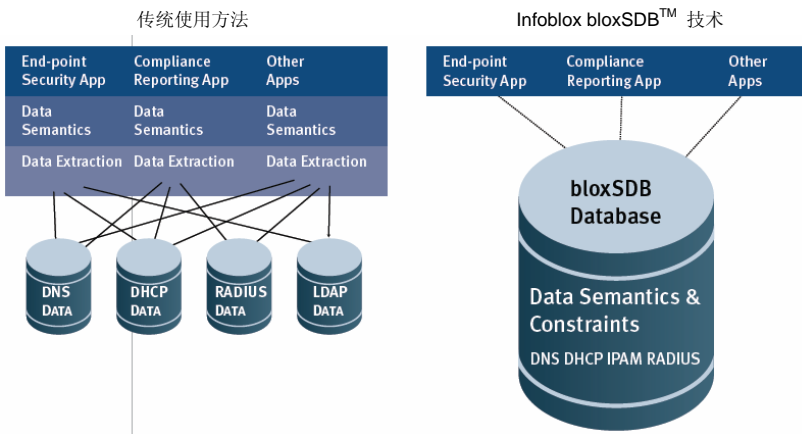
Infoblox NIOS 模块与套餐

Infoblox NIOS 软件具有多个功能独特的模块，针对不同客户的需求，Infoblox 将不同的 NIOS 软件模块组成多个软件套餐，如右表所示。

SOFTWARE PACKAGES	NIOS SOFTWARE MODULES											
<i>Infoblox software packages run on Infoblox network services appliance.</i>	DNS	DHCP	IPAM	NTP	RADIUS	RADIUS Proxy	TFTP/HTTP	Syslog NG Proxy	Grid	AD Agent	VitalQIP Integration	NAC Foundation
DNSone	◆	◆	◆	◆	—	◆	◆	◆	—	—	—	◆
DNSone with Grid	◆	◆	◆	◆	—	◆	◆	◆	◆	—	—	◆
Network Services for Authentication (NSA)	—	—	—	◆	◆	◆	◆	◆	◆	◆	—	—
Network Services for VitalQIP (NSQ)	—	—	—	◆	—	◆	◆	◆	◆	—	◆	—
Network Services for VoIP (NSV)	—	◆	◆	◆	—	◆	◆	◆	◆	—	—	◆
Network Services Suite (NSS)	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	—	◆

DNS 模块

具有高效能、多功能的 DNS 服务，采用业界标准的 BIND 通讯协议引擎，并且修改使其可与 bloxSDB 数据库一起运作，此组合提供了通过验证之通讯协议引擎的好处，也兼具复杂数据使用子系统的效益，以确保交易的完整性，避免使用档案系统所容易导致的数据损毁、错误与遗失。DNS 模块主要功能有：弹性部署并设定 Primary、Secondary、Forwarding 或 Caching 等角色、具有 Anycast 特性、动态 DNS (DDNS) 实时更新、支持 GSS-TSIG 签署、支持 IPv6 与 IPv4 双堆栈 (Dual Stack)、使用单一图形应用程序管理 DNS 数据与服务、区域锁定以及主机名称与名称服务套表等。



▲ 传统数据库解决方案与 bloxSDB 整合式数据库的差异

IPAM 模块

IP 地址管理 (IPAM) 协助客户管理企业级的 DNS 与 IP 地址数据，支持一致性的处理、监控与工作管理，以提供适当的集中式稽核与报表。Infoblox 在 IP 地址管理 (IPAM) 上采用全新的方法，特别是结合目前最新的数据管理 (分布式数据库) 技术，以及专为建构网络服务而设计的特定硬设备，提供第一且唯一的整合式 DNS、DHCP 和 IPAM 设备。IPAM 模块主要功能有：整合式 IP 管理控制台、地址使用追踪、动态地址控管、装置分类、IP 地址状态浏览器与临界通知、网络套表、整体搜寻、资源回收文件 (Recycle Bin) 以及数据一致性检查。

RADIUS 模块

主要是为网络装置与用户提供可靠且高可用性的认证服务，藉由标准 RADIUS 认证服务与 Infoblox Grid 技术的整合，企业只要简单地各处使用 Infoblox 设备，即可强化企业提供分散而可靠、安全、无间断的认证服务能力。其可支持 Microsoft Active Directory /LDAP、本机用户、使用 MAC 地址或 PEAP/EAP-MSCHAPv2 与个人端凭证 (EAP-TLS) 认证，以及自动支持多种认证方式，具有 Grid 用户身份复制以及 HA 故障复原机制。

基础服务

Infoblox NIOS 软件提供一组在分布式网络中非常有用的基础服务，包含：TFTP、HTTP、NTP、Syslog NG Proxy 与 RADIUS Proxy。

DHCP 模块

提供高效能、多功能的 DHCP 服务，采用业界标准 ISC DHCP 通讯协议引擎的强化版本，同时与 Infoblox bloxSDB 数据库技术紧密结合。Infoblox 的强化让 DHCP Server 在短短几秒之内即能重新启动，避免完全重新启动所需的作业。Infoblox 在 DHCP 故障复原的建置上，可以避免采用标准方法的已知限制，同时亦可提供可靠的故障复原作业，避免在标准 DHCP 建置中，经常会出现的闭锁状况与错误。

此外，此模块也具有以下功能：DHCP 租用信息的使用报告、切割/合并网络、单一图形应用程序管理 DHCP 数据与服务、进阶 DHCP 选项编辑器等等。

Grid 模块

是 Infoblox 专利申请中的核心技术，提供全功能的系统管理、数据分散与系统可用性，用以连接分散各地的设备，使其成为一个 Infoblox 网络 (Grid)，让一致化、集中管理的设备系统可以分享一个共有的、实时的分布式数据库。在 Infoblox Grid 中各个设备之间，可以透过 SSL 而建立安全的通讯，同时也使用复杂的异动管理技术，维持数据的完整性，范围包含：(1) 通讯协议—DNS, DHCP, RADIUS, LDAP, TFTP, NTP 等，(2) 数据—IP 地址、MAC 地址、使用者凭证、交易纪录、时间等，(3) 档案—设备软件、装置韧体与设定文件、管理政策。

Grid 模块有弹性运作与统一管理特性，同时包含：实时、安全、全系统的数据更新，数据不会损毁、错误或遗失，个别、角色导向的网络装置、数据与服务管理，具备智能型自动预防措施提供简易的装置预先配置与自动回复，以及灾难复原与 Grid Master 升级。

NAC Foundation 模块

让 Infoblox DHCP 服务具备智能型、政策导向的控管机制，可将其组件与单一或多个解决方案整合，而提供一个崭新的 NAC 解决方案。NAC Foundation 模块亦有助于流程的自动化，包含 DHCP Server MAC 过滤器的建置，以及根据用户的环境设定政策而将装置归属到特定网络区段。此模块功能有：针对使用者注册的管理与认证提供整合式专属 Web 网站、整合式 DHCP 认证、访客存取、自动设定 MAC 过滤器的登入时限、整合 McAfee Enterprise Policy Orchestrator (ePO)、设定使用者类别、MAC 和 IP 与使用者信息的纪录连结。



网络服务设备规格

Infoblox 设备支持各种小、中、大型的网络架构，并且拥有独立配置的特性，可以弹性地提供最理想的网络服务。

	Infoblox-250	Infoblox-550	Infoblox-1050	Infoblox-1550/1552	Infoblox-2000
DNS Queries Per Second	3,000	12,000	24,000	36,000	75,000
DHCP Leases Per Second	25	75	150	225	700
Capacity (Database Objects)	12,500	25,000	150,000	400,000	1,200,000

DNS 技术规格

RFCs supported 1034 and 1035
Dynamic update, RFC 2136
Incremental zone transfer, RFC 1995
Notification of zone changes, RFC 1996
Secret key transaction authentication (TSIG), RFC 2845
Classless IN-ADDR.ARPA delegation, RFC 2317

Protocol engine BIND 9.3.4

- Additional Capabilities**
- Secure dynamic DNS updates using TSIG
 - Conditional forwarding
 - Microsoft Active Directory support
 - Infoblox Views
 - IP-address-based access lists on queries, zone transfers, and dynamic updates
 - Zone import tools
 - Customizable TTL settings

DHCP 技术规格

RFCs supported RFCs 3046, 2131 and 1531
BOOTP, RFCs 1534 and 2132

Protocol engine DHCPD 3.0.1

- Additional Capabilities**
- VLSM (Variable Length Subnet Mask) support
 - CIDR (Classless Inter-Domain Routing) support
 - Multiple subnets per segment (supernetting)
 - "Static leases" based on MAC address (manual allocation)
 - MAC-address-based filtering
 - Address availability checking before assignment
 - DHCP relay agent/Option 82 support
 - Secure DHCP-DNS integration updates DNS when leases are issued
 - Advanced DHCP Options Editor
 - Windows, Unix, and Mac OS compatibility
 - External syslog server support

RADIUS 技术规格

Protocol engine FreeRADIUS 1.1.3

- Authentication Methods**
- PAP - Password Authentication Protocol
 - CHAP, MS-CHAP and MS-CHAPv2 - Challenge Handshake Authentication Protocol
 - EAP - Extensible Authentication Protocol for 802.1x port-based authentication
EAP-TLS, EAP-MSCHAPv2, EAP-GTC
 - PEAP - Protected Extensible Authentication Protocol for 802.1x port-based authentication
PEAP/EAP-GTC, PEAP/ EAP-MSCHAPv2 (authentication method natively supported by Microsoft Windows clients)
 - EAP/TLS - Extensible Authentication Protocol Transport Layer Security, provides mutual authentication, requires client certificates
 - EAP-TTLS/EAP-PAP, EAP-TTLS/EAP-CHAP, EAP-TTLS/EAP-MS-CHAP, EAP-TTLS/EAP-MS-CHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-TTLS/EAP-GTC

授权经销商

Infoblox 授权代理商



上海达友信息科技有限公司

Docutek Solutions (Shanghai), Inc.

地址：上海徐汇区中山西路 2025 号永升大厦 1724 室

电话：+86-21-64392970 传真：+86-21-64397261 转 808

网址：www.docutek.com.cn