Using SSL for Remote PowerShell in GreenLight

The following GreenLight article explains briefly what kind of steps you have to perform in order to use SSL (https via tcp 5986) for PowerShell.

example is based for using a self-signed certificate on the Windows Host

Configuration

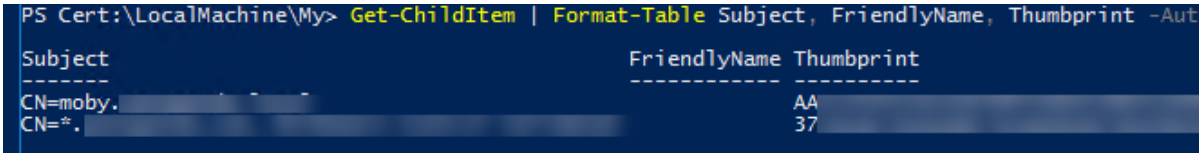
Enabling RemotePowerShell (unencrypted communication should not be allowed in this UseCase)

- Open PowerShell on Windows Host and execute the following 4 commands
  - Enable-PSRemoting –force
  - set-item -force WSMan:\localhost\Service\Auth\Basic $true
  - set-item -force WSMan:\localhost\Client\AllowUnencrypted $false
  - set-item -force WSMan:\localhost\Service\AllowUnencrypted $false

Check if there are already Certificates in the Certificate Store (open Powershell on Host)

- Set-Location Cert:\LocalMachine\My
- Get-ChildItem | Format-Table Subject, FriendlyName, Thumbprint -AutoSize

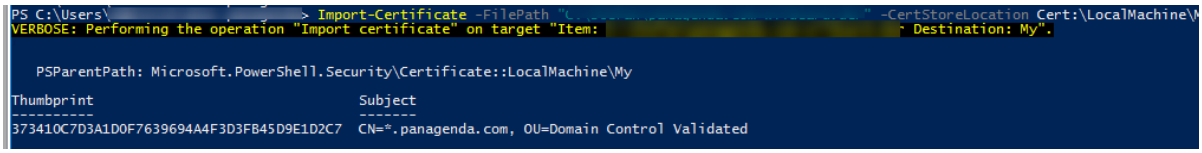
you should get a list of certificates back (otherwise the list is just empty)



Import Certificate (with PowerShell) - CER

- Import-Certificate -FilePath "<path to certificate>" -CertStoreLocation Cert:\LocalMachine\My -Verbose

you should get something like this



For PFX, use the command

Import-PfxCertificate -FilePath "<path to pfx>" -CertStoreLocation Cert:\LocalMachine\My -Verbose

Create Self Signed Certificate

- New-SelfSignedCertificate -DnsName <hostname> -CertStoreLocation Cert:\LocalMachine\My

Now we have imported or created a selfsigned certificate which can be used for the Remote PS Call

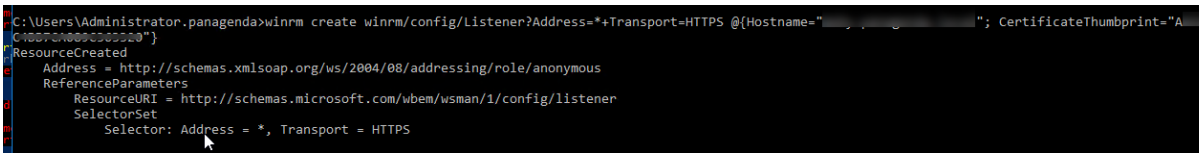
Next Steps explain how you connect the certificate with the WS-MAN remoting

Copy the correct Thumbprint from Store

- *Get-ChildItem | Format-Table Subject, FriendlyName, Thumbprint -AutoSize*
- copy the ThumbPrint you want to use

Open command prompt (**with cmd**)

- *winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>"; CertificateThumbprint="<your thumbprint >"}*



This binds now the certificate with HTTPS on the Host

Please adjust the Address and Hostname parameter based on your needs! If you use a Wildcard SSL certificated, make sure that hostname is equal the CN name in the certificate

In case a listener with the same Address and HTTPS is configured, please make sure you clean it up first

You can remove an existing entry (for Address=* and Transport HTTPS) by just using

- *winrm delete winrm/config/Listener?Address=*+Transport=HTTPS*

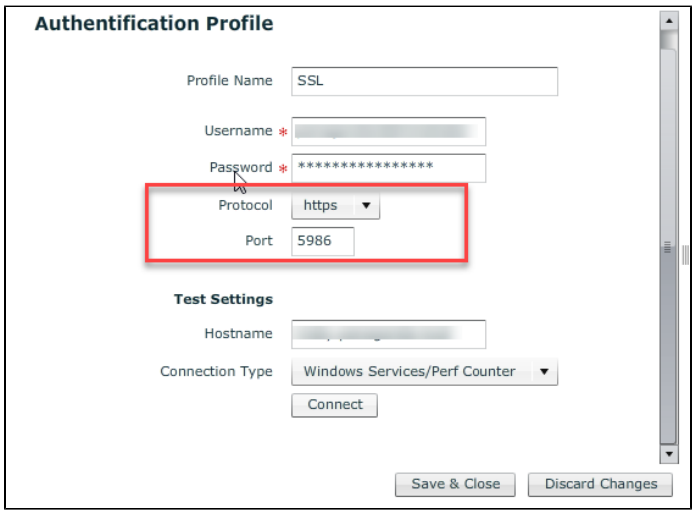
Inbound Firewall Setting

Make sure that Inbound connection to TCP Port 5986 is allowed on the Windows Host !

Last Step is the GreenLight Config

The Only thing which you need to do is to configure the right Authentication Profile

Use https as the protocol and Port 5986



Test the Connection ....If everything is correct, you should get a "Success Message" back

Assign this Authentication Profile now to an Windows Host within GreenLight