SOP Upload SSL certificate for an existing Application

Status of SOP:

Endorsed.

Related Platform	Component
Azure	Azure Application Gateway

POSSIBLE CAUSE:

- Service request from application team to upload new SSL certificate for an existing application.

This kind of request comes if: -

There is a hostname update or FQDN change in an existing application, then new certificate with updated details needs to be updated in application gateway repo.

Problem

How to upload SSL certificate for an existing 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:

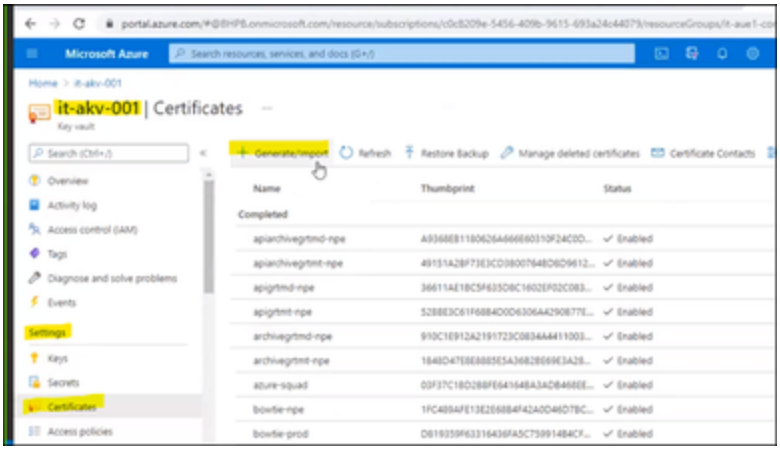
- Certificate should be attached by the user in SR along with application name, application gateway
- Certificate should be attached by user in **.pfx** format

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.

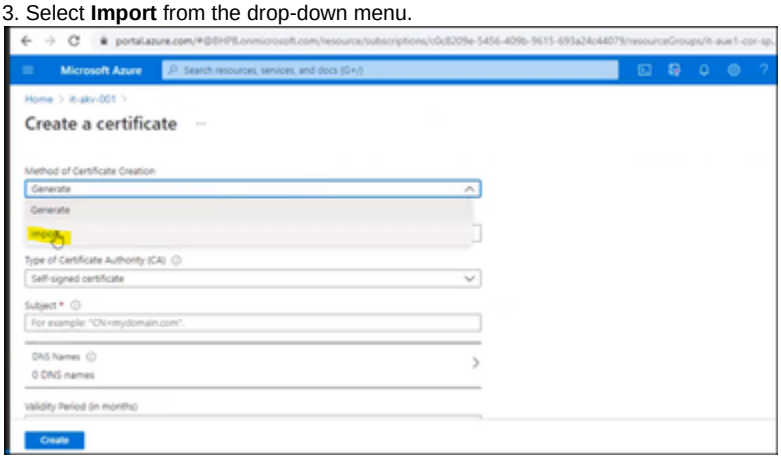
Solution

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.



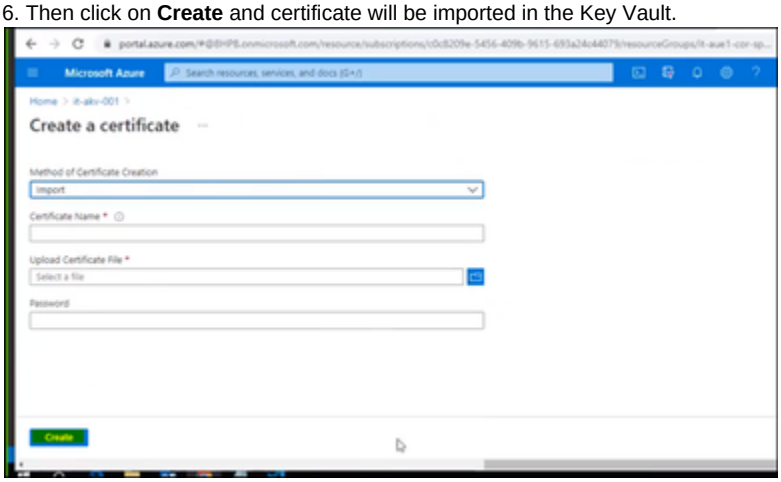
4. Fill in the certificate name in below format:

- npe/prod-applicationName

  Here npe stands for Non-Prod

5. Browse .pfx file from your local computer and type in the password shared by the user for 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)

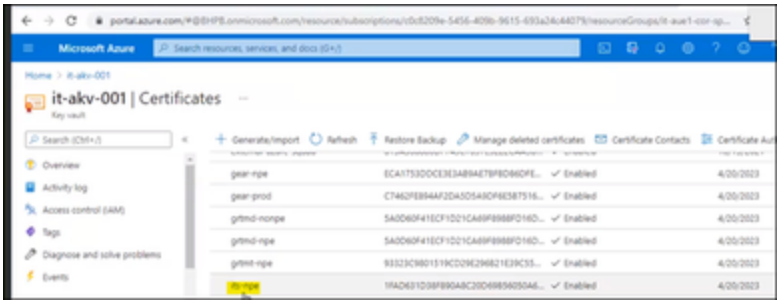
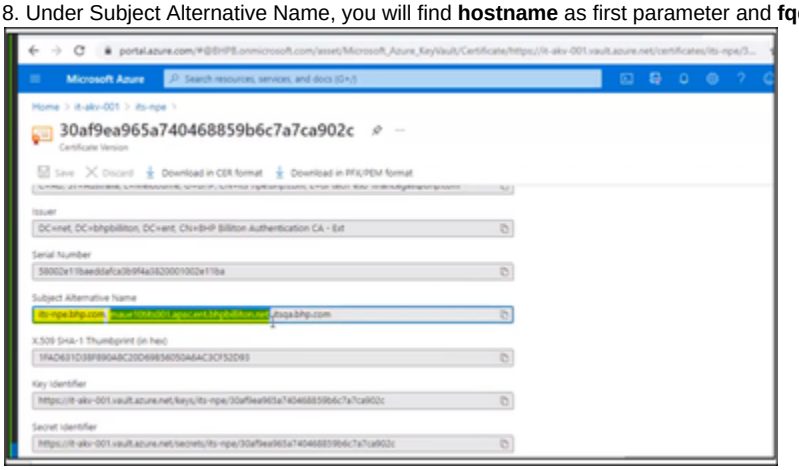


Fig (b)

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.

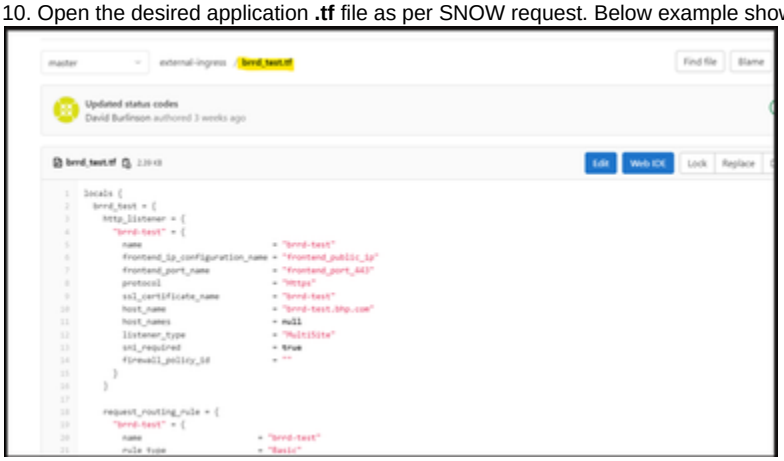
- If the application is internet facing, go to below external-ingress gateway repo:

  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. Open the desired application **.tf** file as per SNOW request. Below example shows a non-prod application file.



11. In this file replace the value of all occurrences of below parameters with the hostname value which you copied in ***STEP h***

- host_name
- host

Then replace the value of **fqdns** in **backend_address_pool** section with new **fqdn** value which was copied in **STEP h**

```
backend_address_pool = {
  name         = "gear-test"
  fqdns        = ["maue10tgea001.apac.ent.bhpbilliton.net"]
  ip_addresses = []
}

probe = {
  name                                      = "gear"
  path                                      = "/"
  interval                                  = 120
  protocol                                  = "Https"
  timeout                                   = 60
  unhealthy_threshold                       = 3
  host                                      = "gear-npe.bhp.com"
  pick_host_name_from_backend_http_settings = false
  match = {
    enabled     = true
    body        = ""
    status_code = ["200", "302"]
  }
```

12. After you make the changes in the file, respective workspace workflow will be triggered.

13. Go to Terraform workspace and apply the changes.

14. Go to Azure portal to validate the changes.

15. Drop an email to Application team to validate the application functionality.