

Windows2008之活动目录权限管理服务思科认证 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/644/2021\\_2022\\_Windows200\\_c100\\_644089.htm](https://www.100test.com/kao_ti2020/644/2021_2022_Windows200_c100_644089.htm)

熟悉Windows Server 2003的朋友，相信对RMS(权限管理服务)都不会陌生，它能够有效的保护我们的数字资产在相应授权范围之外不会泄露。在Windows Server 2008中，这一重要特性得以改进和提升，微软把它称之为AD RMS(Active Directory Rights Management Services)，即活动目录权限管理服务。相对于2003下的RMS有了较大的改进与提升，例如：不需要单独下载即可安装、不再需要连接到Microsoft去进行登记等等。AD RMS系统包括基于Windows Server 2008的服务器(运行用于处理证书和授权的Active Directory 权限管理服务 (AD RMS) 服务器角色)、数据库服务器以及AD RMS客户端。AD RMS系统的部署为组织提供以下优势：- 保护敏感信息。如字处理器、电子邮件客户端和行业应用程序等应用程序可以启用AD RMS，从而帮助保护敏感信息。用户可以定义打开、修改、打印、转发该信息或对该信息执行其他操作的人员。组织可以创建子自定义的使用策略模板(如“机密 - 只读”)，这些模板可直接应用于上述信息。- 永久性保护。AD RMS可以增强现有的基于外围的安全解决方案(如防火墙和访问控制列表 (ACL))，通过在文档本身内部锁定使用权限、控制如何使用信息(即使在目标收件人打开信息后)来更好地保护信息。- 灵活且可自定义的技术。独立软件供应商 (ISV) 和开发人员可以使用启用了AD RMS的任何应用程序或启用其他服务器(如在Windows或其他操作系统上运行的内容管理系统或门户服务器)，与AD

RMS 结合使用来帮助保护敏感信息。启用 ISV 的目的是为了将信息保护集成到基于服务器的解决方案(如文档和记录管理、电子邮件网关和存档系统、自动工作流以及内容检查)中。

硬件和软件注意事项 AD RMS 中的功能在 Windows Server 2008 中，通过使用服务器管理器，可以设置 AD RMS 的以下组件：

- Active Directory Rights Management Services。Active Directory 权限管理服务 (AD RMS) 角色服务是一项必需的角色服务，用于安装发布和使用受权限保护的内容所用的 AD RMS 组件。
- 联合身份验证支持。联合身份验证支持角色服务是一项可选的角色服务，允许联合身份借助 Active Directory 联合身份验证服务来使用受权限保护的内容。

简要部署 AD RMS 硬件和软件注意事项 安装 AD RMS 服务器角色时，系统会同时安装必需的服务，其中的一项就是 Internet 信息服务 (IIS)。AD RMS 还需要一个数据库(如 Microsoft SQL Server)，该数据库可与 AD RMS 在同一服务器上运行，也可以在远程服务器和 Active Directory 域服务林中运行。下表介绍了运行具有 AD RMS 服务器角色的基于 Windows Server 2008 服务器的最低硬件要求和建议。注：可用于 Windows Server 2008 的 Server Core 安装选项以及面向基于 Itanium 的系统的 Windows Server 2008 的一组有限服务器角色。下表介绍了运行具有 AD RMS 服务器角色的基于 Windows Server 2008 服务器的软件要求。对于通过启用操作系统上的功能可以满足的要求，可通过安装 AD RMS 服务器角色根据需要配置这些功能。注：启用了 AD RMS 的客户端必须具有启用了 AD RMS 的浏览器或应用程序(如 Microsoft Office 2007 中的 Microsoft Word、Outlook 或 PowerPoint)。为了创建受权限保

护的内容，需要具备 Microsoft Office 2007 Enterprise、Professional Plus 或 Ultimate。为获得附加安全性，可以将 AD RMS 与其他技术(如智能卡)集成在一起。正式部署AD RMS 接下来，开始正式配置安装AD RMS服务器。

1. 安装一台Windows Server 2008，计算机名称为“WS2008-ADRMS”。
2. 配置TCP/IP属性登录系统后，单击“开始”，单击“控制面板”，双击“网络和共享中心”，单击“查看状态”。单击“属性”。在“本地连接属性”窗口中双击“Internet协议版本4(TCP/IPv4)”。输入相关信息。
3. 将WS2008-ADRMS加入到域。单击“开始”，右键点击“我的电脑”，单击“属性”。单击“改变设置”。在“系统属性”窗口中单击“更改”。输入要加入的域名，单击“确定”。输入一个有权限加入域的用户和密码。最后进行确认并重启计算机即可。
4. 将用户“ADRMS-admin”添加到本地Administrators(管理员)组中。
5. 添加 AD RMS Server 角色使用“ADRMS-admin“登录到”ADRMS“服务器上。单击”开始“，点击”管理工具“，单击”服务器管理器“。在”用户帐户控制“窗口单击”继续“。单击”添加角色“；在”添加角色向导“中单击”下一步“；
- 6.勾选”Active Directory Rights Management Services“后单击”添加必需的角色服务“。系统自动勾选相关的服务，单击”下一步“，出现”Active Directory Rights Management Services简介“，单击”下一步“。选择安装的角色服务，默认为”Active Directory仅限管理服务器“，单击”下一步“。选择”新建AD RMS群集“，单击”下一步“。
7. 在”配置数据库“页面，选择”使用其他数据库服务器“，单击”选择“，输入数据库服务器名称后单击”确定“。在

”数据库实例“中选择”默认“，并单击”验证“。最后单击”下一步“。在”服务帐户“页面中，单击”指定“。在”添加角色向导“窗口输入前面创建的用户和密码。单击”确定“。

8.在”群集键存储“页面，保持默认选择”使用AD RMS集中管理的密钥存储“，单击”下一步“。在”群集密钥密码“页面输入一个密码。在”群集网站“页面，选择”默认网站“，单击”下一步“。在”群集地址“页面，选中”使用未加密的连接(https://)“，“端口”采用默认的“80”，单击“验证”。最后单击“下一步”。来源：考试大的美女编辑们

9.在“许可证证书名称”页面输入一个名称。在“SCP注册”页面，保持默认的“立即注册AD RMS服务连接点”。出现“Web服务器简介(IIS)”页面，单击“下一步”。系统列出相关的web服务器的角色服务。单击“下一步”。在“确认”页面对相关信息进行总览，没问题的时候就单击“安装”。系统会显示正在进行安装的过程。成功后会显示一个信息页面，其中要求必须注销后再重新登录才可以管理AD RMS。单击“关闭”并注销系统。重新登录后，单击“开始”，单击“管理工具”，单击“Active Directory Rights Management Services”。在“用户帐户控制”窗口单击“继续”。打开AD RMS管理器。在此可对AD RMS进行相关的管理操作。至此，整个服务器RMS安装部署完成。

管理 AD RMS 在Windows Server 2008中，由于有了服务器管理器的存在，众多任务的管理已经变得相当简单。服务器角色使用 Microsoft 管理控制台 (MMC) 管理单元来进行管理。使用 Active Directory Rights Management Services 控制台可以管理 AD RMS。具体打开方式为：单击“开始”，指向“管理工具”，然

后单击“ Active Directory Rights Management Services ”即可。  
编辑特别推荐: 右键菜单快速整理Windows7磁盘碎片  
Windows安全性饱受质疑 100Test 下载频道开通, 各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)