

可靠、安全的核心网络服务

Infoblox的 NIOS™ 软件，在 Infoblox 设备中运行，负责传送不间断的核心网络服务—包括 DNS、DHCP、IPAM、RADIUS、TFTP、NTP等—这些服务对所有基于IP的网络都是至关重要的。无论企业规模大小，采用设备发送这些服务已经为业界推荐的最佳选择，因为设备固有的可靠性、可管理性、可扩展性、及安全性比通用服务器上软件的特性更出色。对于大型企业，分布式的 Infoblox 设备可以连接成统一的网格，提供无可比拟的可管理性、可控制性、可视性及服务可恢复性。

Infoblox NIOS 4.1r3 软件主要的新增特性和功能包括：IPv6 双堆栈网络互联，完全集成并支持 IPv6 上的 DNS，新的 IPAM 功能，例如回收站、区域锁定、及增强版的审计日志，新的 NAC Foundation 模块，可提供 DHCP 认证、McAfee 集成及受控的网络门户。

Infoblox NIOS 软件是一款加固安全性的、实时操作系统，内置一个零管理数据库，并对高可用性操作有很好的支持。Infoblox NIOS 提供的系列模块支持多种网络服务，包括：

- 域名系统 (DNS) 提供名称服务；
- 动态主机配置协议 (DHCP) 提供地址分配服务；
- IP 地址管理提供网络可见性和网络控制服务；
- 强制网络门户与 NAC Foundation 模块提供的网络访问控制服务；
- 认证服务 (RADIUS) ；
- HTTP 与普通文件传输协议 (TFTP) 提供的配置服务；
- 网络时间协议 (NTP) 提供时间同步服务
- Syslog 提供的日志服务

同时 Infoblox NIOS 软件所支持的其他模块提供了独有的功能。其中主要的是网格模块，它采用了 Infoblox 正在申请的专利技术，可以把分布式的设备连接成 Infoblox 网络：统一化的、集中管理的设备系统共享统一的、实时的数据库。Infoblox 网络在设备中采用了安全通信技术 SSL，并使用复杂的事务管理技术来维护数据完整性。这样可以保证网格中的所有设备都能获得正确的数据，并且在出现设备故障和广域网失效的情况下，网格仍能提供服务而不出现数据丢失和损毁。Infoblox 的网格技术支持智能数据复制以减少网格的带宽，并确保每个位置都部署“大小合适”的设备。配合 Alcatel-Lucent VitalQIP® 使用的集成模块把 Infoblox 设备和网格的优势扩展到 Alcatel-Lucent VitalQIP® 远程服务器软件中。

每个 Infoblox 设备中安装的 Infoblox NIOS™ 软件都包括了强大的 API，可供外部应用调用并与内部的设备和服务相交互。通过 API，第三方应用可以从现有的 DNS 和 DHCP 系统导入数据，在 Infoblox 设备的 bloxSDB™ 数据库中读取和更改数据，完成管理性操作，以及导出数据进行存储和输出报表。

Infoblox 工具箱中的软件能够极大地减少与 Infoblox API 交互的工作。Infoblox 的售后支持和专业的服务团队提供的工具箱库可以处理数据的导入 / 导出和移植任务。Infoblox ID Aware™ DHCP 工具箱可从认证的 Infoblox ID Deal Partners 处获得，用于连接 Infoblox DHCP 服务，使之成为一个网络访问控制 (NAC) 解决方案。

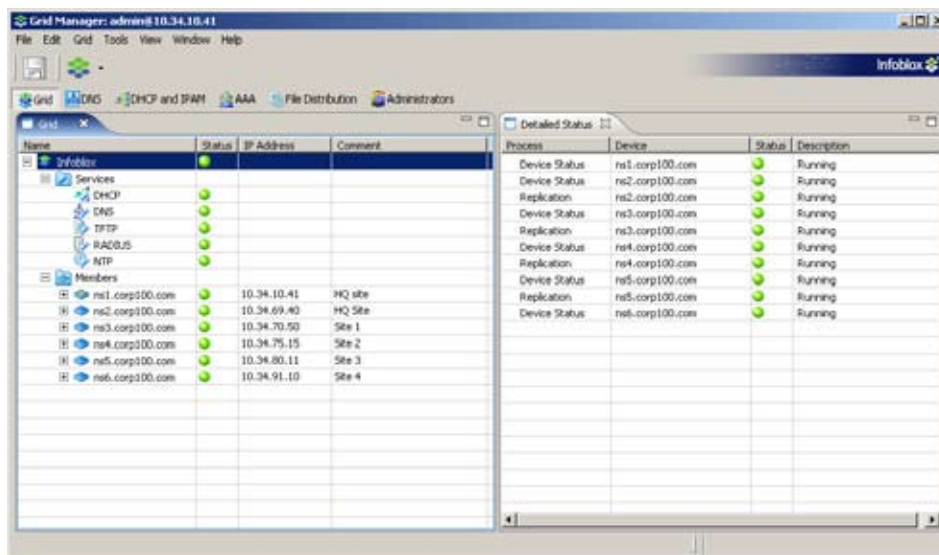
特性与优势

高可用性服务高可用性 (HA) 服务由 bloxHA™ 技术所支持，该服务使用业界标准的虚拟路由冗余协议 (VRRP)，为活动设备和备份设备提供 5 秒内的网络故障恢复功能，还采用 bloxSYNC™ 技术确保实时数据库同步，消除数据丢失与重复。总之，这两种技术使得 DNS, DHCP, RADIUS, TFTP, 及其他核心服务一直保持工作状态，及时升级，并且消除了常见的一些难题，例如发布重复的 IP 地址。

数据表

集成化的、零管理的数据库Infoblox NIOS软件把全部的网络数据—包括IP地址、主机名称、MAC地址、用户保密凭证、及其它数据—保存在bloxSDB数据库中，该数据库是专门设计用来支持集成化的网络服务的，并且为IP网络数据的管理和服务提供了无法比拟的一致性，同时保证性能不受损失。

便于使用的网络用户界面：Infoblox NIOS软件包括Infoblox网络管理能够在任何装有Windows XP或者Linux系统的PC上运行。以数据为中心的界面以流水线的方式管理复杂的、重复性的管理操作，因此管理员可以把精力集中于数据和服而不是设备和协议。新增功能包括精细管理，通过DNS区域锁定实现，及通过回收站恢复对大型DNS区域和DHCP网络的意外删除，增强了可用性和性能。这样就减少了管理时间并消除了很多常见的数据项错误。



Infoblox 网络管理器对所有服务、设备及数据的管理实现了统一化。

集成化的管理 Infoblox NIOS 软件提供了实在的操作效率，降低了用户的总成本。例如，创建一个 DHCP 范围时会自动创建一个相关的 DNS 记录，这样就能降低网管员的任务量。用户保密凭证被自动分配到提供 RADIUS 服务的网络中，同一份证书可被所有提供 RADIUS 的设备共享。文件可被上载至网络主控，然后自动分配给所有支持 TFTP 和 HTTP 的文件处理设备。所有这些特性都可以节省时间，提高服务质量。

精细化的，基于角色的管理管理员可以委派其他管理员来管理特定的区域、网络、设备，甚至特定的资源记录类型，管理员还可以为被委派的其他管理员创建“只读”资料。这将允许公司向不同部门的员工下发不同的管理授权，只把部分网络资源授予他们，并且大量使用审计日志进行记录。

安全性加固：Infoblox NIOS 软件具有强化的安全性，能经得住政府和军事部门对安全扫描和入侵要求的考验。发现新变化时，底层的 Infoblox NIOS 软件可在简单的操作下在数分钟内进行升级。入侵这样的系统要比入侵有漏洞的通用操作系统困难很多。管理通信采用安全套接字层（SSL）加密过的VPN来保证管理的安全性。

数据表

INFOBLOX NIOS 模块与套件

Infoblox 套件将NIOS软件模块进行不同的组合来处理不同的客户需要，如下表所示。所有套件都可在任一种型号的Infoblox 设备上获得，有特别说明的除外。

软件套件	NIOS 软件模块											
	DNS	DHCP	IPAM	NTP	RADIUS	RADIUS Proxy	TFTP/ HTTP	Syslog NG Proxy	网络	AD Agent	VITALQIP 集成	NAC FOUNDATIONS
Infoblox套件运行在Infoblox网络服务设备上。												
DNSONE	●	●	●	●	-	●	●	●	-	-	-	●
带有网络的DNSONE 套件	●	●	●	●	-	●	●	●	●	-	-	●
提供鉴定服务的网络服务套件(NSA)	-	-	-	●	●	●	●	●	●	●	-	-
提供VITALQIP服务的网络服务套件(NSQ)*	-	-	-	●	-	●	●	●	●	-	●	-
提供VoIP服务的网络服务套件(NSV)	-	●	●	●	-	●	●	●	●	-	-	●
网络服务套件(NSS)	●	●	●	●	●	●	●	●	●	●	-	●

* 在 INFOBLOX-550、1050、1550、1552、及2000型设备上配备。

DNS 模块

Infoblox DNS 模块提供高性能、多特性的 DNS 服务，采用改进的业界标准 BIND 协议引擎与 bloxSDB 数据库一起工作。这种组合既具备成功协议引擎的优点，又具备成熟数据子系统的优点，能确保事务的完整性，消除数据损毁、出错及丢失等问题，而这些问题常在单文件数据系统中出现。

特性与优势

灵活部署： Infoblox DNS模块可以配置为任何一种角色，包括授权级（首选）、二级、转发级、以及缓存级—所有这些级别都具有高性能。

可靠的DNS服务： 如果DNS服务不可用，整个网络就会瘫痪。因此，该服务必须具有不间断的可用性。bloxHA技术允许两台设备进行组合，形成HA双机，可供可靠的DNS服务。如果活动设备失效，备用设备就会在5秒内接管并继续提供DNS服务，不会出现数据丢失与重复。另外，DNS协议引擎与bloxSDB数据库的这种独特组合可以接受多种更改—例如为区域添加记录—而不用重启服务。这样就消除了许多服务中断现象，而服务中断经常在传统的、基于BIND的DNS服务器升级数据时出现。

Anycast： 为了获得全局分布的、高可靠性的DNS体系结构，企业可以采用Anycast功能将一个IP地址信息发布给由许多分布的设备提供的DNS服务。IP地址可以通过OSPF路由协议发布出去，而当DNS不可用时，IP地址会从路由表中撤销。这样就可以在全局范围分配负载，自动把查询从不工作的设备上转移出来。

实时升级： 动态 DNS (DDNS) 的升级内容会被实时地复制给所有Infoblox网络中的DNS服务器。目前业界的其它DNS服务器还不能提供实时复制DDNS升级的功能。在一个需要准确DNS数据且要求安全性或定位设备—如打印机，在网络上只是一个名称—的环境下，DDNS的实时升级功能是非常重要的。

数据表

GSS-TSIG: 从 Microsoft 客户端发出的动态 DNS (DDNS) 升级可以采用 GSS-TSIG 技术和客户端的 Active Directory 保密凭证进行数字签名。Infoblox DNS 服务器接受 GSS-TSIG 签名的 DDNS 升级信息，并且可以把提供的保密凭证和 Active Directory 内存储的保密凭证进行对比验证。这样用户就可以把 Microsoft Windows 服务器上负责 DNS 的那部分负载转移出来，同时又不损害安全性。Infoblox 基于设备的 GSS-TSIG 解决方案是独一无二的。

支持双堆栈 IPv6 和 IPv4: Infoblox DNS 服务器支持原版 IPv6 和 IPv4。对 IPv6 的支持包括转发区域 (AAAA) IPv6 DNS 记录和 ip6.arpa IPv6 DNS 反向区域。具有 IPv6 联网支持的 DNS 服务器可以让管理员为区域数据传输，以及查询访问列表配置 IPv6 地址；这些 DNS 服务器还能基于 IPv6 地址为查询和区域数据传输提供响应。

单一图形化的应用程序可管理 DNS 数据和服务: 对 DNS 数据的管理任务可以安全地委派给管理员，委派方式可以按照设备、区域及资源记录类型进行划分。

区域锁定: 为防止管理性更改冲突，确保多个管理员同时工作时不出现无法预料的意外结果。区域被管理员锁定后，其他管理员无法对其进行更改直到锁定解除。与其它只能在全局范围进行锁定的系统不同的是，Infoblox 区域锁定功能提供了精细化的管理，可以在区域级进行锁定。

主机名称模板: 管理员可以强制实行命名规范，定义出主机名称模板，然后将其用在网格中、设备中或者区域中。管理员还可以方便地查看报表，找出并修正不符合模板的过时记录。

名称服务器模板: 这个强大的功能允许管理员将更改信息自动传播给多个设备的各个区域中。例如，在一个由 50 台设备提供服务的 500 个区域的系统中，更改一个域名服务器的 IP 地址，该服务器是所有域名区域的辅助服务器—在传统的系统中，该操作需要 25,000 个更改，现在只需要一次操作即可。

DHCP 模块

Infoblox DHCP 模块提供高性能、多特性的 DHCP 服务，采用增强版的、业界标准的 ISC DHCP 协议引擎，与 Infoblox bloxSDB 数据库技术紧密集成。Infoblox 的增强特性使 DHCP 的“服务器重启”只在数秒钟之内，避免了完全重启而进行的多项操作，例如 MAC 过滤器更新，因此减少了服务短缺。另外，Infoblox 所实现的 DHCP 故障恢复功能考虑到了标准方法的缺陷，它是被证明能够提供可靠故障恢复操作，避免了在标准 DHCP 中经常出现的死锁和出错问题。

特性与优势

可靠的 DHCP 服务: DHCP 是一项核心网络服务，被广泛地用来给 PC 和服务器自动提供 IP 地址，在新网络设备层出不穷的今天，例如 IP 电话、RFID 阅读器、数码相机及其它设备等，该服务更是显得尤为重要。Infoblox 提供了多种方法以确保此关键服务的可用性。Infoblox bloxHA 和 bloxSYNC 技术使采用高性能双机部署的设备具有 5 级亚秒的故障恢复能力，同时保证活动设备和备份设备之间的完全同步，防止发布重复 IP 地址。Infoblox 还支持 DHCP 故障恢复协议，使位于不同网络的设备也可以具有高可用性。有了 DHCP 故障恢复功能，一个 DHCP 服务器就可以备份多个远程 DHCP 服务器，在提供可靠性的同时节约了成本。

历史 DHCP 租赁信息报表: Infoblox DHCP 服务存储了所有 DHCP 租赁的历史信息，它们被保存在内置的 bloxSDB 数据库中，以便日后检索。这不仅帮助管理员快速定位故障，还可以按照复杂的要求追踪一些安全问题。

分割 / 联合网络: 当企业开始发展壮大，无论其通过组织的扩展还是通过兼并收购，都需要对其 DHCP 网络配置有灵活的控制。分割 / 联合网络功能使企业方便地顺应当今动态的网络。分割网络功能使管理员可以迅速、简洁、且准确的进行子网划分，并且使子网继承主网的配置。联合 / 扩展网络功能的独到之处在于它允许管理员把相对较小的网络“扩展”成较大的网络，而不丢失配置信息，包括固定地址、动态范围、以及其它 DHCP 选项。

单一图形化的应用程序可管理 DHCP 数据和服务: 对于 DHCP、IP 地址数据、和运行在 Infoblox 设备上的 DHCP 服务器，对它们的管理可以安全地委派给设备管理员和子网管理员。使用 Infoblox 网络管理应用程序对 DHCP、IP 地址数据、

数据表

及 DHCP 服务进行管理具有快速、方便、及高效等特点。

高级 DHCP 选项编辑器对于许多应用来说，配置 DHCP 选项很关键，例如用户配置、VoIP、及无线接入点等。配置 DHCP 选项较为复杂。NIOS 内含一个图形用户界面的选项编辑器，可以简化标准和自定义 DHCP 选项配置工作。

IPAM 模块

IP地址管理(IPAM)功能使客户能够在企业范围管理DNS和地址数据，进行统一的管理和监控，同时提供适当的集中化审计和报表功能。

Infoblox IPAM 模块采取了新的方法来处理IP地址管理 (IPAM)。简言之，Infoblox 结合当今最尖端的数据管理技术 (分布式数据库) 和最尖端的发送网络服务的载体 (专门设计的设备)，来提供首创的、独一无二的集成DNS、DHCP、及IPAM的设备。与一般新、旧版本的IPAM系统不同的是——一般的IPAM系统都是数据发送体系结构中的一些插件——而Infoblox的方法可以简述为“内置而非插件”。

Infoblox 采用了独创的技术，提供的关键特性使用户获利极大，而这些特性在同类竞争产品中还没有出现，这些特性包括丰富的 IPAM 特性集合、系统全部组件冗余、无缝软件升级、一键式灾难恢复、实时报表、鲁棒数据管理、以及低廉的部署成本和管理成本。

特性与优势

集成化的IP管理控制台：在一个网络用户界面屏幕上，管理员能够通查他们所管理的IP网络，可以按照参数进行排序，例如IP地址、MAC地址、使用状态、设备类型、及位置等——因此简化了许多例行的IP管理任务。因为IPAM功能、实时DNS和DHCP服务都是在同一个数据库中进行操作，所以即便是在最具动态特性的环境下，所有信息都保持同步。

追踪历史地址：该功能允许管理员进行更好地计划、管理，通过IP地址状态 (动态、静态、可用、保留 / 停用)、主机名称、MAC地址、DHCP 租赁信息 (包括租赁日期 / 时间、剩余租期、最近续约时间、强制释放的IP地址) 等信息形成报表，完成复杂的任务要求。

动态地址控制：允许管理员使用DHCP在网络上部署新设备，例如打印机，而不用手动配置设备的网络设置。一旦该设备配置到了网络上，管理员可以将其地址由“动态”更改为“固定”。

设备分类：管理员可以对每个设备进行分类，使用丰富的预设类型 (例如台式机、笔记本、路由器、服务器、打印机等) 或者使用用户自定义的设备类型。每种设备类型，无论是预定义的还是用户自定义的，都提供了用于说明通用信息的字段，例如设备位置、拥有者、生产商、及型号——同时提供了自定义字段，可由管理员进行定义以满足企业特定的要求。

IP地址状态浏览器与阈值报警：阅读器显示了使用中的动态和静态IP地址，以及使用率的百分数。可以为企业中的每个网络设置高、低阈值标准，当需要扩大阈值范围或重新分配阈值时，可以使用与阈值捆绑的电子邮件报警和SNMP traps来提供提醒服务。

网络模板：当创建新的网络时，模板提供了自动生成功能并能强制实行统一标准。模板包括了网络中所有的参数，例如固定IP地址、动态IP地址、以及DHCP选项。在企业完成大规模配置任务时，例如为新增的部门和零售商店进行配置，模板允许企业“克隆”相同的配置。

全局查找：允许用户在全部数据库对象中进行查找，包括动态数据，例如DHCP租赁和DDNS主机数据，并且查找结果在查询窗口中示出，可以对查询结果直接进行编辑或修改。

回收站：网络管理器把所有的管理性删除都存放在一个回收文件内，管理员可以通过一系列的点击来撤销删除。管理员错误地删除了大量数据时，回收站十分有用。

数据表

数据一致性检查: Infoblox 网络管理器软件自动完成多级别的数据一致性及其检查。对于一台主机，管理员可以同步保留 DNS 转发记录和反向区域记录，避免出现不一致的区域数据。输入 IP 地址时，它们会通过动态的检查，管理员会收到出错提示以避免输入无效的数据。

NAC FOUNDATION 模块

Infoblox NAC Foundation 模块对 Infoblox 的 DHCP 服务有智能化的、基于策略的控制，是提供大量 NAC 解决方案的基础，这些方案中的集成组件可以来自一个或多个厂商。

每个允许在 IP 网络上进行通信的设备都包含一个唯一的、强制编码的设备身份标识，称为 MAC 地址。设备发出的每个 DHCP 请求中都会出现其 MAC 地址。Infoblox DHCP 服务器有能力维护 MAC 地址列表，即所谓的 MAC 过滤器，能根据设备地址是否在特定的 MAC 过滤器中来完成不同的行为（例如，分配不同地址范围外的地址）。

向 DHCP 服务器的 MAC 过滤器设置数据和根据用户可配置策略将设备分配到特定网段等操作过程都可通过 NAC Foundation 模块自动处理。例如，管理员可能对于认证过的员工和设备将网络分为一个或多个网段：一个客访网段，仅可访问 Internet 和 / 或受限的公共服务器；和一个隔离网段，仅可访问 Infoblox 设备，或者访问端点扫描与修复系统。这样就可以控制用户和设备对敏感的网络资源进行访问，并能阻止有害软件从敌意用户或受感染的设备中传入。

NAC Foundation 模块完全与 Infoblox NIOS 软件和网格技术集成。所有组件，包括强制网络门户在内都是内置的，都从 Infoblox 网格技术获得好处，例如集中化管理和高可用性故障恢复。NAC Foundation 模块提供了若干关键特性，用户从中获利极大。

特性与优势

集成的强制网络门户: 提供用户熟悉的、像“酒店门户”一样的用户接口，便于管理用户注册与认证。门户中的页面可以方便地进行自定义以适应每个企业的需要，包括企业的 logo、用户使用协议、客服电话等。

集成化的 DHCP 认证: 使用了多种业界标准的认证机制，包括 RADIUS、Active Directory、LDAP 或者本地 NIOS 用户账号。认证机制可以“堆栈化”，以便实现复杂的认证策略，例如：“首先在 AD 服务器上进行认证，若能通过则进入系统，否则检查本地 NIOS 用户数据库。”

客访进入: 客访进入功能可在强制网络门户上启用，可以为每个企业定制该功能，定制内容包括登录时必须的字段，例如姓、名、是否访客等。输入数据时，访客会被放入一个特定的 MAC 过滤器中，然后从访客网络中分配一个 IP 地址。

自动化的 MAC 过滤器记录超时: 系统可以被配置为，在配置的时间超时后自动移除 MAC 记录—包括访客和认证用户的 MAC 记录。这样就可以灵活地配置用户重新认证的频率。

与 MCAFEE ENTERPRISE POLICY ORCHESTRATOR (EPO) 集成: 解决方案可以被设置为查询 EPO 服务器，确定一个客户是否应该被分配一个授权网络中的 IP 地址。EPO 检查可被设置为按照三个参数的组合进行 IP 地址分配：客户是否在 EPO 服务器上注册过；客户是否安装了 MPE 扫描器；以及客户是否在可配置的时间段内同 EPO 服务器进行过通信。

指派用户类别: 将 DA 组信息自动映射到特定的 DHCP 范围。系统可被设置为按照用户的 AD 组成员所属来分配一个 IP 地址，该地址来自另一个网络范围。例如，金融部门的员工分配的 IP 地址在一个网络范围内，而其他所有员工分配的 IP 在另一个网络范围内。

记录与连接用户的 MAC 和 IP 信息: 用户经过认证后，用户名放入 MAC 过滤器中，因此创建一个“链接”把用户、IP 和 MAC 地址联系在一起，便于审计。

RADIUS 模块

Infoblox 的 RADIUS 模块为网络设备和用户提供可靠的高可用性的认证服务。把标准的RADIUS认证服务与Infoblox网络技术进行合并, 并采用易于使用的 Infoblox 设备, 增长中的企业就有能力发布可靠的、安全的、不间断的认证服务, 使之服务于整个企业。

802.1X是业界标准的网络访问认证协议, 是有线和无线网络环境下关键的安全保证, 是实现新安全机制的基础, 例如网络访问控制 (NAC)。802.1X需要三个组件: 请求方, 即运行在客户设备上的一个软件; 网络接入设备, 通常为一个无线接入点或一个有线交换机; 和一个认证服务器, 它采用RADIUS并与网络接入设备进行通信。有了802.1X, 认证服务器就成为网络体系结构中的关键组件。如果认证服务器失效, 或无法访问, 所有访问网络的请求都会被拒绝。因此, 网络认证服务器必须进行最高可靠性的部署, 整个系统的设计必须具有鲁棒性, 以防止服务器失效或者连接远程访问设备的WAN链接失效, 以及集中化的用户目录失效。

特性与优势

与Microsoft Active Directory 相连的Infoblox 网络连接器: 该应用程序安装在Microsoft Windows 服务器上, 并把Active Directory 中保存的用户保密凭证复制到Infoblox的网络主控中, 然后网络主控把该信息复制给有RADIUS模块运行的网络设备上。如果WAN与远程站点的连接失效, 远程站点的设备仍能对试图进入无线网络的用户进行认证。管理员设置好时间间隔后, 与MicrosoftActive Directory 相连的Infoblox 网络连接器会周期性的把变更信息发送给网络主控设备。

本地用户存储: 根据本地用户信息, 提供RADIUS服务并直接与Infoblox网络主控联系, 不需要与Active Directory 或LDAP用户存储相连。

网络中复制用户保密凭证: 所有Infoblox中的设备都可以自动且安全地同步用户名与密码, 确保数据的一致性与强化的实时安全性。

PEAP/EAP-MSCHAPv2与客户端认证 (EAP-TLS) 鉴定: 该解决方案支持Microsoft内置的802.1X供应方程序中采用的认证方法, 因此不需要额外的客户端软件。

自动支持大量认证方法: RADIUS模块被自动进行配置, 可支持大量流行的认证方法, 包括: PAP、CHAP、MS-CHAP、MS-CHAPv2、EAP-TLS、EAP-MSCHAPv2、EAP-GTC、PEAP/EAP-MSCHAPv2、PEAP/EAP-GTC、EAP-TTLS/EAP-PAP、EAP-TTLS/EAP-CHAP、EAP-TTLS/EAP-MS-CHAP、EAP-TTLS/EAP-MS-CHAPv2、EAP-TTLS/EAP-GTC以及客户端证书。RADIUS认证服务的部署得到了极大的简化。

HA与故障恢复: RADIUS模块提供多级别的高可用性。如果远程站点的设备失效, 而WAN连接正常工作, 那么远程站点的网络接入设备可被配置为自动进行故障恢复, 与中心RADIUS服务器进行连接。设备还可以采用HA双机部署, 以增强远程站点的可靠性。

生成自签名的证书、CSRs、和自动证书复制: 许多认证方法需要RADIUS服务器配备X.509证书RADIUS模块可以生成一个自签署的RADIUS服务器证书, 以便简化操作。证书签署请求 (CSRs) 可以被创建并传送到证书中心 (CA), 在那里得到签署并获得增强安全性的客户端证书。客户端证书可代替用户名和密码进行客户认证 (如无线接入的笔记本), 只要客户端所连接的网络使用802.1X认证。一份证书可以在被所有Infoblox网络中的RADIUS服务器所共享, 只需网络主控把证书复制给所有设备即可。

基于MAC地址的认证: 许多环境下都部署了无线设备 (如无线PDA、条形码扫描器、POS系统、以及VoIP电话), 因其不具备802.1X供应程序, 它们在接入无线网络时无法采用802.1X进行认证。在这样的环境下, 设备的MAC地址可以添加到RADIUS服务器的用户数据库中, 并作为保密凭证使用。当设备试图访问网络时, 交换机或无线接入点把设备的MAC地址传送给RADIUS服务器。RADIUS服务器会检查用户数据库, 查找对应的MAC地址, 如果找到, 设备就会被允许进入网络。

数据表

网络模块

Infoblox网络模块把各种设备连接成为一个统一的、核心网络服务平台。这个核心体系结构允许企业发布、组合核心的信息和服务，并保证数据完整性，包括：

- 协议（DNS、DHCP、RADIUS、LDAP、TFTP、NTP等）
- 数据（IP地址、MAC地址、用户保密凭证、事务日志、时间等）
- 文件（设备软件、设备固件与配置文件、策略等）

网络模块提供了全面的系统管理、数据传送、及系统可用性方面的功能。

特性与优势

可恢复性操作：企业可以采用单独（或HA双机）设备，将其部署在LAN或WAN环境下，创建可恢复的网格。Infoblox网络对单个设备失效可以进行恢复，并在单个LAN或WAN连接失效的情况下继续提供服务，并在失效设备更替时或LAN / WAN连接恢复时，自动对网格中的所有单元重新同步。

统一化管理：Infoblox网格中的设备和数据可以被作为一个整体来进行管理，不需要考虑数据的实际存放位置。这种在网格级别上而非单个设备上的可视化服务极大地减少了管理负担和可能的配置错误。Infoblox网格可以从任何位置进行完全远程的管理。

实时、安全、系统级的数据升级：传统系统只能按照计划传送DNS和DHCP数据，与此不同的是，只要网络发生变化，例如设备增加、删除、或更改，网络模块就可以实时同步多个设备上的数据库。不断涌现的应用，如无线组网和VoIP，会导致IP地址和DNS数据经常性的变动，这就要求这些变动必须立即在网络上体现出来，从而确保应用继续正常运行。

无数据损毁、出错、或丢失：数据在Infoblox网格的设备中进行交换时采用了成熟的分布式数据库技术，具有完全的事务完整性。在WAN失效、设备失效、以及高负载的条件下，数据能保持完整和正确。这一点在当今的动态网络环境下尤为重要，因为不正确的数据可以导致应用程序不可用、产生安全漏洞、以及引起兼容性问题。

简化的、基于角色的网络设备、数据、和服务管理：通过单一用户接口就可对多个设备配置数据项目，流水线式操作。例如，创建新的DNS区域、将其映射到若干设备中（如名称服务器）、为其配置特定的区域参数—在一个对话框内就可完成。这种方法简化了网格设备的初始配置和后续的管理，而不是每个设备都单独设置、单独管理。

智能化的设备自动预配置和自动恢复：设备还没有出现在网络中时，就可以在管理系统中对它们进行预配置。类似的，如果网格中的设备出现硬件故障，恢复的速度就和更替设备、配置少量参数（如IP地址）的速度一样快。所需的软件、配置信息、所属网络及服务都会自动启动。

灾难恢复与网格主控晋升：网格中的任何设备（或HA双机）都可委派成主控候选，而且，它会不断接收到网格主控的完整数据和配置信息。如果网格主控失效或者无法连接，管理员就可以“提升”任何一个主控候选，将其作为网格主控，它会与所有成员设备进行接触，接管网格的管理控制—使用简单操作—数分钟内完成。

基本服务（TFTP、HTTP、NTP、SYSLOG NG PROXY及RADIUS PROXY）

Infoblox NIOS 软件提供了一套基本服务，在分布式的网络中非常有用，包括TFTP、HTTP、NTP、Syslog NG Proxy 及 RADIUS Proxy。对于如像 IP 电话那样的应用，在 Infoblox 的解决方案中，仅仅这些服务的价值就让投资者快速获得投资回报。

特性与优势

TFTP 与 HTTP 提供的可靠配置服务：IP 电话和其它设备需要间歇地更新固件和配置文件。解决这一需要地传统方式—使用标准文件服务器—难于提供安全性，而且需要作出大量的工作来确保所有设备都有正确地文件。Infoblox 文件发送服务提供了安全的、可靠的、可管理的解决方案。对于部署在Infoblox中的设备，固件和配置镜像文件只上传一次，而后自动发送到网络中的所有设备上，既节省了时间又确保设备可以访问到关键的文件。文件可以通过 TFTP 或者 HTTP 发送到本地设备中。

网络时间协议提供的时间同步服务：为网络上的设备提供准确的时间服务，不仅仅是方便用户，而是对安全和日志服务非常关键。在需要证明网络时间来自可信来源的情况下，Infoblox NTP服务提供了对NTP认证的支持。

RADIUS Proxy 提供的分布式认证、授权和记帐服务：RADIUS proxy把来自远端的认证请求进行合并，然后将其发送给中心RADIUS 服务。这样，使用 RADIUS 进行 802.1X 认证的设备在部署时得到简化，例如无线接入点、RFID 阅读器、IP 电话等设备。Infoblox RADIUS 代理服务与所有业界标准的 RADIUS 服务器兼容。

Syslog NG Proxy 提供的强化的、可靠的日志服务：Syslog NG 代理允许多个设备发送日志信息至 Infoblox 设备，然后这些日志信息被 Infoblox 设备转发至中心日志服务器上。这样简化了网络设备的日志服务配置，例如防火墙、交换机、路由器以及无线接入点。中心日志服务器、居间防火墙、路由器这些有访问控制列表的设备可以进行一次配置，以获取来自 Infoblox 设备的日志信息，而单个网络设备可被配置为向 Infoblox 设备发送日志信息。

数据表

DNS 技术规范

RFCs支持的	1034和1035 动态升级, RFC 2136 增量区域数据传输, RFC 1995 区域变化通知, RFC 1996 密钥事务鉴定 (TSIG), RFC 2845 无类别的 IN-ADDR.ARPA 美国国防部高级研究计划署授权, RFC 2317
协议引擎	BIND 9.3.4
更多功能	<ul style="list-style-type: none"> • 使用TSIG进行安全的DNS升级 • 秘密传送 • Microsoft Active Directory 支持 • Infoblox 视图 • 为查询、区域传送、以及动态升级建立基于IP地址的访问列表 • 区域导入工具 • 可自定义的TTL设置

DHCP 技术规范

RFCs支持的	RFCs 3046, 2131 和 1531 BOOTP, RFCs 1534 和 2132
协议引擎	DHCPD 3.0.1
更多功能	<ul style="list-style-type: none"> • VLSM (可变长子网掩码) 支持 • CIDR (无类域间路由) 支持 • 段内多子网 (supernetting) • 基于MAC地址的“静态租赁” (手动分配) • 基于MAC地址的过滤 • 地址分配前可用性检查 • DHCP中继代理 / Option 82支持 • 租期发布时, 安全的DHCP-DNS集成升级 • 高级DHCP选项编辑器 • Windows, Unix和MAC OS兼容 • 外部系统日志服务器支持

RADIUS 技术规范

协议引擎	自由远程身份验证拨号用户服务 1.1.3
认证方法	<ul style="list-style-type: none"> • PAP – 密码认证协议 • CHAP, MS-CHAP 和 MS-CHAPv2 – 挑战认证握手协议 • EAP – 为使用802.1x协议, 基于端口的鉴定提供的“可扩展鉴定协议” EAP-TLS, EAP-MSCHAPv2, EAP-GTC • PEAP – 为802.1x基于端口的鉴定提供的“保护可扩展鉴定协议”, PEAP/EAP-GTC, PEAP/ EAP-MSCHAPv2 (这些鉴定方法由Windows客户端提供原生的本地支持) • EAP/TLS – “可扩展鉴定协议, 传输层安全”, 提供双向鉴定, 需要客户端证书 • 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

Infoblox 产品质保与服务声明

标准的硬件质保期为一年。系统软件的质保期为90天, 软件符合声明规范。可选的、扩展硬件和软件质保声明的服务产品也是可以获得的。推荐使用可选产品, 以确保设备得到最新的软件功能升级, 从而保证系统的安全性和可用性。Infoblox同时提供专业的服务和培训课程。此文档内容若有变更, 恕不另行通知。Infoblox有限公司不在此文档中的错误负责。