**3 node type service fabric environment in Azure with an application gateway**

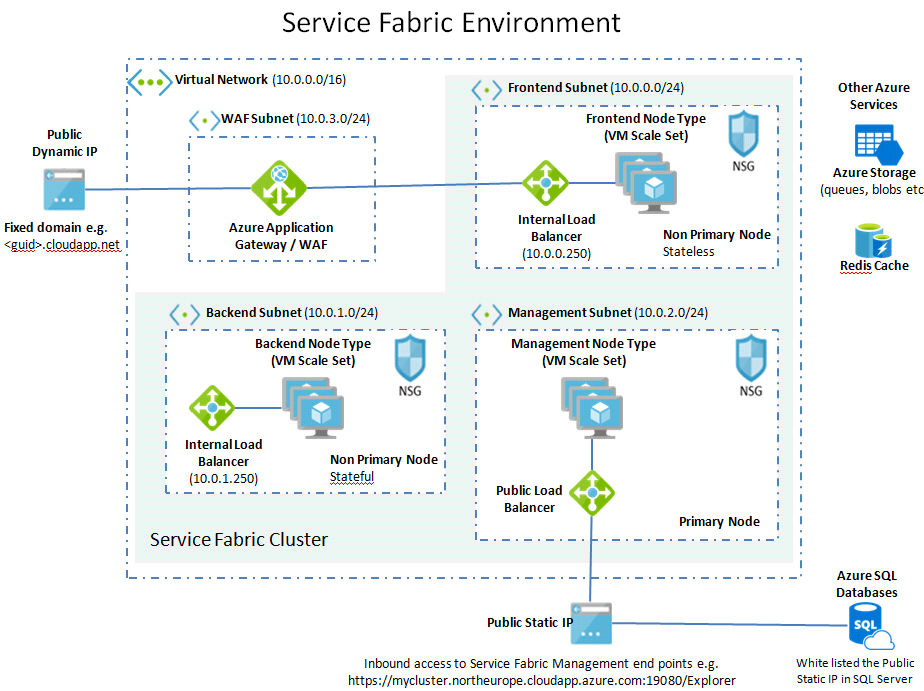
This script/ARM template will create a service fabric environment in Azure which contains 3 node types, FrontEnd, BackEnd, and Management. The idea for this originally came from:

<https://brentdacodemonkey.wordpress.com/2016/08/01/network-isolationsecurity-with-azure-service-fabric/>

But we will put an Application Gateway in front which all internet traffic can be routed through to the FrontEnd node. And will be using an existing Virtual Network and Subnets to deploy service fabric into.

The template originally came from the Azure Portal when creating a new service fabric cluster there is the option of saving it as a template. It was then customised as the portal wizard does not let you do certain things. Most of the customisations came from this site: <https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-patterns-networking>

This is what we will build:



The FrontEnd node type is where we put any stateless services.

The BackEnd node type is where we would put any stateful services.

The Azure service fabric services will run on the Management / Primary node type.

* This has a public static outbound IP number, so we can connect to view the status of the cluster.
* It can also host services which need to connect out to a third party which have IP security on their firewall. The third party then only needs to add this IP number to their firewall.
* We can also use this to securely access an Azure SQL database that has IP restricted access.

The steps below are my notes for creating the service fabric environment:

1. **Create Service Fabric dependencies.**

* Public Static IP (for Management nodeType)
* Key Vault (for service fabric certificates)
* Active Directory Application (for authentication)
* Resource Group to put service fabric cluster in
* Existing Virtual Network with 4 subnets for:
  + FrontEnd
  + BackEnd
  + Management
  + WAF / Application Gateway

Edit & change the parameters as required in this script:

Azure-CreateDependanciesForServiceFabricPlatform.ps1

Execute the script

*Note: this script will prompt you yes/no to create each of the above items.*

If you’re creating a non-development version we do not want to use a self-signed certificate so say ‘no’ when prompted. After the script has run you then need to manually add certificates into the key vault. Details here:

<https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-creation-via-portal#add-certificates-to-key-vault>

<https://blogs.technet.microsoft.com/kv/2016/09/26/get-started-with-azure-key-vault-certificates/>

1. **Create the Service Fabric Environment**

This will create a 3 nodeType service fabric environment FrontEnd, Backend and Management nodeTypes.

The management node type is set as the Primary.

*Note the NSG’s are not assigned to the Subnet but they are created by the script.*

Go to folder:

secureTemplateAnd3NodeTypeWithApplicationGatewayAndExistingSubnet

Copy the parameters.json file and then change the parameters.

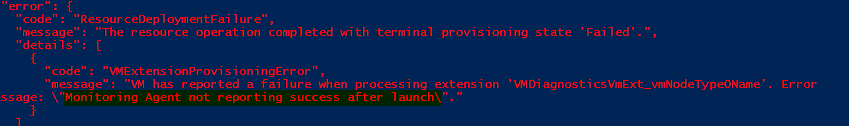
Note: By default the script creates the minimum number of VM’s all at Standard A0 size. If this is a non-development environment you will want to change the VM size to be:

* Minimum number of instances
  + Set to 5 on Management/Primary node type
  + Set to 5 on Backend node type (stateful)
  + Set to 2 on Frontend node type (stateless)
* Size (set to Standard D1\_V2 the minimum supported spec for all node types)
* Reliability Level of the cluster should be minimum of Silver in production (default is Bronze)
  + Static IP parameters (change to match those you just setup):
    - existingStaticIPResourceGroup
    - existingStaticIPName
    - existingStaticIPDnsFQDN
  + Specifiy the existing Virtual network and subnet names:
    - virtualNetworkName
    - existingVNetRGName
    - subnet0Name
    - subnet1Name
    - subnet2Name
    - subnetWAFName
  + Active Directory parameters (change to match those you just setup):
    - aadTenantId
    - aadClusterApplicationId
    - aadClientApplicationId
  + Certificate parameters (change to match those you just setup):
    - SourceVaultValue
    - certificateUrlValue
    - certificateThumbprint
  + VM login parameters (used if you ever need to RDP into a cluster machine):
    - adminUserName
    - adminPassword
  + Other parameters

Execute the deploy script:

.\deploy.ps1 -subscriptionId <yourAzureSubscriptionIdHere> -resourceGroupName mycluster -deploymentName mycluster -parametersFilePath .\parameters.json

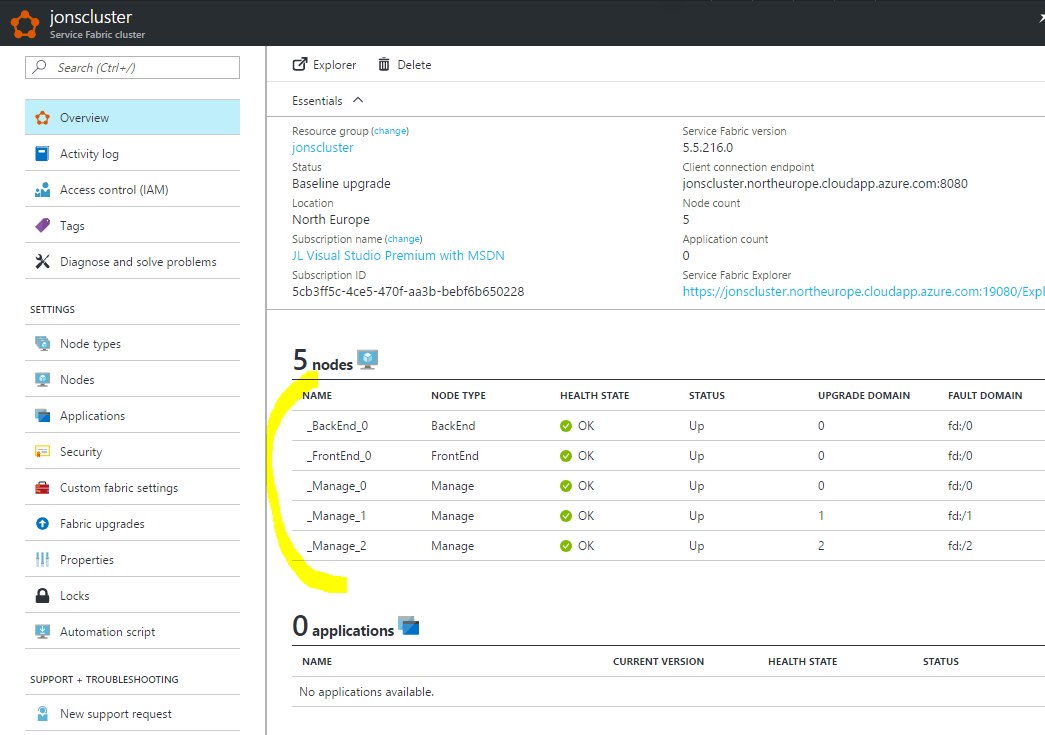
If after a long time it errors with this message ‘Monitoring Agent not reporting success after launch’



Then you should be fine as Service Fabric will automatically recover the nodes that this failed for.

1. **After deployment**

Go to the Azure portal and find your service fabric cluster and you should eventually see the nodes (they may take some time to appear).



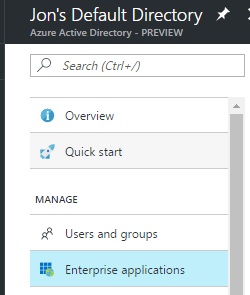
Once the deployment has finished and you can see in the Azure Portal that the nodes in the cluster are running you should be able to view the cluster e.g.

https://jonscluster.northeurope.cloudapp.azure.com:19080/Explorer

This should prompt you to login. If you see a message:

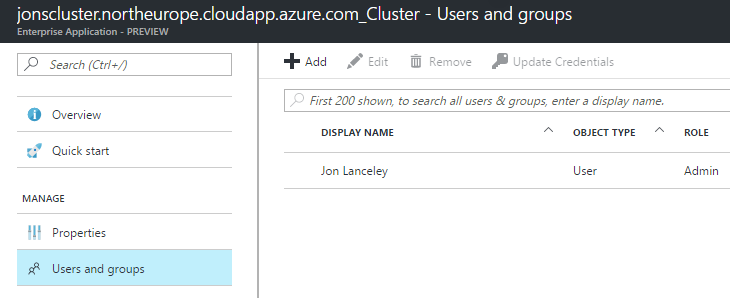
AADSTS50105: The signed in user 'jon.lanceley\_xxxxxxxxx.com#EXT#@jonlanceleyxxxxxxxx.onmicrosoft.com' is not assigned to a role for the application '9df93f43-6682-4004-addd-1522a4e13439'.

Go to Azure Active Directory -> Enterprise Applications -> All Applications

****

Find the cluster server application (not the client one)

Add the user as an Admin

****