Uploading AP-DATA Email Gateway to Azure

Introduction

Email Gateway for Microsoft Office 365 is a virtual appliance that, when deployed in a Microsoft Azure environment, allows outbound email from Exchange Online to be analyzed for data loss or theft. Email containing sensitive data can be permitted, quarantined, or encrypted. Sensitive attachments can also be dropped.

The first step to deploying the gateway in Azure is to configure a Virtual Network (VNet) and Virtual Private Network (VPN).

The next step is to create an Azure VM for the Email Gateway.

Ordinarily you would create the VM from an image in the Azure Marketplace. However, you can also download the Email Gateway image from My Account on the Forcepoint website and upload it to Azure manually.

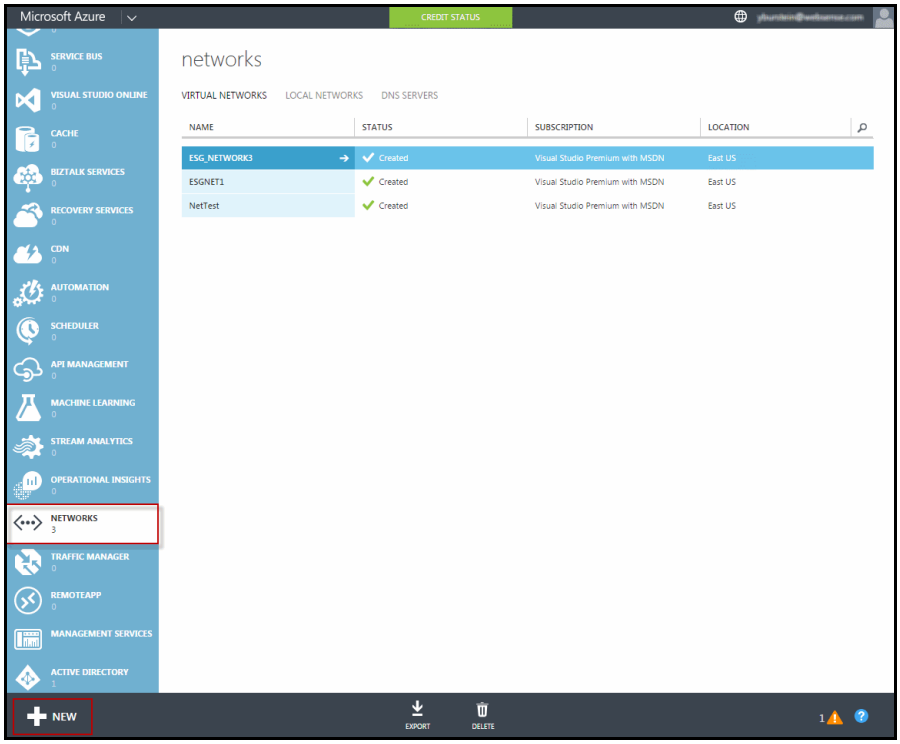
For details on using the Azure Marketplace, refer to the TRITON AP-DATA Installation Guide.

This document describes the manual process.

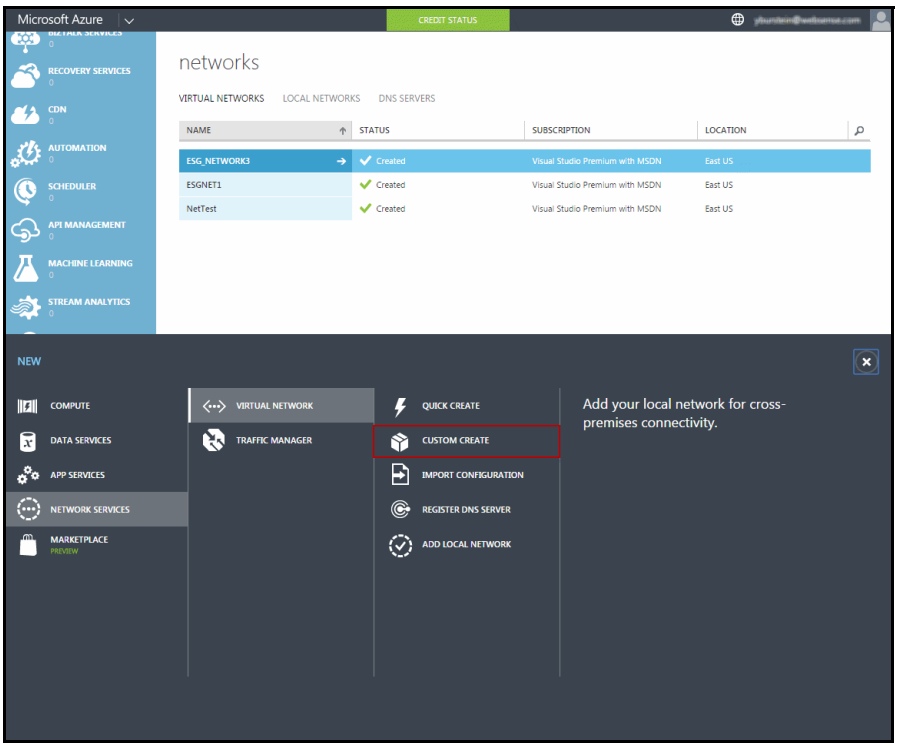
Configure a Virtual Network and VPN in Azure

1. Log onto the Azure Portal, https://manage.windowsazure.com.

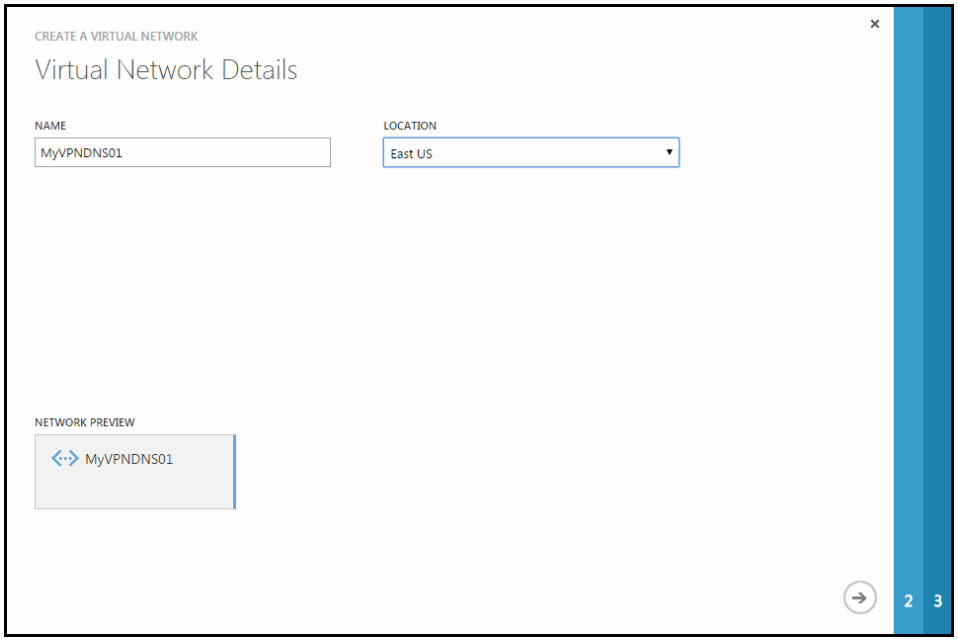
2. Click **Networks** and then **New** to create a new virtual network.



3. Click **Custom Create**.

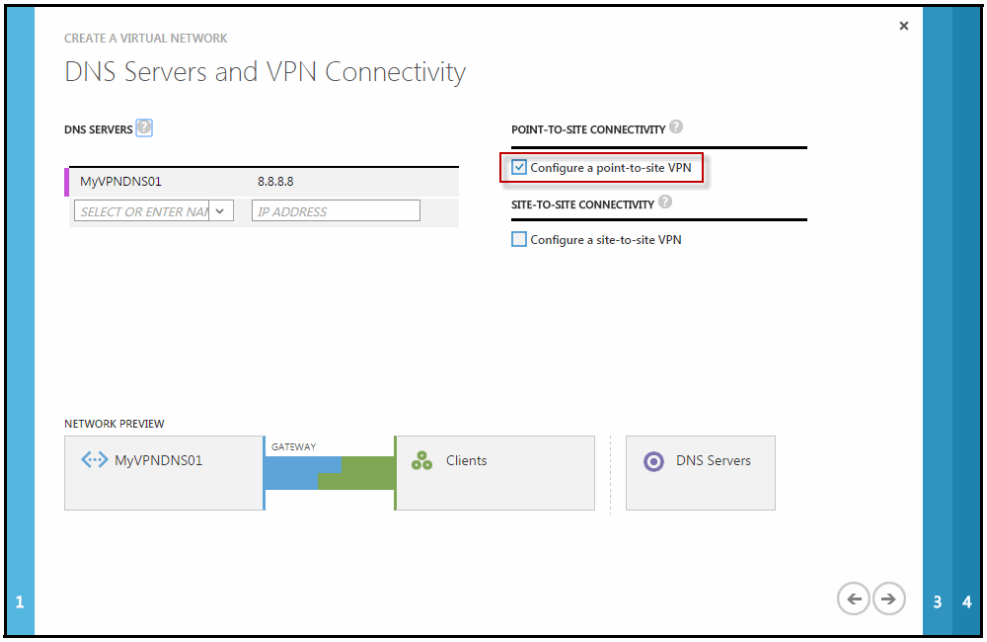


4. Enter a name for the virtual network you are creating, choose a location, then click >. Location refers to the physical location (region) where you want your resources (VMs) to reside. Choose the location closest to you. It will be used for all the other components such as the storage space and the VM.

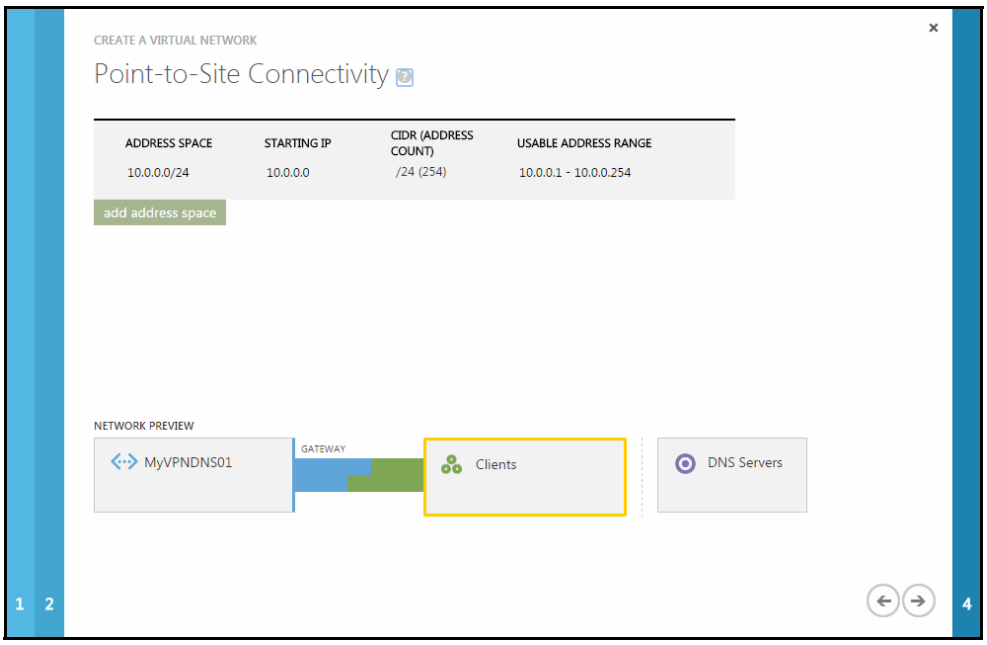


5. Enter the name and IP address of your DNS server if you want to connect one to the VPN, then select **Configure a point-to-site VPN** and click >. Leave DNS servers blank if you do not plan to use one.

   For instructions on creating site-to-site VPNs, see this Microsoft article.



6. Configure the VPN client's IP range. Include a starting IP and address count. It cannot be the IP range that you are using for your on-premises components or you will have a routing issue on your management server and SQL servers. For example, if your on-premises servers are using 10.x.x.x, use 192.168.x.x or 172.16.x.x as the starting IP for this virtual network. You do not need to create more than one address space. Click > when done.



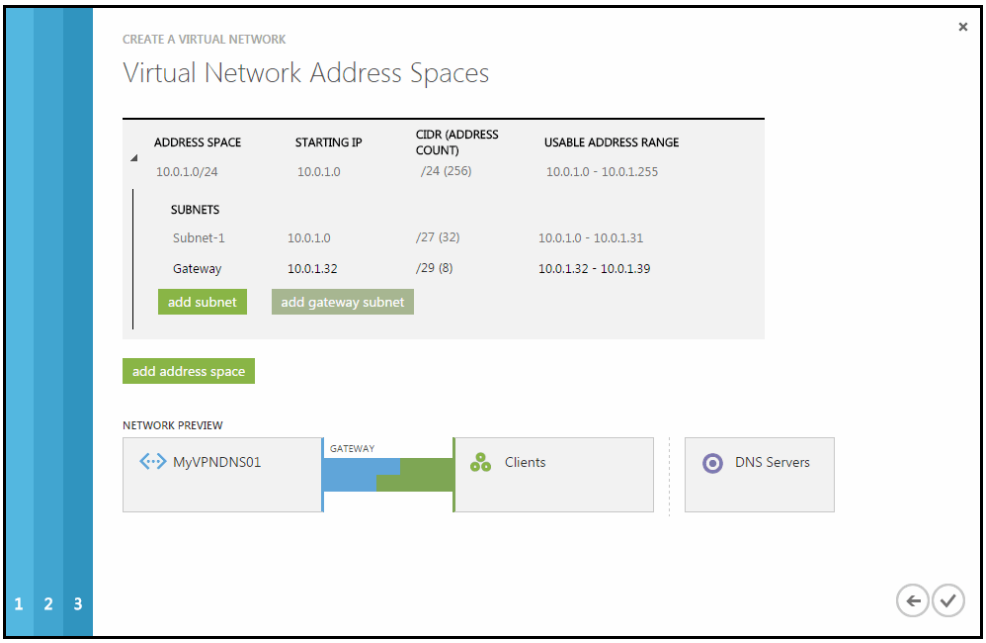
7. Specify the address range that you want to use for your virtual network. The VM that you create in Azure will be allocated an IP from this VPN's range.

   Click **Add Gateway Subnet** to create a subnet for the gateway (required).

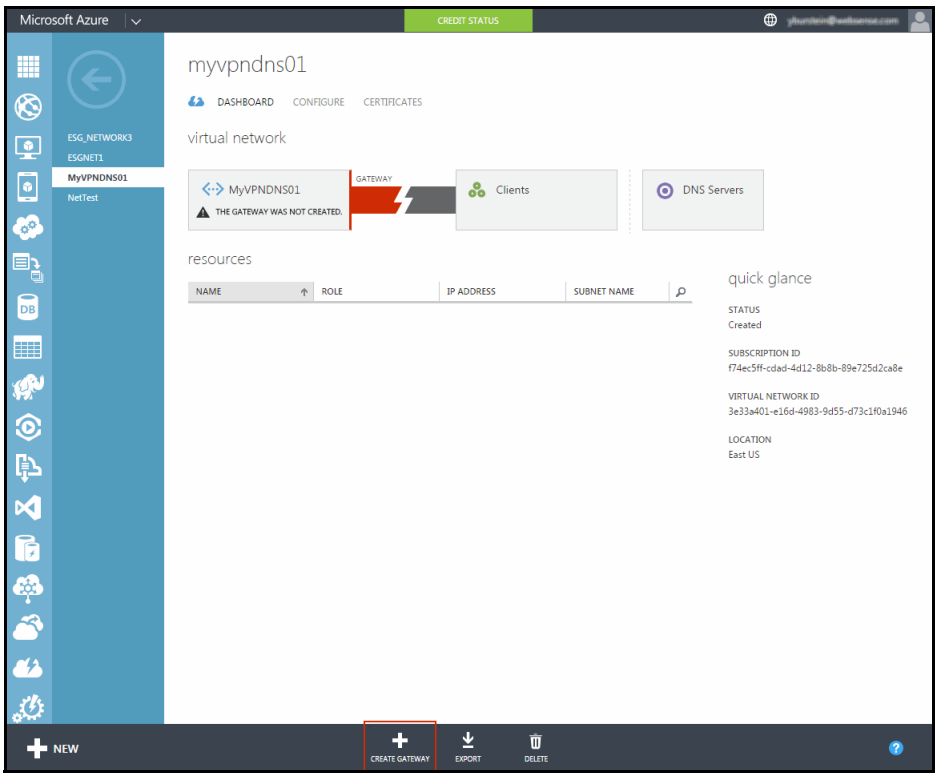
   Click the check mark when done.

   For best practice use a 29-bit subnet mask. This ensures that your IP address pool has 6 addresses and helps ensure a speedy recovery in case of disconnection.

> **Note**
> None of the virtual IP addresses should be on same subnet as the local management server IP. Keeping them on separate subnets prevents problems with the automatic VPN connection script that you will be using later in this procedure.

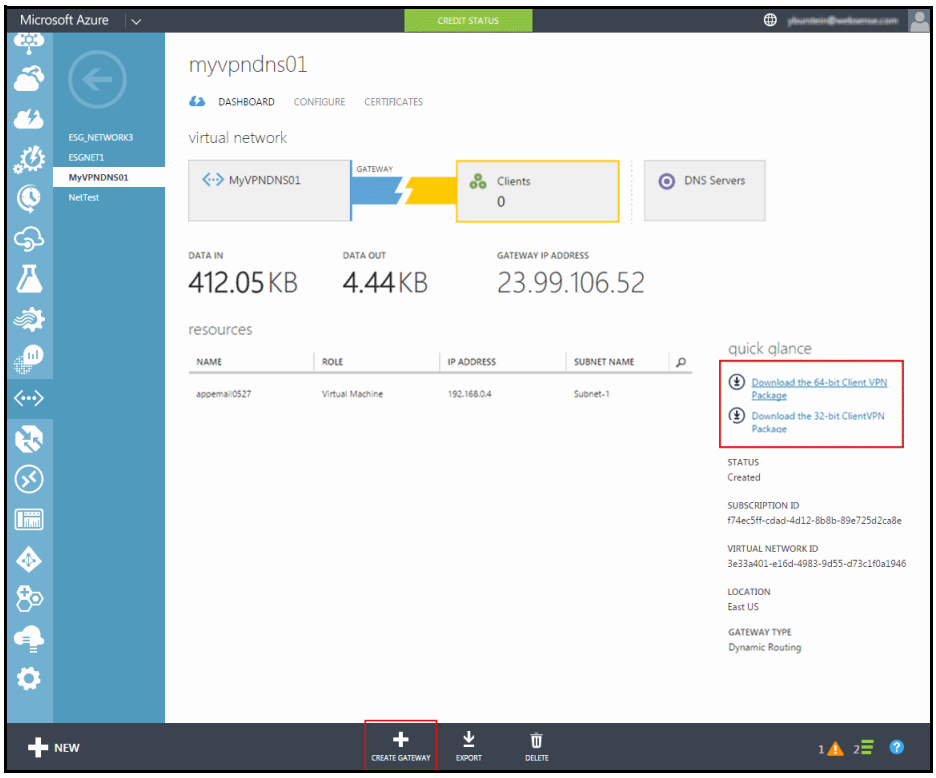


8. Select the network you just created from the resulting list then click **Create Gateway** to create the gateway. This can take 15-30 minutes.



9. Create security certificates to authenticate VPN clients. For instructions, see this Microsoft article. You need to:
   a. Generate a self-signed root certificate
   b. Upload the root certificate file to the Azure Portal
   c. Generate a client certificate
   d. Export and install the client certificate

10. Download the 32- or 64-bit client VPN package to a local machine and install it.



11. Open the VPN client software and click **Connect** to connect the client to the virtual network.
12. Run **ipconfig** on the VPN client's command line to find the IP address assigned to it.
13. If your TRITON management server will use a remote SQL database, be sure to place the database on this same VPN network. Install the VPN client software on the remote SQL Server machine as well and connect it to the VPN. Note its client IP address as well.

Upload the TRITON AP-DATA Email Gateway image file to Azure

1. Visit My Account, select **TRITON AP-DATA Gateway > Version 8.3 > AP - DATA Email Gateway for Microsoft Office 365**.
2. Download and unzip the gateway image file, **DataEmailGateway830.7z**. (It can take more than an hour to download.)
3. While it is downloading, open the Azure PowerShell console. If you do not already have it, follow instructions here to install and configure it.
4. Do one of the following to connect to the Azure cloud:

   Option 1: Add an Azure account

   a. Open the Azure PowerShell console.

   b. Type:

```
Add-AzureAccount
```

c. In the sign-in window, type the username and password of your work or school account.

d. Azure authenticates and saves the credential information, and then closes the window.

Option 2: Use a certificate

e. Open the Azure PowerShell console.

f. Type:

```
Get-AzurePublishSettingsFile.
```

g. A browser window opens and prompts you to download a **.publishsettings** file. It contains information and a certificate for your Microsoft Azure subscription.

h. Save the .publishsettings file.

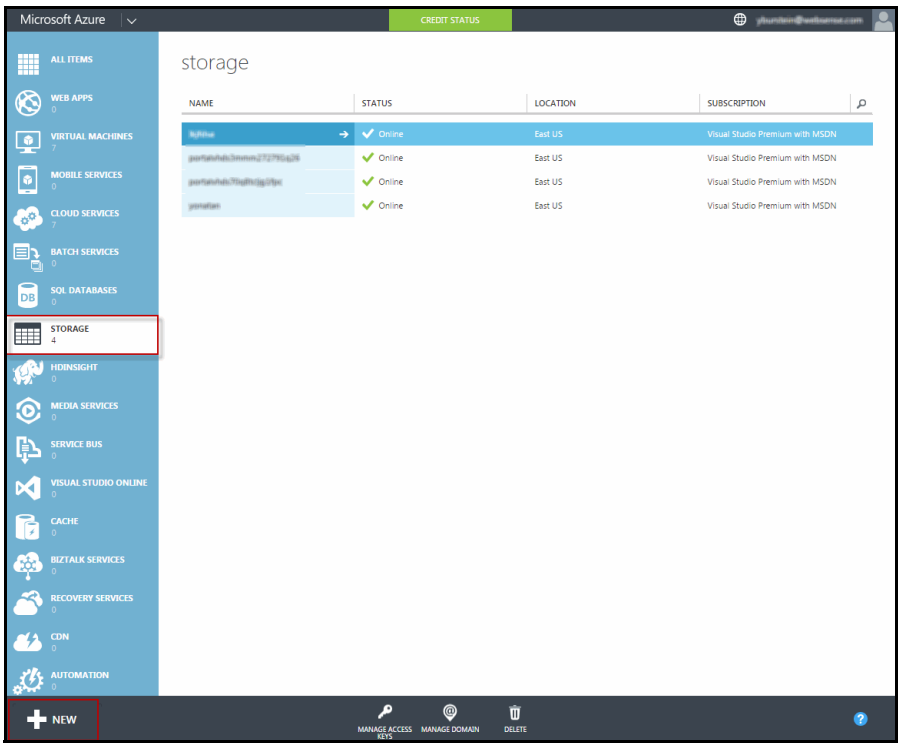
i. Type:

```
Import-AzurePublishSettingsFile <PathToFile>
```

Where <PathToFile> is the full path to the **.publishsettings** file.

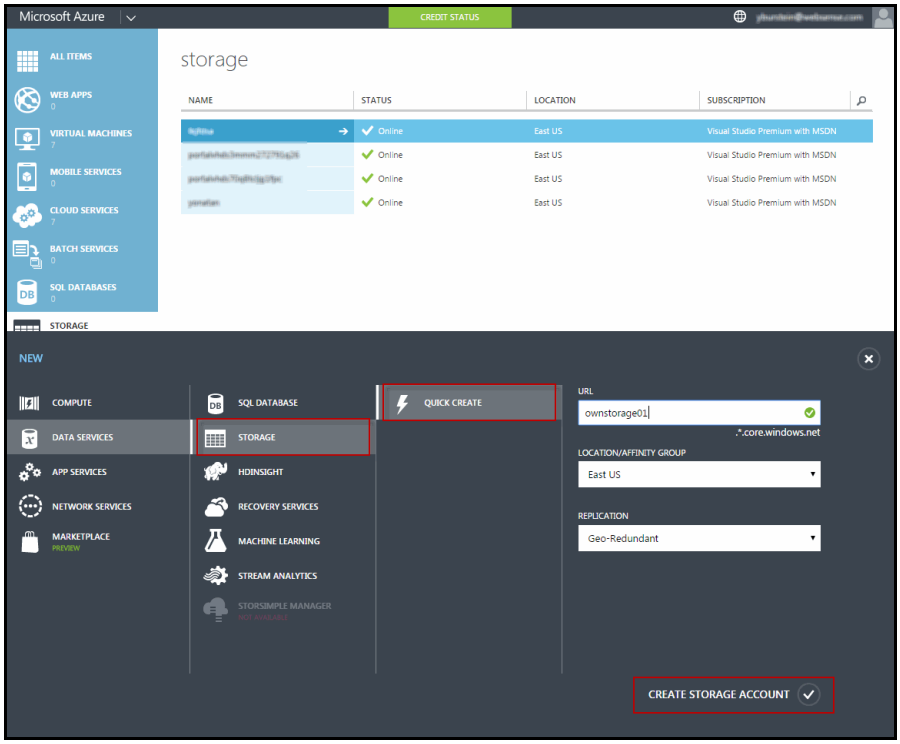
5. If you don't already have one, create a storage account on Azure (such as "https://ownstorage01.blob.core.chinacloudapi.cn/uploadimage01")

a. In the Azure Portal, click **Storage** in the left navigation pane, and then click **New**.

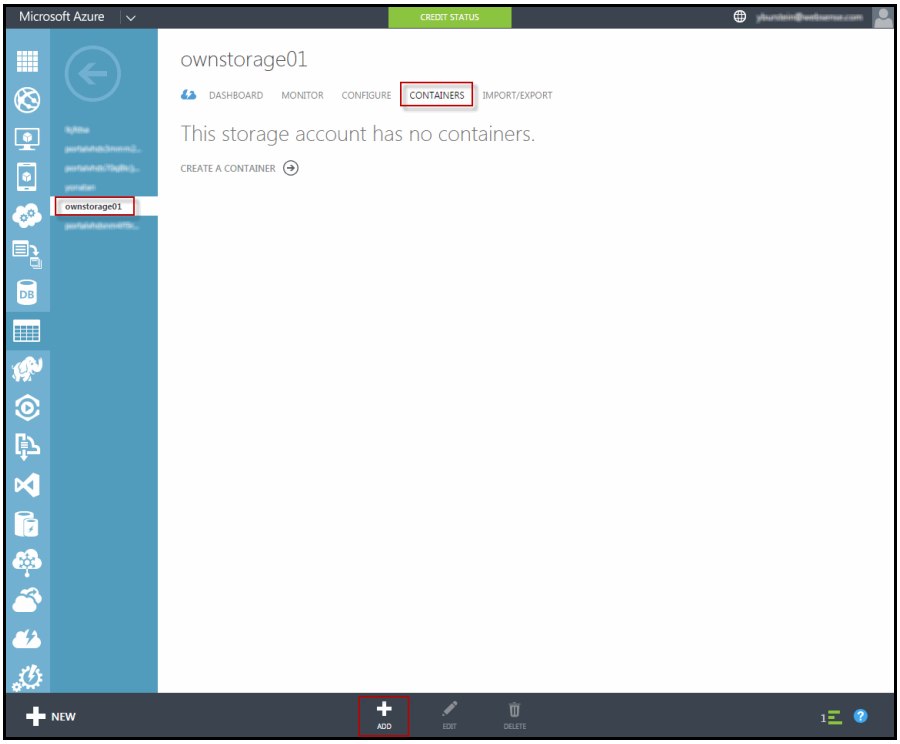


b. Click **Data Services > Storage > Quick Create** and then enter a URL for the storage account. Azure is a cloud service, so all services you create for it are available online. Enter **storage** if you want the URL to be https:/ storage.*.core.windows.net. Choose the location that you used when you created your virtual network.

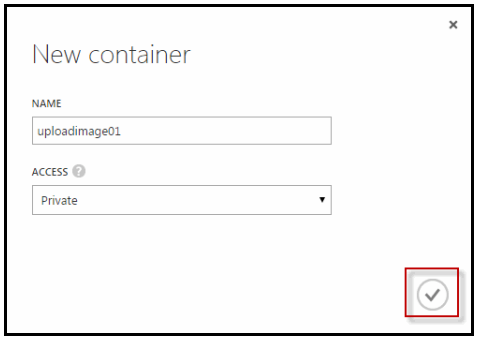
   Click **Create Storage Account** when done.



c. Click the storage URL, then click **Containers** and **Add**.



d. Enter a name for the new storage container and indicate the type of access you want for it. Choose private if you want only authenticated and registered users to have access to it.



6. In the PowerShell console, run a command like the following to upload the Email Gateway virtual hard disk (VHD) that you acquired from Forcepoint to the storage location. This can take 1-2 hours.

```
Add-AzureVhd -Destination "https://
ownstorage01.blob.core.chinacloudapi.cn/uploadimage01/
Forcepoint-Email-Gateway.vhd" -LocalFilePath
"C:\VHD\Disk\DataEmailGateway820.vhd"
```

This command format is like:

```
Add-AzureVhd -Destination "<StorageURL>/<YourImagesFolder>/
<AzureVHDName>" -LocalFilePath "<PathToForcepointVHDFile>"
```

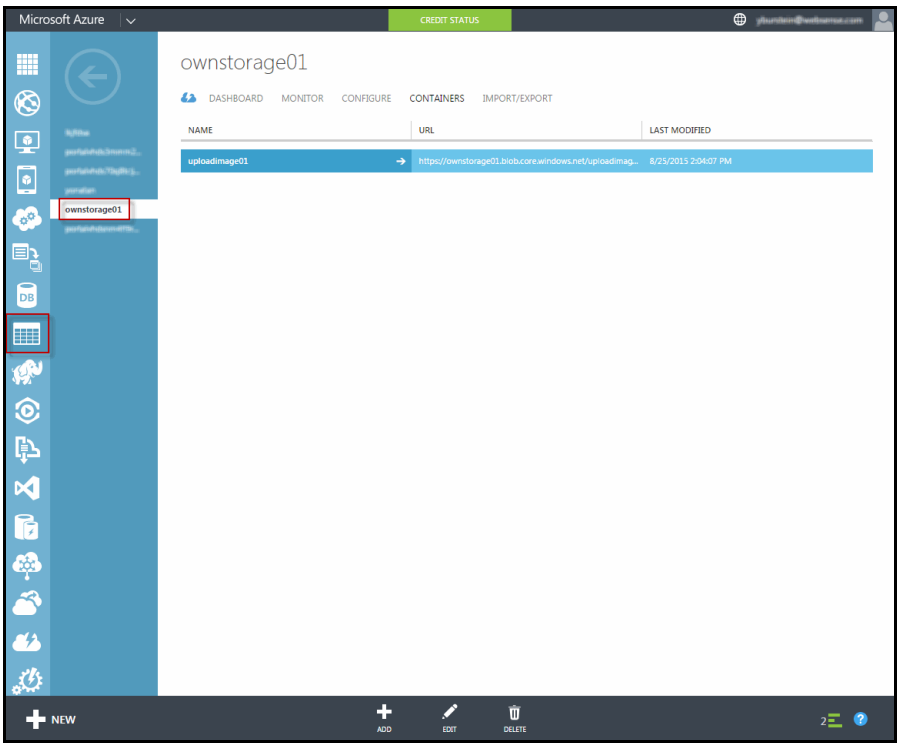
The parameters:

- C:\VHD\Disk\DataEmailGateway820.vhd - path to the virtual hard disk that you downloaded from Forcepoint.com.
- https://ownstorage01.blob.core.chinacloudapi.cn/uploadimage01/ - URL of the storage account that you created on Azure.
- Forcepoint-Email-Gateway.vhd - a name for the virtual hard disk on Azure.

It can take a few hours to upload the file.

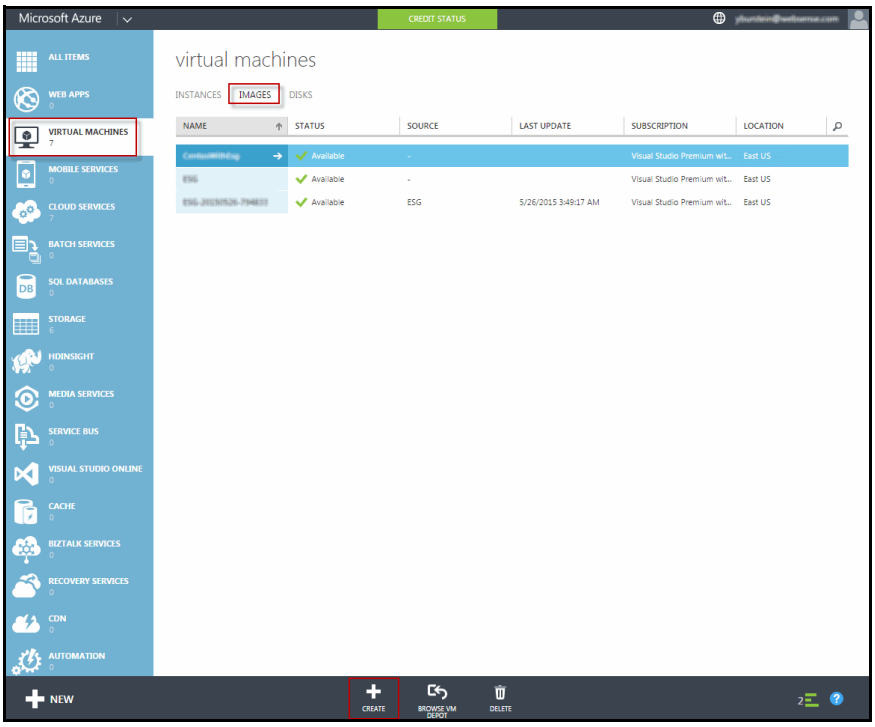
Create a Email Gateway VM in Azure

1. In the Azure Portal, click **Storage > uploadimage01** to see details about the new storage container.

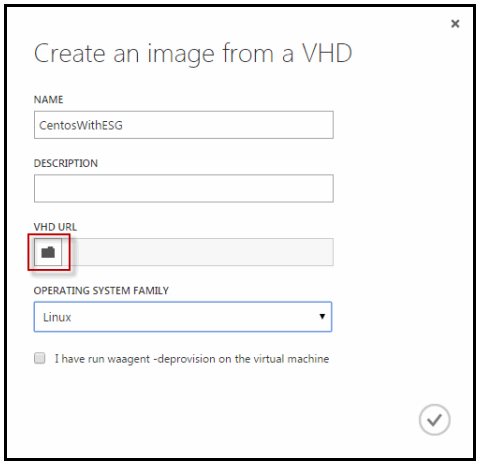


2. Create a virtual machine image from the virtual hard disk you just uploaded:

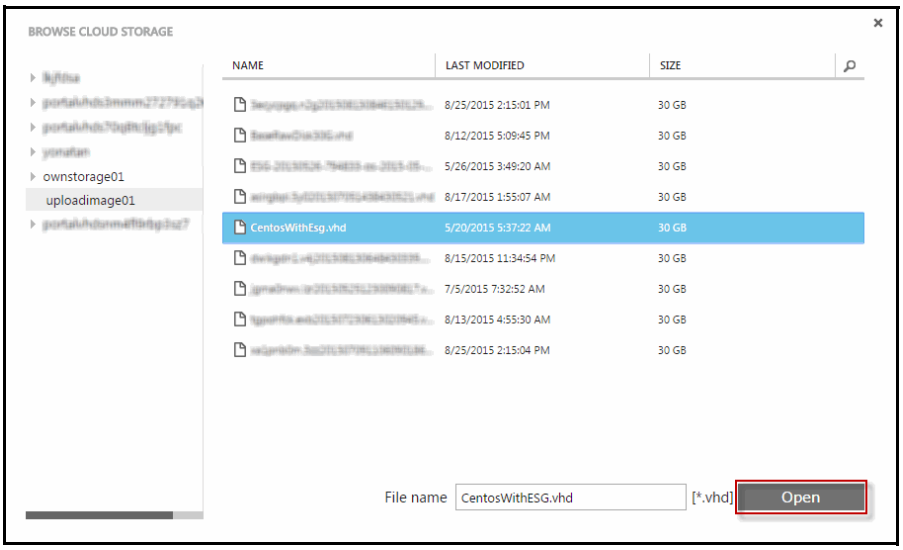
a. Click **Virtual Machines > Images** and then click **Create**.



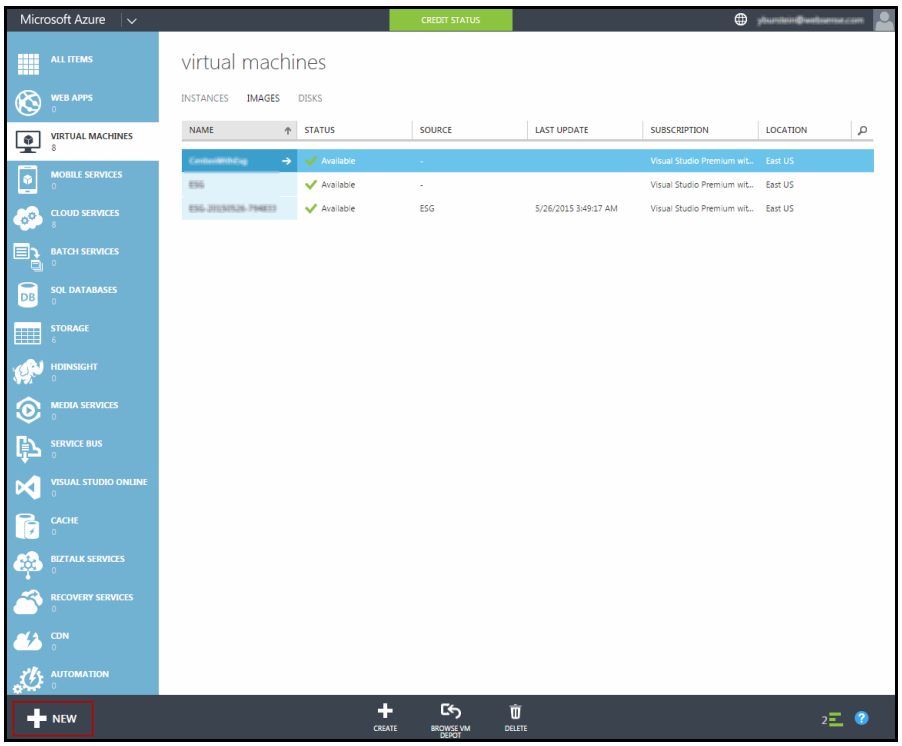
b. Enter a name and description for the VM image. For VHD URL, select the URL of the Email Gateway image file (.vhd) you just uploaded. From Operating System Family, select **Linux**. Also select the box, **I have run waagent - deprovision the virtual machine**.



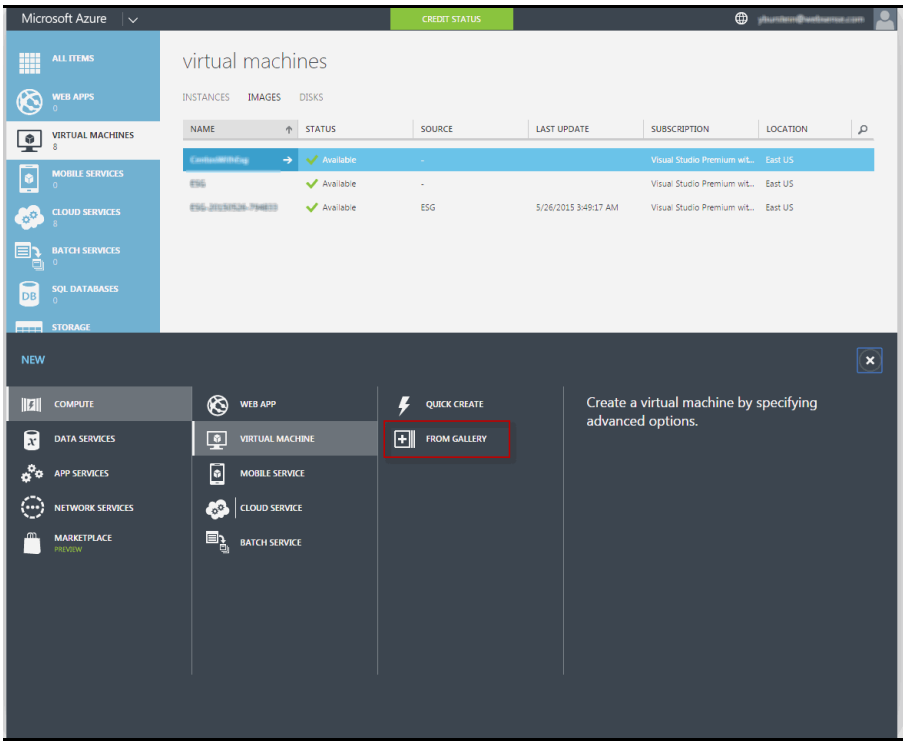
c. Click **Open**.



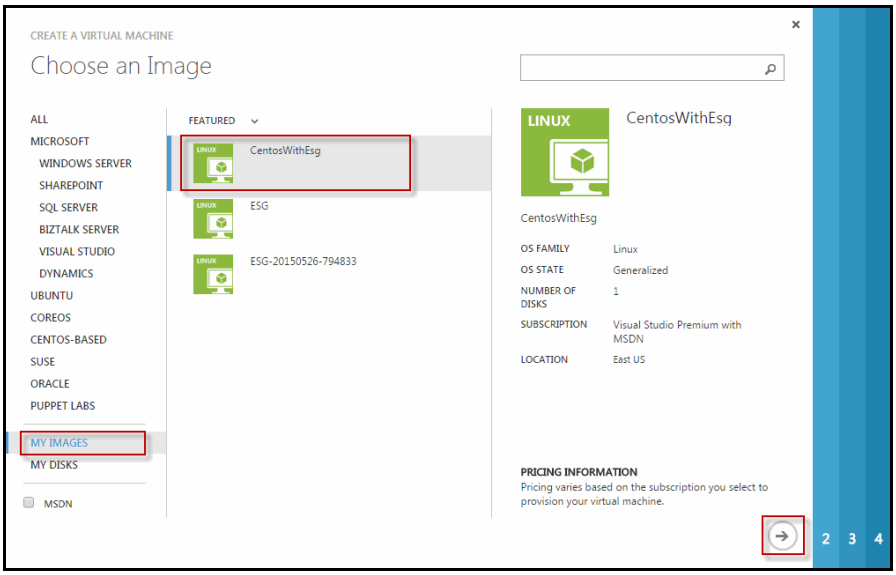
3. Create a virtual machine from the virtual machine image you just created:
   a. Click **Virtual Machines** and then click **New**.



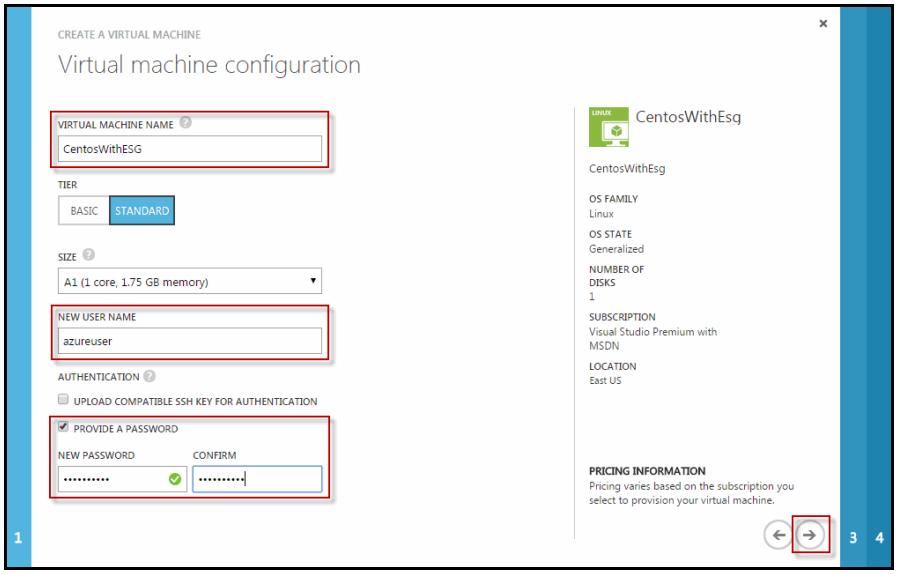
b. Click **Compute > Virtual Machine > From Gallery**.



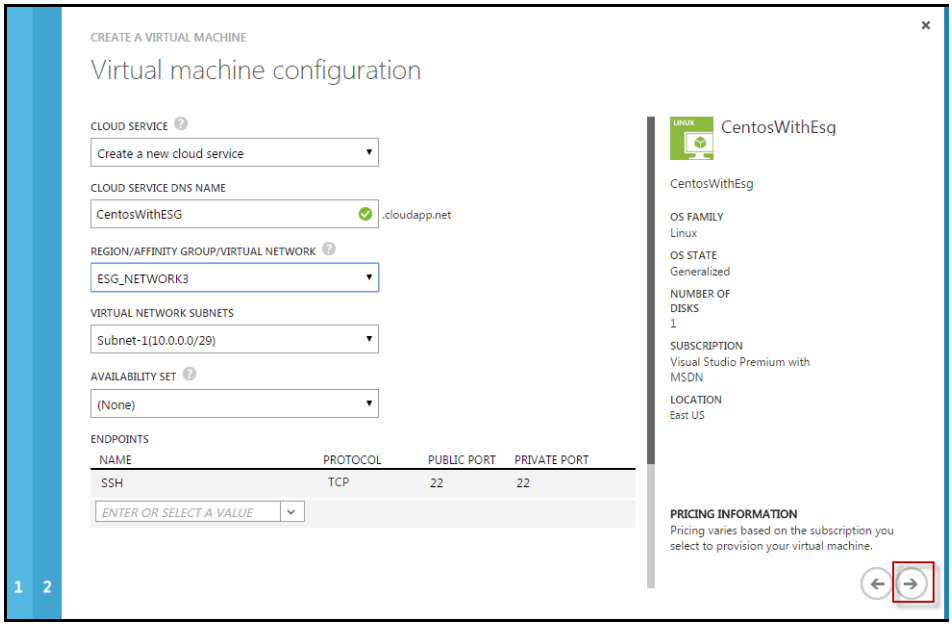
c. Click **My Images** and then choose an image and click >.



d. Complete the fields as prompted and then click >. For enterprise use, it is best practice to select a minimum size of 4 cores and 7 GB of memory (A3 standard). The A3 setting handles up to 75 email messages per second and uses 4.2 GB memory. For new user name, enter a user who will be able to log onto the VM.



4. Configure the VM networking. Select the DNS name, region, and virtual network subnet that you used when you created the virtual network. Also select a cloud service and, for load balancing, an availability set. Click > when done.



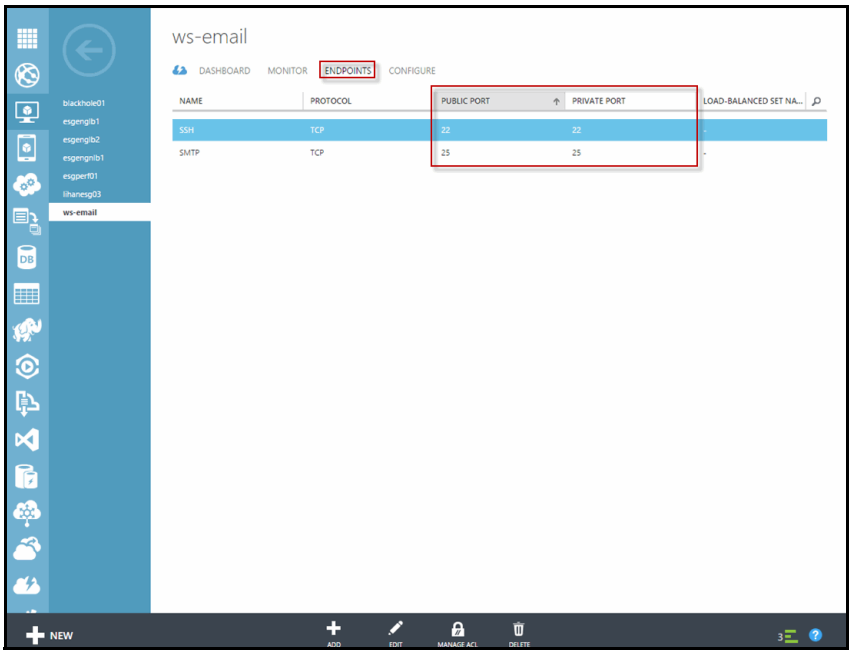
5. Ensure that SSH port 22 is listed for your endpoints.

   Azure endpoints (distinct from TRITON DLP endpoints) map public IP addresses and ports to the private IP address and port of the VM in the cloud service. The

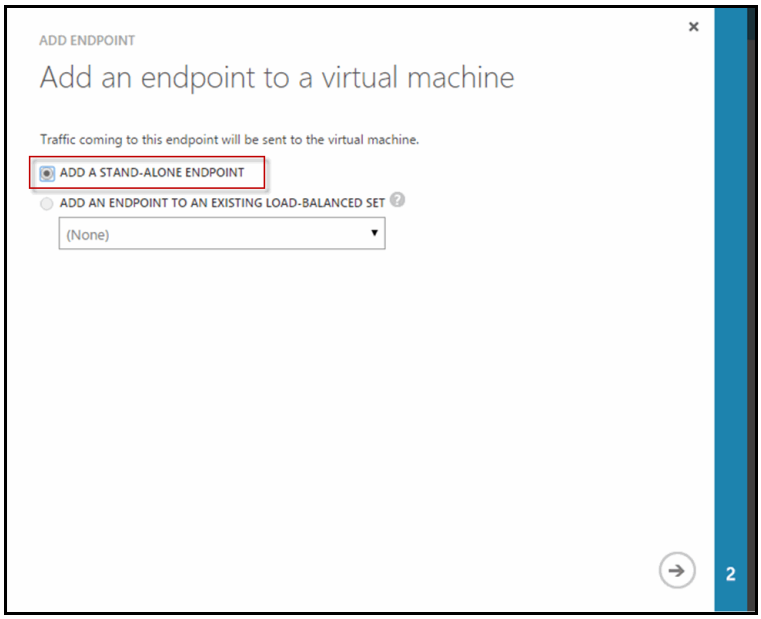
private port is the port that the service is listening on the local computer. The public port is the port that the service is listening on externally. In some cases this is the same port, which is the case for PowerShell.

Port 22 must be open to configure or log onto the VM.

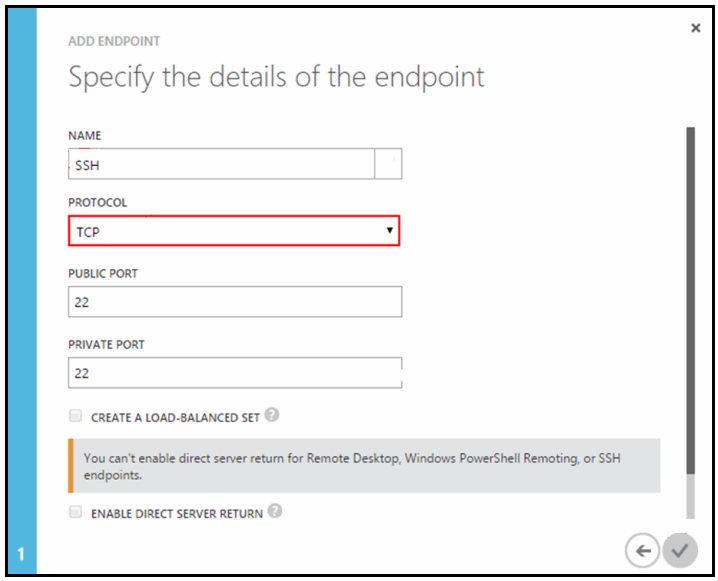
a. Select **Endpoints** from the top menu (Dashboard, Monitor, Endpoints, Configure). SSH port 22 should be listed. If it is not, click **Add** to add it and then click **->**.



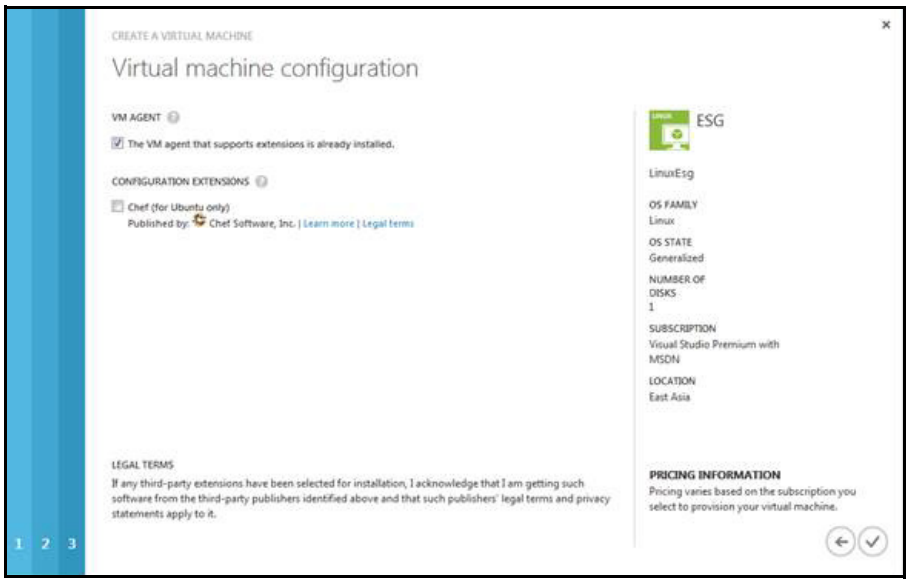
b. Select **Add a stand-alone endpoint**. (For load balancing multiple VMs, select **Add an endpoint to an existing load-balanced set**. See *Scalability and load balancing*, page 100 for details.)



c. Specify details for the endpoint and then click ->.
   - Name: SSH
   - Protocol: TCP
   - Public Port: 22
   - Private Port: 22



6. A final screen appears:



7. To view information about the virtual machine you just created, select Virtual Machines, then click your VM name. Make note of the SSH details. You will need them to log onto the VM.
8. Optionally, attach more disks to the virtual machine.
    a. In the virtual machine, select **Attach> Attach empty disk**.
    b. Attach two disks. The first disk size can be 50 GB and the second disk size can be 100 GB.

Final steps

To complete your Email Gateway deployment, do the following:

1. Configure the Email Gateway VM.
2. Install TRITON management components for the virtual appliance.
3. Configure the appliance in the TRITON Manager.
4. Configure mail flow in Exchange Online.

For step-by-step instructions, see the TRITON AP-DATA Installation Guide in the Forcepoint Technical Library.