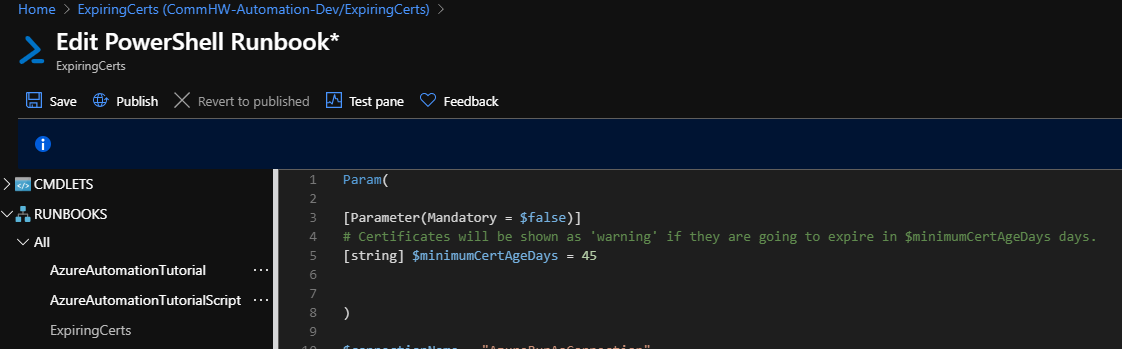
**Usage of Azure Certificate Scanner**

**Azure Cert Scanner:**

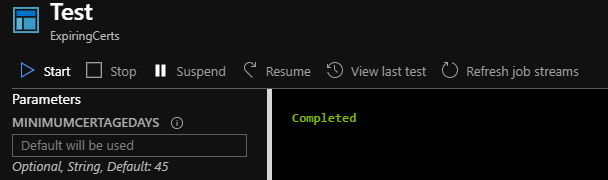
This scanner is a PowerShell script that can be run as an automation account to scan across the resource groups under the subscription.

Follow the below onetime setup steps to scan and report the certificates & its details used across resource groups

1. Setup Azure Automation account -
   1. Create an Automation account ex: ‘CommHW-Automation-Dev’
   2. Setup Run As account to use in Automation Runbooks (needs owner permissions) ex: ‘AzureRunAsConnection’
2. Copy the embedded Script to Check Expiring Certificate and create as a new runbook under the automation account
   1. This script which takes number of days as an input (days before the certificate expiry to send email)
   2. Uses Run AS Account that you created in step 1 so no specific user credentials required
   3. The scripts scan all the certificates in all resource group of the subscription.



1. After the runbook is created click on edit 🡪 TestPane 🡪 Start.
   1. You can enter number of days as input, if not entered it takes 45 days.
   2. Click on start to scan the certificates.



* 1. Once the scan is completed you will see the below kind of result.
  2. The plain text one is like ‘information’ kind with what certificate referred in what resource group and expires in how many number of days
  3. The red colored ones are like ‘warning’ kind if the certificate is going to expire with in the input parameter ‘number of days’ (by default 45 days). It also gives resource group in which its referred.

