

认证及 802.1X 的基本网络服务

Infoblox公司对于认证的网络服务（NSA）套件为网络设备以及用户提供了可靠以及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。

对认证的网络服务的优势

- 消除性能瓶颈
- 如果广域网（WAN）连接失败，保证本地可存活性
- 经由Infoblox网络自动复制用户证书至远程设备
- 自动同步来自Microsoft Active Directory的用户证书
- 安全，强化平台
- 设备能够被部署为HA对以及故障切换模式以获得最大可用性

802.1X认证： 新机会，新挑战

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(aka the authenticator)，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承受性，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。

Infoblox公司已经将网络服务的初始版本定位为对于一种特定应用程序的认证套件（分布式802.1X认证）。功能增强使得更多的应用从富策略能力中受益。



对于认证套件的网路服务在所有的Infoblox设备平台上都是可用的。

提供分布式远程身份验证拨号用户服务（RADIUS）服务

对认证套件的网路服务包含了对远程身份验证拨号用户服务（RADIUS）协议和需要802.1认证的认证方法的支持，以及对 Infoblox 网络模块的支持。Infoblox 网络技术允许数百个设备提供遍布于一个企业网络中的带有中央控制以及自动复制所存储的用户证书的认证服务。用户证书能够存在于N IOS™软件中的内建数据库或者Microsoft Active Directory 软件之中。在 Active Directory 环境中，用户证书由Microsoft 域控制器中安全的被复制至网路控制器中并且存储于内建的Infoblox bloxSDB™ 数据库中。这些证书接着经由一个安全的虚拟专用网被复制至该网路中所有的Infoblox设备中。当一个设备被部署于一个部门办事处中时，它甚至能够在广域网（WAN）短缺致使 Infoblox 网路主控制器（以及 Active Directory 服务器）无法连接时为 802.1X 提供认证服务。Infoblox NIOS 软件还拥有内建的基于硬件的高可用性技术，这种技术通过激活被部署于冗余对中的设备而提供了一层额外的可靠性。

对认证的网络服务的优势

- 消除性能瓶颈
不是为所有的设备提供一台中心远程用户拨号认证系统服务器，该认证负载被分布于所有布署于远程站点的 Infoblox 设备中。
- 如果广域网（WAN）连接失败，保证本地可存活性
远程设备复制该用户证书并且甚至在网路控制器不可到达的情况下继续提供服务。
- 经由 Infoblox 网路自动复制用户证书至远程设备
一旦证书被加载至网路控制器上，它就被实时复制到远程设备中。
- 自动同步来自 Microsoft Active Directory 的用户证书
Active Directory 的 Infoblox 复制代理自动将新的或者更改后的用户名以及密码送进 Infoblox 网路控制器中。
- 安全，强化平台
Infoblox 设备被安全强化过并且是抗篡改和抗攻击的。
- 设备能够被布署为HA对以及故障切换模式以获得可用性增强
管理员能够轻松的设计并且布署支持任何想要的可用性水平的认证服务。

特性与优势

对认证套件的网路服务提供比任何替代品更加低成本的可靠、可控制并且安全的认证服务。该套件还包括 NTP、TFTP/HTTP 文件下载，以及Syslog代理，这种代理允许组织将网路服务集成至一个单一平台上并且集中对其控制。该NSA套件单独可用或者作为其它 Infoblox 套件的可选附加。带有此完整网路服务套装包，Infoblox 设备能够在单一的设备或设备网路中提供一种完整的网路服务 (包括DNS、 DHCP、 RADIUS、 NTP、 TFTP、 HTTP以及 Syslog 代理)。

用于 Active Directory 的网路连接器：用于 Active Directory 的 Infoblox 网路连接器由 Active Directory 复制用户证书并且安全的将它们送至网路控制器，网路控制器随后将此数据复制至网路中的设备上。如果连接至远程站点的广域网连接断开，该设备仍然能够认证用户试图访问无线网络。该代理按照由管理员决定的周期的基础上向网路控制器发送变更。

本地用户存储：不需要本地 Active Directory 或者 LDAP 目录服务器而提供远程身份验证拨号用户服务。

网路中复制用户保密凭证：所有Infoblox中的设备都可以自动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/EAPGTC 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。同样, 为了增强的可靠性, 设备能够部署为以HA对。

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RADIUS操作。证书签署请求 (CSR) 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。同样, 当一个证书被复制至设备时, 该证书能够被在一个 Infoblox 网络中的所有远程身份验证拨号用户服务服务器共享。

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。当这些设备试图访问无线网络时, 无线接入点把设备的MAC 地址传送给将 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无线网络。

更多优势

Infoblox NIOS 核心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。

弹性网络技术: 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 Infoblox 网络。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, 自动对网络中的所有单元重新同步。

统一化管理: Infoblox 网络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 网络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: 该网络模块跨越了多重设备实时同步数据库以响应变更。这保证了在用户名以及密码上的变更被迅速反射而遍及扩展环境。

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。这种方法简化了网络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。

数据表

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

部件编号

带有NSA套件的 Infoblox-250设备, 300授权	IB-250-300-NSA
带有NSA套件的 Infoblox-550 设备	IB-550-NSA
带有NSA套件的 Infoblox-1050 设备	IB-1050-NSA
带有NSA套件的 Infoblox-1550 设备	IB-1550-NSA
带有NSA套件的 Infoblox-1552 设备	IB-1552-NSA
带有NSA套件的 Infoblox-2000 设备	IB-2000-NSA

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。