**Azure中快速搭建FTPS服务**

Kyle Fu 2017/03/05

标签：Azure FTPS FTP

## FTP，FTPS 与 SFTP 的区别

FTP （File Transfer Protocol）是一种常用的文件传输协议，在日常工作中被广泛应用。不过，FTP协议使用明文传输。如果文件传输发生在公网，会将所有密码凭据、操作指令，以及传输的文件内容，都以明文的方式暴露出来，特别是在公有云广泛应用的今天，这种传输方式对数据安全有极大的隐患。

针对这种情况，FTPS和SFTP应运而生。虽然这两种传输方式都基于FTP，而且名字非常相近。即便它们的目的都是为了使文件传输更安全，它们的实现原理也有很大的差别。

FTPS全称是File Transfer Protocol over SSL。SSL是一个用来在安全连接中对数据进行加密和解密的协议。FTPS使用SSL来加密、解密所有的数据连接，所以它的安全性比明文传输的FTP协议要高很多。

SFTP全称是Secure File Transfer Protocol，是SSH内嵌的协议。它借助Linux/Unix的SSH协议来加密文件传输过程。使用SFTP时，不需要启动FTP服务，只要在SSHD中开启了SFTP的相关配置，并启动SSHD服务即可运行。

下文中，我将介绍如何在Azure中快速搭建FTPS服务。

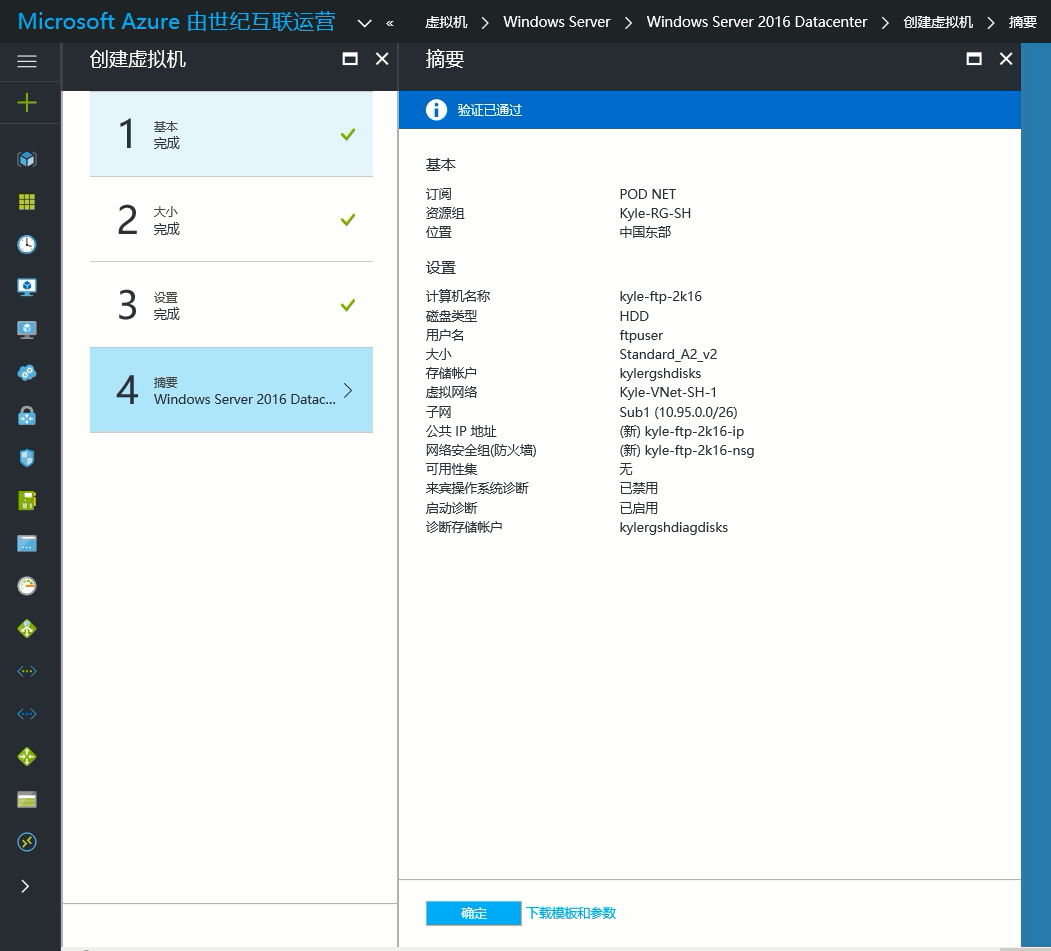
## 搭建步骤

### 在Azure中部署Windows Server 2016 Datacenter

本文的介绍中，我在Azure门户预览里使用Windows Server 2016 Datacenter来部署承载FTPS服务的虚拟机。如果您使用Windows Server 2008 或者 2012，也可以参考本文来搭建FTPS服务。配置过程基本一致。

虚拟机创建的过程中需要注意的是，创建公共IP地址时，需要使用**静态IP**。这样可以确保虚拟机重启后，IP不会改变。在后面的步骤里，这个IP还需要配置到FTPS服务的防火墙中。如果因重启而改变了， 会导致FTPS服务无法访问。

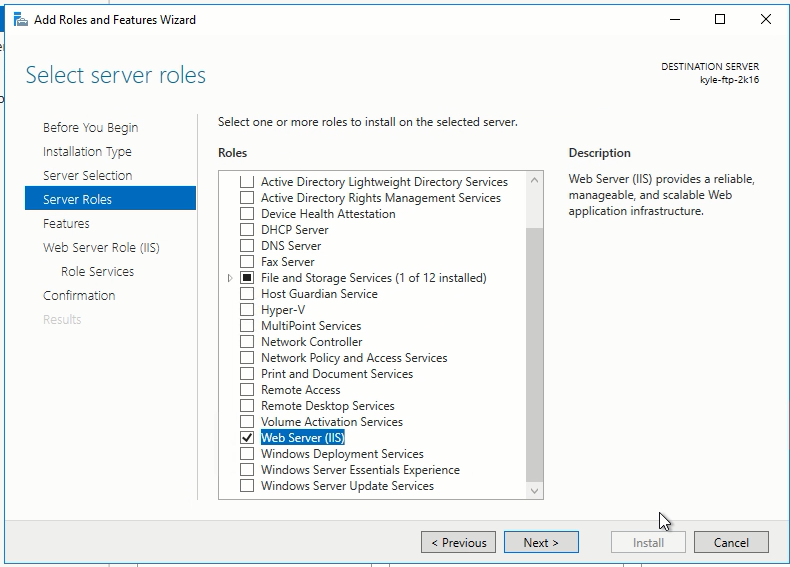


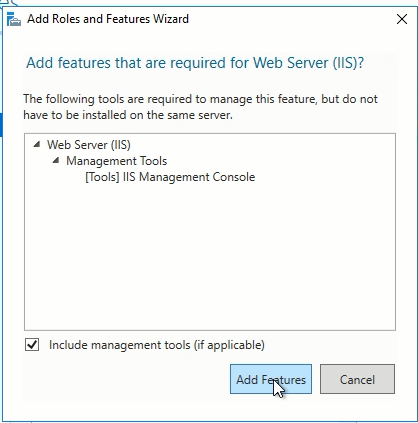


### 配置服务器角色和功能

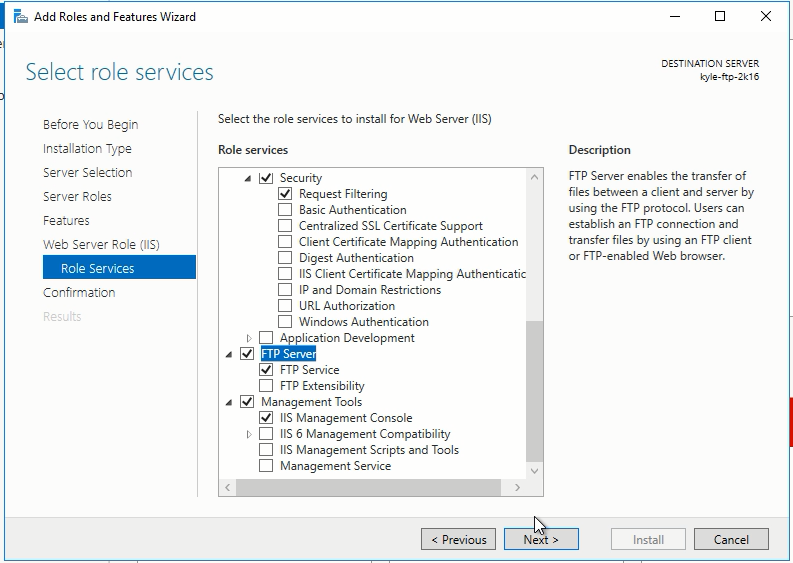
虚拟机部署好后，使用远程桌面连接登录到这台虚拟机。

在服务器角色配置中选择**Web Server ( IIS )**。

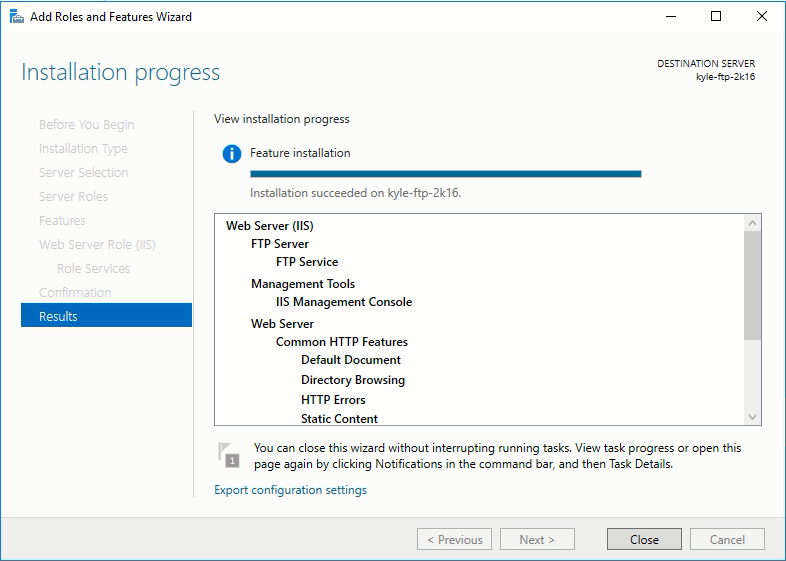




在IIS的角色服务配置中选择**FTP Server**，并确保选中了**FTP Service**。

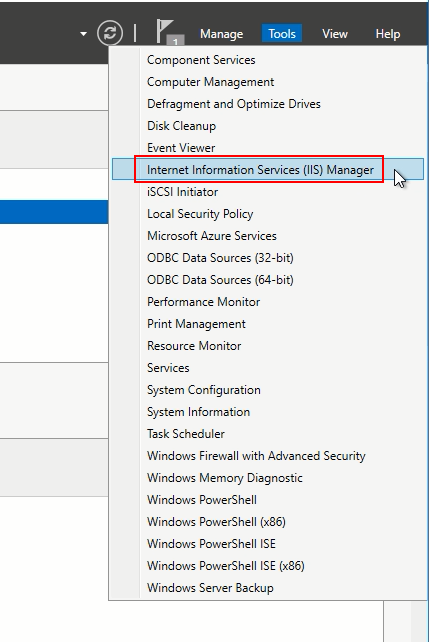


然后确认安装，并等待安装完成。

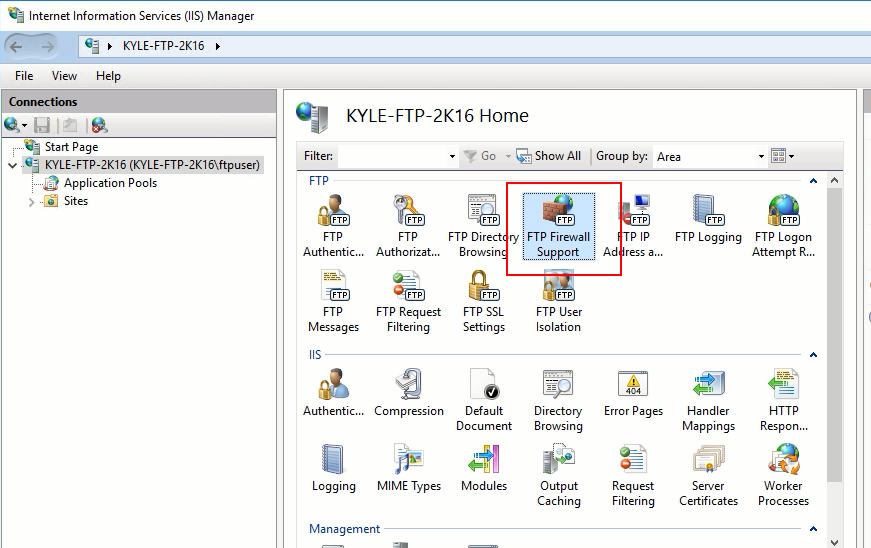


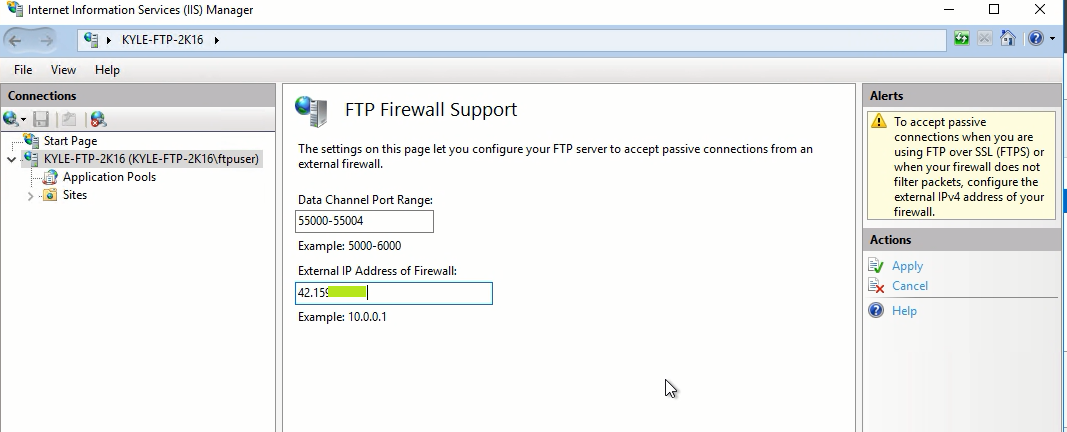
### 配置全局FTP防火墙规则

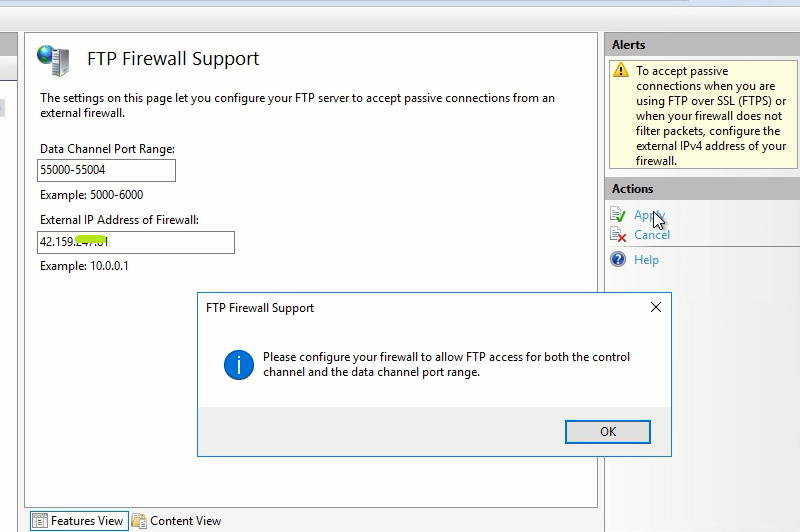
打开Internet Information Services (IIS) Manager。



双击**FTP Firewall Support**，打开全局FTP防火墙配置。在数据通道端口范围中，填入**55000-55004**。这些端口将在FTP被动连接中用来传输数据。另外，将虚拟机的**公共IP地址**填入外部IP地址框内。完成后，点击右侧的**Apply**。弹出的对话中不用理会，直接点击**OK**即可。

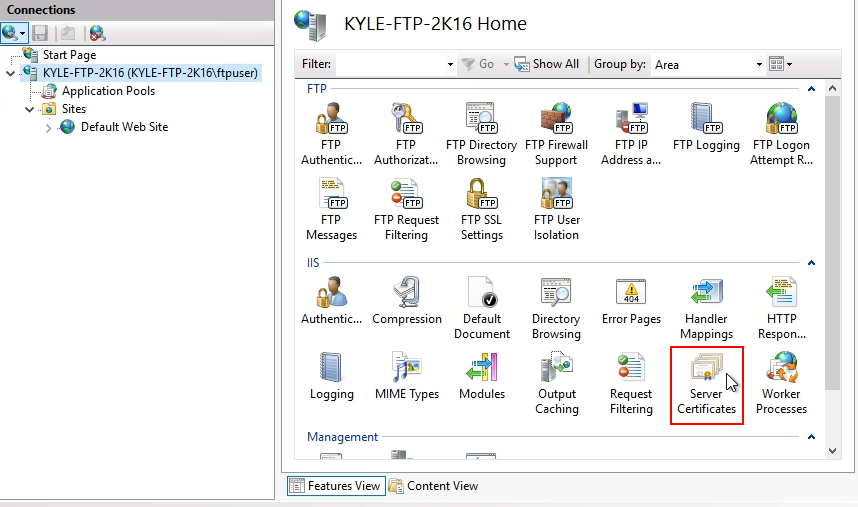


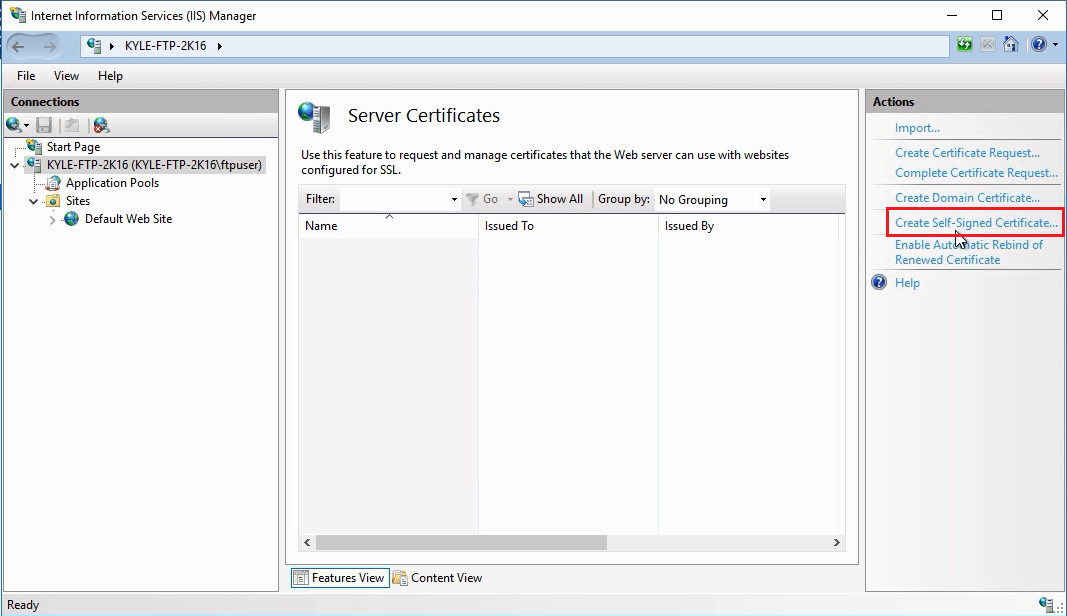




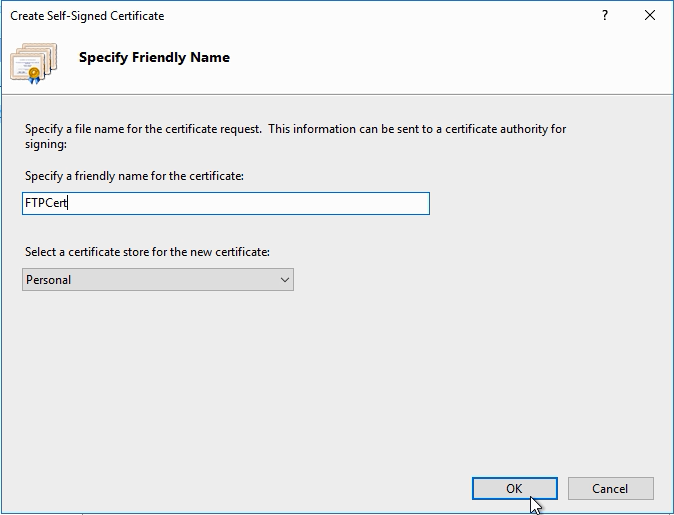
### 创建自签名证书

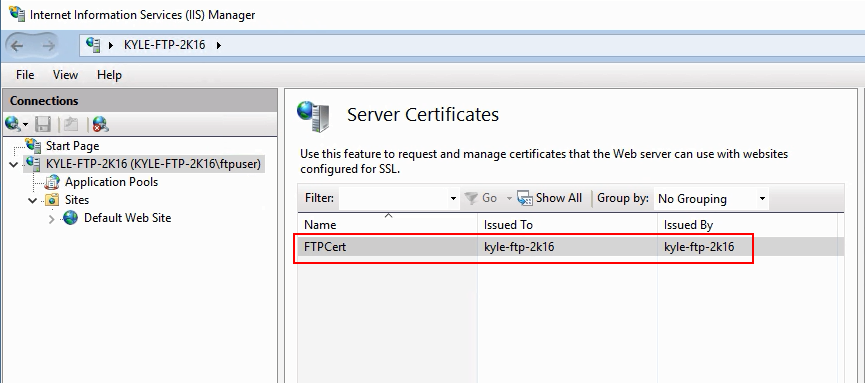
还是在Internet Information Services (IIS) Manager窗口中，双击**Server Certificate**。然后在打开的窗口右侧点击**Create Self-Signed Certificate…**。





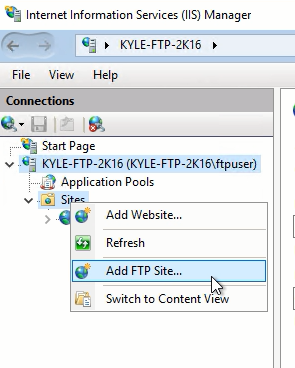
在弹出的创建证书窗口中，输入证书的名字，然后点击OK。创建好后能在窗口中看到刚创建的自签名证书。





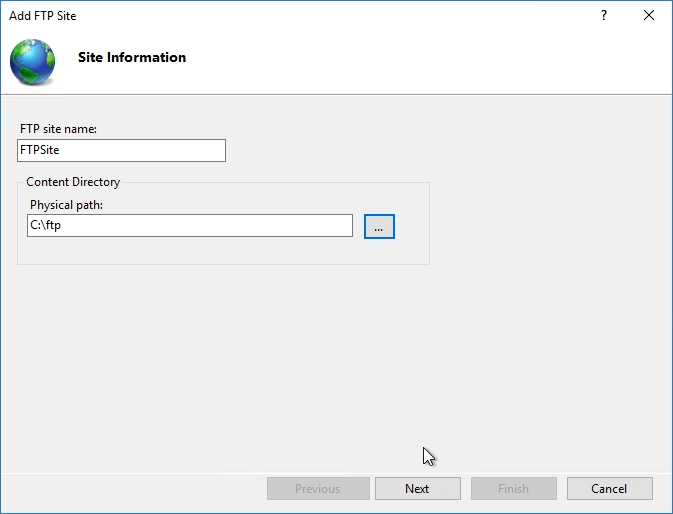
### 创建FTP站点

继续在Internet Information Services (IIS) Manager窗口中，选中**Site**。然后在右键菜单中，点击**Add FTP Site…**。

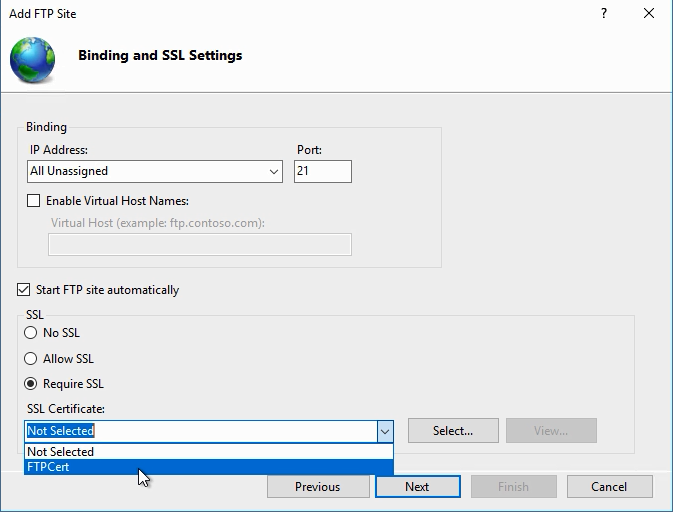


在Add FTP Site向导中，为FTP站点起个名字，并选择物理路径。

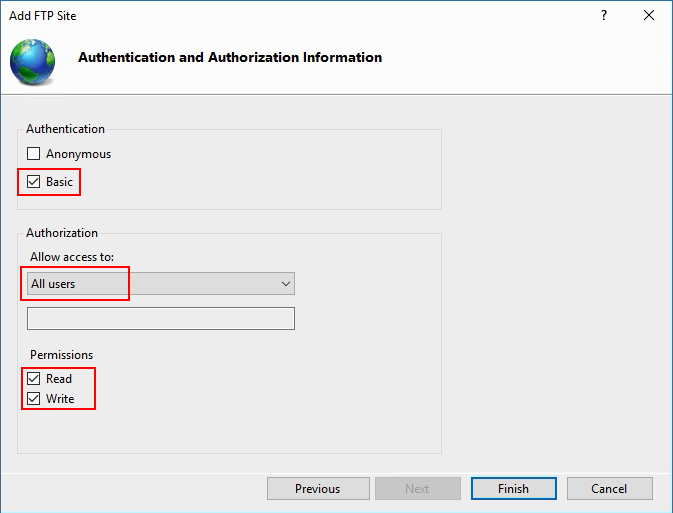
这里有两点需要注意。一是**不要将FTP目录放置在D盘**。因为D盘是临时盘，机器重启后，里面的文件会被全部移除。二是**所选的路径需要对FTP账号开放读写权限**。这里我使用登录虚拟机的管理员账号来访问FTP。如果您使用新建的账号来登录FTP，务必确认该账号对您配置的FTP目录有读写权限。



Binding and SSL Settings步骤里，在SSL Certificate的下拉菜单中，选中刚才创建的自签名证书。其他配置保持不变。

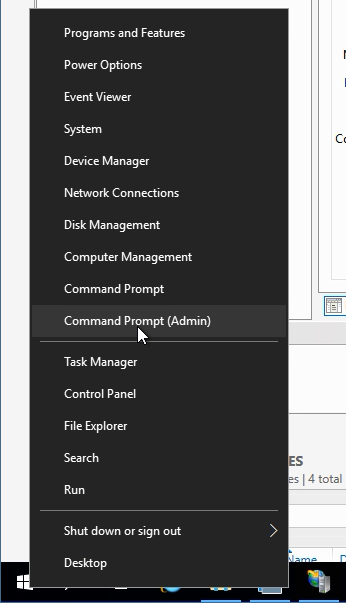


Authentication and Authorization Information步骤中，Authentication选择**Basic**，这样可以使用用户名和密码来登录。Authorization中，Allow access to选择**All users**, Permissions选择**Read**和**Write**。完成后点击**Finish**。



### 重启FTP服务

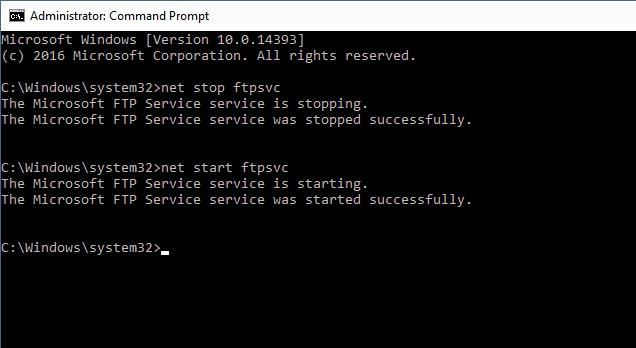
在左下角的Windows徽标点击右键，开启管理员模式的命令提示符窗口。



然后在命令提示符中，输入以下命令来重启FTP服务。重启的目的在于使之前的配置生效，特别是防火墙配置。

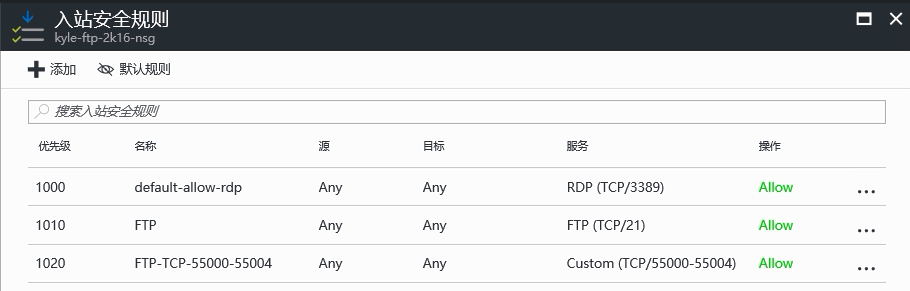
***net stop ftpsvc***

***net start ftpsvc***



### 配置网络安全组（NSG）

回到Azure门户预览页面，找到虚拟机对应的网络安全组，然后为FTP服务所需的端口添加对应的入站安全规则。这里需要添加的有两个规则。一是FTP控制命令所需的TCP 21端口，二是之前在虚拟机中，为FTP服务添加的数据通道端口，TCP 55000至55004。添加完成后，如下图所示。



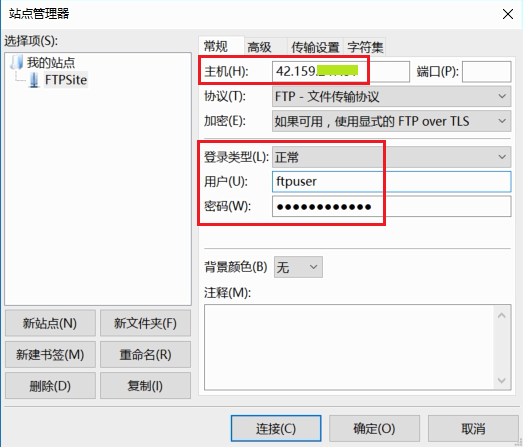
## FTP客户端配置

以上步骤完成后，FTPS服务器就搭建好了。下一步就可以使用客户端来实现对FTPS服务的访问了。

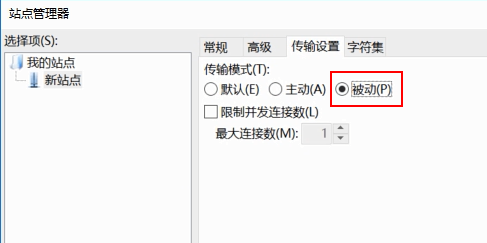
这里有一点需要注意，使用IIS管理器创建的自签名证书，与FileZilla Client 3.24不兼容。所以如果您要使用FileZilla Client，可以使用低一点的版本，或者别的FTP客户端，例如Flash FXP。下文中我以FileZilla Client 3.21版为例。

在客户端运行FileZilla，新建一个FTP站点。其中主机填入之前创建的虚拟机的公共IP。端口可以不填，因为在下面的协议中，默认选择了FTP，所以这里端口会默认使用TCP 21。

登录类型选择**正常**，并输入**用户名**和**密码**。这里用户名和密码就是我之前用来登录FTPS服务器的用户名和密码。当然，您也可以填入您在服务器中单独为FTP服务创建的账号和密码。

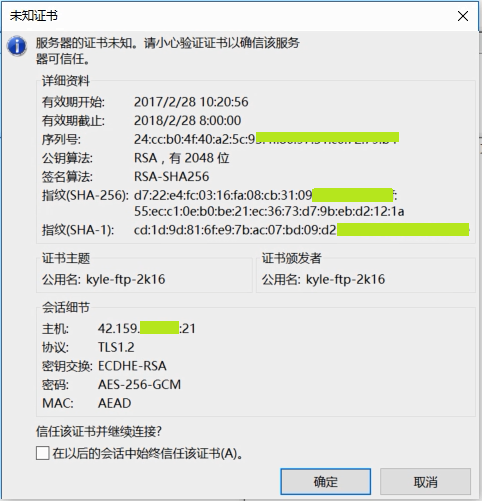


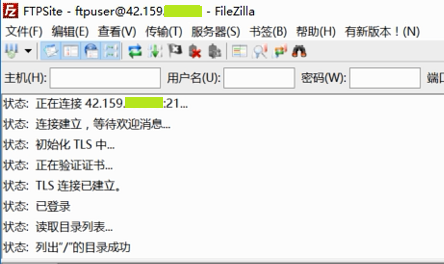
在**传输设置**标签下，选择**被动**传输模式。



设置完成后，点击连接。

FileZilla Client第一次连接到FTPS服务器时，因为我们的证书为自签名证书，客户端无法确认其有效性，所以会弹出未知证书的警告。直接点击**确定**即可。





这样，客户端就连接到FTPS服务了。

## 小结

本文的配置步骤非常简单，不到30分钟就能完成包括虚拟机创建在内的所有步骤。整个FTPS服务的搭建有以下几个关键点，我为大家总结一下：

* 虚拟机配置静态公共IP；
* FTP服务防火墙中配置被动模式的数据端口；
* 网络安全组（NSG）创建对应的入站规则；
* FTP客户端使用被动模式传输数据。

本文中使用的是IIS自带的FTP服务搭建的FTPS站点。如果您要在Azure的虚拟机中使用其他FTP Server软件来部署，也需要确保完成以上几个关键步骤。