
(/about)

.NET, Web and Windows 10 Developer

Email (mailto:Edi.Wang@outlook.com) | GitHub (https://github.com/EdiWang) | Weibo (http://weibo.com/wyjexplorer)

图解：如何在Windows Azure上搭建SSTP VPN（你们懂的）

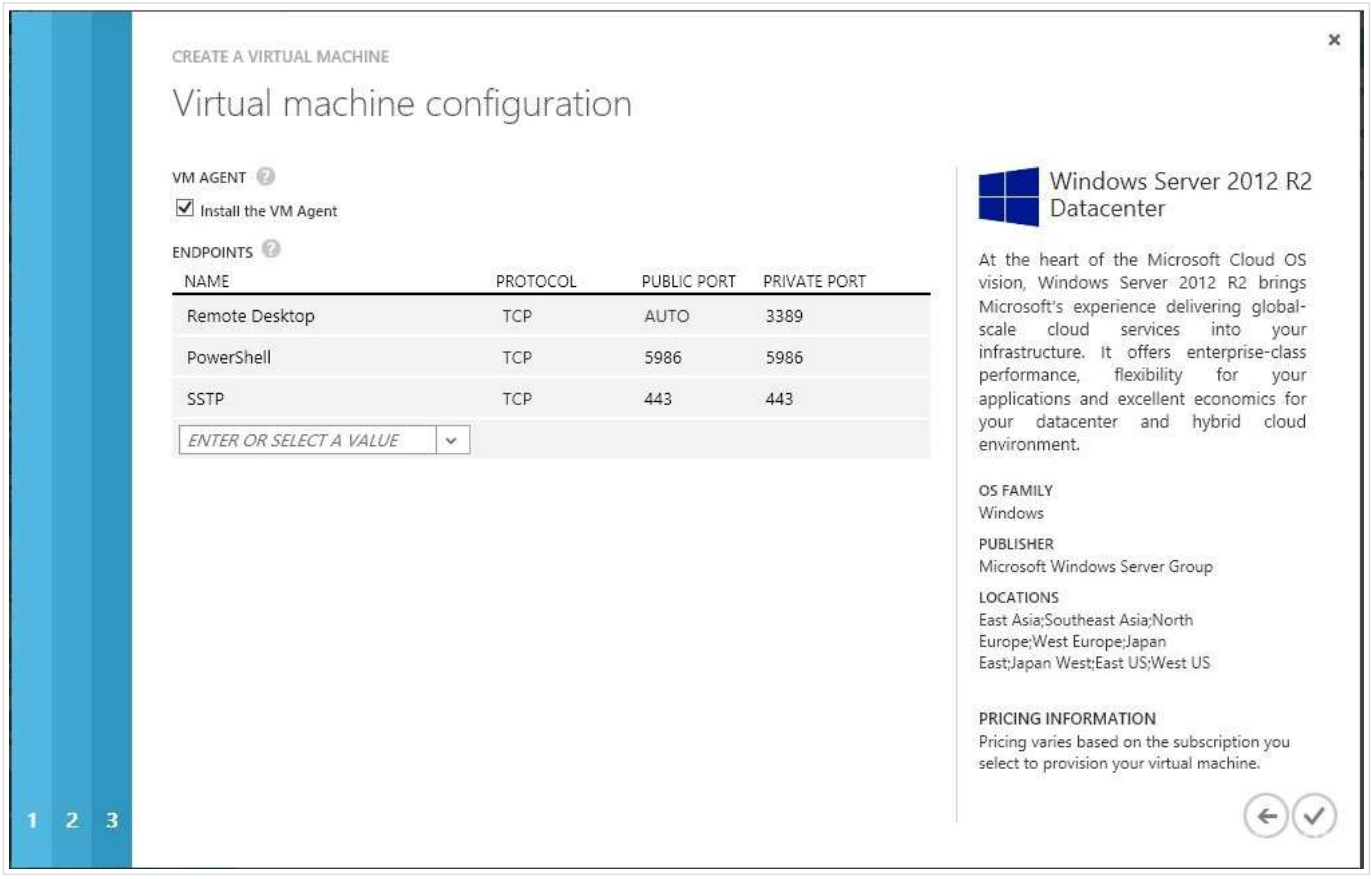
2014-3-9 15:22 (UTC +8:00)

在国内，VPN是用来干嘛的大家都懂的。很久之前我尝试用Azure的Virtual Network搞VPN结果惨败了。最近微博上有基友写了篇文章亲测可行，原文在 这里 (http://blogs.msdn.com/b/lighthouse/archive/2013/07/30/how-deploy-sstp-and-l2tp-vpn-in-windows-azure-windows-server-2012.aspx) 。可惜是英文的。所以我的这篇文章仅仅是用原作者的步骤进行翻译和补充。

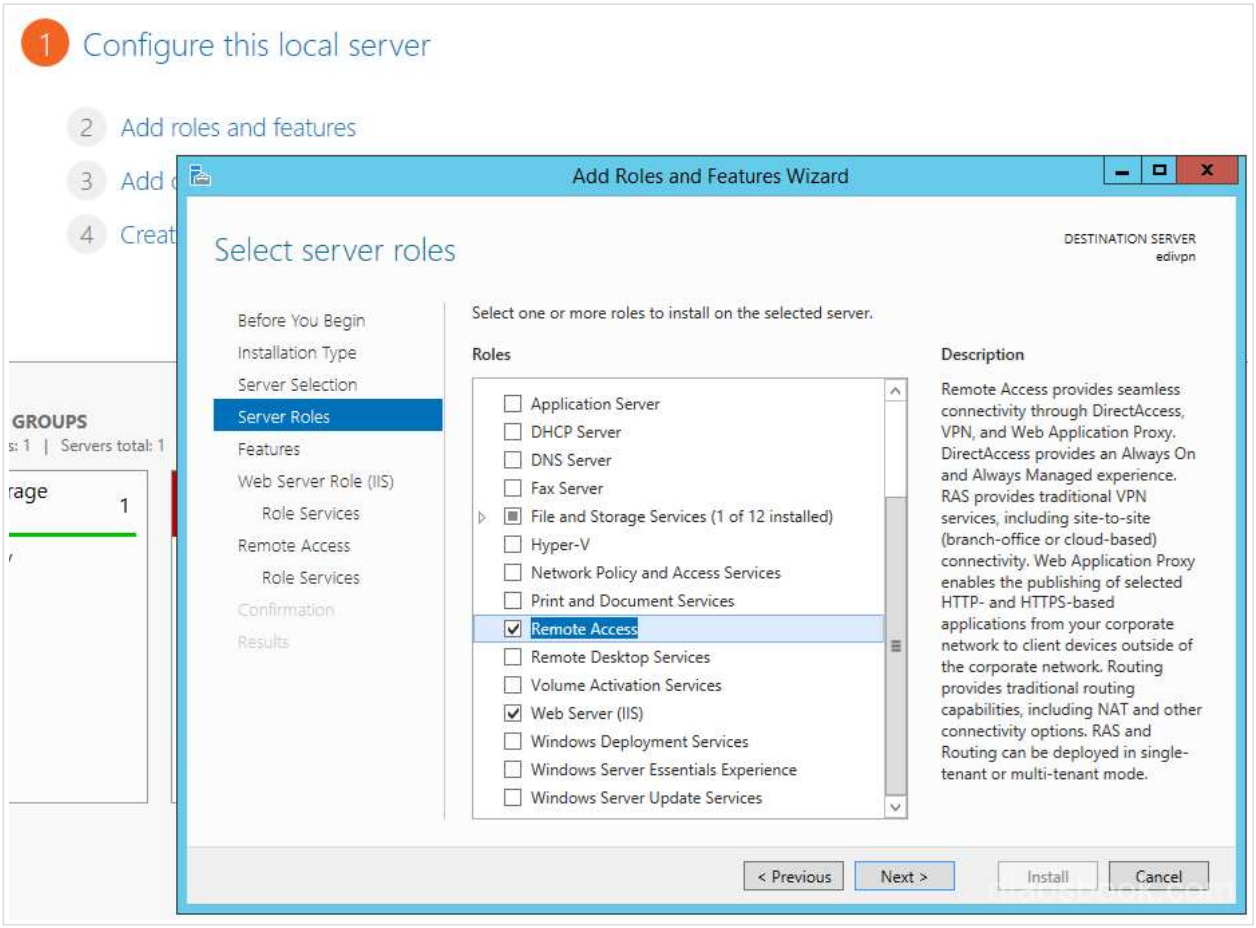
注意，本文的方法不适用于国内世纪互联运营的Windows Azure！

一、服务器设置

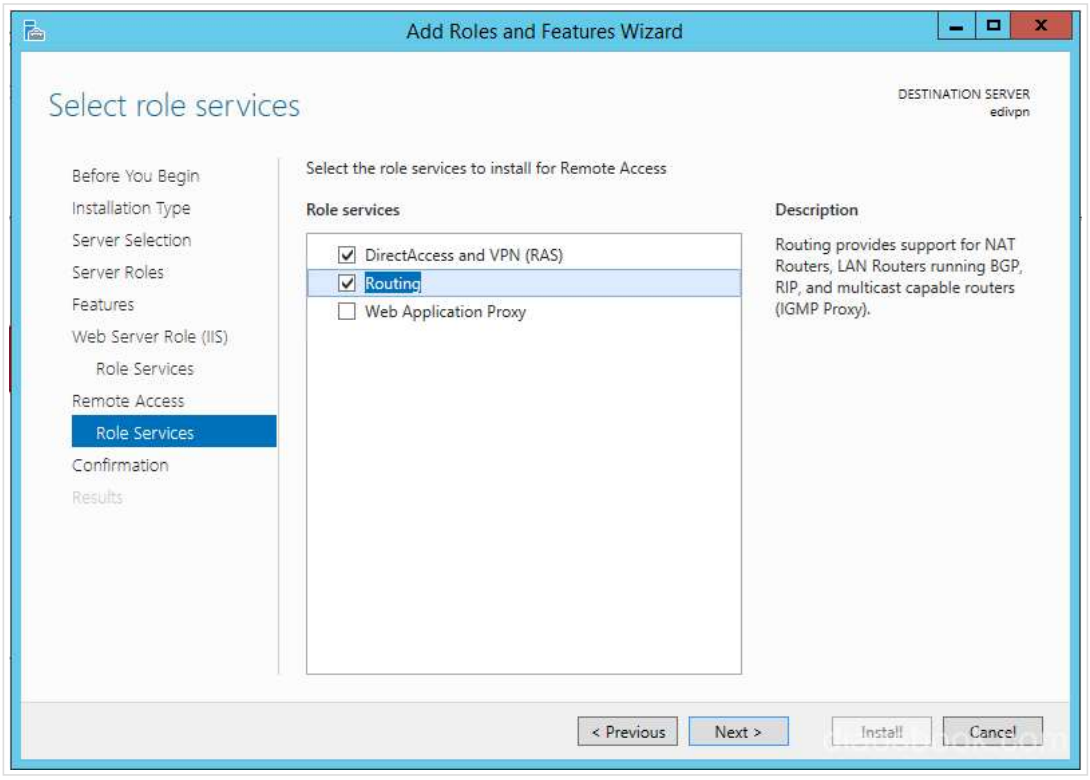
首先，从0开始，你需要创建一个新的VM。我选择Windows Server 2012 R2，所有步骤和创建普通VM都一样，但最后在防火墙设置里一定要打开TCP 443端口：



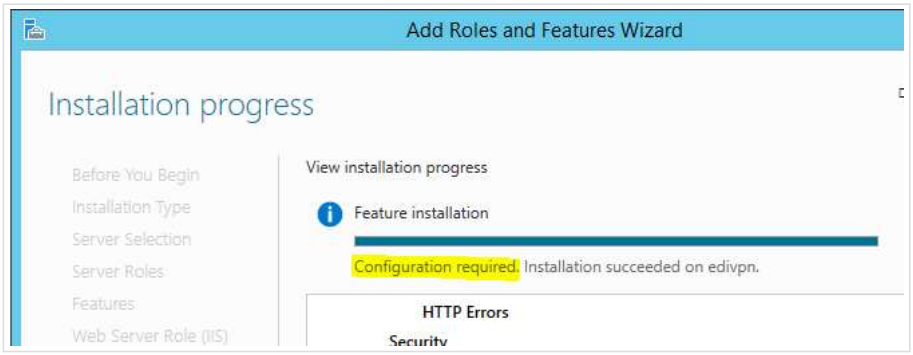
创建完成后，远程桌面进去，在自动弹出的“Server Management”里面点击“Add roles and features”，一路Next到“Server Roles”，然后勾选Remote Access。



再一路Next到"Role Services"，选择"DirectAccess and VPN(RAS)"、"Routing"。



然后一路Next并慢慢等待安装。安装完成后你会发现还需要配置才可以使用：



点击"Server Manager"右上角的旗帜图标，选择"Open the Getting Started Wizard"

在弹出的向导中选择最后一项：Deploy VPN Only

然后在本机名称（就是你的VM名称，我这里是EDIVPN）上点击右键，选择"Configure and Enable Routing and Remote Access"

在弹出的向导中选择"Custom configuration"

然后把"VPN access"和"NAT"选上，一路next到底。

最后向导会提示你需要启动服务，点击"Start service"

接下来我们需要配置一个VPN使用的安全证书。新建的VM虽然有个默认证书但不符合我们的要求，最后导出的时候无法选择private key，所以我们要用大微软的工具自己生成一个证书。

工具叫做Internet Information Services (IIS) 6.0 Resource Kit Tools，到这里下载： http://www.microsoft.com/en-us/download/details.aspx?id=17275 (http://www.microsoft.com/en-us/download/details.aspx?id=17275)

安装完成后在你的开始屏幕，App里能找到selfssl这个工具，以管理员身份运行

然后运行这条命令生成SSL证书：

记住，此处你的VM名字一定要用大小写区别于你在azure里创建的VM名字。比如我在azure里用的是edivpn，那么这里我就要用EdiVPN。总之一定要有区别！

```
selfssl.exe /N:cn=你的VM名字.cloudapp.net /V:3650
```

3650的意思是有效期为10年。选择Y确认，不要在意那个"Error opening metabase"的错误。

然后运行"mmc"，点击File， Add/Remove Snap-in

选择Certificates，点击Add，然后选择Computer account

选择Local computer，点击Finish，一路到底。

在Certificates, Personal, Certificates下面找到刚才用selfssl创建的证书，这里要注意区分大小写。这就是为什么刚才在selfssl的时候用大小写区别机器名。

在证书上点击右键，All Tasks，选择Export。

一路Next，在private key的一部里选择“Yes，export the private key”

然后建议大家设置个密码保护证书，以免被别人拿去用你的VPN。

最后给整数取个有意义的名字然后保存下来。**然后也拷贝一份到你本地机器上。**

现在回到Routing and Remote Access的窗口。右击你的机器名，打开Properties对话框。

在Security标签页下方，选择刚才用selfssl创建的证书（现在知道为什么要区别大小写了吧）

然后再IPv4标签页里，选择“Static address pool”，并根据自己需分配一个地址段给你的VPN客户端使用。

点击OK退出对话框。这时候会要你重启服务，点击Yes重启。

然后展开IPv4节点，在NAT下面右键，选择New Interface...

这里选择你VM的外部连接，也就是互联网连接。**这个连接每次VM重启都会变，所以每次重启VPN服务器后都要重新设置一下。不然你的VPN虽然能连上但不能上网！！！**

选择"Public interface connected to the Internet"，勾选"Enable NAT on this interface"

完成设置后，我们还需要创建VPN账户。运行lusrmgr.msc（撸瑟管理？）打开用户账户管理。

在Users下面建立你的VPN账号。**千万不要选择“User must change password at next logon”**

账户创建完成后无需加入管理员组。但需要在账户属性的Dial-in标签页里面选择“Allow access”

至此，服务器上的设置全部完成。

二、客户端设置

双击安装刚才拷贝到你本机的安全证书，在导入向导里选择“本地计算机”

证书储存里面选择“受信任的根证书颁发机构”

导入完成后，在网络与共享中心里新建一个VPN连接。

VPN服务器的地址一定要用azure自带的那个.cloudapp.net的域名，**不要绑定自己的域名不然肯定会爆。**

然后别急，先不要连接，不然还是要爆！

在适配器设置里找到你的vpn连接，在安全选项卡里选择SSTP，需要加密，允许使用这些协议，Microsoft CHAP

现在你就可以使用VPN了。输入你刚才在服务器上创建的账号密码连接到你的VPN虚拟机。

显示已连接就说明SSTP的连接成功了。

然后你们懂的：

最后总结一下要注意的地方：

1. Extra Small的VM是免费的，但不要直接建立这种VM，先建个small，再改成extra small（注意重启后重新配置NAT）

2. 如果你是用现有的VM搞VPN，注意在Azure的防火墙设置里打开TCP 443端口

3. Azure VM的位置随意，即使在East Asia也是可以**的。但你的Azure一定要是Global版的，国内世纪互联的那个是不可以**的。

VPN (/tags/list/VPN) SSTP (/tags/list/SSTP)