SOP Onboard New Application to existing Application Gateway

Status of SOP:

Endorsed

Related Platform	Component
Azure	Azure Application Gateway

POSSIBLE CAUSE:

- Service request from application team to upload SSL certificate for new application (Onboard New Application)

This kind of request comes if: -

A new application needs to be onboarded to application gateway then its certificate will be uploaded in application gateway repo.

Problem

How to onboard new application to an existing application gateway?

OR

How to upload SSL certificate for new application?

PROCESS:

Raise a Normal Change Request

Open a Normal Change Request to implement the SR. Please go to page 20 of the below *Change Control document* :

Service Management: As-Is Change Management (ServiceNow)

Please select the respective Cloud Factory assignment group when raising a change request in Service Now

Cloud Network - Hub Connectivity - Azure

WORKFLOW OF THE SNOW REQUEST

Verify the SNOW request for below points:

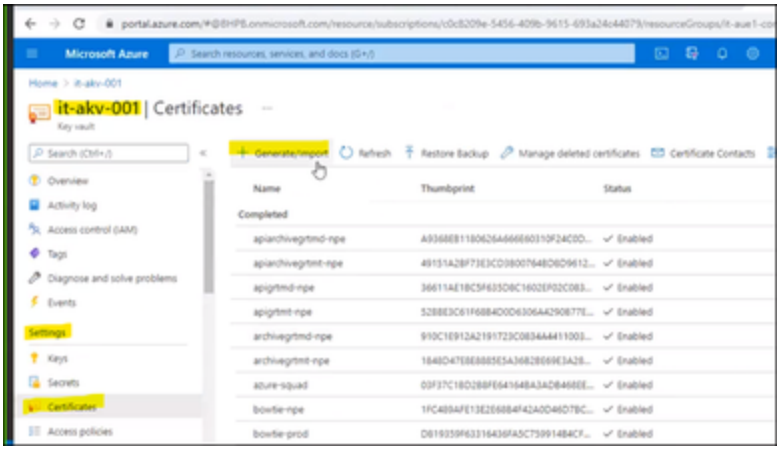
- Certificate should be attached by the user in SR along with application name, application gateway
- Certificate should be attached by user in **.pfx** format

If user hasn't provided the password for certificate proactively, drop an email to user for the password. This password would be used while importing the certificate in Key Vault.

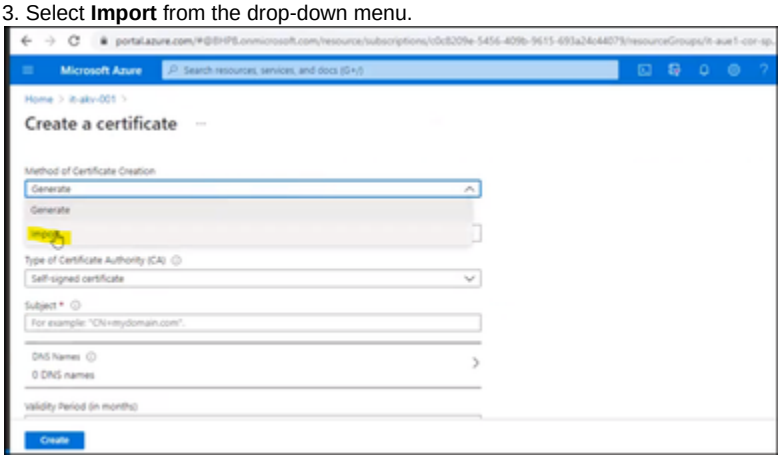
Solution

1. Go to Azure portal and search for ***it-akv-001*** Key vault which is present in **BHP-Technology-Shared Services** subscription.

2. Go to **Certificates** under **Settings** and click on **Generate/Import** to import the certificate.



3. Select **Import** from the drop-down menu.



4. Fill in the certificate name in below format:

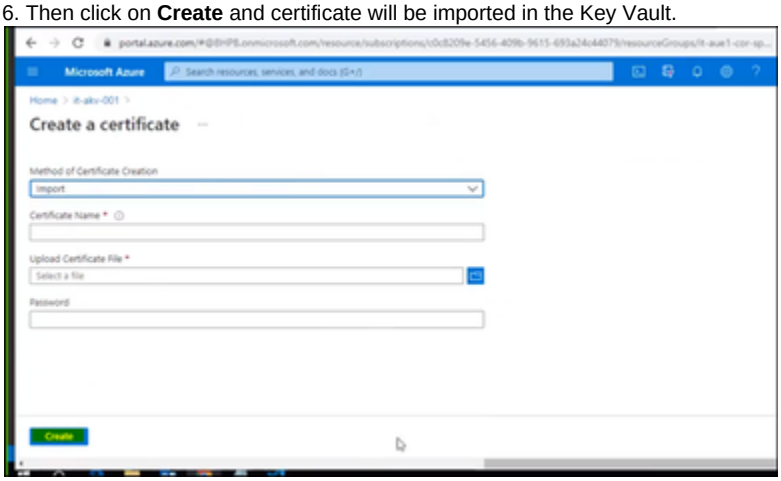
ApplicationName-npe/prod

For e.g. abc-npe, abc-prod

Here npe stands for Non-Prod

5. Browse the .pfx file from your local computer and type in the password shared by the user to import the certificate.

6. Then click on **Create** and certificate will be imported in the Key Vault.



7. Click on **Certificate Name (Fig a)** and then **CURRENT VERSION (Fig b)**.

Fig (a)

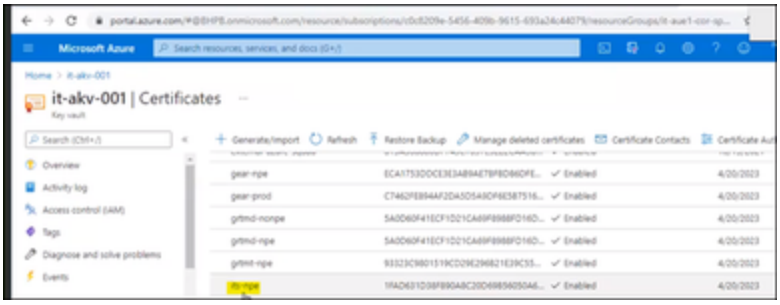
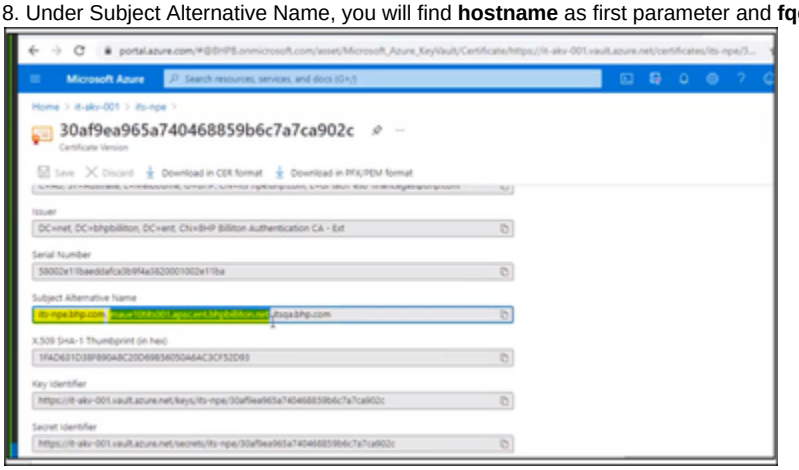


Fig (b)

8. Under Subject Alternative Name, you will find **hostname** as first parameter and **fqdn** as second parameter. Copy both values.



9. Choose the Application Gateway repo based on the type of application.

- If the application is internet facing, go to below external-ingress gateway repo:

  https://gitlab.com/bhp-cloudfactory/azure-foundations/external-ingress

- If its an internal application, go to below internal-ingress gateway repo:

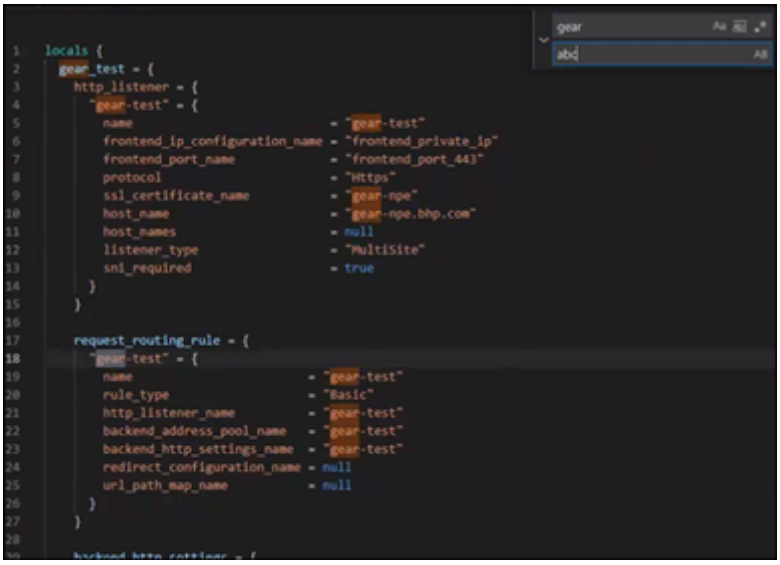
  https://gitlab.com/bhp-clodfactory/azure-foundations/internal-ingress

10. Since its new application onboarding, we need to create the .tf file for the new application in the desired application gateway repo which we selected in last step.

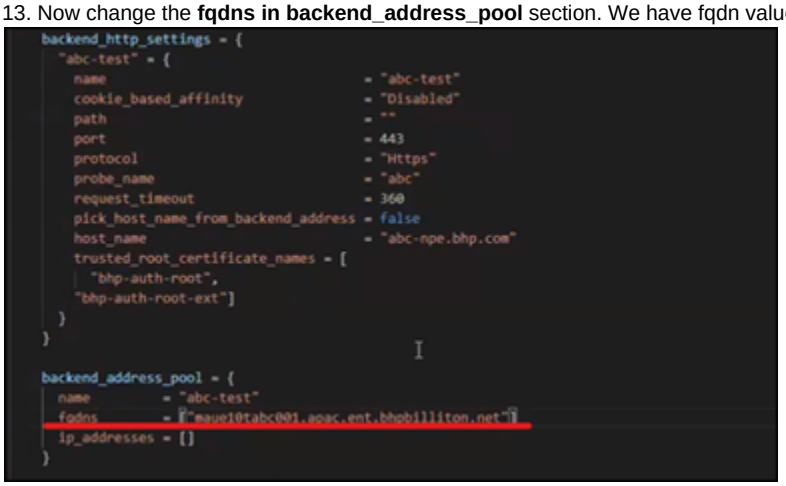
11. If its non-prod application, copy any application test.tf file or if its prod, copy prod.tf file. Change the name of newly create file as per the requested application. For e.g. if the name of new application is **“abc”** and its non-prod, then file name would be:

abc-test.tf

12. Since we have **abc-test.tf** file created in last step, now modify its content. Open this file and replace all occurrences of other application name with new application name (Here its **abc**). For example, if we have copied **gear non-prod** application file then replace all occurrences of **ge ar** with **abc.**



13. Now change the **fqdns in backend_address_pool** section. We have fqdn value from **STEP h**



14. Now make the changes in corresponding region files (**meta files**).

For Non-Prod application, below meta files will be modified

meta_aue1_npe.tf

meta_ause1_npe.tf

For Prod application, below meta files will be modified

meta_aue1.tf

meta_ause1.tf

Sections which would be modified in the meta files are:

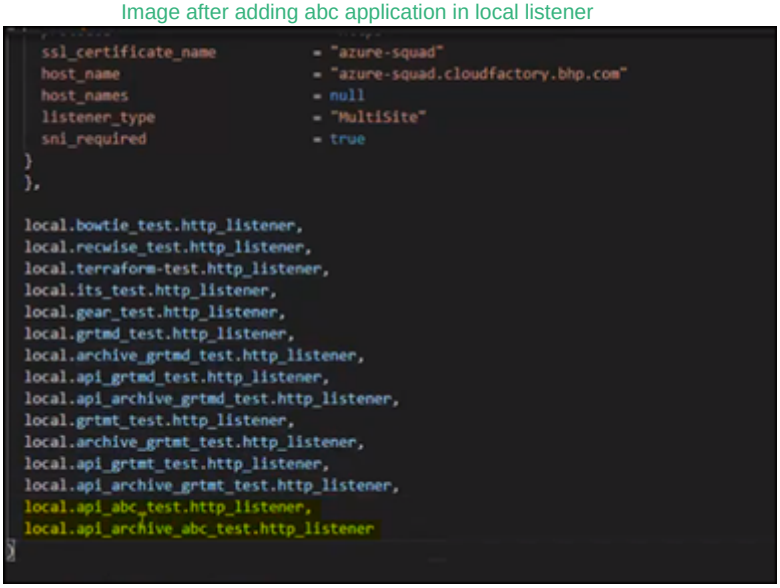
- http_listener

- request_rotuing_rule
- backend_http_settings
- backend_address_pools
- probes

Under these sections add corresponding new application values for **local.** Sample screenshot for **http_listener section** is given below:

Image before adding new application abc values

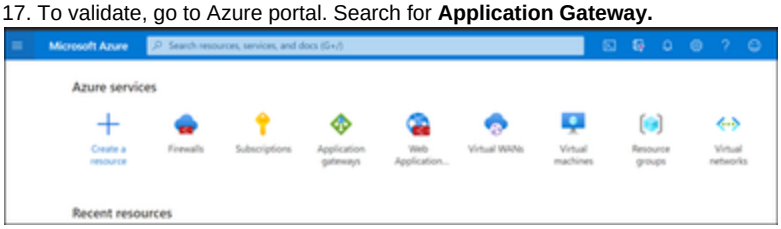
Image after adding abc application in local listener



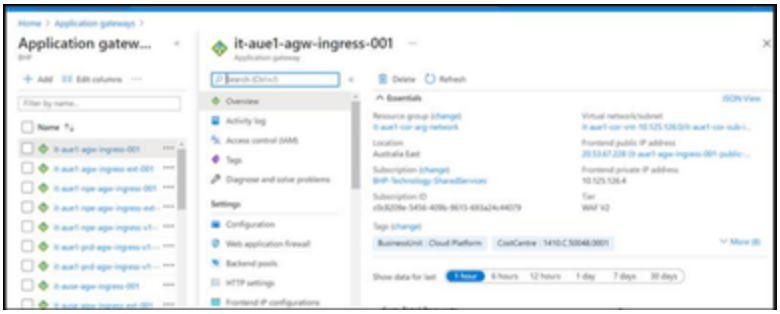
15. After you make the changes in the files, respective workspace workflow will be triggered.

16. Go to Terraform workspace and apply the changes.

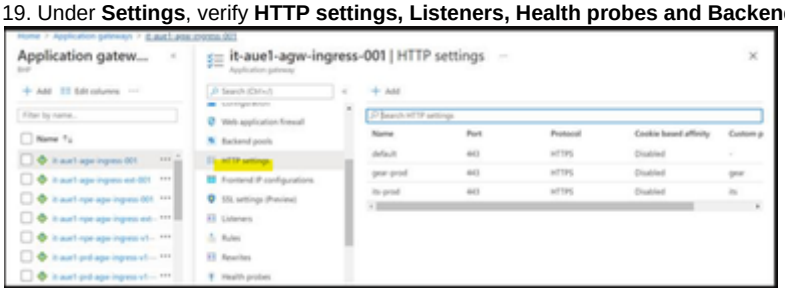
17. To validate, go to Azure portal. Search for **Application Gateway.**

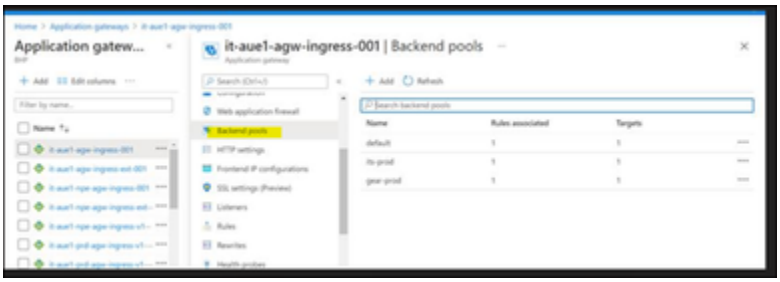


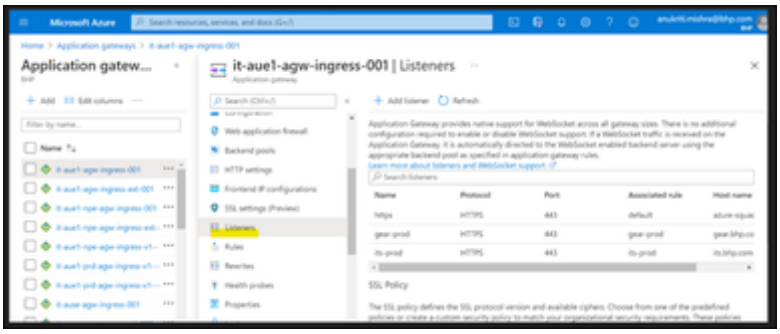
18. Select the desired App Gateway.

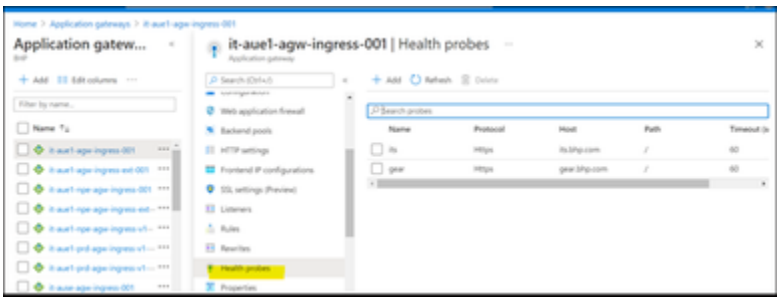


19. Under **Settings**, verify **HTTP settings, Listeners, Health probes and Backend pools for** the required application.









Related articles

- AWS VPC Endpoints configuration change
- Monitoring GitLab Access Audit Report
- Renewal / Upload SSL certificate for existing Application

- Update the Task memory unit
- Update the Task CPU limit