Uploading AP-DATA Email Gateway to Azure

Uploading AP-DATA Email Gateway to Azure | TRITON AP-DATA | v8.3.x | 15-Dec-2016

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 <u>TRITON AP-DATA</u> <u>Installation Guide</u>.

This document describes the manual process.

Configure a Virtual Network and VPN in Azure

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

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

Micr	osoft Azure 🛛 🗸		CREDIT STATUS) phurshean	ewebuenue.com
		networks				
×		VIRTUAL NETWORKS LOCA	AL NETWORKS DNS SERVERS			
		NAME	STATUS	SUBSCRIPTION	LOCATION	Q
		ESG_NETWORK3	→ ✓ Created	Visual Studio Premium with MSDN	East US	
		NetTest	✓ Created	Visual Studio Premium with MSDN	East US	
~^^						
31/2						
ан.л (()						
4						
Л						
	0 OPERATIONAL INSIGHTS					
<>	0 NETWORKS	1				
	3 TRAFFIC MANAGER					
	0 MANAGEMENT SERVICES					
	1		¥_ <u>_</u> π_			
	NEW		EXPORT DELETE			i 🔔 🕜

3. Click Custom Create.

Micro	osoft Azure 🛛 🗸			CREDIT STATUS		plantinipente	sense.com 🚨
		networks					
	0	VIRTUAL NETWORKS LOCA	L NETWORKS DNS SER	VERS			
<i>**</i> >	CDN 0	NAME	↑ STATUS	SUBS	CRIPTION	LOCATION	Q
st.	AUTOMATION 0	ESG_NETWORK3	→ 🗸 Created	Visua	I Studio Premium with MSDN	East US	
٩	SCHEDULER 0	ESGNET1	✓ Created	Visua	I Studio Premium with MSDN	East US	
4	API MANAGEMENT	NetTest	Created	Visua	I Studio Premium with MSDN	East US	
Д	MACHINE LEARNING						
	0 STREAM ANALYTICS						
Sak .	0						
NEW							×
Ŧ	COMPUTE		K L	QUICK CREATE	Add your local ne	twork for cross-	
	DATA SERVICES		R 🔊	CUSTOM CREATE	premises connecti	vity.	
<u>د</u>	APP SERVICES						
(C)							
				REGISTER DAS SERVER			
			\odot	ADD LOCAL NETWORK			

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.

virtual Network Deta	Is		
IAME	LOCATION		
MyVPNDNS01	East US	•	
ETWORK PREVIEW			
↔ MyVPNDNS01			

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.

CREATE A VIRTUAL NETWORK	×
DNS Servers and VPN Connectivity	
DNS SERVERS 🕜 POINT-TO-STFE CONNECTIVE	TY 🕜
MyVPNDNS01 8.8.8.8 SELECT OR ENTER NAX IP ADDRESS STE-TO-SITE CONNECTIVITY Configure a site-to-site Configure a site-to-site	te VPN
NETWORK PREVIEW	
ATEWAY	DNS Servers
NETWORK PREVIEW	DNS Servers

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.

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE	
10.0.0/24	10.0.0.0	/24 (254)	10.0.0.1 - 10.0.0.254	
add address space				
NETWORK PREVIEW	GATEWAY			
NETWORK PREVIEW	SATEWAY	So Cit	ients ONS S	ervers

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.

CF	reate a virtual netw /irtual Netw	ork Addres	s Spaces				
	ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RAN	GE		
	10.0.1.0/24	10.0.1.0	/24 (256)	10.0.1.0 - 10.0.1.255			
	SUBNETS						
	Subnet-1	10.0.1.0	/27 (32)	10.0.1.0 - 10.0.1.31			
	Gateway	10.0.1.32	/29 (8)	10.0.1.32 - 10.0.1.39			
	add subnet	add gateway subn	et				
	add address space						
NE	ETWORK PREVIEW						
	↔ MyVPNDNS01	GATEWAY	% CI	ients	O DNS	Servers	

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.

Microsoft Azure	×	CREDIT STATUS		the second seco
	myvpndns01			
\otimes	Ashboard configure certific	CATES		
ESG_NETWOR ESGNET1	virtual network			
MyVPNDNS0 NetTest	1 GATEWAY	Clients	O DNS Servers	
<u></u>	THE GATEWAY WAS NOT CREATED.			
	resources		SUBNET NAME	< glance
DB	INNINE 1. NOLL	IF RUCED	STATUS Created	1
			SUBSCR f74ec5f	IPTION ID f-cdad-4d12-8b8b-89e725d2ca8e
(C)			VIRTUA 3e33a4	L NETWORK ID 01-e16d-4983-9d55-d73c1f0a1946
			LOCATI East US	ON
Гр Пр				
₩ 				
it.				
NEW	CREATE	► ± 亩 Gateway Export delete		0

- 9. Create security certificates to authenticate VPN clients. For instructions, see <u>this</u> 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

- myvpndns01 42 DASHBOARD CONFIGURE CERTIFICATES virtual network ↔ MyVPNDNS01 So Clients ONS Servers 0 DATA IN GATEWAY IP ADDRESS Л 412.05 KB 4.44KB 23.99.106.52 Ż resources quick glance NAME IP ADDRES SUBNET NAME Download the 64-bit Client VPN
 Package $\langle \cdots \rangle$ appemail0527 Virtual Machine 192.168.0.4 Subnet-1 Download the 32-bit ClientVI Package R STATUS 5 Created SUBSCRIPTION ID f74ec5ff-cdad-4d12-8b8b-89e725d2ca8e VIRTUAL NETWORK ID ◈ 3e33a401-e16d-4983-9d55-d73c1f0a1946 LOCATION ঠি East US GATEWAY TYPE A Dynamic Routing Ö
- 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.

Ŧ

Ū

1▲ 2 ②

- 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

- Visit <u>My Account</u>, 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 <u>here</u> 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:

NEW

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**.

Mic	rosoft Azure 🛛 🗸		CREDIT STATUS		#sunitein@websense.com	
	ALL ITEMS	storage				
\otimes	WEB APPS 0	NAME	STATUS	LOCATION	SUBSCRIPTION	D
•	VIRTUAL MACHINES	3ijfeba →	V Online	East US	Visual Studio Premium with MSDN	
	MOBILE SERVICES	partandukämmen272795428	Online	East US	Visual Studio Premium with MSDN	
		histingne herstenense ontrestitische	✓ Online	East US	Visual Studio Premium with MSDN	
	7					
	0					
DB	SQL DATABASES					
	STORAGE 4					
(P)	HDINSIGHT 0					
\odot	MEDIA SERVICES					
Ĩ.	SERVICE BUS					
	U VISUAL STUDIO ONLINE					
	0					
7	0					
4	BIZTALK SERVICES					
Ő	RECOVERY SERVICES					
2 2	CDN 0					
33	AUTOMATION					
ł	NEW			те	(>

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.

Microsoft	Azure 🗸 🗸				CREDIT STATUS					ncam
ALL T	TEMS	storage								
КО инев.	APPS	NAME		STATUS		LOCATION	N		SUBSCRIPTION	Q
	JAL MACHINES	NgReta	→	V Online		East US			Visual Studio Premium with MSDN	
		parlainhaisinnm	272796636	V Online		East US			Visual Studio Premium with MSDN	
	ILE SERVICES	perfaishes:75edte	(ing liftper)	V Online		East US			Visual Studio Premium with MSDN	
	D SERVICES	yanatian		V Online		East US			Visual Studio Premium with MSDN	
BATC	H SERVICES									
DB SOL D	DATABASES									
STOR	AGE									
NEW										×
							URL			
Сом	PUTE	DB SQL	DATABASE	_ <i>;</i>	QUICK CREATE		ownstorage	01	0	
	A SERVICES	то вто	RAGE						.*.core.windows.net	
o APP	SERVICES	😥 нал	NSIGHT				East US	NETY GROUP	•	
		A REC								
							REPLICATION			
PREVI	E CALE		CHINE LEARNING				Geo-Redun	dant	Ť	
		💐 STRI	EAM ANALYTICS							
								CREATE S		

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.

NAME		
uploadimage01		
ACCESS 🕜		_
Private	•	
		1

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.

Micro	osoft Azure 🛛 🗸		CREDIT STATUS	🌐 yiturtiring websense.com 💄
		ownstorage01		
		42 DASHBOARD MONITOR CO	DNFIGURE CONTAINERS IMPORT/EXPORT	
		NAME	URL	LAST MODIFIED
		uploadimage01	→ https://ownstorage01.blob.core.windows.net	/uploadimag 8/25/2015 2:04:07 PM
	ownstorage01			
<u></u>	performing an overlitter.			
∎ 5				
DB				
1 P				
\odot				
<u>ا</u>				
+	NEW		ADD EDET DELETE	2 📃 🕐

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

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

Microsoft Azure 🛛 🗸			CREDIT STATUS		۲	yhuntein@webuense.com
ALL ITEMS	virtual machi	nes				
	INSTANCES IMAGES	DISKS				
VIRTUAL MACHINES	NAME 🔶	STATUS	SOURCE	LAST UPDATE	SUBSCRIPTION	LOCATION
	Contact#fibExp ->	🗸 Available	-		Visual Studio Premium wit	East US
0 MOBILE SERVICES	696	🗸 Available			Visual Studio Premium wit	East US
	656-20250526-794833	🗸 Available	ESG	5/26/2015 3:49:17 AM	Visual Studio Premium wit	East US
DB SQL DATABASES						
STORAGE 6						
- NEW		CREATE		DELETE		2 🗾 🥝

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.

CentosWithES	3		
DESCRIPTION			
VHD URL			
OPERATING SYST	EM FAMILY		
Linux		•	
		 _	

c. Click Open.

BROWSE CLOUD STORAGE				×
> lkjifdsa	NAME	LAST MODIFIED	SIZE	P
 portak/hds3mmm272795q3 	Seconder-oppitistersterstros.	8/25/2015 2:15:01 PM	30 GB	
 portak/hds70q8tcljg5fpc 	Beselfav/Disk305ahd	8/12/2015 5:09:45 PM	30 GB	
ownstorage01	ESG-21031626-794838-es-2103-05	5/26/2015 3:49:20 AM	30 GB	
uploadimage01	mingdogi Syll210,517161436431621, and	8/17/2015 1:55:07 AM	30 GB	
 portak/hdonm#ft8rbp3isz7 	CentosWithEsg.vhd	5/20/2015 5:37:22 AM	30 GB	
	• eviger1 v421538531648431338	8/15/2015 11:34:54 PM	30 GB	
	🕒 (gmaðrum (grötti stöljal) sötöldi (h	7/5/2015 7:32:52 AM	30 GB	
	• https://doi.eo/c210.51723360.3020545.v.p.	8/13/2015 4:55:30 AM	30 GB	
	And an approximation of the second	8/25/2015 2:15:04 PM	30 GB	
	File nam	CentosWithESG.vhd	[*.vhd] Open	

3. Create a virtual machine from the virtual machine image you just created:

Microsoft Azure 🛛 🥆			CREDIT STATUS		•	yhundein@websense.com	
ALL ITEMS	virtual machir	nes					
	INSTANCES IMAGES I	DISKS					
VIRTUAL MACHINES	NAME 🔶	STATUS	SOURCE	LAST UPDATE	SUBSCRIPTION	LOCATION	D
	${\rm CostooMriticg} \rightarrow $	💙 Available	4 (A)		Visual Studio Premium wit	East US	
	E56	🗸 Available	-		Visual Studio Premium wit	East US	
	ESG 311531526-794833	🗸 Available	ESG	5/26/2015 3:49:17 AM	Visual Studio Premium wit	East US	
DB SOL DATABASES							
STORAGE 6							
		CREATE		TE		2 \Xi 🧯	>



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

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

CREATE A VIRTUAL MACHIN	NE	×	
Choose an In	nage	٩	
ALL MICROSOFT WINDOWS SERVER SHAREPOINT SQL SERVER BIZTALK SERVER VISUAL STUDIO DYNAMICS UBUNTU COREOS CENTOS-BASED SUSE ORACLE PUPPET LABS MY JIANGES MY JISKS	NAGE FATURED ►	CentosWithEsg CentosWithEsg CentosWithEsg MARKING MARKING SFAMILY Linux CentosWithEsg MARKING SFAMILY Linux CentosWithEsg MARKING SFAMILY CentosWithEsg MARKING SFAMILY CentosWithEsg MARKING SFAMILY CentosWithEsg MARKING SFAMILY CentosWithEsg MARKING SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos SFAMILY Centos Cen	
MSDN MSDN		Pricing varies based on the subscription you select to provision your virtual machine.	
		→ 2	3 4

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.

VIRTUAL MACHINE NAME O	CentosWithEsg CentosWithEsg
BASIC STANDARD	OS FAMILY Linux OS STATE
SIZE 💿 A1 (1 core, 1.75 GB memory)	Generalized NUMBER OF DISKS 1
NEW USER NAME azureuser	SUBSCRIPTION Visual Studio Premium with MSDN
	LOCATION East US
UPLOAD COMPATIBLE SSH KEY FOR AUTHENTICATION PROVIDE A PASSWORD NEW PASSWORD CONFIRM	
	PRICING INFORMATION Pricing varies based on the subscription you select to provision your virtual machine.

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.

viituai machi	ne coniguratio	ЛТ		
CLOUD SERVICE				CentosWithEsg
Create a new cloud servic	e 🔻			
CLOUD SERVICE DNS NAME				CentosWithEsg
CentosWithESG	.clo	udapp.net		OS FAMILY
REGION/AFFINITY GROUP/VIR				Linux OS STATE
ESG_NETWORK3	•			Generalized
VIRTUAL NETWORK SUBNETS				NUMBER OF DISKS
Subnet-1(10.0.0/29)	•			1 SUBSCRIPTION
AVAILABILITY SET				Visual Studio Premium with MSDN
(None)	•			LOCATION East US
ENDPOINTS				
NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT	- 1
SSH	TCP	22	22	
ENTER OR SELECT A VAL	UE 🗸			PRICING INFORMATION
				Pricing varies based on the subscription

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.)

ADD ENDPOINT	~
Add an endpoint to a virtual machine	
Traffic coming to this endpoint will be sent to the virtual machine.	
ADD A STAND-ALONE ENDPOINT	
ADD AN ENDPOINT TO AN EXISTING LOAD-BALANCED SET	
(None)	

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

SSH PROTOCOL TCP PUBLIC PORT 22	
PROTOCOL TCP PUBLIC PORT 22	
TCP • •	
PUBLIC PORT	
22	
PRIVATE PORT	
22	
CREATE A LOAD-BALANCED SET 🕖	

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 <u>TRITON AP-DATA Installation Guide</u> in the Forcepoint Technical Library.