

Create an App for Azure (part 5)

Cloud, CSS, Docker, HTML, PHP

🗣 Language 🛛 🚖 Skills : 5

The digital transition has pushed software companies and enterprises to migrate their applications to the web. Azure cloud services have provided the ideal platform, the right services, and the tools to go digital while keeping full control over the data. This publication proposes the creation of a simple application by discovering some of these services and tools.

Published Wednesday June 22nd 2022, 18:14 Modified Monday August 26th 2024, 10:04

By Olivier Paudex

Security on Azure

Unlike virtual machines (VMs), services in Azure are public. That is, they are shared by multiple people. They are also called **PaaS**, for **"Platform as a Service"**, or **"tenants"**, because they are just an application instance of a global server.

This publication is composed of several parts. This being the 5th part.



However, there are opportunities to make these services private. This publication will talk about several things:

- The DNS.
- SSL certificates.
- Virtual networks.
- Private endpoints.
- The **"Application Gateway"** service.

DNS

So far, the application responds to the following URL: "https://[app name].azurewebsites.net/".

This is not very practical. Most of the time, an application should respond to a custom domain name. To achieve this, nothing could be easier.

- Reserve a domain name
- Create a record in your domain of type **CNAME**
- The application, in this example, will take the name **"docker.fuyens.ch"**.
- His target is the URL given by Azure.



	×
Editer un enregistrement DNS pour fuyens.ch	
Туре	CNAME record
CNAME	L'enregistrement CNAME permet de faire d'un domaine un alias vers un autre. Cet alias hérite de
Source	tous les sous-domaines de l'original.
docker.fuyens.ch	
Cible	
app-imagesgallery-westeu-001.azurewebsites.net	
TTL	
5 minutes	
ENREGISTRER ANNULER	
The CNAME regis	stration
Return to the application and add your new custom dom	nain name.
 Click on the "Custom Domains" tab. Add your custom domain name. 	
The name is now bound to the application, but is not yet red.	secure. You can see the "Not Secure" warning in
You can try entering the URL, in my example: http://doc warn you that the site is not secure.	ker.fuyens.ch . This works, but the browser will



App Senice	ry-westeu-001 Custom domains	app-imagesgallery-westeu-001	×	App-imagesgaller App Service (P Search (Std+r)) • organization Coner	y-westeu-001 Custom domains
Settings Configuration	Custom Domains			Settings Configuration Authoritation	Ustom Domains
Authentication Application insights	Problems: () Description	Custom domain *		Application insights Mentity	Configure and manage custom domains assigned to your app. Learn more IP address:
1. Identity	Custory Donuin Welfcation D: ADDRESS(00):656FEBA(TAXD0022017)0CTTSAEBIED450879989495EEBACKET7C4			Rackups Gastam domaine	26502.65 Custom Donain Welfkadon ID: ①
Custom domains	HTTPS ON/n O	docker.fuyens.ch	\sim	TLS/SSL settings	ASSISTERSOSSISTERAAVAZORIZETZIGTYAALDREDASIET990-09FEBACREZTCA HTTPS ON /: ()
 TLS/SSL settings TLS/SSL settings 	+ Add custom domain			 TIS/SSL settings (preview) Networking 	+ Add custom domain
1 Networking	Status Filter Not fease (0) Secure (0)			😒 Scale up (App Service plan)	Stelue Filter
Scale up (App Service plan)	SSL STATE ASSISSED CUSTOM DOMAINE SSL Binding	Mall Land		 Scale out (App Service plan) Websales 	SSL STATE ASSIGNED CUSTOM DOMAINS SSL Birds
 Websieks 	Secure app-imagesgallery-wester-ObLasserwebeltec.net.	validate		💷 Push	Secure app imagengalisty-wetten-001.acunwebsber.net
				D _p NySCL in App	U hat Secure docket Approach Add bind

The SSL certificate

To remedy this problem, you need to subscribe to an SSL certificate.

- Copy the IP address of the application (see image above).
- Copy the verification ID of the custom domain.
- Return to your DNS.
- Create a **TXT** record and name it **"asuid.docker.fuyens.ch"**, in my example.
- Paste the verification ID into it.



Editer un enregistrement DNS pour fuye	ens.ch
Туре	TXT record
ТХТ	L'enregistrement TXT permet d'insérer un texte quelconque dans un enregistrement DNS. Il peut
Source	être utilisé pour vérifier l'authenticité du propriétaire d'un domaine.
asuid.docker.fuyens.ch	
Cible	
A5299E2F8505956FE9A47A7008238720CF76AE	B6ED4
TTL	
5 minutes	*
The TXT reco	be many vendors on the market
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, in command-line savvy). 	ord for custom domain verification he many vendors on the market. if necessary (with SSLShopper or OpenSSL, if you're more
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, in command-line savvy). Return to the KeyVault. 	ord for custom domain verification he many vendors on the market. if necessary (with SSLShopper or OpenSSL, if you're more
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, in command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". 	ord for custom domain verification he many vendors on the market. if necessary (with SSLShopper or OpenSSL, if you're more
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, in command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". Select "Import". 	ard for custom domain verification the many vendors on the market. if necessary (with SSLShopper or OpenSSL, if you're more
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, it command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". Select "Import". Enter a name for the certificate. Select your PEX-formatted certificate. 	he many vendors on the market. if necessary (with SSLShopper or OpenSSL, if you're more
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, it command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". Select "Import". Enter a name for the certificate. Select your PFX-formatted certificate. Enter the password you gave when created the certificate. 	ating the certificate.
 The TXT record Create a certificate by choosing one of the Convert your certificate to PFX format, it command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". Select "Import". Enter a name for the certificate. Select your PFX-formatted certificate. Enter the password you gave when created and the password you gave you	ating the certificate.
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, it command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". Select "Import". Enter a name for the certificate. Select your PFX-formatted certificate. Enter the password you gave when created and the part of the	ating the certificate.
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, it command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". Select "Import". Enter a name for the certificate. Select your PFX-formatted certificate. Enter the password you gave when created and the password you gave you ga	he many vendors on the market. if necessary (with SSLShopper or OpenSSL, if you're more
 The TXT reco Create a certificate by choosing one of the Convert your certificate to PFX format, it command-line savvy). Return to the KeyVault. Click on the "Certificates" tab. Click on "Generate/Import". Select "Import". Enter a name for the certificate. Select your PFX-formatted certificate. Enter the password you gave when created the password you gave you gave when created the password you gave you	and for custom domain verification the many vendors on the market. if necessary (with SSLShopper or OpenSSL, if you're more ating the certificate.



Key-westeu-001 Certific Key wurdt Starch (Cuti/) Activity log co Activity log co Activity log co Diagnose and solve problems in Diagnose and solve problems in Extends in Extends in Secrets in Certificates in Access collicies in	Cates … Generate/Import	Create a certificate Method of Certificate Creation Certificate Name * Upload Certificate File * Password	 Import ✓ ImagesGallery ✓ [*] certificate.pfx*
	Importing the certifica	te into the KeyVault	
 Click on the Click on "Pri Click on "Im Select the ce 	ivate Key Certificates (.pfx). port Key Vault Certificate". ertificate.		
Home > app-imagesgallery-westeu-001	i .		Select certificate from Azure \times
🏮 app-imagesgallery-	westeu-001 TLS/SSL settings		
 Search (Ctrl+/) « Settings Configuration Authentication Application Insights Identity Backups Custom domains TLS/SSL settings TLS/SSL settings (preview) 	 Refresh Delete bindings Buy Certificate Private Key Certificates (pfx) Private Key Certificates (pfx) Public Key Certificates (cer) Private Key Certificate Private Key certificates (pfx) Private Key Certificates 	FAQs ed to the certificate store for your app download from the Azure Management Import Key Vault Co	Subscription * Fuyens Subscription Key vault * Key-westeu-001 Certificate * ThagesGallery (Thumbprint:59488550CF18A602F3D7A63E86 ertificate

Importing a certificate from KeyVault

- Click on the **"Custom Domains"** tab.
- Click on "Add binding".
- Select the certificate.



		mone / applinagesgallery-wester-o	-wester-001 Custom domains	
two : approxyclefy webs 601 applyter applyter constrained and apply	TLS/SSL Binding ×	Appl-Intagesgalitery Applemics Applemics Authentication Applemics Authentication Applemics Semity	Average - voir Custom domains C Reach & Tradebelow Association of the custom domain State Filer	
Openne dawake Ski 1501 Akildada Cultifut Octavatis Ski 1501 Ski 1501 0 (norm dawake) Ski 1501 Akildada Cultifut Octavatis Ski 1501 Ski 1501 1 (norm dawake) Ski 1501 Ski 1501 Ski 1501 Ski 1501 1 (norm dawake) Ski 1501 Ski 1501 Ski 1501 Ski 1501 1 (norm dawake) Ski 1501 Ski 1501 Ski 1501 Ski 1501	docker Joyenuth (394883500718440071074438866070382) V TLSS50, Type: * V 2N8 52. V	Backups Custom domains	SSL STATE ASSIGNED CUSTOM DOMAINS Secure app-imagesgallery-westeu-001.aturewebsites.net	SSL Bindi
Networking		 TLS/SSL settings TLS/SSL settings (preview) Networking 	Secure docker.fuyens.ch	SNI SSL

This time, our application is validated by a certificate.

Virtual networks

While our application is public, the same is not true for all other services (database, storage, keyvault). We'll remedy this by creating virtual networks and privatized access.

- Create a **"Virtual network (Vnet)"**.
- Select the network resource group.
- Enter a name like "vnet-backend-westeu-001".
- Add the subnet "snet-appservices-westeu-001" and apply the IP network "10.0.1.0/24" to it.
- Add the subnet "snet-privateendpoint-westeu-001" and apply the IP network "10.0.2.0/24" to it.

Create virtual netwo	ork …		Basics IP Addresses Security	Tags Review + create ied as one or more address prefixes	in CIDR notation (e.g. 192.168.1.0/24)	L.
Basics IP Addresses Securit	y Tags Review + create		IPv4 address space			
Azure Virtual Network (VNet) is the f Azure resources, such as Azure Virtu networks. VNet is similar to a traditic benefits of Azure's infrastructure su	fundamental building block for your private network in Azure. VNet enables m al Machines (VM), to securely communicate with each other, the internet, and nal network that you'd operate in your own data center, but brings with it add h as scale, availability, and solation. Learn more about virtual network	any types of on-premises ditional	10.0.0/16 10.0.0 - 10.0.255.255 (65	5536 addresses)		Û
			Add IPv6 address space			
Project details						
Project details Subscription * ①	Fuyens Subscription	~	The subnet's address range in CIDR notat network.	ion (e.g. 192.168.1.0/24). It must be	contained by the address space of th	e virtual
Subscription * ① Resource group * ①	Fuyens Subscription rg-networks-westeu-001 Create new	× ×	The subnet's address range in CIDR notat network. + Add subnet 📋 Remove subnet	tion (e.g. 192.168.1.0/24). It must be	contained by the address space of th	e virtual
Project details Subscription * ① Resource group * ① Instance details	Fuyens Subscription rg-networks-westeu-001 Create new	~ ~	The subnet's address range in CIDR notat network. + Add subnet I Remove subnet Subnet name	iion (e.g. 192.168.1.0/24). It must be Subnet address range	contained by the address space of th NAT gateway	e virtual
Project details Subscription * Resource group * Instance details Name *	Fuyens Subscription rg-networks-westeu-001 Create new vnet-backend-westeu-001	✓	The subnet's address range in CIDR notat network. + Add subnet Remove subnet Subnet name snet-appservices-westeu-001	ion (e.g. 192.168.1.0/24). It must be Subnet address range 10.0.1.0/24	contained by the address space of th NAT gateway -	e virtual
Project details Subscription * Resource group * Instance details Name * Region *	Fuyens Subscription rg-networks-westeu-001 Create new vnet-backend-westeu-001 West Europe	 ✓ ✓ ✓ ✓ 	The subnet's address range in CIDR notat network. Add subnet Remove subnet Subnet name snet-appservices-westeu-001 snet-privateendpoint-westeu-001	ion (e.g. 192.168.1.0/24). It must be Subnet address range 10.0.1.0/24 10.0.2.0/24	contained by the address space of th NAT gateway	e virtual

Creating the "Backend "Vnet

- Start with another Vnet.
- Enter a name like **"vnet-frontend-westeu-001"**.
- Add the subnet "snet-appgateway-westeu-001" and apply the IP network "10. 1.1.0/24".



• Add the subnet "snet-privateendpoint-westeu-001" and apply the IP network "10.1.2.0/24" to it.

Private endpoints

Private endpoints allow you to add a private IP address to a public service, such as storage or database.

Storage

- Add an endpoint (private endpoint).
- Select the storage resource group.
- Enter a name like "pe-storage-westeu-001".
- Enter a name for the network card like "pe-storage-nic-westeu-001".
- Select the resource type "Microsoft.Storage/storageAccounts".
- Select **"blob"** for the sub-resource.
- Select the subnet "Private endpoint", previously created.
- Select integration with a private DNS zone.

Create a private endpo	int …	Create a private endp	point
Resource Virtu Use private endpoints to privately connect virtual network, but can be in a different r Project details Subscription * Resource group *	al Network: ① DNS ③ Tags ④ Review + create t to a service or resource. Your private endpoint must be in the same region as your egion from the private link resource that you are connecting to. Learn more Fuyens Subscription	✓ Basics ✓ Resource ③ V Private Link offers options to create pr an Azure storage account. Select which Connection method ⊙	Irtual Network DNS Tags Review + create Tresources like your private link savice, a SQL server, or resource you would like to connect to using this private endpoint. Learn more Connect to an Azure resource in my directory. Connect to an Azure resource by resource ID or alias.
Instance details Name * Network Interface Name * Region *	pe-storage-westeu-001 ✓ pe-storage-nic-westeu-001 ✓ West Europe ✓	Resource type * ③ Resource * ③ Target sub-resource * ③	Introsoft.Storage/storageAccounts Stimagesgallerywesteu001 blob





Configuring a private endpoint for the storage service



- Start for the database by selecting the database resource group and resource type "Microsoft.Sql/servers".
- Select the subnet "Private endpoint", previously created.

The safe

The safe is doing very well!

It has two private endpoints. One for the "backend vnet", so the application can retrieve secrets. The other for the "frontend vnet" so that the "application gateway" service can retrieve the SSL certificate there.

- Recommence a third time for the KeyVault.
- Select the resource type "Microsoft.KeyVault/vaults".
- Select the vnet "backend" once.
 Recommence one last time for the Keyvault.
- Select the resource type "Microsoft.KeyVault/vaults".
- Select the virtual network "frontend" and the subnet "private endpoint" once.

The three services are now linked to the virtual network "Backend".

The vault service is also linked to the virtual network "Frontend".



Integration of the application into the virtual network

To integrate an application into a virtual network, simply select it.

- Return to the application.
- Click the "Networking" tab.
- Click "Vnet Integration".
- Click "Add Vnet".
- Select the vnet "backend".
- Select the subnet "appservices".

App Service	westeu-001 Networking … ⊙ Refesh 🖉 Send us your feedback			↔ VNet Integration … app-imagespalley-westers 001 o ^d Disconnect ◯ Refresh	app-imagespilley-wester-001 Subscription Faynes Subscription
Deployment andertials Deployment adds: Deployment denter Settings Configuration Application Insights leterity leterity	Inhoused Traffic Manage access and incoming services. Features & Access relation O OII El App assigned address O II	Web App These cuttors domains direct traffic to your web app. Domains docker flagren.ch app: imagesplitty-wested 001 accreases-	Octower Torffe: Set of parts rays dependencies like distance. Feetures Col Main insegution Off ** What insegution Off ** influed connections Off	Vitet Configuration Securely access resources available in or through your Azure + Add Wet Vitet Details	Virtual Viencek Virtual Viencek Viete Laam more Salaret Create New Salaret Salaret
Backup: Counter identifies TLS/SSL settings TLS/SSL settings (provides) Networking TLS/SSL settings (provides) Solar out (App Service plan) Solar out (App Service plan) Solar out (App Service plan)	Intound address		Distance Distance	We NUL Net Cont LOCATION Net Cont What Address Space Sara Address Nat Configured	gund

Integrating an application into a virtual network

Disabling access rights to different services

To secure the infrastructure, go around the three services and disable access to the public network.

- In the storage account, click "Networking", then select "Disable public network access".
- Idem for the database server.
- In the vault, there is no disabling possible, so select "Selected networks" and in the exceptions, select "No" for "Allow trusted Microsoft services to bypass this firewall".



stimagesgallerywest	teu001 Networking - ×				key-westeu-001	Networking -	-
Sourch (201-) Sourch (201-) terms Source transm	Remails and interal networks Photo industrial Caston duration ☐ time × Distant © Industrial	sqlav-imagesgi _{90 sele} 2 Sectoria	llery-westeu-001 Netwo	rting X	Servings Repr Repr Repr Repr Repr Repr Repr Repr Repr	⁴ El tare × transi charges 4 Alter acres free:	 Adveck Id orderedes Experiende specification Cody ordered kay our disease case account fish king wash. Lasar sease
E cottaves E cottaves E charas E	Another sectors are set and an and an another sector are set and an another set and	Si Figures Single Section 2014 Single Section 2014	Palat anna Addressendo Kosti Addressendo Kosti Addressendo Lan anna Addressendo Kosti Addressendo Anna Addressendo Addressen		 Senters Contract of Contract Access added Security Security Security Security Instruction Lands Marchan Marchan Marchan Compared readings Compared readings Compared readings Verify Verify Verify 	Utad reservice 0 What reservice Reserved 0 Parket on COR Parket on COR Park	Alternational Mariane Mari Mariane Mariane Mar

Verifying access

Verify that the application is still working

- Try to connect to the database using **Azure Data Studio**, there should be a connection error.
- Idem for storage with **Azure Storage Explorer**.



The Application Gateway

The Application Gateway allows you to create, as the name implies, a single gateway at the entrance to the infrastructure. It filters authorized protocols, and redirects traffic to one or more applications or services. Among other things, it allows:

- Add a single public IP address as input to our infrastructure.
- Add security by creating listening rules on a particular protocol.
- Add a firewall option to our infrastructure.
- Balance loads across multiple resources, redirecting traffic to a resource based on the URL.

Security resources are among the most expensive elements of the Azure cloud. A front-end gateway like the one used for this demo app can cost about **\$6 per day**. So be careful not to leave it running longer than necessary.

Azure Managed Identity (AMI)

The gateway application will use the SSL certificate in place of the application. To access the **"Keyvault"** containing the certificate, it must register with the **"Keyvault"** service. Unlike the **"Apps service"** which uses a **"System assigned"** identity, the **"Application gateway"** service will have to use a **"User assigned"** identity. To accomplish this, it must go through an **"Azure Managed Identity"** or AMI.

- Create an Azure User Managed Identity.
- Copy its ID from the **"Overview"** page.
- Go back to the Keyvault.
- Add an access rule.
- Add the "GET" right for the "Secret permissions".
- Click on "Select principal".
- Paste in the AMI ID.
- Add the keyvault access for the AMI.



Accessing the Keyvault from the Application Gateway

- Click on the "Networking" tab of the Keyvault.
- Select "Selected networks".
- Do not add any virtual networks.
- Select "No" for the exception "Allow trusted Microsoft services to bypass this firewall".
- Be sure to verify that you have configured two private endpoints.

key-imgallery-westeu-001 Networking - Service Status Freedals and virtual instruction Dennice Service Status Overvice Service Status Acting vig Network Status Acting vig Network Status Overvice Service Status Overvice Network Status Overvice Network Status Overvice Network Status Overvice Network Status Overvice Status relative Status Overvice Status relative Status Overvice Status relative Status Overvice Status relative Status Status relative Status Add residual relatives Vibrat orderative Status relative status	
Settings No virtual networks are selected.	Settings
Boom Forest Fo	[*] Koys [™] Koys [™] Certificates [™] Certificates [™] Access policies [™] Access policies [™] Access policies [™] Security [™] Security [™]

Keyvault configuration with two private endpoints

Application Gateway

Basics tab

- Create an Application Gateway.
- Give it a name.
- Leave the minimum number of instances at 0.
- Add the maximum number of instances at 2.
- For the virtual network configuration, add the virtual network "**frontend**" and the subnet "**app** gateway".



"Frontends and Backends" tab

- For the **"Frontends"** tab, add a new public IP address.
- For the **"Backends"** tab, add a backend pool and associate the application with it as the target.

			Add a backend pool.
			A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool one control utimal machines utimal machines erely rate. It addresses domain
Create application of Instance details Applications generals " Region * Ther © Enable subscoling Minimum instance court * ©	gar image galleway ✓ gar image galleway into 401 ✓ Write Europe ✓ Seconder V2 ✓ ® tes © too ✓ 0 ✓ 2 ✓	Create application gateway	names, or an App Service. Name * Add backernd pool without targets Bockand targets 1 kem Target type Target App Services Y app-imagesgallery-westeu-001
Availability zone	None V	private P address, or one of loads type. Fronterd IP address type	IP address or FQDN
Configure virtual network	ver:froteof.wste.01	Public IP address * [Plenoj age-inagesgalitovj-ip-weeten-201] V Add new	
Subnet * ①	Create new Create new set-appgateway-wested-001 (10.1.1.0/24)		
			Add Cancel
		The creation of the "Frontend" and "Backend"	
Configura	ation tab		
Configura			
Once the "F	rontend" and the "Ba	ckend" are added, the Application (Gateway needs to connect them
through rou	iting rules that will filter	the allowed protocols. This is called	a" listener" .
		-	
✓ Basics ✓ Fronte	nds ✓ Backends ① Configuration ③) Tags 6 Review + create	
✓ Basics ✓ Fronte Create routing rules that I	nds ✓ Backends ① Configuration) Tags 6 Review + create d more backend pools, add a second frontend IP configuration if you haven't alrea	ady, or edit previous configurations.
✓ Basics ✓ Fronte Create routing rules that I	nds ✓ Backends ① Configuration ③) Tags (6) Review + create d more backend pools, add a second frontend IP configuration if you haven't alrea	ady, or edit previous configurations.
✓ Basics ✓ Fronte Create routing rules that I	nds ✓ Backends ① Configuration ③ link your frontend(s) and backend(s). You can also ad) Tags (6) Review + create d more backend pools, add a second frontend IP configuration if you haven't alrea	ady, or edit previous configurations.
✓ Basics ✓ Fronte Create routing rules that I	nds ✓ Backends ① Configuration ③ link your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP) Tags (Review + create d more backend pools, add a second frontend IP configuration if you haven't alres	ady, or edit previous configurations. Backend pools + Add a backend pool
✓ Basics ✓ Fronte Create routing rules that I Pui	nds ✓ Backends ① Configuration ③ ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- steru-001 (20.224 128 108)	Tags (a) Review + create d more backend pools, add a second frontend IP configuration if you haven't alreat Routing rules	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendnool-wester:(011
V Basics V Fronte Create routing rules that I Pui we	nds V Backends ① Configuration ③ ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- steru-001 (20.224.128.108)) Tags (6) Review + create d more backend pools, add a second frontend IP configuration if you haven't alres Routing rules	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendpool-westeu-001
✓ Basics ✓ Fronte Create routing rules that I Pul we	nds ✓ Backends ① Configuration ③ link your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- blic: agw-imagesgallery-ip- blic: agw-imagesgallery-ip- blic: agw-imagesgallery-ip- blic: agw-imagesgallery-ip- blic: agw-imagesgallery-ip- blic: agw-imagesgallery-ip-	Tags Review + create d more backend pools, add a second frontend IP configuration if you haven't alreation Image: Configuration of the second frontend IP configuration of the second frontend IP configuration if you haven't alreation Image: Configuration of the second frontend IP configuration of the second frontend IP configuration if you haven't alreation Image: Configuration of the second frontend IP configuration of the second frontend	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendpool-wester-001
V Basics V Fronte Create routing rules that I Pul we	nds ✓ Backends ① Configuration ③ ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- steu=-001 (20.224.128.108)	Tags Review + create d more backend pools, add a second frontend IP configuration if you haven't alrest Routing rules Add a routing rule Routing rules Routing rules	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendnool-wester-001
V Basics V Fronte Create routing rules that I Pul we	nds ✓ Backends ① Configuration ③ link your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- ster = 001 (20.224 128 108)	Tags Review + create d more backend pools, add a second frontend IP configuration if you haven't alree Routing rules Utility and a routing rule Routing rules Routing rules	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendpool-westerr-001
✓ Basics ✓ Fronte Create routing rules that I Pul we Click 4	nds ✓ Backends O Configuration () ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- streu-001 (20 224 128 108) O **********************************	(a) Tags (a) Review + create If more backend pools, add a second frontend IP configuration if you haven't already Image: Configuration of the pools of	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendronol-wettert-001
 Basics Fronte Create routing rules that I Pul We Click 4 Name 	nds ✓ Backends ① Configuration ③ ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- streu-001 (20.224.128.108) "Add a routing rule". e it.	Image: The second point of the second front of the seco	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- harkendnool-wester=001
 ✓ Basics ✓ Fronte Create routing rules that I Pul We Click 4 Name Give if 	nds ✓ Backends O Configuration (3) link your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- wster-001 (20224 128 108) "Add a routing rule". e it.	Tags Review + create Inclusion of the pools, add a second frontend IP configuration if you haven't already of the pools. Routing rules Routing rules Routing rules	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendnonl-westerr.nnt
 Basics Fronte Create routing rules that I Pul We Click 4 Name Give it 	nds ✓ Backends O Configuration (3) ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- steur-001 (20.224.128.108) "Add a routing rule". e it. t a priority of 100.	P Tags • Review + create d nore backend pools, add a second frontend IP configuration if you haven't alreation Routing rules Routing rules Routing rules	ady, or edit previous configurations. Backend pools + Add a backend pool agw-imagesgallery- backendnool-wester + 001
 Basics Create routing rules that I Put Put Put Click 4 Name Give it 	nds V Backends O Configuration (3) ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- streu-001 (20.224.128.108) "Add a routing rule". t a priority of 100.	P Tags Review + create d more backend pools, add a second frontend IP configuration if you haven't alreation. Routing rules Add a routing rules Routing rules Routing rules	ady, or edit previous configurations. Dackend pools + Add a backend pool agw-imagesgallery- backendonol-wester + 001
 Basics Create routing rules that I Pul we Click 4 Name Give it 	nds V Backends O Configuration (3) ink your frontend(s) and backend(s). You can also ad Frontends + Add a frontend IP blic: agw-imagesgallery-ip- streu-001 (20:224 128 108) "'Add a routing rule". e it. t a priority of 100.	Tags	ady, or edit previous configurations. Dackend pools + Add a backend pool agw-imagesgallery- backendnonl-westerr.001



- Add a "Listener" and associate HTTPS protocol and port 443 with it.
- Select "Choose a certificate from Key Vault".
- Select the AMI and Keyvault.
- Paste the certificate's secret ID URL.

Microsoft recommends that in this regard, only the path to the certificate should be given, without its ID. This makes it easier to renew the certificate.

- Create a new "Backend setting".
- Name it.
- Select HTTPS protocol and port 443.
- Select "Yes" the "Use well known CA certificate".

Configure a routing rule to send traff listener and at least one backend tar	ic from a given frontend IP address to one or more backend targets. A routing rule must contain a get.	Add Backend settin	g	×
Rule name *	agw-imagesgallery-rules-westeu-001	← Discard changes and go back to re	puting rules	
Priority * ① *Listener *Backend targets	100	Backend settings name * Backend protocol Backend port *	agw-imagesgallery-backendsettings-westeu-001 HTTP () HTTPS 443	~
A listener "listens" on a specified po gateway will apply this routing rule.	rt and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application	Trusted root certificate For end-to-end SSL encryption, the b servers to this Backend setting.	ackends must be in the allowlist of the application gateway. Upload the public	certificate of the backend
Listener name * () Frontend IP * () Protocol ()	Public V	Use well known CA certificate Additional settings	• Yes No	
Port * ① Https Settings	443	Cookie-based affinity Connection draining	Enable Disable Enable Disable Disable	
Choose a certificate Cert name *	Upload a certificate O Choose a certificate from Key Vault	Request time-out (seconds) * ① Override backend path ①	20	
	ami-westeu-001	Host name By default, Application Gateway does backend, Multi-tenant services like A	: not change the incoming HTTP host header from the client and sends the head pp service or API management rely on a specific host header or SNI extension t	der unaltered to the o resolve to the correct

The routing rule and its parameters

The health probe

The health probe is used to monitor and test that the gateway application is working properly.

- Create a health probe ("probe-health").
- Name it.
- Very important! Give the "host", the name of your application on the certificate. In my case, this one is "docker.fuyens.ch".



- Select "No" for the "Pick host name from backend settings".
- Select "Yes" for the "Pick port from backend settings" option.
- Enter "/" for the ("path").
- Select the backend settings.
- Leave the other options as default.
- Check "I want to test the backend health before adding the health probe".
- Click **"Test"**.

Name	cert-imagesgallery-probe-westeu-001	
Protocol *	O HTTP 💿 HTTPS	
Host * ①	docker.fuyens.ch	
Pick host name from backend settings	🔿 Yes 💿 No	
Pick port from backend settings	• Yes O No	
Path * ①	/	
Interval (seconds) * 🕕	30	
Timeout (seconds) * 🕕	30	
Unhealthy threshold \star \bigcirc	3	
Use probe matching conditions	🔿 Yes 💿 No	
Backend settings ①	cert-imagesgallery-backendsettings-westeu-001	
✓ I want to test the backend h Test Discard	ealth before adding the health probe	
	Health Probe Creation	



The result should be a green check mark.

If not, check your certificate name, which should match the probe. If it still doesn't, go back to the Keyvault and temporarily allow Microsoft services to access it.

 Exception

 Allow trusted Microsoft services to

 bypass this firewall

 Image: Comparison of the service of the servic

• Test the probe one last time by clicking on **"backend health"** and make sure you have the green check mark.

Restrict access to the application.

Now that the infrastructure has an "application gateway", we can close public access to the application.

- Return to **"App services"**.
- Click "Networking".
- Click "Access restriction".
- Add a rule that only allows the application gateway subnet to access the application.



		Sedit Access Restriction ×
		General settings
Deployment slots		Name
Deployment Center	Inbound Traffic Manage access and incoming services.	agw-access
ettings		
Configuration		Priority *
Authentication	Features	300
Application Insights	🌏 Access restriction 🛛 🥥 On	
ldentity	App assigned addr O Off	Action
🕈 Backups	<i>> Private endpoints</i>	Allow Deny
Custom domains		
TLS/SSL settings	Inbound address	Description
TLS/SSL settings (preview)	20.50.2.85	agw-access
🔋 Networking		
Scale up (App Service plan)		Source settings
Scale out (App Service plan)		Subscription *
B WebJobs		Fuyens Subscription 🗸 🗸
Push		Virtual Network *
		vnet-frontend-westeu-001 🗸
		Subnet *
		snet-appgateway-westey-001

Application-level access restriction

Conclusion

Here it is, this long publication is now complete. It validates all of my research and various tests I undertook to build a secure infrastructure around an application that uses **"PaaS"** services on Microsoft's Azure cloud. I also covered the use of containers with Docker and the use of SSL certificates.