# 配置有Microsoft RADIUS的Cisco VPN 3000集中器

## 目录



## 简介

Microsoft互联网验证服务器(IAS)和Microsoft商用互联网系统(MCIS 2.0)是现在可以得到的。因为使用在主域名控制器的活动目录其用户数据库， Microsoft Radius服务器是方便的。您不再需要维护独立的数据库。它也支持点对点隧道协议(PPTP) VPN连接的40位和128-bit加密。参考Microsoft清单：配置拨号的IAS和VPN请访问 文档欲知更多信息。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档不限于特定的软件和硬件版本。

### 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 安装并且配置在Windows 2000的RADIUS服务器和Windows 2003年

## 安装RADIUS服务器

如果不安排RADIUS服务器(IAS)已经安装，请执行这些步骤为了安装。如果已经安排RADIUS服务器安装，请继续对配置步骤。

1. 插入Windows服务器光盘并且启动设置程序。
2. 点击**安装添加组件**，然后单击**添加/删除Windows组件**。
3. 在组件中，请点击**网络服务**(但是请勿选择也请勿清除复选框)，然后单击**详情**。
4. 检查**互联网认证服务**并且点击OK键。
5. 单击 **Next**。

## 配置有IAS的Microsoft Windows 2000服务器

完成这些步骤为了配置RADIUS服务器(IAS)和开始服务为了安排可用于验证VPN集中器的用户。

1. 选择**Start > Programs > Administrative Tools >互联网认证服务**。
2. 用鼠标右键单击**互联网认证服务**，并且点击从出现的子菜单的**属性**。
3. 去RADIUS选项为了检查端口的设置。如果您的RADIUS验证和RADIUS认为的用户数据报协议(UDP)端口与在验证和核算提供的(1812和1645验证的， 1813和1646认为的)默认值有所不同，请键入您的端口设置。完成后，单击**确定**。**注意：** 请勿更改默认端口。分离端口通过使用逗号使用多个端口设置验证或核算请求。
4. 用鼠标右键单击**客户端**并且选择**新的客户端**为了添加VPN集中器作为验证、授权和统计(AAA)客户端到RADIUS服务器(IAS)。**注意：** 如果冗余配置在两Cisco VPN 3000集中器之间，必须也添加备份Cisco VPN 3000集中器到RADIUS服务器作为RADIUS客户端。
5. 输入友好名称并且选择作为**协议Radius**。
6. 定义VPN集中器用一个IP地址或DNS名在下一个窗口。
7. 从客户端供应商滚动条选择**思科**。
8. 输入一共享机密。**注意：** 您必须记住您使用的*确切的*机密。您需要此信息为了配置VPN集中器。
9. 单击 **完成**。
10. 双击**Remote access Policy**并且双击在窗口的右侧出现的策略。**注意：** 在您安装IAS后，Remote access Policy应该已经存在。在Windows 2000，授权根据用户帐户和Remote access Policy的拨入属性授权。提供网络管理员在授权连接尝试的更加灵活性的Remote access Policy是一组条件和连接设置。Windows 2000 Routing and Remote Access service和Windows 2000 IAS确定是否的两使用Remote access Policy接受或拒绝连接尝试。在两种情况下， Remote access Policy存储本地。参考Windows 2000 IAS文档关于连接尝试如何的更多信息处理。
11. 选择**批准远程接入**并且单击**编辑配置文件**为了配置拨入属性。
12. 选择协议使用在Authentication选项的验证。检查**Microsoft加密的身份验证版本2**并且不选定其他身份验证协议。**注意：** 在此拨入配置文件的设置必须匹配在VPN 3000集中器配置和拨入客户端的设置。在此示例MS-CHAPv2使用没有PPTP加密的验证。
13. 仅在Encryption选项检查**不加密**。
14. 点击OK键为了结束拨入配置文件，然后点击OK键为了关上Remote access Policy窗口。
15. 用鼠标右键单击**互联网认证服务**并且点击在控制台结构树的**启动服务**。**注意：** 您能也使用此

功能终止服务。

16. 完成这些步骤为了修改用户允许连接。选择**Console > Add/Remove Snap-in**。单击**添加**并且选择**卡扣式的本地用户和的组**。单击 **Add**。确保选择**本地计算机**点击**芬通社**和**OK**。
17. 展开 **Local User and Groups**，然后单击左窗格中的“Users”文件夹。在右窗格中，请双击用户(VPN用户)您希望对允许。
18. 去Dial-in选项并且选择**允许**在远程访问许可下(拨入或VPN)。
19. 单击**应用**并且**好**为了完成操作。如果需要您能关上控制台管理窗口和救会话。您修改的用户当前能访问有VPN客户端的VPN集中器。记住IAS服务器只验证用户信息。VPN集中器仍然执行组验证。

## 配置有IAS的Microsoft Windows 2003服务器

完成以下步骤以配置具有 IAS 的 Microsoft Windows 2003 Server。

**注意：** 这些步骤假设本地计算机上已安装 IAS。如果未安装，请通过**控制面板 > 添加/删除程序**进行添加。

1. 选择**管理工具> Internet 验证服务**并右键单击 RADIUS 客户端，以添加新的 RADIUS 客户端。键入客户端信息后，单击**确定**。
2. 输入友好名称。
3. 定义VPN集中器用一个IP地址或DNS名在下一个窗口。
4. 从客户端供应商滚动条选择**思科**。
5. 输入一共享机密。**注意：** 您必须记住您使用的*确切的*机密。您需要此信息为了配置VPN集中器。
6. 单击 **OK** 完成操作。
7. 去**Remote access Policy**，用鼠标右键单击在**对其他接入服务器的连接**，并且选择**属性**。
8. 选择**批准远程接入**并且单击**编辑配置文件**为了配置拨入属性。
9. 选择协议使用在Authentication选项的验证。检查**Microsoft加密的身份验证版本2**并且不选定其他身份验证协议。**注意：** 在此拨入配置文件的设置必须匹配在VPN 3000集中器配置和拨入客户端的设置。在此示例MS-CHAPv2使用没有PPTP加密的验证。
10. 仅在Encryption选项检查**不加密**。
11. 完成后，单击**确定**。
12. 用鼠标右键单击**互联网认证服务**并且点击在控制台结构树的**启动服务**。**注意：** 您能也使用此功能为了终止服务。
13. 选择**Administrative Tools > Computer Management > System Tools > Local Users及 Groups**，用鼠标右键单击在**用户**并且选择**新用户**为了添加用户到本地计算机帐户。
14. 添加用户时用Cisco密码“VPNPassword”和检查此配置文件信息。在“常规”选项卡上，确保选中**口令永不过期**选项而不是“用户必须更改口令”选项。在Dial-in选项，请选择**允许的**选项(或请通过Remote access Policy留下控制访问默认设置)。完成后，单击**确定**。

# 配置RADIUS验证的Cisco VPN 3000集中器

完成这些步骤为了配置RADIUS验证的Cisco VPN 3000集中器。

1. 连接到有您的Web浏览器的VPN集中器，并且从左帧菜单选择**Configuration > System > Servers > Authentication**。
2. 单击**添加**并且配置这些设置。服务器类型= RADIUS认证服务器= IP地址或主机名您的RADIUS服务器(IAS)服务器端口= 0 (0=default=1645)服务器秘密=同一样在部分的步骤8关于

Configure RADIUS服务器

3. 单击**添加**为了添加对运行的配置的更改。
4. 单击**添加**，选择服务器类型的**内部服务器**，并且单击**应用**。您需要此以后为了配置IPSec组(您需要仅服务器类型=内部服务器)。
5. 配置VPN集中器PPTP用户的或VPN客户端用户的。**PPTP**完成这些步骤为了为PPTP用户配置。选择**Configuration > User Management > Base Group**，并且点击**PPTP/L2TP**选项卡。选择**MSCHAPv2**并且不选定在PPTP身份验证协议部分的其他身份验证协议。单击**应用**在页底端为了添加对运行的配置的更改。现在，当PPTP用户连接时，他们由RADIUS服务器(IAS)验证。**VPN 客户**完成这些步骤为了为VPN客户端用户配置。选择**Configuration > User Management > Groups**并且单击**添加**为了添加一新的组。键入组名(例如， Ipsecuser)和密码。此密码使用作为预先共享密钥隧道协商。去IPSec选项和集合验证**RADIUS**。这允许通过RADIUS验证服务器将验证的IPSec客户端。单击**添加**在页底端为了添加对运行的配置的更改。现在，当IPSec客户端联络并且使用您配置的组时，他们由RADIUS服务器验证。

# 验证

当前没有可用于此配置的验证过程。

# 故障排除

## WebVPN验证发生故障

您可以使用这些部分提供的信息对您的配置进行故障排除。

- 问题：WebVPN用户不能验证RADIUS服务器，然而能成功验证与VPN集中器的本地数据库。他们收到错误例如“登录失败”和此消息。**原因**：当使用时，这类问题经常发生除集中器的内部数据库的之外所有数据库。当他们首先连接到集中器，并且必须使用默认验证方法时，WebVPN用户点击基本组。通常此方法设置为集中器的内部数据库并且不是已配置的RADIUS或其他服务器。**解决方案**：当WebVPN用户验证时，集中器检查服务器列表定义在**Configuration > System > Servers > Authentication**并且使用名列前茅一个。确保移动服务器您希望WebVPN用户用到顶部此列表验证。例如，如果RADIUS应该是认证方法，您需要搬到RADIUS服务器列表的顶部推送验证到它。**注意：** 正因为WebVPN用户最初点击基本组不意味着他们被限制给基本组。另外的WebVPN组在集中器可以配置，并且用户可以分配到他们由RADIUS服务器有属性25的人口与**OU=groupname的**。参考锁定用户到VPN 3000集中器Group使用更多详细说明的一个RADIUS服务器。

## 用户认证失效活动目录

在激活目录服务器中，在失败用户的用户属性的帐户选项卡，您能看到此复选框：

**[x]不要求预验证**

如果此复选框非选定，请**检查它**，并且设法再验证与此用户。

# 相关信息

- Cisco VPN 3000 系列集中器
- Cisco VPN 3002 硬件客户端
- IPsec 协商/IKE 协议
- RADIUS (远程拨入用户验证服务)支持页面
- 远程用户拨入认证系统(RADIUS)
- 技术支持和文档 - Cisco Systems