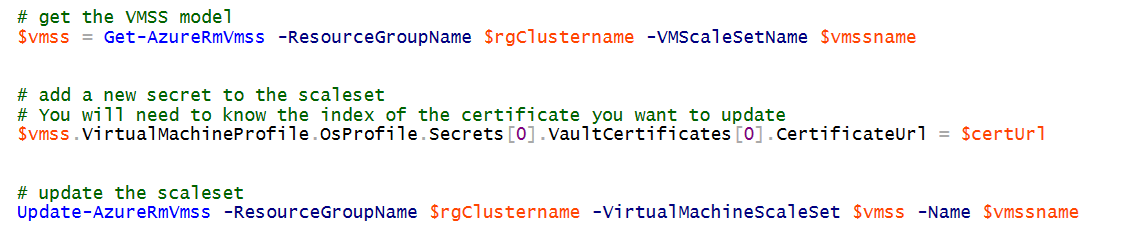
1) Keyvault certificate stored on the VM scaleset.



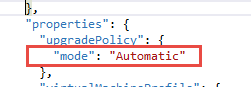
You will need to know the secret URL for the new certificate and the index of the certificate as it sits on the nodes.

If you are not sure what the index is of the certificate you want to replace, you will at least need to know the current certificate secret URL. If you execute the following PowerShell command:

$myURL = $vmss.VirtualMachineProfile.OsProfile.Secrets[x].VaultCertificates[x].CertificateUrl

As you go through the different index values, $myURL will contain the current secret URL.

If your scale set is set to automatically update, when you execute the **Update-AzureRmVmss** command, all nodes will be updated. You can look in the ARM script (click on your cluster scale set name) and find this property.



One thing to note here, the commands above will not delete the certificate from the node, it simply replaces the secret url in the list of secrets associated with that node. You would need to manually remove the old certificate from the machine.

You can also invalidate a certificate (secret URL) in the vault just to make sure no one else uses it by running the **Set-AzureKeyVaultSecretAttribute** command like:  
  
Set-AzureKeyVaultSecretAttribute -VaultName contosovault -Name servicecert-Version e3391a126b65414f93f6f9806743a1f7 -Enable 0

2) Key vault certificate update in Key Vault

Update the value of the key vault secret primaryKeyVaultCertificate and secondaryKeyVaultCertificate to point to the new value in the below JSON format.  It is the Base64 encoding of the following JSON Object which is encoded in UTF-8:

{

"data":"",

"dataType":"pfx",

"password":""

}