

Aruba 集成 Windows NPS 实现 802.1X 认证

北京力尊信通科技股份有限公司



		目录	
1.	配置	Windows Server 2008	3
	1.1 <u>;</u>	安装 AD+DC+DNS	3
	1.2 <u>+</u>	安装证书服务+IIS	10
	1.3	配置 IIS 开启 https	19
	1.4 <u>+</u>	安装 NPS	21
	1.5 '	管理 NPS(RADIUS 服务器)计算机证书	25
	1.6	配置 NPS	28
2.	配置	Aruba 无线控制器	38
	2.1 j	配置 EAP-PEAPv0(EAP-MSCHAPv2)认证	38
	2.2 j	配置 EAP-TLS 认证	39
3.	证书管	查理与配置客户端测试 802.1X 认证	40
	3.1 [°]	管理 NPS(RADIUS 服务器)的证书	40
	3.2 '	管理无线客户端的证书	41
	3.	2.1 没有加域的客户端安装根 CA 证书	41
	3.	2.2 没有加域的客户端安装用户证书	51
	3.	2.3 加域的客户端手动安装用户证书	55
	3.	2.4 加域的客户端通过组策略自动安装用户证书	55
	3.3 j	配置客户端测试连接 802.1X 认证	62
4.	实现F	用户角色控制	63



802.1X 认证是企业在部署无线网络时首选的无线认证方式,部署 802.1X 认证必须要有 RAIDUS 服务器,如果企业中没有 RAIDUS 服务器,可以选择购买 Aruba ClearPass 产品,也可以选择 Windows NPS 作为 RADIUS 服务器,使用企业员工的 AD 账号来进行认证。

本文章将详细讲解如何一步一步配置 Aruba 无线控制器集成 Windows NPS 来实现 802.1X 认证。

802.1X 认证的 EAP 类型有多种,通常在企业中最常见的就两种类型:

- EAP-PEAPv0 (PEAP-MSCHAPv2): 使用用户名/密码方式认证无线客户端
- EAP-TLS: 使用用户证书认证无线客户端

本手册基于的网络拓扑环境如下:



WP版分路 IIS(Web服务器) NPS(RADIUS服务器)



1. 配置 Windows Server 2008

Windows Server 2008 执行以下功能:

- Domain Controller (DC): 域控制器; ٠
- Active Directory (AD):存储用户账号,作为认证的用户数据库; •
- DNS: 安装域控制器必须安装 DNS 服务器; ٠
- Certificate Services:安装证书服务在服务器上,服务器作为根 CA,为服务器颁发计算机证书,为无线客户 • 端颁发用户证书;
- IIS: Web 服务器,无线客户端可以通过浏览器申请用户证书; ٠
- **NPS:** RADIUS 服务器, 网络接入策略; •

1.1 安装 AD+DC+DNS

点击服务器管理器 > 角色 > 添加角色



选中 Active Directory 域服务,点击添加必需的功能



点击下一步





点击**下一步**

添加角色向导	×
Active Directo	ry 域服务
开始之前 服务器角色 确认 进度 结果	Active Directory 域服务為合 Active Directory 域服务(4D DS)存储有关网络上的用户、计算机和其他设备的信息。AD DS 有助于管 理员安全地管理该信息,并有助于用户目的资源共享和协作。 自用目录的应用程序 (例如 Microsoft Exchange Server)和其他 Windows 服务器技术 (例如组策略)也需要 AD DS。 主意事项 ① 若要有助于确保在某台服务器中断的情况下用户仍然可以登录到网络,请至少为域安装两个域控制 ③ AD DS 要求将 DNS 服务器安装在网络上。如果未安装 DNS,系统会提示您在该服务器上安装 DNS 服务器角色。 ① 安装 AD DS 之后,使用 Active Directory 域服务安装向导 (depromo.exe)使服务器成为全功能域 控制器。 ① 安装 AD DS 将会同时安装目录服务所需的 DPS 命名空间、DPS 复制和文件复制服务。 其他信息 AD DS 概述 安装 AD DS 将会同时安装目录服务所需的 DPS 命名空间、DPS 复制和文件复制服务。 (上一步 (2) 下一步 (1) 安裝 (1) 取消

点击**安装**

添加角色向导	×
确认安装选择	
开始之前 服务器角色 Active Directory 域服务	若要安装以下角色、角色服务或功能,请单击"安装"。 ① 2 条提示性消息显示如下
确认	 安装完成之后,可能需要重新启动该服务器。
进度	🔿 Active Directory 域服务
结果	
	.NET Framework 3.5.1





点击关闭, Active Directory 域服务安装完成

添加角色向导		X
安装结果		
开始之前 服务器角色 Active Directory 域服务 确认 进度 结果	Extractional Contractional Contractity Contractional Contractional Contractional	-

Active Directory 域服务安装完成之后,创建一个新的域,点击**开始 >** 输入 dcpromo







点击下一步



选择**在新林中新建域**,点击下一步

 Active Directory 域服务安装向导 选择某一部署配置 您可为现有林或新林创建域控制器。 	
 ○ 现有林 (3) ○ 向现有域添加域控制器 (A) 	
○ 在现有林中新建域 (C) 此服务器将成为新域中的第一个域控制器。	输入 FQDN: stonex.com , 点击 下一步
● 在新林中新建域 (0)	● Active Directory 或服务安装同导 ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲
有关可能的部署配置的详细信息	键入新目录林根级域的完全限定的域名 (FQDN)。
	目录林根级域的 FQDN(F): stonex.com 例如: corp.contoso.com







选择林功能级别,这里我选择 Windows Server 2008 R2,点击下一步

on Active Directory 域服务安装向导	×	
设置林功能级别 选择林功能级别。		
林功能级别(F): <mark>Windows Server 2008 R2</mark> 详细信息(D): Windows Server 2008 R2 林功能级别提供 Windows Server 2008 林功能 级别中可用的所有功能,以及以下附加功能: - 回收站,启用后,它提供运行 Active Directory 域服务时 完整还原删除的对象的功能。 默认情况下,在该林中创建的任何新域将在 Windows Server 2008 R2 词 功能级别下操作。	安装 DNS 服务器,点击 下一步 Active Directory 域服务安装向导 其他域控制器选项	×
 ▲ 您将只能向该林添加运行 Windows Server 2008 № 或更高版 本的域控制器。 有关<u>域和林功能级别</u>的详细信息 < 上一步(B) 下一步(N) > 	为此域控制器选择其他选项。 ▼ DNS 服务器 (D) ▼ 全局编录 (G) ■ 只读域控制器 (RODC) (R) 其他信息 (A): 林中的第一个域控制器必须是全局编录服务器且不能是 RODC。 ▲ 建议您将 DNS 服务器服务安装在第一个域控制器上。	
	有关 <u>其他域控制器选项</u> 的详细信息 < 上一步 (B) 下一步 (X) > 取消	i

选择**是**

▲ Active Directory 域服务安装向导 ▲ Active Directory 域服务委装向导 ▲ 无法创建该 DNS 服务器的委派,因为无法找到有权威的父区 域或者它未运行 Windows DNS 服务器。如果您要与现有 DNS 基础结构集成,应在父区域中手动创建对该 DNS 服务器的委 派,以确保来自域 "stonex.com"以外的可靠名称解析。否 则,不需要执行任何操作。 是否要继续?	点击 下一步	
	on Active Directory 域服务安装向导	×
<u> </u>	数据库、日志文件和 SYSVOL 的位置 指定将包含 Active Directory 域控制器数据库、日志文件和 SYSVOL 的 文件夹。	
	为获得更好的性能和可恢复性,请将数据库和日志文件存储在不同的卷上。	

数据库文件夹 (0):	
C:\Windows\NTDS	浏览 (R)
日志文件文件夹 (L):	
	A Solution and S





设置目录服务还原的密码,点击下一步

on Active Directory 域服务安装向导	×		
目录服务还原模式的 Administrator 密码			
目录服务还原模式 Administrator 帐户不同于域 Administrator 帐户。 为 Administrator 帐户分配一个密码,将在以目录服务还原模式启动此想 制器时使用该帐户。我们建议您选择一个强密码。	或控		
密码 (r): →→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→	_	点击 下一步	
关于 <u>目录服务还原模式密码</u> 的详细信息	Martive 摘要	Directory 域服务安装向导	×
(10 完一步 (10))	检将新城林城站其要 可参有查该域的 功功点他更以与关	密的选择 (R): 服务器配置为新林中的第一个 Active Directory 域控制器。 名为"stonex.com"。这也是新林的名称。 NetBIOS 名称为"STONEX"。 能级别: Windows Server 2008 R2 能级别: Windows Server 2008 R2 : Default=First=Site=Name 选项: 改选项,单击"上一步"。要开始操作,单击"下一步"。 名这些设置导出到一个应答文件中以用于其他无人 写出设置 (R) 要作。	•
		〈上一步 (8) 下一步 (8) 〉	取消

点击**完成**





安装完成之后需重启计算机





1.2 安装证书服务+IIS

点击服务器管理器 > 角色 > 添加角色



点击**下一步**

法持久久有民		
涂加用巴回 导		<u> </u>
开始之前		
- 开始之 <u>刖</u>	此向导帮助您在此服务器上安装角色。根据要求此服务器执行的任务来确定要安装的角色,例如共同主要支持。	
服务器角色	亭又怕购土村附如。 ————————————————————————————————————	
确认	继续操作之前,请验证以下事项:	
讲度	• Administrator 帐户具有强密码	
结果	・ 已配罟网络设罟,例如静态「IP」地址 ・ 已安装 Windows Update 中的最新安全更新	
	如果您必须结果工还的任何操作,请取消此问号,结果操作,然后再次运行问号。	
	若要继续,请单击"下一步"。	





选中 Active Directory 证书服务,点击下一步

Fixer And	添加角色向导		×
开始之前 法择要安装在此服务器上的一个或多个角色。 加CS 角色服务 女装类型 CA 类型 CA 类型 Active Directory 联合身份验证服务 Active Directory 联合身份验证服务 DEWEN Active Directory 联合身份验证服务 DEWEN Active Directory 联合身份验证服务 DEWEN Active Directory 联合身份验证服务 DEWEN Active Directory 证据账会 DEWEN Active Directory 证据账会 DEWEN Active Directory 证据账会 DEWEN Max DEWEN Active Directory 证据账会 DEWEN Attive Directory 证据 DEWEN Max DEWEN Directory THMS DEWEN Directory THMS DEWEN Directory THMS DEWEN CA 全部 DEWEN Max DEWEN Directory THMS DEWEN Directory THMS DEWEN Directory THMS	选择服务器角色		
	开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 确认 进度 结果	 法择要安装在此服务器上的一个或多个角色。 角色(R): Active Directory Rights Management Services Active Directory 联合身份验证服务 Active Directory 校型目录服务 Active Directory 证书服务 DNCP 服务器 DNS 服务器(已安装) Hyper-V Web 服务器(IIS) Windows Server Update Services Windows 部署服务 传真服务器 打印和文件服务 应用程序服务器 远程桌面服务 	描述: Active Directory 证书服务(AD CS)用于创建证书颁发机构和相关的 角色服务,可以使您颁发和管理在 各种应用程序中所使用的证书。

点击**下一步**

添加角色向导		×
Active Directo	ory 证书服务简介	
开始之前 服务器角色	Active Directory 证书服务(AD CS) Active Directory 证书服务(AD CS)提供证书基础结构以启用方案,如安全无线网络、虚拟专用网、 Internet 协议安全(IPSec)、网络访问保护(MAP)、加密文件系统(EPS)和智能卡登录。	
AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 确认	 注意事项 ● 安装证书颁发机构(CA)之后,无法更改该计算机的名称和域设置。如果您想更改计算机名称,加入一个域或者使该服务器升级为域控制器,请完成这些更改,然后再安装 CA。有关详细信息,请参阅证书颁发机构命名。 其他信息 Active Directory 证书服务概述 管理证书颁发机构 证书颁发机构命名。 	





选中**证书颁发机构 Web 注册**,默认就会选中**证书颁发机构**

添加角色向导		×
选择角色服务		
开始之前 服务器角色 AD CS <u>角色服务</u> 安装类型 CA 类型 CA 类型 AU 加密 CA 名称 有效期 证书数据库 确认 进度 结果	选择为Active Directory 证书服务安装的角色服务: 角色服务 (b): □ 证书颁发机构 Web 注册 ● 既机响应程序 ● 网络设备注册服务 ● 证书注册 Web 服务 ● 证书注册策略 Web 服务 ● 证书注册策略 Teb 服务	描述: <u>证书颁发机构 Web 注册</u> 提供了简单 的 Web 界面,使用户可以执行诸如 请求和续订证书、检索证书吊销列 表(CBL)和执行智能卡证书注册等任 务。
	〈上一步 (8) 下一步 (8) >

添加**证书颁发机构 Web 注册**,需安装 IIS 服务器

添加角色向导	×
 是否添加 证书颁发机构 Web 注册 所需的角色服务和功能。 无法安装 证书颁发机构 Web 注册,除非同时安装所需的角色服务和功能。 角色服务 (R): · Web 服务器 (IIS) · Web 服务器 ·····························	
添加所需的角色服务 (A) 取消	
① <u>为何需要这些角色服务和功能?</u>	///



点击**下一步**

添加角色向导		×
选择角色服务		
 开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 A钻 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果 	选择为Active Directory 证书服务安装的角色服务: 角色服务 (&): ① 证书颁发机构 Web 注册 ① 证书颁发机构 Web 注册 □ 联机响应程序 □ 网络设备注册服务 □ 证书注册 Web 服务 □ 证书注册策略 Web 服务	描述: <u>证书颁发机构 web 注册</u> 提供了简单 的 web 界面,使用户可以执行诸如 请求和续订证书、检索证书吊销列 表(CRL)和执行智能卡证书注册等任 务。
	〈上一步 (8) 下一步 (8)) >安裝 (I)取消

选中**企业**,点击**下一步**

添加角色向导		X
指定安装类型		
开始之前 服务器角色	证书颁发机构可以使用 Active Directory 中的数据来简化证书颁发和管理。指定您需要设置企业(还是独立 CA。	CA
AD CS	● 企业 @)	
角色服务	如果此 CA 是某个域的成员且可以使用目录服务来颁发和管理证书,请选择此选项。	
安装类型		
CA 类型	・ 392 (A) 如果此 CA 不使用目录服务数据来颁发或管理证书,请选择此选项。独立 CA 可以是域的成员。	
私钥		
加密		
CA 名称		
有效期		
证书数据库		
Web 服务器(IIS)		
备色服务		





选中**根 CA**,点击**下一步**

添加角色向导	×
🌇 指定 CA 类型	
 开始之前 服务器角色 私D CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIIS) 角色服务 确认 进度 结果 	可以配置根 ca 和从属 ca 的组合来创建分层公钥基础结构 (PKD)。根 ca 是发布其自己的自签名证书 的 Ca。从属 ca接收来自其他 Ca 的证书。指定您需要设置根 ca 还是从属 Ca。 (*) 根 ca(R) 如果您是第一次安装或您是公钥基础结构中唯一的证书颁发机构,请选择此选项。 (*) 子级 ca(R) 如果您的 Ca 将从公钥基础结构中更高的另一个 Ca 获取其 Ca 证书,请选择此选项。
	有关公钥基础结构 (PIII)的详细信息
	< 上一步 (P) 下一步 (M) > 安裝 (II) 取消

选中**新建秘钥**,点击**下一步**

添加角色向导	×
设置私钥	
 开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 AU CA 类型 AU A	 若要生成证书并颁发给客户端,CA必须有一个私钥。指定您要新建私钥还是使用现有私钥。 新建私钥(R) 加集您没有私钥或者要新建一个私钥以增强安全性,请使用此选项。系统将要求您选择加密服务提供保产指定私钥的密钥长度。若要颁发新证书,还必须选择一个哈希算法。 使用现有私钥(0) 使用现达项可确保重新安装 CA 时与先前颁发的证书的连续性。 适择一个证书并使用其关联私钥(0) 加果您在此计算机上有一个现有证书,或者如果您希望导入一个证书并使用其关联私钥,请选择此选项。 近择此计算机上的现有私钥(2) 如果您已保留来自以前安装的私钥或需要使用其他来源的私钥,请选择此选项。





点击**下一步**

添加角色向导		×
野子 为 CA 配置加密		
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 AU T加密 CA 本称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果	据要新建私钥,您必须首先选择加密服务提供程序、哈希其法和适合您颁发的证书的特定用途的容 说 也。 为密钥长度选择更高的值将导致更强的安全性,但会增加完成签名操作所需的时间。 正 法律师 cs fot for for the for th	
	< 上一步 (P) 下一步 (M) > 安裝 (I) 取消	

点击**下一步**

添加角色向导		×
配置 CA 名称		
开始之前 服务器角色	键入公用名称以识别此 CA,此名称会被添加到由该 CA 颁发的所有证书中。可分辨名称的后缀值是自 动生成的,但可以修改。	
AD CS	此 CA 的公用名称 (C):	
角色服务	stonex-AD-CA	
安装类型	可分辨名称后缀 (0):	
CA 类型	DC=stonex, DC=com	
私钥		
加密		
CA 名称	可分辨名称的预览(V): CNT-stanavaAD=CA_DCT-stanava_DCT-sam	
有效期	CA-Stonex AD CA, DC-Stonex, DC-Com	
证书数据库		
Web 服务器(IIS)		
各合肥冬		





点击**下一步**

添加角色向导	×
设置有效期	
 开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 CA 名称 	会将一个证书颁发给此 CA 以保护与其他 CA 和请求证书的客户端之间的通信。CA 证书的有效期可以 基于许多因素,包括 CA 的预期目的以及为保护 CA 您已采取的安全措施。 为此 CA 生成的证书选择有效期(V):
有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果	
	有关设置证书有效期的详细信息。 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.
	< 上一步 (P) 下一步 (M) > 安裝 (I) 取消

点击**下一步**

添加角色向导		×
配置证书数据库		
开始之前 服务器角色	证书数据库记录所有证书请求、已颁发的证书以及已吊销或过期的证书。CA 可使用该 视管理活动。	数据库日志来监
AD CS	证书数据库位置(C):	
角色服务	C:\Windows\system32\CertLog	浏览 (0)
安装类型	□ 在此位置使用来自上次安装的现有证书数据库(0)	
CA 类型	证书数据库日志位置 (E):	
私钥	C:\Windows\system32\CertLog	浏览 (B)
加密		
CA 名称		
有效期		
证书数据库		
Web 服务器(IIS)		
各分肥冬		





点击**下一步**, 安装 IIS 服务器

添加角色向导		×
Web 服务器(IIS)		
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 AU CA 类型 AU CA 类型 AU DD CA 名称 有效期 证书数据库 Yeb 服务器(IIS) 角色服务 确认 进度 结果	Web 服务器 (UIS) 简介 Web 服务器と具有特定软件的计算机,这些软件使服务器可以从客户端计算机接受请求并对这些请求返回响应。Web 服务器更有特定软件的计算机,这些软件使服务器可以从客户端计算机接受请求并对这些请求返问本意。 Internet 信息服务 (UIS) 7.0, 是一个集成了 IIS 7.0、&SF.NET 和 Windows Communication Foundation 的统一 Web 平台。UIS 7.0 还具有安全性增强、诊断简单和委派管理的特点。 ● 使用 Windows 系统资源管理器 (WSBM)有助于确保等同对待 Web 服务器通信,特别是此计算机上存 在多个角色时。 ● Web 服务器 (UIS)角色的默认安装包括角色服务的安装,该安装使您能够使用静态内容、进行最小 自定义 (如默认的文档和 WTFP 错误)、监视和记录服务器活动以及配置静态内容压缩。	
	< 上一步 (P) 下一步 (M) > 安裝 (II) 取消	

点击**下一步**

添加角色向导		×
选择角色服务		
开始之前 服务器角色	选择为Web 服务器(IIS)安装的角色服务: 角色服务(R):	描述:
AD CS		· 持和对 ASP.NET、ASP 以及 Web 服
角色服务	□ □ 常儿 HTTP 功能	务器扩展的可选支持。可以使用
安装类型	▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Web 服务器米承载内部或外部网站,或为开发人员提供创建其干
CA 类型	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Web 的应用程序的环境。
私钥	✔ HTTP 错误	
10家	✓ HTTP 重定向	
CA 名称	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	
有效期	□ NET 扩展性	
证书数据库	ASP	
Web 服务器(IIS)	CGI	
	✓ ISAPI 扩展	





点击**安装**

添加角色向导		×
确认安装选择		
开始之前 服务器角色 AD CS 角色服务	若要安裝以下角色、角色服务或功能,请单击"安装"。 ① 1 条警告消息,2 条提示性消息显示如下 ③ 安装完成之后,可能需要重新启动该服务器。	-
安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认	 ▲ Active Directory 证书服务 证书颁发机构 ④ 安装了证书颁发机构之后,将无法更改此计算机的名称和域设置。 CA 类型: 企业根 CSP: CSP: RSA#Microsoft Software Key Storage Provider 哈希算法: SHA1 密钥长度: 2048 允许 CSP 交互操作: 已禁用 证书有效期: 2021/7/23 14:02 可分辨名称: CN=stonex-AD=CA, DC=stonex, DC=com 证书数据库位置: C:\Windows\system32\CertLog 证书颜发机构 Web 注册 	
进度 结果	● Web 服务器(IIS) ● 查找有关 Windows 系统资源管理器(WSBM)以及它如何帮助优化 CPU 使用情况的详细信 ■ Web 服务器 T印、保存或通过电子邮件发送此信息	_
	< 上一步 (r) 下一步 (r) > 安装 (r) 取消	

点击关闭,完成安装 Active Directory 证书服务和 IIS 服务器



角已服为 确认 进度 结果	目录浏览 HTTP 错误 HTTP 重定向 应用程序开发 ASP ISAPI 扩展
	打印、保存或通过电子邮件发送安装报告。 1991年——————————————————————————————————
	< 上一步 (P) 下一步 (R) > 关闭 (D) 取消



1.3 配置 IIS 开启 https

无线客户端需要通过 https 访问证书服务器才能申请用户证书,因此需要配置 IIS 支持 https 访问, IIS 默认不支持 https 访问。

选中 Internet 信息服务 (IIS 管理器),选中 Default Web Site,点击绑定



点击**添加**







添加网站绑定		<u>?</u> ×
类型(T):	IP 地址(I):	端口 (0):
https 💌	全部未分配	443
主机名(H):		
SSL WHY (S):		
ad. stonex. com		
		确定取消

点击**关闭**,配置完成

弦绑定					<u>?</u> ×
类型	主机名	端口	IP 地址	绑定信	添加(A)
http		80	*		
https		443	*		· 编辑 U.L.
					删除(R)
					浏览 (B)
•				F	
					关闭(C)



1.4 安装 NPS

点击服务器管理器 > 角色 > 添加角色



点击下一步

添加角色向导		×
开始之前		
<mark>开始之前 服务器角色</mark> 确认 进度 结果	此向导帮助您在此服务器上安装角色。根据要求此服务器执行的任务来确定要安装的角色,例如共 享文档或主持网站。 继续操作之前,请验证以下事项: · Administrator 帐户具有强密码 · 已配置网络设置,例如静态 IP 地址 · 已安装 Windows Update 中的最新安全更新 如果您必须结束上述的任何操作,请取消此向导,结束操作,然后再次运行向导。 若要继续,请单击"下一步"。	





选中**网络策略和访问服务**,点击**下一步**

添加角色向导		×
选择服务器角色		
开始之前 服务器角色 网络策略和访问服务 角色服务 确认 进度 结果	法择要安装在此服务器上的一个或多个角色。 角色 (R): Active Directory Kights Management Services Active Directory 联合身份验证服务 Active Directory 轻型目录服务 Active Directory 轻型目录服务 Active Directory 证书服务 (已安装) DHCP 服务器 DDCP 服务器 Active Directory 证书服务 Active Directory 证书服务 DDCP 服务器 DDCP 服务器 DDCP 服务 Active Directory 证书服务 Active Directory 证书 Active Directory 证书 Active Directory 证书 Active Directory 证书 Active Directory 证书 Active Directory 证书 Active Directory Explored Active Directory 证书 Active Directory Theorem Active Directory Theorem Ac	描述: ■ 始策略和访问服务提供网络策略 服务器(NPS)、路由和远程访问、健 康注册颁发机构(HBA)和主机凭据授 权协议(HCAP);这些将有助于网络 的健康和安全。

点击**下一步**

添加角色向导		×
网络策略和访问用	贤务	
开始之前 服务器角色 网络策略和访问服务	网络策略和访问服务简介 网络策略和访问服务允许提供本地和远程网络访问权限,并允许使用网络策略服务器(BPS)、路由和远 程访问服务、健康注册授权机构(BBA)和凭据授权协议(BCAP)定义和强制用于网络访问身份验证、授权 和客户端健康的策略。	
角色服务 确认 进度 结果	注意事项 ① 可以将 MPS 部署为远程身份验证拨入用户服务(RADIUS)服务器和代理,也可以将其部署为网络访 问保护(MAP)策略服务器。在使用此向导安装 MPS 之后,即可使用 MPS 控制台在 MPAS 主页配置 MPS。 ① MAP 可帮助确保与网络连接的计算机与组织网络和客户端健康策略兼容。在使用此向导安装 MPS 之后,即可使用 MPS 控制台在 MPAS 主页配置 MAP。	
	其他信息 网络策略和访问服务概述 NAP 强制方法 NPS 中的网络访问保护(MAP) 网络策略服务器	





勾选**网络策略服务器**,点击**下一步**

添加角色向导		×
选择角色服务		
开始之前 服务器角色 网络策略和访问服务 角色服务 确认 进度 结果	选择为网络策略和访问服务安装的角色服务: 角色服务 (R): ● 网络策略服务器 ● 商田和远程访问服务 ● 商田和远程访问服务 ● 商田和远程访问服务 ● 商田 ● 通程注册机构 ● 主机凭据授权协议 百兰角色服务的详细信息	描述: 网络策略服务器(MPS)允许创建和增强组织范围的网络访问策略,以用于客户端健康、连接请求验证和连接请求验证和连接请求授权。使用 MPS,还可以部署网络访问保护(MAP),即一个客户端健康策略的创建、加强和修正的技术。
	< 上一步 (3) (下一步 (3)) > 安裝 (I) 取消

点击**安装**

添加角色向导		×
确认安装选择		
开始之前 服务器角色 网络策略和访问服务	若要安装以下角色、角色服务或功能,请单击"安装"。 ① 1 条提示性消息显示如下	,
角色服务	 安装完成之后,可能需要重新启动该服务器。 	
确认	🔗 网络策略和访问服务	
进度	网络策略服务器	
结果		





点击**关闭**,NPS 安装完成

添加角色向导		×
安装结果		
开始之前 服务器角色 网络策略和访问服务 角色服务 确认 进度 结果	Image: State St	
	< 上一步 (P) 下一步 (M) > 关闭 (D) 取消	



1.5 管理 NPS (RADIUS 服务器) 计算机证书

执行 802.1X 认证, RADIUS 服务器需要向认证的无线客户端提供一张计算机证书,以便客户端确认正在与他们交 互的是合法的 RADIUS 服务器,而不是伪装的。管理计算机证书使用管理控制台(MMC).

点击 开始	>	输入	mmc,	打开管理控制台
--------------	---	----	------	---------

程序 (1)	
👼 mm c	
▶ 22 登看更多结果	
mmc	≥ 注销 ▶

点击文件 > 添加/删除管理单元

-	控制台1 - 「控制台	根节点]			×
	文件() 操作(A)	查看(V) 收藏夹()) 窗口(W) 帮助(H)	_ 8 >	<
4	新建(N)	Ctrl+N			
	打开(0)	Ctrl+O			=
	保存(S) 另存为(A)	Ctrl+S	此视图中没有可显示的项目。	 控制台根节点 ▲	
	添加/删除管理单元	τ̈́(M) Ctrl+M		更多操作 🛛 🕨	,
L	选项(2)				
L	最近使用过的文件				
L	退出(X)				
L					

- 退出程序并提示保存文档。		



选择证书 > 点击添加



x

点击**完成** 选择计算机 请选择需要这个管理单元管理的计算机。 -这个管理单元将始终管理: ● 本地计算机(运行此控制台的计算机)(L): 🔘 另—台计算机 (A): 🗌 浏览(R). 🔲 从命令行启动时,允许更改所选计算机。这只有在保存控制台的情况下才适用(\)。





26

x

取消

< 上一歩(3) 下一歩(3) >

点击**确定**

 添加或刪除管理单元 您可以在计算机上为此控制 哪些扩展项。 可用的管理单元(S): 管理单元 ⑩性能监视器 ⑩远程桌面 ◎远程桌面 ◎远程桌面服务管理器 ⑩远程桌面会话主 卿证书 ⑩证书预发机构 卿证书模板 ፪ 组策略 Starter 	制台选择可用的管理单元并配置所说 <u>供应商</u> Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	約一组管理单元。对于可扩展的管 所选管理单元 œ): ■ 控制台根节点 ↓ 证书 (本地计算机)	★ 理単元,您可以配置要启用 编辑扩展(X) 删除(X) 上移(U) 下移(D)
■ 313×44,533×36448 ■ 313×44,533×36448 ■ 313×6448 ■ 315×6448 ■ 315×6458 ■ 315×6458	Microsoft Microsoft Microsoft		高级(V)
通过: 证书管理单元允许您浏览	自己的、一个服务的或一台计算机的	前证书存储内容。	确定取消

点击个人 > 证书, 可以查看所有计算机证书

ad.stonex.com 就是根 CA 颁发给 RADIUS 服务器的计算机证书

注意:如果 NPS 单独安装在一台 Windows Server 2008 服务器上,则默认没有这张证书,需要手动申请一张计算机证书.

🧱 控制台1 - 〔控制台根节	ī点\证书(本地计算机)	\个人\证书]						
🚟 文件(F) 操作(A) 查	看(V) 收藏夹(O) 窗	口(W) 帮助(H)						_ 8 ×
a 🖨 🖄 🔁 👘	1 🗟 🛛 🖬							
📔 控制台根节点	_ 颁发给 ▲	颁发者	截止日期	预期目的		友女	操作	
🗆 🗊 证书(本地计算机)	🔄 ad. stonex. com	stonex-AD-CA	2017/7/23	客户端身份验证,	服务器身份验证	、无	证书	
 □ ○ 个人 ○ 证书 □ ○ 企业信任 □ ○ 企业信任 □ ○ 受信任的发布者 □ ○ 死信任的证书 □ ○ 第三方根证书颁发 □ ○ 受信任人 □ ○ 受信任人 □ ○ 受信任的设备 	stonex-AD-CA	stonex-AD-CA	2021/7/23	〈所有〉		- ⟨ ,	更多操作	
个人 存储含有 2 个证书。								



1.6 配置 NPS

配置 NPS 分为三个步骤:

- 1. 在 Active Directory 中注册服务器,授权 NPS 从域中读取用户的拨入属性
- 2. 添加 RAIDUS 客户端
- 3. 创建网络策略

点击服务器管理器 > 角色 > 网络策略和访问服务 > 右击 NPS (本地) > 选中在 Active Directory 中注册服

务器



■ 服务器管理器					- U ×
文件() 操作(A) 引	查看(V) 帮助	00)			
Lange State Lange Lang	ctory 域服f ctory 证书f IIS)	服务器管理器 (AD) 获取有关此服务器状态	态的概述,执行首要管理任务,并添加或删除服务	器角色和功能。	
	方问服务	◇ 服务器摘要		👔 服务器摘要帮助	
 ① ● □ ● □ ● □ ● □ ● □ ● □ ● □ ● □ ● □ ●	导入配置 (E 导出配置 (E 启动 NPS 用 停止 NPS 用 在 Active 属性 (R) 帮助 (H)	:) () 服务 (S) 服务 (D) Directory 中注册服务器 (G) 	ad.stonex.com stonex.com 192.168.1.200, IPv6 已启用 已禁用 已禁用 00486-001-0001076-84753 (已激活) 台の)	 ● 更改系统属性 ● 查看网络连接 ● 配置远程桌面 ■ 配置服务器管理器远程管理 	
I		 중全信息 Windows 防火墙: Windows Update: 上次检查更新的时间: ▲上次刷新时间: 今天 11:30 酉 	域:启用 未配置 从未安装 <mark>2置刷新</mark>	 중 转到 Windows 防火墙 公 配置更新 分 检查新角色 ▲ 运行安全配置向导 へ 配置 IE ESC 	

点击**确定**

点击**确定**

×

网络策略服务器

若要启动 NPS 来对 Active Directory 中的用户执行身份验证,运行 NPS 的计算机必须有从该域读取用户拨入属性的权限。

是否要授予该计算机从 stonex.com 域读取用户拨入属性的权限?



网络策略服务器

现已授权该计算机从域 stonex.com 中读取用户的拨入属性。

要授权该计算机从其他域中读取用户的拨入属性,则必须将该计算机 注册为该域中的 RAS/IAS 服务器组成员。



×







填写 RADIUS 基本信息: 友好名称、IP 地址、共享密钥, 点击确定



致。(共享机密区分大	小写。		
 ● 手劫(0) サ京和密(0): 	○ 生成 (G)		
确认共写机密(0):			
			HIN 244
		Ľ	



点击 NPS (本地) > 策略 > 右击网络策略 > 新建

1. 服务器管理器		
文件() 操作(A) 查看(V) 帮助(H)		
🗢 🔿 🙍 🖬 🚺 🖬		
🛼 服务器管理器 (AD)	RADIUS 客户端	操作
		BADIUS 客户端 ▲
王 Active Directory 政服分 田 Active Directory 证书昭冬	使用、MADIUS 各户端,可以指定网络访问服务器,以提供刘网络的访问权限。	
 Image: A sective billectory from (5,00) Image: A sective	11, 7 1	
Ⅲ ¥eb 服务器(IIS)	友好名称 IP 地址 设备制造商 支持 NAP	
□ ♪ 网络策略和访问服务	aruba-controller 192.168.1.100 RADIUS Standard No	查看▶
		🞑 刷新
■ RADIVS 客户端		2 帮助
_ 📑 远程 RADIVS 服务器组		
🗄 🍢 网络访问保州 🛛 刷新 (37)		
1 11 11 11 11 11 11 11 11 11 11 11 11 1		
田 續 功能		
王 🍙 诊断		
🗉 🏬 配置		
田		
	J	
刷新当前选择。		

输入**策略名称**,点击**下一步**

新建网络策略	×
指定网络策略名称和连接类型 可以为您的网络策略指定一个名称和要应用该策略的连接类型.	
策略名称(A): [aruba_wireless_access_policy] 网络连接方法 选择向 NFS 发送连接请求的网络访问服务器类型。您可以选择网络访问服务器的类型或特定于供应商的类型,也可以不 行选择。如果您的网络访问服务器是 802.1X 身份验证交换机或无线访问点,请选择"未指定"。	 进
 ● 网络访问服务器的类型(S): ▼Unspecified ● 供应商特定(V): 10 = 	





指定条件: 如果某个连接请求匹配了制定条件, 则击中该网络策略。

点击**添加**,添加指定条件,这里我们选择 NAS 标识符 (**dot1x**) 作为条件,一旦某个连接请求匹配了该 NAS 标识符,则击中该网络策略;

指定条件可以添加多个,至少需要一个指定条件

新建网络策略		×
	指定条件 指定用于确定是否针对某个连接请求评估此网络策略的条件.至少需要一个条件.	
条件(C):		
条件	值	
条件描述:		
	添加 @) 编辑 @) 删除 @)	
	上一步 (P) 下一步 (P) 完成 (P) 取消]

选中 NAS 标识符,点击添加,输入 NAS 标识符 dot1x,点击确定





点击**下一步**

新建网络策略	<u>د</u>	<
	指定条件 指定用于确定是否针对某个连接请求评估此网络策略的条件。至少需要一个条件。	
条件(C): 条件 金 NAS 标	值 识符 dot1x	
条件描述:		
NAS 标识符务	条件指定了网络访问服务器 (NAS) 名称的字符串。可以使用模式匹配语法指定 NAS 名称。 添加 (D) 编辑 (E) 删除 (B)	
	上一步 (P) 下一步 (N) 完成 (P) 取消	

点击**下一步**







配置身份验证方法,这里我们添加 EAP-PEAPv0 (PEAP-MSCHAPv2) 和 EAP-TLS 两种 802.1X 认证

点击添加,选中智能卡或其他证书 (即 EAP-TLS 认证),点击确定

新建网络策略			×	
	配置身份验证方法			
	配量建設清水需要与此來留低配的一种較多种對t 802.1% 或 VPN 部署 NAP, 则必须在连接请求策■	7短证方法。怎必须为 BAF 另份短证的量 BAF 关证 各中配置受保护的 EAP, 它将改写网络策略身份验证;	· 如来使用 改量.	
可按 EAP 类型	例出的顺序在 NFS 和客户端之间协商这些类型。	•		
EAP 类型(T)	:	上移 (U) 下移 (W)		
 添加 (D) 安全级别较低 ✓ Microsoft ✓ 用户可! ✓ Microsoft ✓ 用户可! ✓ m密的身份 二 未加密的身份 二 允许客户端 □ 仅执行计算 	编辑 (2) 删除 (3) Shop 份验证方法: 加密的身份验证版本 2 (MS-CHAP-v2)(V) 以在密码过期后更改密码 (4) 加密的身份验证 (MS-CHAP)(Y) 以在密码过期后更改密码 (X) う验证 (CHAP)(C) 對验证 (CHAP)(C) 對验证 (CHAP, SPAP)(S) 粘连接而不需要协商身份验证方法 (L)。 氧机健康检查 (M)		<mark>添加 EAP</mark> 身份验证方法() Microsoft: 營 Microsoft: 勞	▲): 智能卡或其他证书 受保护的 EAP(PEAP) 安全密码(EAP-MSCHAP v2) 确定 取消
		上一步 (P) 下一步 (N) 完成 (P)	取消	

选中智能卡或其他证书,点击编辑,可以查看 EAP-TLS 认证方式向无线客户端表明其身份,提供的计算机证书是

ad.stonex.com

新建网络策略		×	
配置身份验证方法 配量连接请求需要与此策略匹配的一 802.1X 或 VPN 部署 NAP,则必须在:	种或多种身份验证方法,您必须为 EAP 身份验证配置 E 连接请求策略中配置受保护的 EAP, 它将改写网络策略多	BAP 类型,如果使用 \$P份验证设置。	
可按 BAP 类型列出的顺序在 NPS 和客户端之间协同	商这些类型。		
BAP 类型(T): Microsoft:智能卡或其他证书	上移(0) 下移(97)		
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	能卡或其他证书属性	×
添加 (0) 编辑 (2) 删除 (2)	Ĩ	至连接完成之前,此服务器 乍凭据。	<b>向呼叫者表明身份。请为服务器选择证书以</b>
安全级别较低的身份验证方法: ▼ Microsoft 加密的身份验证版本 2 (MS-CHAP-v	2)(V)	正书颁发给(II):	ad. stonex. com





## 点击添加,选中 Microsoft: 受保护的 EAP (PEAP),点击确定

新建网络策略			×		
	<b>配置身份验证方法</b> 配置连接请求需要与此策略匹配的一种或多种身份 802.1% 或 VPN 部署 NAP,则必须在连接请求策略	验证方法,您必须为 EAP 身份验证配置 EAP 类型, 中配置受保护的 EAP,它将改写网络策略身份验证说	. 如果使用 2重.		
可按 EAP 类型列 EAP 类型(T): Microsoft: 智	山出的顺序在 NFS 和客户端之间协商这些类型。 R能卡或其他证书	上移(0) 下移(9)			
添加(D) <b>安全级别较低f</b> ▼ Microsoft 力 ▼ 用户可以 ▼ Microsoft 力 ▼ 用户可以 ■ 加密的身份 ■ 未加密的身份 ■ 允许客户端道 ■ 仅执行计算机	编辑 (E) 删除 (R) <b>的身份验证方法:</b> 如密的身份验证版本 2 (MS-CHAP-v2)(V) 在密码过期后更改密码 (H) 如密的身份验证 (MS-CHAP) (Y) 在密码过期后更改密码 (X) 益证 (CHAP) (C) 分验证 (PAP, SPAP) (S) 主接而不需要协商身份验证方法 (L)。 机健康检查 (M)		<mark>添加 EAP</mark> 身份验证方法(A) Microsoft: 受f Microsoft: 支言	: 果护的 EAP (PEAP) 主密码 (EAP=MSCHAP v2) 确定 取消	
		上一步 (P) 下一步 (X) 完成 (P)	取消		

选中 Microsoft: 受保护的 EAP (PEAP),点击编辑,可以查看 Microsoft:受保护的 EAP (PEAP)认证方式向 无线客户端表明其身份,提供的计算机证书是 ad.stonex.com,内层 EAP 是 EAP-MSCHVPv2。

新建网络策略	×
記置身份验证方法 配置连接请求需要与此策略匹配的一种或多种身份验证方法。您必须为 E 802.1X 或 VPN 部署 NAP,则必须在连接请求策略中配置受保护的 EAP,	IAP 身份验证配置 EAP 类型。如果使用 它将改写网络策略身份验证设置。
可按 EAP 类型列出的顺序在 NPS 和客户端之间协商这些类型。	
EAP 类型(T): Microsoft: 智能卡或其他证书 Microsoft: 受保护的 EAP (PEAP) 下移(W)	法择服务器用于向客户端提供身份证明的证书。"远程访问策略"中为 "受保护的 KAP"配置的证书会覆盖此证书。 证书颁发给 (I): [ad. stonex. com ▼ 友好名称:
添加 (D) 编辑 (E) 删除 (R) 安全级别较低的身份验证方法:	颁发者:     stonex=AD=CA       截止日期:     2017/7/23 14:12:17
▼ Microsoft 加密的身份验证版本 2(MS-CHAP-v2)(V)	▶ 自用快速重新连接 (7)





点击**下一步** 

新建网络策略	×
<b>配置身份验证方法</b> 配置達接请求需要与此策略匹配的一种或多种身份验证方法,您必须为 EAP 身份验证配置 EAP 类型,如果使用 802.1% 或 VPN 部署 NAP,则必须在连接请求策略中配置受保护的 EAP,它将改写网络策略身份验证设置,	
Microsoft: 資保护的 EAP (PEAP)	
<ul> <li>添加(0) 編辑(8) 刪除(8)</li> <li>安全级别较低的身份验证方法:</li> <li>✓ Microsoft 加密的身份验证版本 2 (MS-CHAP-v2)(V)</li> <li>✓ 用户可以在密码过期后更改密码(0)</li> <li>✓ Microsoft 加密的身份验证(MS-CHAP)(Y)</li> <li>✓ D. 用户可以在密码过期后更改密码(0)</li> </ul>	
<ul> <li>▼ 用戶可以在密码过期后更改密码 (0)</li> <li>□ 加密的身份验证 (CHAP) (C)</li> <li>□ 未加密的身份验证 (PAP, SPAP) (S)</li> <li>□ 允许客户端连接而不需要协商身份验证方法 (L)。</li> <li>□ 仅执行计算机健康检查 (M)</li> </ul>	
上一步 (P) 下一步 (N) 完成 (C) 取消	

点击**下一步** 

新建网络策略	×
<b>配置约束</b> 约束是指网络策略的非 请求,约束是可选的;	其他参数,这些参数是匹配连接请求所必需的。如果约束与连接请求不匹配,NPS 将自动拒绝该 如果不希望配置约束,请单击"下一步"。
为此网络策略配置约束。 如果连接请求与所有约束都不匹配, <b>约束 (S)</b> :	将拒绝网络访问。
<ul> <li>约束</li> <li></li></ul>	指定在断开连接前服务器可以保持空闲的最长时间(分钟) 经过最长空闲时间之后断开 (D)





点击**下一步** 

新建网络策略		×
<b>配置设置</b> 如果与策略的所有网	络策略条件和约束都匹配,则 NPS 将对连接请求应用设置。	
配置此网络策略的设置。 如果条件和约束与连接请求匹配,」 <b>设置 (S)</b> :	且该策略授予访问权限,则应用这些设置。	
BADIUS 属性         ◆ 标准         ✓ 供应商特定         网络访问保护         ● NAP 强制	若要将其他属性发送到 RADIUS 客户端,请选择 RADIUS 标准属性,再单击"编辑"。如果不配置属性,则属性不会被发送到 RADIUS 客户端。请参阅 RADIUS 客户端文档以了解所需的属性。 属性(T):	
<ul> <li>▶ 扩展的状态</li> <li>路由和远程访问</li> <li>● 多链路和带宽分配协议(BAP)</li> <li>● IP 筛选器</li> <li>→ 加密</li> </ul>	Framed-Protocol PPP Service-Type Framed	
☑ IP 设置	<b>添加 @)</b> 编辑 @) 删除 @)	
	上一步 (P) 下一步 (N) 完成 (F) 取消	

## 点击**完成**

正在完成	成新建网络策略
您已经成功创建了下列网	络策略: ····································
aruba_wireless_acce	ss_policy
策略条件:	
条件    值	
NAS 标识符 dot1x	
<b>策略设置</b> :	
<b>策略设置</b> : 条件	值
<b>策略设置</b> : 条件 身份验证方法	值 EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP
<b>策略设置</b> : 条件 身份验证方法 访问权限	▲ EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP 授权访问
<b>策略设置:</b> 条件 身份验证方法 访问权限 更新不兼容的客户端 WAP 2841	
<b>策略设置</b> : 条件 身份验证方法 访问权限 更新不兼容的客户端 NAP 强制 Framed=Protocol	值 EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP 授权访问 True 允许完全网络访问 PPP
<b>策略设置</b> : 条件 身份验证方法 访问权限 更新不兼容的客户端 NAP 强制 Framed-Protocol Service-Type	值 EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP 授权访问 True 允许完全网络访问 PPP Framed ▼
<b>策略设置</b> : 条件 身份验证方法 访问权限 更新不兼容的客户端 NAP 强制 Framed-Protocol Service-Type	值 EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP 授权访问 True 允许完全网络访问 PPP Framed ▼
<b>策略设置:</b> 条件 身份验证方法 访问权限 更新不兼容的客户端 NAP 强制 Framed-Protocol Service-Type 若要关闭此向导,请单击	值 EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP 授权访问 True 允许完全网络访问 PPP Framed ▼ **完成"。
<b>策略设置</b> : 条件 身份验证方法 访问权限 更新不兼容的客户端 NAP 强制 Framed=Protocol Service=Type 若要关闭此向导,请单击	值 EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP 授权访问 True 允许完全网络访问 PPP Framed ▼ **完成"。
<b>策略设置:</b> 条件 身份验证方法 访问权限 更新不兼容的客户端 NAP 强制 Framed=Protocol Service=Type 若要关闭此向导,请单击	值 EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP 授权访问 True 允许完全网络访问 PFP Framed







# 2.配置 Aruba 无线控制器

Aruba 控制器的 Controller ip 为 192.168.1.100

两个 VLAN 接口: Interface vlan 10 地址为 172.16.1.1/24, interface vlan 20 地址为 172.16.2.1/24

三个用户角色, Staff、Leader、IT

AP 所属的 AP Group 名称为 Demo-AP-Group

以上网络配置不体现在此文档

## 2.1 配置 EAP-PEAPv0 (EAP-MSCHAPv2) 认证

aaa authentication-server radius win-nps-server host 192.168.1.220 key aruba123 nas-identifier dot1x

#配置认证服务器,设置 NAS-ID 为 dot1x,以击中匹配设置的策略 (aruba_wireless_access_policy)

aaa server-group nps-server-group auth-server win-nps-server

#配置认证服务器组

aaa profile peap-aaa-profile authentication-dot1x peap-auth-dot1x dot1x-default-role Staff dot1x-server-group nps-server-group #配置 AAA Profile #用户通过认证后拿到的默认用户角色为 Staff

wlan ssid-profile peap-ssid-profile essid PEAP opmode wpa2-aes #配置 SSID Profile

wlan virtual-ap peap-vap-profile

aaa-profile peap-aaa-profile ssid-profile peap-ssid-profile vlan 10 #配置 Virtual AP Profile #用户通过认证后,默认拿到的 IP 地址属于 Vlan 10

ap-group Demo-AP-Group virtual-ap peap-vap-profile



#添加 virtual AP Profile 到 AP 组 Demo-AP-Group 下

## 2.2 配置 EAP-TLS 认证

aaa authentication-server radius win-nps-server host 192.168.1.220 key aruba123 nas-identifier dot1x

#配置认证服务器,设置 NAS-ID 为 dot1x,以击中匹配设置的策略 (aruba_wireless_access_policy)

aaa server-group nps-server-group auth-server win-nps-server

#配置认证服务器组

aaa profile eap-tls-aaa-profile authentication-dot1x eap-tls-auth-dot1x dot1x-default-role Staff dot1x-server-group nps-server-group #配置 AAA Profile #用户通过认证后拿到的默认用户角色为 Staff

wlan ssid-profile eap-tls-ssid-profile essid PEAP opmode wpa2-aes #配置 SSID Profile

wlan virtual-ap eap-tls-vap-profile aaa-profile eap-tls-aaa-profile ssid-profile eap-tls-ssid-profile vlan 10 #配置 Virtual AP Profile #用户通过认证后,默认拿到的 IP 地址属于 Vlan 10

ap-group Demo-AP-Group virtual-ap eap-tls-vap-profile

#添加 virtual AP Profile 到 AP 组 Demo-AP-Group 下

#### 以上步骤完成完成以后, AP 会是放出两个 SSID, PEAP 和 EAP-TLS



# 3.证书管理与配置客户端测试 802.1X 认证

根据 802.1X 认证类型的不同,无线客户端和 RADIUS 服务器所需要的证书也不同, EAP-PEAPv0 (EAP-MSCHAPv2) 和 EAP-TLS 认证所需的证书如下:

认证类型	安装在客户端上的证书	安装在 RAIDUS 服务器上的证书	
	根 CA 证书	计算机证书	
EAP-PEAPv0 (EAP-MSCHAPv2)	用于验证 RADIUS 服务器的合法性	向客户端证明其身份	
	用户证书	计算机证书	
	向 RADIUS 服务器证明其身份合法性	向客户端证明其身份	
EAP-ILS	根 CA 证书	根 CA 证书	
	用于验证 RADIUS 服务器的合法性	用于验证用户证书的合法性	

注意: 以上为 EAP 终结在 RADIUS 服务器上的情况

根 CA 证书是 CA 认证中心给自己颁发的证书,是信任链的起始点。安装根 CA 证书意味着对这个 CA 认证中心的信任。

## 3.1 管理 NPS (RADIUS 服务器) 的证书

管理 NPS (RADIUS 服务器) 证书参考 1.5 章节

NPS 上的计算机证书和根 CA 证书如下图所示

🧱 控制台1 - 〔控制台根节	点\证书(本地计算机)\个	·人\证书]						
🚠 文件(F) 操作(A) 查禮	昏(V) 收藏夹(D) 窗口(	W) 帮助(H)						_ 8 ×
🧇 🔿 🖄 🛅 🗋 🧕	🗟 🛛 🖬							
<ul> <li>空 詞台根节点</li> <li>□ 词 证书(本地计算机)</li> <li>□ □ 个人</li> <li>□ □ で书</li> <li>□ □ で括</li> <li>□ □ 受信任的根证书</li> <li>□ □ 受信任的发布者</li> <li>□ □ 受信任人</li> <li>□ □ 受信任人</li> <li>□ □ 受信任人</li> <li>□ □ 可能未受信任的相</li> <li>□ □ 和</li> </ul>	预发给 ▲ Can ad. stonex. com 文 stonex-AD-CA	前发者 stonex-AD-CA stonex-AD-CA	截止日期 2017/7/23 2021/7/23	预期目的 客户端身份验证, <所有>	服务器身份验证	友死	<mark>操作</mark> 证书 更多操作	•
						Þ		
个人 存储含有 2 个证书。								



## 3.2 管理无线客户端的证书

对于 Windows 客户端来说,可以分为加域的客户端和没有加入域的客户端(工作组模式)两种:

- 没有加入域的客户端,需要手动安装根 CA 证书和用户证书
- 加入域的客户端, 会自动安装根 CA 证书, 用户证书可以手动安装, 也可以通过域策略自动下发安装。

#### 3.2.1 没有加域的客户端安装根 CA 证书

没有加入域的客户端(工作组模式)需要手动导入根 CA 证书到计算机,如果客户端加入了域则可以省略此步骤。有两种方法可以导入根证书:

● 方案一: 客户端需要接入网络, 以访问证书服务器的共享文件夹方式来导入根 CA 证书

#### 点击开始 > 输入\\192.168.1.220

الله 🖳 🖓 🖓 📭			
₽ 查看更多结果			
\\192.168.1.220	×	关机	

#### 输入用户名和密码,点击确定

Windows 安全	×
输入网络密输入您的密码和	码 R连接到: 192.168.1.220
	stonex.com\administrator ••••••• 域: stonex.com 同 记住我的凭据
😢 登录	失败: 未知的用户名或错误密码。
	确定取消



## 打开文件夹 CertEnroll

				x
	▶ 192.168.1.220 ▶	▼ 4 搜索 192.168.1.2	20	٩
组织 ▼ 网络和共享•	中心 查看远程打印机		₩ <b>-</b> ▼	0
<ul> <li>☆ 收藏夹</li> <li>↓ 下载</li> <li>■ 桌面</li> <li>2 最近访问的位置</li> </ul>	CertEnroll 共享 sysvol 共享	netlogon 共享		
<ul> <li>□ 库</li> <li>■ 视频</li> <li>■ 图片</li> <li>■ 文档</li> <li>→ 音乐</li> </ul>				
🖳 计算机 🎒 本地磁盘 (C:) 🗖	-			
3 个对象				

## 点击 ad.stonex.com_stonex-AD-CA 进行安装

🔾 🔿 🗸 惧 🕨 网络	▶ 192.168.1.220 ▶ CertEnroll	▼ 4 搜索 CertEnro	
组织 ▼ 新建文件封	ξ		≣ - 🔟 🔞
<ul> <li>□ 库</li> <li>● 视频</li> <li>● 图片</li> <li>● 文档</li> <li>● 音乐</li> <li>● 计算机</li> </ul>	▲ 名称 ad.stonex.com_stonex-AD-CA Insrev_stonex-AD-CA 能 stonex-AD-CA 能 stonex-AD-CA+	修改日期 2016/8/14 11:23 2016/8/14 11:24 2016/8/14 11:24 2016/8/15 15:58	类型 大小 安全证书 ASP 文件 证书吊销列表 证书吊销列表
<ul> <li>▲ 本地磁盘 (C:)</li> <li>③ DVD 驱动器 (D:)</li> <li>● 网络</li> <li>● 4 个对象</li> </ul>	■ ▼ ◆ 脱机状态: 脱机 脱机可用性: 不可用	m	Þ

#### 点击**打开**

打开文件 - 安全警告	X
你要打开业文件吗?	





#### 点击**安装证书**



#### 选择将证书存储在受信任的根证书颁发机构,点击下一步

证书导入向导 X
证书存储 证书存储是保存证书的系统区域。
Windows 可以自动选择证书存储,或者您可以为证书指定一个位置。
◎ 根据证书类型,自动选择证书存储 (U)
◎ 将所有的证书放入下列存储 (P)
<del>证书存储:</del> 受信任的根证书颁发机构





#### 点击**完成**

证书导入向导	×
	正在完成证书导入向导
	单击"完成"后将导入证书。 您已指定下列设置: 用户选定的证书存储 受信任的根证书颁发机构 内容 证书
	< 上一步 (B)

#### 选择**是**



#### 点击**确定**,根证书安装完成





● 方案二: 从服务器导出根 CA 证书, 再导入到客户端计算机上

#### 右击根证书 (stonex-AD-CA) -> 所有任务 -> 导出



#### 点击**下一步**





![](_page_45_Picture_7.jpeg)

#### 点击**下一步**

![](_page_46_Picture_2.jpeg)

#### 选择证书导出的路径,点击下一步

证书	<b>持出向导</b>		X
3	<b>要导出的文件</b> 指定要导出的文件名。		
	文件名(F): C:\Vsers\Administrator\Desktop\AD.cer	浏览 (8)	

![](_page_46_Picture_5.jpeg)

![](_page_46_Picture_6.jpeg)

## 点击**完成**

证书导出向导	×	
	正在完成证书导出向导	
	您已成功地完成证书导出向导。 您已指定下列设置: 文件名    C:\Users\Adminis 导出密钥    否 数据包括证书路径中所有证书 否 文件格式    DBR 编码二进制 X	
		点击 <b>完成</b> ,证书导出成功
		<b>证书导出向导</b> 📕
		导出成功。
	< 上一步 (B) 完成 取消	确定

## 证书导出成功之后,可通过 USB 介质将根证书复制到客户端计算机上,如下所示,点击进行安装

![](_page_47_Picture_4.jpeg)

![](_page_47_Picture_5.jpeg)

#### 点击**安装证书**

![](_page_48_Picture_2.jpeg)

#### 选择将证书存储在受信任的根证书颁发机构,点击下一步

证书导入向导 X
证书存储 证书存储是保存证书的系统区域。
Windows 可以自动选择证书存储,或者您可以为证书指定一个位置。
◎ 根据证书类型,自动选择证书存储 (U)
◎ 将所有的证书放入下列存储 (P)
<del>证书存储:</del> 受信任的根证书颁发机构

![](_page_48_Picture_5.jpeg)

![](_page_48_Picture_6.jpeg)

#### 点击**完成**

证书导入向导	×
	正在完成证书导入向导
	单击"完成"后将导入证书。 您已指定下列设置: 用户选定的证书存储 受信任的根证书颁发机构 内容 证书
	< 上一步 (B)

#### 选择**是**

![](_page_49_Picture_4.jpeg)

#### 点击**确定**,根证书安装完成

![](_page_49_Picture_6.jpeg)

![](_page_49_Picture_7.jpeg)

根证书安装完成之后,可通过证书管理器工具控制台 (certmgr.msc)进行查看验证

点击 <b>开始</b>	>	输入	certmgr.msc,	打开 <b>证书管理工具控制台</b>
		11776 4	· · · · · · · · · · · · · · · · · · ·	

程序 (1)			
ᡖ certmgr			
▶ 宣君更多结果			
certmgr.msc	×	关机	

🚡 certmgr - [证书 - 当前用户\受信(	任的根证书颁发机构\证书]		-			
文件(F) 操作(A) 查看(V) 帮助(H)						
🗢 🔿 🙋 📅 📋 🙆 😖 🛛	? 📷					
<ul> <li>□ 证书 - 当前用户</li> <li>▶ □ 个人</li> <li>▶ □ 双右灯が相ばまが原始われ</li> </ul>	颁发给 IIII Baltimore CyberTrust Root	颁发者 Baltimore CyberTrust Root	截 20			
<ul> <li>▲ 受信任的很证书颁发机构</li> <li>◎ 证书</li> <li>▶ ◎ 企业信任</li> <li>▶ ◎ 中级证书颁发机构</li> <li>▶ ◎ Active Directory 用户对象</li> <li>▶ ◎ 受信任的发布者</li> <li>▶ ◎ 天信任的证书</li> <li>▶ ◎ 第三方根证书颁发机构</li> <li>▶ ◎ 受信任人</li> <li>▶ ◎ 受信任人</li> </ul>	Class 3 Public Primary Certifi Copyright (c) 1997 Microsoft DigiCert Global Root CA GTE CyberTrust Global Root Microsoft Authenticode(tm) Microsoft Root Authority Microsoft Root Certificate A NO LIABILITY ACCEPTED, (c)	Class 3 Public Primary Certifica Copyright (c) 1997 Microsoft C DigiCert Global Root CA GTE CyberTrust Global Root Microsoft Authenticode(tm) Ro Microsoft Root Authority Microsoft Root Certificate Aut NO LIABILITY ACCEPTED, (c)97 stonex-AD-CA	20 19 20 20 20 20 20 20 20 20 20			
<ul> <li>▶ □□ 祉予注册申请</li> <li>▶ □□ 智能卡受信任的根</li> </ul>	Thawte Timestamping CA	Thawte Timestamping CA VeriSign Class 3 Public Primary	20 20			
受信任的根证书颁发机构存储含有12个证书。						

![](_page_50_Picture_5.jpeg)

## 3.2.2 没有加域的客户端安装用户证书

打开浏览器, 输入地址 https://192.168.1.220/certsrv

#### 选择**继续浏览此网站 (不推荐)**

🏉 证书错误:	导航已阻止 - Windows Internet Explorer	_	x
<b>S·</b>	https://192.168.1.220/certsrv     ▼		<del>ب</del> 9
👷 收藏夹	🚖 🙋 建议网站 🔻 🤌 网页快讯库 🔻		
🏉 证书错误	会 导航已阻止	工具(0) ▼	• 🕄
8	此网站的安全证书有问题。		^
	此网站出具的安全证书是为其他网站地址颁发的。		
	安全证书问题可能显示试图欺骗您或截获您向服务器发送的数据。		
	建议关闭此网页 , 并且不要继续浏览该网站。		
	◎ 单击此处关闭该网页。		
	፟፟፟፟ ⑧ 继续浏览此网站(不推荐)。		
	● 更多信息		
完成	Sinternet   保护模式: 启用	100% 🕄	• •

## 输入用户名和密码,点击**确定**

Windows 安全	X
正在连接到 19	2.168.1.220.
	WIN7-DEMO\stonex.com
	stonex.com\wuxl

![](_page_51_Picture_7.jpeg)

![](_page_51_Picture_8.jpeg)

## 选择**申请证书**

🏉 Microsoft Active Directory 证书服务 - Windows Internet Explorer
🕞 🕞 🗢 💈 https://192.168.1.220/certsrv/ 🔹 😵 证书错误 🗟 🍫 🗙 👂 Bing 🖉 🗸
🖕 收藏夹 🛛 🍰 💋 建议网站 ▼ 🥔 网页快讯库 ▼
Microsoft Active Directory 证书服务
Nicrosoft Active Directory 证书服务 stonex-AD-CA 主页
动物体田
<u> </u>
使用此网站为您的 Web 浏览器、电子邮件客户端或其他程序申请证书。通过使用证书,您可以向通过 Web 进行通信的用户确认您的身份、签名并加密邮件,并根据您申请的证书类型执行其他安全任务。
您也可以使用此网站下载证书颁发机构(CA)证书、证书链,或证书吊销列表(CRL),或者查看挂起申请的状态。
有关 Active Directory 证书服务的详细信息,请参阅 <u>Active Directory 证书服务文档</u> .
<b>选择一个任务:</b> <u>申请证书</u> <u>查看挂起的证书申请的状态</u> <u>下载 CA 证书、证书链或 CRL</u>
 完成

#### 选择**用户证书**

🥖 Microsoft Active Directory 证书服务 - Windows Internet Explorer	
	+ م
🚖 收藏夹 🛛 🍰 建议网站 ▼ 🤌 网页快讯库 ▼	
Microsoft Active Directory 证书服务	工具(0) ▼ 🔞 ▼
<b>Microsoft</b> Active Directory 证书服务 stonex-AD-CA	主页
申请一个证书	
选择一个证书类型: 用户证书	
或者,提交一个 <u>高级证书申请</u> 。	

![](_page_52_Picture_5.jpeg)

![](_page_52_Picture_6.jpeg)

#### 选择**是**

![](_page_53_Picture_2.jpeg)

#### 点击**提交**

![](_page_53_Picture_4.jpeg)

#### 选择**是**

ĺ	Web访问确认。	X	

	是(Y) 否(N)
	您应该只允许已知网站代表您执行数字证书操作。 是否要允许此操作?
-	https://192.168.1.220/certsrv/certfnsh.asp
	此网站正在尝试代表您执行数字证书操作。

![](_page_53_Picture_8.jpeg)

#### 点击**安装此证书**

🏉 Microsoft Active Directory 证书服务 - Windows Internet Explorer	
🕞 🕞 🗢 💋 https://192.168.1.220/certsrv/certf 👻 😵 证书错误 🗟 🍫 🗙 👂 Bing	• ٩
🖕 收藏夹 🛛 ลៀ 建议网站 🔻 🤌 网页快讯库 🔻	
Microsoft Active Directory 证书服务     Solution     Solution	工具(0) ▼ 😢 ▼
<b>Microsoft</b> Active Directory 证书服务 stonex-AD-CA	主页
江井口炳华	
您申请的证书已颁发给您。	
安装此证书	
□保存响应	
	_
完成	€ 100% <b>▼</b>

#### 证书安装成功

![](_page_54_Picture_4.jpeg)

![](_page_54_Picture_5.jpeg)

![](_page_54_Picture_6.jpeg)

可通过证书管理器工具控制台进行查看验证

🔚 certmgr - [证书 - 当前用户\个人\	证书]		
文件(F) 操作(A) 查看(V) 帮助	(H)		
🗢 🔿 🔁 🗊 📋 🙆 😹	? 🗊		
🗊 证书 - 当前用户	颁发给	颁发者	截
<ul> <li>▲ 11×</li> <li>□ 证书</li> <li>▶ ○ 受信任的根证书颁发机构</li> <li>▶ ○ 企业信任</li> <li>▶ ○ 中级证书颁发机构</li> <li>▶ ○ 中级证书颁发机构</li> <li>▶ ○ 在tive Directory 用户对象</li> <li>▶ ○ 受信任的发布者</li> <li>▶ ○ 不信任的证书</li> <li>▶ ○ 第三方根证书颁发机构</li> <li>▶ ○ 受信任人</li> </ul>	wuxl	stonex-AD-CA	2
<ul> <li>▷ □ 证书注册申请</li> <li>▷ □ 智能卡受信任的根</li> </ul>	<		4

#### 3.2.3 加域的客户端手动安装用户证书

加域的客户端手动安装用户证书步骤与没有加域的客户端安装用户证书一样,参考 3.2.2 章节

#### 3.2.4 加域的客户端通过组策略自动安装用户证书

点击开始 -> 管理工具 -> 证书颁发机构, 右击证书模板, 点击管理

🍃 certsrv - 〔证书颁发机构(本地	])\stonex-AD-CA\证书模板]		
文件(P) 操作(A) 查看(V) 帮助	) (ዘ)		
🗢 🔿 🙎 💁 👔			
🙀 证书颁发机构 (本地)	名称	预期目的	
🖃 🚽 stonex-AD-CA	🚇 目录电子邮件复制	目录服务电子邮件复制	
📄 吊销的证书	🛛 🚇 域控制器身份验证	客户端身份验证,服务器身份验证,	
📄 颁发的证书	🛛 💀 EFS 故障恢复代理	文件恢复	
📔 挂起的申请	🛛 🖳 基本 EFS	加密文件系统	
📔 失败的申请	🗵 域控制器	客户端身份验证,服务器身份验证	
□ 证书稿 ⁺⁺ 管理 (0)	└────────────────────────────────────	服务器身份验证	
	] 计算机	客户端身份验证,服务器身份验证	
新建(11)	▶】用户	加密文件系统,安全电子邮件,客户	
	→】从属证书颁发机构	〈全部〉	
	系统管理员	Microsoft 信任列表签名,加密文件	
刷新 (2)			

![](_page_55_Picture_8.jpeg)

![](_page_55_Picture_9.jpeg)

#### 右击**用户**,点击**复制模板**

🚇 证书模板控制台				
文件(F) 操作(A) 查看(V) 帮	助(H)			
🗇 🔿 🔲 🗉 🗈 📝 🗖				
🗷 证书模板(ad. stonex. com)	模板显示名称 ▲	最低支持的 CA	版本 预	期 ▲ 操作
	🗟 Exchange 用户	Windows 2000	7.1	证书植板 (ad stoney 🔺
	🖳 IPSec	Windows 2000	8.1	IL DE K (au. stones
	🖳 IPSec(脱机申请)	Windows 2000	7.1	■」●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
	🖳 Kerberos 身份验证	Windows Server 2003	110.0 客	
	│ 凰 OCSP 响应签名	Windows Server 2008	101.0 00	SP H/P
	🖳 RAS 和 IAS 服务器	Windows Server 2003	101.0 客	沪嶺 ┃ 更多操作 ▶
	A Web 服务器	Windows 2000	4.1	
	🖳 从属证书颁发机构	Windows 2000	5.1	
	🖳 代码签名	Windows 2000	3.1	
	🖳 根证书颁发机构	Windows 2000	5.1	
	🖳 工作站身份验证	Windows Server 2003	101.0 客	户站
	图 基本 EFS	Windows 2000	3.1	
	图 计算机	Windows 2000	5.1	
	图 交叉证书颁发机构	Windows Server 2003	105.0	
	图 交换注册代理(脱机请求)	Windows 2000	4.1	
	图 仅 Exchange 签名	Windows 2000	6.1	
	图 路由器 (脱机请求)	Windows 2000	4.1	
		Windows Server 2003	105.0 密	
	图 目录电子邮件复制	Windows Server 2003	115.0 目	录月
	凰 通过身份验证的会话	Windows 2000	3.1	
		Windows 2000	4.1	
	图 信任列表签名	Windows 2000	3.1	_ 11
		Windows 2000	3.1	
		Windows 2000	4.1	
	▲ 域控制 所有任务(K) ▶	Windows Server 2003	110.0 客	户ÿ
		Windows 2000	4.1	
		Windows 2000	6.1	
	▲ 帮助(H)	Windows 2000	11 1	
-				

#### 点击**确定**

![](_page_56_Picture_4.jpeg)

#### 更改模板名称,这里更改名称为自动颁发用户证书

植板的属性			×
发布要求	取代模板	扩展	安全
常规	请求处理	使用者名称	服务器
模板显示名称 Œ	):		
自动颁发用户证	书		
最低支持的 CA:	Windows Server	2003 Enterprise	
模板名(T):			
自动颁发用户证	书		

![](_page_56_Figure_7.jpeg)

![](_page_56_Picture_8.jpeg)

切换至使用者名称,确保证书信息中不包含电子邮件名,否则有些创建的用户没有设置电子邮件名,自动颁发证书

#### 时会报错。

新模板的属性	×
发布要求 取代模板 扩展 友全	Į
常规   请求处理 使用者名称   服务;	×
○ 在请求中提供 (S)	
■ 使用现有证书中的使用者信息进行自动注册续订请求 (W)	
<ul> <li>● 用 Active Directory 中的信息生成(B)</li> <li>要加强使用者名称之间的一致性并简化证书管理,请选择这个选项。</li> <li>使用者名称格式(N):</li> <li>完全可分辨名称</li> <li>一、</li> <li>一、在使用者名称中包括电子邮件名(C)</li> <li>将这个信息包括在另一个使用者名称中:</li> <li>电子邮件名(C)</li> <li>□ DNS 名(D)</li> <li>○ 用户主体名称(UPN)(U)</li> <li>□ 服务的主体名称(SPN)(V)</li> </ul>	
确定 应用 (A)帮.	 助

切换至**使用者名称,**选中 Domain Users,勾选允许**读取、注册和自动注册的权限** 

□ 市水20世 发布要求 □ 取代模板	使用者   扩照	名称 民	服务器 安全
且或用户名(G):			
🍇 Authenticated Users			
🔏 Administrator			
Real Domain Admins (STONEX\Do	main Admins	)	
🚜 Domain Users (STONEX\Dom	ain Users)		
💐 Enterprise Admins (STONE	X\Enterpris	e Admin	(z)
	添加	D)	删除(R)
omain Users 的权限(P)	添加	D) 允许	删除(R) 拒绝
omain Users 的权限(P) 完全控制	添加	D) 允许	删除(R) 拒绝
omain Users 的权限(P) 完全控制 读取	添加	D) 允许	删除(R) 拒绝
omain Users 的权限(P) 完全控制 读取 写入	添加	D) 允许	删除(R) 拒绝
omain Users 的权限(P) 完全控制 读取 写入 注册	<u>添加</u> 1	๗) <u> 允许</u> □ □ □ □ □ □ □	删除(R) 拒绝 日 日 日
omain Users 的权限(F) 完全控制 读取 写入 注册 自动注册	<u>添加</u> )	_即 … 允许 □□□□	删除(R) 拒绝 日 日 日 日
omain Users 的权限(P) 完全控制 读取 写入 注册 自动注册	<u>添加</u> )	¹⁰⁾ 允许 ロ ロ ロ ロ ロ ロ	删除(B) 拒绝 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日

![](_page_57_Figure_6.jpeg)

![](_page_57_Picture_7.jpeg)

## 新建证书模板:自动颁发用户证书,步骤完成

🚇 证书模板控制台					
文件(F) 操作(A) 查看(V) 帮	助(H)				
♦ ♦ 🔂 🗙 🖬 🛃 🖬	1				
🗵 证书模板(ad. stonex. com)	模板显示名称 ▲	最低支持的 CA	版本	预期Ⅰ▲	操作
	│ 🖳 OCSP 响应签名	Windows Server 2008	101.0	OCSP	证书模板 (ad_stonex ▲
	🖳 RAS 和 IAS 服务器	Windows Server 2003	101.0	客户	
	│ ً ፼ Web 服务器	Windows 2000	4.1		●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
	🛛 🖳 从属证书颁发机构	Windows 2000	5.1		白动场华田百江北
	🖳 代码签名	Windows 2000	3.1		日初頑友用尸脏节
	🖳 根证书颁发机构	Windows 2000	5.1		● 更多操作 ●
	🖳 工作站身份验证	Windows Server 2003	101.0	客户社	
	🖳 基本 EFS	Windows 2000	3.1		
	🛛 🖳 计算机	Windows 2000	5.1		
	🛛 🖳 交叉证书颁发机构	Windows Server 2003	105.0		
	🛛 🕺 交換注册代理(脱机请求)	Windows 2000	4.1		
	🖳 仅 Exchange 签名	Windows 2000	6.1		
	🖳 路由器 (脱机请求)	Windows 2000	4.1		
	🛛 🐵 密钥恢复代理	Windows Server 2003	105.0	密钥	
	🛛 🗐 目录电子邮件复制	Windows Server 2003	115.0	目录刖	
	🖳 通过身份验证的会话	Windows 2000	3.1		
	🖳 系统管理员	Windows 2000	4.1		
	🖳 信任列表签名	Windows 2000	3.1		
	🖳 用户	Windows 2000	3.1		
	🖳 域控制器	Windows 2000	4.1		
	🚇 域控制器身份验证	Windows Server 2003	110.0	客户。	
	🖳 只是用户签名	Windows 2000	4.1		
	🖳 智能卡登录	Windows 2000	6.1		
	🖳 智能卡用户	Windows 2000	11.1		
	🖳 注册代理	Windows 2000	4.1		
	🖳 注册代理 (计算机)	Windows 2000	5.1		
	團 自动颁发用户证书	Windows Server 2003	100.2	加密	
	•				
34 证书模板					

## 打开证书颁发机构,右击证书模板 -> 新建 -> 要颁发的证书模板

🍹 certsrv - [证书頒发机构 (本	地)\stonex-AD-CA\证书模板]		
文件(F) 操作(A) 查看(V) 帮	)助(H)		
🗢 🔿 🙇 🙆 👔			
🔖 证书颁发机构 (本地)	名称	预期目的	
🖃 🝶 stonex-AD-CA	🛛 🚇 目录电子邮件复制	目录服务电子邮件复制	
🥂 📫 吊销的证书	📲 國 域控制器身份验证	客户端身份验证,服务器身份验证,	
📄 颁发的证书	🛛 🚇 BFS 故障恢复代理	文件恢复	
挂起的申请	🛛 🚇 基本 EFS	加密文件系统	
📃 失败的申请	🛛 🚇 域控制器	客户端身份验证,服务器身份验证	
□ 业书模称	│	服务器身份验证	
		客户端身份验证,服务器身份验证	
新建(11)	▶ 要颁发的证书模板(T)	加密文件系统,安全电子邮件,客户	
本手の	风周虹节顶反机构	〈全部〉	
	系统管理员	Microsoft 信任列表签名,加密文件	
刷新 (F)			
导出列表 (L).			
帮助(H)			

![](_page_58_Picture_5.jpeg)

![](_page_58_Picture_6.jpeg)

## 选中自动颁发用户证书,点击确定

启用证书模板		×
在此证书颁发机构上选择启用 注意:如果最近创建的证书模 可能需要等待。 组织中的所有证书模板可能都 有关详细信息,请参阅 <u>证书</u> 称	一个证书模板。 板没有出现在此列表上,则在有关此模板的信息复制到所有域控制器之前 不适用于您的 CA。 <mark>就板概念</mark> 。	
名称	预期目的▲	1
風 密钥恢复代理	密钥恢复代理	-
🗷 工作站身份验证	客户端身份验证	
風 智能卡用户	安全电子邮件,客户端身份验证,智能卡登录	
風 智能卡登录	客户端身份验证,智能卡登录	
風 注册代理	证书申请代理	
回 注册代理 (计算机)	证书申请代理	1
🚇 自动颁发用户证书	客户端身份验证,安全电子邮件,加密文件系统	
風 路由器 (脱机请求)	客户端身份验证	
風 通过身份验证的会话	客户端身份验证	1
1		-
	确定 取消	

🍃 certsrv - [证书颁发机构(本地	])\stonex-AD-CA\证书模板]		
文件()》 操作(A) 查看(V) 帮助	) (H)		
🗢 🔿 🖄 🙆 😫			
<ul> <li>□ 证书颁发机构(本地)</li> <li>□ stonex-AD-CA</li> <li>□ 吊销的证书</li> <li>□ 颁发的证书</li> <li>□ 强发的申请</li> <li>□ 失败的申请</li> <li>□ 证书模板</li> </ul>	<ul> <li><b>全称</b> ☑ 自动颁发用户证书 ☑ 目录电子邮件复制 ☑ 域控制器身份验证 ☑ BFS 故障恢复代理 ☑ 基本 BFS ☑ 域控制器 ☑ Web 服务器 ☑ 计算机 ☑ 用户 ☑ 从属证书颁发机构 ☑ 系统管理员</li></ul>	预期目的 客户端身份验证,安全电子邮件,加 目录服务电子邮件复制 客户端身份验证,服务器身份验证, 文件恢复 加密文件系统 客户端身份验证,服务器身份验证 服务器身份验证 客户端身份验证,服务器身份验证 加密文件系统,安全电子邮件,客户 〈全部〉 Microsoft 信任列表签名,加密文件	

![](_page_59_Picture_4.jpeg)

#### 点击开始 -> 管理工具 -> 组策略管理,

#### 点击林 -> 域 -> stonex.com, 右击 Default Domain Policy -> 编辑

星组策略管理				
≦ 文件() 操作(A) 查看(V)	窗口(W) 帮助(H)			_8
🄄 🔿   🖄 🗊   👗 🧟   🚺 🗄	1			
Magame管理 □ Aa 林: stonex.com □ 論 域 □ 論 stonex.com	Defaul 作用域 链接	t Domain Policy 详细信息   设置   委派		
🗾 Default Domain I	编辑(E)	]显示链接(L): stonex.com	m	•
🛨 🗾 Domain Controll	强制 (M)	域和组织单位链接到此 GPO(T):		
<ul> <li>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</li></ul>	✓ 已启用链接(L) 保存报告(S)		<u>强制   已启用锁</u>   否 - 是	接 路径
⊞ 📑 ₩MI 筛选器 団 🛅 Starter GPO 田 晴 站占	查看(V) 🔸 🕨			s context. Com
超策略建模 建 组策略结果	刪除(0) 重命名(M) 刷新(7)	的设置只应用于下列组、用户和计算	〔机(S):	
	帮助(H)	nticated Users		
	添加 ₩ <b>MI 筛</b> 此 GPO 5 (元>	1(0) 删除(R)	属性 (P)	] [开(0)
1换此链接的已启用链接属性				

#### 点击**用户配置 -> 策略 -> 安全设置 -> 公钥策略**

选中**证书服务客户端 – 自动注册**,选择**已启用**,勾选以下三项,点击确定

<b>」</b> 组策略管理编辑器			
文件(F) 操作(A) 查看(V) 帮助(H)			
🗢 🔿 🙍 💼 🗎 🖬			
🗐 Default Domain Policy [AD. STONEX. COM]	Ⅰ 对象类型		
🖂 👰 计算机配置	📔 企业信任		
🛛 🖸 策略	■ 🚰 受信任人		
🗉 🚞 首选项	🛛 🚮 证书服务客户端 - 证书注册策略		
🗆 💰 用户配置	🛛 🚮 证书服务客户端 - 凭据漫游		
	🚮 证书服务客户端 - 自动注册		
		江北肥冬安白洲 一 白动注册 居林	21
□ ■ Windows 设置		虹节撒方脊广阔 日初注册 禹社	كك
		注册策略配置	
日 🤷 安全设立			
日日 公田東船		白玉注四田白石油的短田江北	
- 正江信任 - 一 一 正江信任 - 一 一 一 一 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二		自幼注册用户和计算机证书	
		間直型すじに	•
王 M Internet Evplorer 维拍		IM 察订过期证书、更新本决证书开删除币销的证书 (R)	

![](_page_60_Picture_7.jpeg)

![](_page_60_Picture_8.jpeg)

通过域策略自动下发用户证书配置完成,配置完成后可通过命令 gpupdate /force 强制更新组策略

加域的客户端使用域账号登录成功后, 会自动安装相应的用户证书。

![](_page_61_Picture_3.jpeg)

# 3.3 配置客户端测试连接 802.1X 认证

EAP-PEAPv0 (PEAP-MSCHAPv2) 的 Windows 客户端配置如下:

PEAP 无线网络属性	×
连接 安全	
安全类型(B): WPA2 - 企业 ▼	
加密类型 (M): AES ▼	
Microsoft: 受保护的 EAP (PEAP) ▼ 设置(S)	
☑ 每次登录时记住此连接的凭据 (R)	
高级设置 (0)	
	[
确定即	消

受保护的 EAP 属性
当连接时: ☑ 验证服务器证书(V) □ 连接到这些服务器(0):
受信任的根证书颁发机构(B):
Stonex-AD-CA VTN-USERFirst-Object UTN-USERFirst-Object VeriSign Class 3 Public Primary Certification Au. VeriSign Class 3 Public Primary Certification Au. VeriSign Universal Root Certification Authority
•
<ul> <li>□ 不提示用户验证新服务器或受信任的证书授权机构 (P)。</li> <li>选择身份验证方法 (S):</li> <li>(EAP-HISCHAP v2)</li> <li>✓ 启用快速重新连接 (P)</li> <li>□ 强制执行网络访问保护 (F)</li> <li>□ 如果服务器未提供加密绑定的 TLV 则断开连接 (D)</li> <li>□ 启用标识隐私 (T)</li> </ul>
确定取消

## EAP-TLS 的 Windows 客户端配置如下:

EAP-TLS 无线网络属性	x
安全类型 (E): ₩PA2 - 企业 ▼ 加密类型 (N): AES ▼	
选择网络身份验证方法 (0): Microsoft:智能卡或其他证书	
高级设置 (0)	

能卡或其他证书属性	<b>X</b>
当连接时:	
◎ 使用我的智能卡 (S)	
◎ 在此计算机上使用证书(C)	
☑ 使用简单证书选择 (建议使用) (M)	
✓验证服务器证书(V)	
一 连接到这些服务器 (0):	
受信任的根证书颁发机构(B):	
Incrosoft Root Certificate Authority 2010	
I Microsoft Root Certificate Authority 2011	
Interest Root Certificate Authority 2011	
stonex-AD-CA	
QuoVadis Root CA 2	
ROOTCA	
📃 Starfield Class 2 Certification Authority	
Starfield Root Certificate Authority - G2	Ψ.
< III	•
查看证书	(E)
🔲 不提示用户验证新服务器或受信任的证书授权机构 0	?) o

![](_page_62_Picture_8.jpeg)

![](_page_62_Picture_9.jpeg)

#### 配置完成之后,可以成功通过 802.1X 认证, 连接无线网络。

![](_page_62_Picture_11.jpeg)

# 4.实现用户角色控制

通过配置网络策略还可以实现用户角色的控制,此处示例是实现不同组的用户获取不同的 User-Role。

新建一个网络策略,点击下一步

新建网络策略
<b>指定网络策略名称和连接类型</b> 可以为您的网络策略指定一个名称和要应用该策略的连接类型。
策略名称(A): Leader_access_policy 网络连接方法 选择向 NPS 发送连接请求的网络访问服务器类型。您可以选择网络访问服务器的类型或特定于供应商的类型,也可以不进 行选择。如果您的网络访问服务器是 802.1X 身份验证交换机或无线访问点,请选择"未指定"。
<ul> <li>● 网络访问服务器的类型(S):</li> <li>□ ▼</li> <li>● 供应商特定(V):</li> <li>□ □</li> </ul>
上一步(37) 一定成(37) 取消

## 此处添加条件, NAS 标识符 dot1x 和用户组 Leader, 点击下一步

指定用于很	₹ <b>1</b> 1 偏定是否针对某个连接请求评估此网络贫	§略的条件,至少需要一个;	条件.
-			
<mark>፟፟፟፟</mark> ቸር):			
条件	值		
🕻 NAS 标识符	dot1x		
4 用户组	STONEX\Leader		

![](_page_63_Figure_7.jpeg)

![](_page_63_Picture_8.jpeg)

点击下一步

新建网络策略		٢
	<b>指定访问权限</b> 如果连接请求与此策略匹配,则配量是要投予网络访问权限还是要拒绝网络访问。	
<ul> <li>已授予访如果客户</li> <li>拒绝访问如果客户</li> <li>切果客户</li> <li>切果客户</li> </ul>	间权限(A) 端连接尝试匹配此策略的条件,则授予访问权限。 (D) 端连接尝试匹配此策略的条件,则拒绝访问权限。 声拨入属性(它将替代 NPS 策略)所决定(S) 端连接尝试匹配此策略的条件,则根据用户拨入属性授予或拒绝访问权限。	
	上一步 (2) 下一步 (3) 完成 (2) 取消	

#### 点击下一步

![](_page_64_Picture_4.jpeg)

![](_page_64_Picture_5.jpeg)

## 点击下一步

新建网络策略 人名法格尔 人名英格尔 人名英格尔 人名英格尔 人名英格尔 人名英格尔 人名英格尔 人名英格尔
<b>配置约束</b> 约束是指网络策略的其他参数,这些参数是匹配连接请求所必需的,如果约束与连接请求不匹配,NPS 将自动拒绝该 请求,约束是可选的;如果不希望配置约束,请单击"下一步",
加集连接请求与所有约束都不匹配,将拒绝网络访问。 <b>约束 约束</b> ② 会话超时         ③ 会话超时         ④ 如叫站 ID         ④ 日期和时间限制         ③ 私S 端口类型
上一步 (2) 下一步 (3) 完成 (2) 取消

## 添加 VSA 属性,点击添加

新建网络策略		×
<b>配置设置</b> 如果与策略的所有网	络策略条件和约束都匹配,则 NPS 将对连接请求应用设置。	
配置此网络策略的设置。 如果条件和约束与连接请求匹配,	且该策略授予访问权限,则应用这些设置。	
设置(S):		_
BADIUS 属性	着要将其他属性发送到 BADIUS 客户端,请选择供应商特定属性,再勇击"编	
🛛 🚳 标准	辑″。如果不配 <u>古禹性,则</u> 禹性不会做友送到 RADIUS 各户端。请参阅 RADIUS   客户端文档以了解所需的属性。	
🔽 供应商特定		
网络访问保护		
NAP 强制	属性(T):	
▲ 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」	_ 名称  供应商  值	
路由和远程访问		
多链路和带宽分配协议(BAP)		
🔒 IP 筛选器		
🛃 加密		
□ IP 设罟	<b>添加 (2)</b> / / / / / / / / / / / / / / / / / /	

上一步 (P) 下一步 (M) 完成 (P) 取消	

![](_page_65_Picture_6.jpeg)

## 选择 Vendor-Specific,点击添加

添加供应商特定属性	×
若要在设置中添加属性,请选择属性,再单击"添加"。	-
要添加一个没有列出的供应商特定属性,请选择"自定义",再单击"添加"。	
供应商(V):	
自定义	
属性 (3):	
名称	
Allowed-Certificate-OID RADIUS Standard	1
Generate-Class-Attribute RADIUS Standard	
Generate-Session-Timeout RADIUS Standard	1
Tunnel-Tag RADIUS Standard	
Vendor-Specific RADIUS Standard	
描述:	
分类专有 NAS 性能支持。	
	- 1
添加(A)关闭(C)	

#### 点击添加

属性信息		×
属性名: Vendor-Specific		
属性号: 26		
属性格式: OctetString		
属性值(T):		
供应商值		添加(A)
		编辑(E)
		删除(R)
		上移(0)
		下移(0)
	确定	

## 输入供应商代码: Aruba 的为 14823

×		供应商特定的属性信息	
			属性名(T): 供应商特定
		•	指定网络访问服务器供应
~	ļ	RADIUS Standard	○ 从列表中选择(S):
1		RADIUS Standard	○ 从列表中选择(S):

![](_page_66_Figure_7.jpeg)

![](_page_66_Picture_8.jpeg)

## 配置属性如下:

配置 VSA(与 RFC 兼容)	×
供应商分配的属性号(V):	
属性格式(A):	
字符串	
<u>属性值(B)</u> :	
Leader	
Г	72

此处的属性值 Leader 就是要定义的 User-role

#### 点击确定

供应商特定的属性信息		×
属性名(T): 供应商特定		
指定网络访问服务器供应问	商。	
○ 从列表中选择(S):	RADIUS Standard	~
● 输入供应商代码(B):	14823	-
指明属性是否符合 RADIUS	S RFC 规格中的供应商特定属性。	
④ 是(Y)。它符合		
○ 否 (07)。它不符合		
配置属性(A)		
	确定	取消

## 点击确定

属性信息	×
属性名: Vendor-Specific	
属性号: 26	
属性格式: OctetString	
属性值 (T):	
供应商 值	添加(A)
供应商代码: 14823 Leader	编辑(E)
	册除(R)
	上移(0)

![](_page_67_Picture_8.jpeg)

![](_page_67_Picture_9.jpeg)

点击关闭

添加供应商特定属性		×
若要在设置中添加属性,请选	择属性,再单击"添加"。	
要添加一个没有列出的供应商	特定属性,请选择"自定义",再单击"添加"。	
供应商 (V)·		
自定义		
名称	供应商	
Allowed-Certificate-OID	RADIUS Standard	
Generate-Class-Attribute	RADIUS Standard	
Generate-Session-Timeout	RADIUS Standard	1.5
Tunnel-Tag	RADIUS Standard	
Vendor-Specific	RADIUS Standard	
100.10		
<b>油</b> 还:		
分类专有 NAS 性能支持。		
	活動の) デ河の)	<b>n</b>
		J

点击下一步

新建网络策略		×
<b>配置设置</b> 如果与策略的所有网	络策略条件和约束都匹配,则 NPS 将对连接请求应用设置。	
配置此网络策略的设置。 如果条件和约束与连接请求匹配,」 <b>设置 (S)</b> :	且该策略授予访问权限,则应用这些设置。	
BADTUS <b>国性</b> 参标准 供应商特定	若要将其他属性发送到 RADIUS 客户端,请选择供应商特定属性,再单击"编 辑"。如果不配置属性,则属性不会被发送到 RADIUS 客户端。请参阅 RADIUS 客户端文档以了解所需的属性。	
✓ KUCHT/E 网络访问保护 易 NAP 强制	属性(T):	
<ul> <li>№ 扩展的状态</li> <li>路由和远程访问</li> <li>● 多链路和带寄分配协</li> </ul>	Vendor-Specific RADIUS Standard Leader	
<ul> <li>↓ (BAP)</li> <li>▲ IP 筛选器</li> </ul>		
M 加密 ☑ IP 设置	<b>添加 @)</b> 编辑 @) 删除 @)	
	,	

![](_page_68_Picture_5.jpeg)

![](_page_68_Picture_6.jpeg)

#### 点击完成

所建网络策略		×
正在完成	<b>戈新建网络策略</b>	
您已经成功创建了下列网络	各策略:	
Leader_access_policy	•	
·		
⁹⁸⁴ 때示Ⅰ · · · · · · · · · · · · · · · · · · ·		٦l
NAS 标识符 dot1x		11
用户组 STONEX\Lea	der	
		-
<b>東略设直</b> :	信	a
- 赤庄 		
访问权限		
更新不兼容的客户端	True	
NAP 强制		
Framed-Protocol	PPP	
Service-Type	Framed	
若要关闭此向导,请单击。	'完成"。	

#### 配置完成之后,属于 Leader 组的用户认证会获取到 User-role: Leader

#### 还可以使用其他的 VSA 属性实现灵活的用户角色/策略控制

## 查看查看还有哪些 ARUBA VSA 属性:

(Aruba650) #show aaa radius-attri	include	14823		
Aruba-Mdps-Device-Version	21	String	Aruba	14823
Aruba-Mdps-Max-Devices	18	Integer	Aruba	14823
Aruba-Location-Id	6	String	Aruba	14823
Aruba-Template-User	8	String	Aruba	14823
Aruba-No-DHCP-Fingerprint	14	Integer	Aruba	14823
Aruba-AirGroup-Device-Type	27	Integer	Aruba	14823
Aruba-Mdps-Device-Profile	33	String	Aruba	14823
Aruba-Mdps-Device-Udid	15	String	Aruba	14823
Aruba-AirGroup-Shared-User	25	String	Aruba	14823
Aruba-Mdps-Device-Serial	22	String	Aruba	14823
Aruba-AP-IP-Address	34	IP Addr	Aruba	14823
Aruba-Auth-Survivability	28	String	Aruba	14823
Aruba-User-Role	1	String	Aruba	14823
Aruba-Port-Id	7	String	Aruba	14823
Aruba-Priv-Admin-User	3	Integer	Aruba	14823
Aruba-Mdps-Device-Product	20	String	Aruba	14823
Aruba-WorkSpace-App-Name	31	String	Aruba	14823
Aruba-AS-Credential-Hash	30	String	Aruba	14823
Aruba-User-Vlan	2	Integer	Aruba	14823
Aruba-AirGroup-Shared-Role	26	String	Aruba	14823
Aruba-Device-Type	12	String	Aruba	14823
Aruba-Mdps-Device-Imei	16	String	Aruba	14823
Aruba-Essid-Name	5	String	Aruba	14823
Aruba-AP-Group	10	String	Aruba	14823
Aruba-AS-User-Name	29	String	Aruba	14823
Aruba-CPPM-Role	23	String	Aruba	14823
Aruba-Mdps-Device-Name	19	String	Aruba	14823
Aruba-Mdps-Provisioning-Settings	32	String	Aruba	14823
Aruba-AirGroup-User-Name	24	String	Aruba	14823
Aruba-Mdps-Device-Iccid	17	String	Aruba	14823
Aruba-Framed-IPv6-Address	11	String	Aruba	14823
Aruba-Named-User-Vlan	9	String	Aruba	14823

![](_page_69_Picture_7.jpeg)