

# Replacing STS Certificate on vCenter Server

## Steps for vCenter Server Appliance (VCSA)

1. Download the script "**fixsts.sh**" from the KB <https://kb.vmware.com/s/article/76719>

"Signing certificate is not valid" X

https://kb.vmware.com/s/article/76719

## "Signing certificate is not valid" - Regenerating and replacing expired STS certificate using shell script on vCenter Server Appliance 6.5/6.7 (76719)

Last Updated: 7/8/2020 Categories: Troubleshooting 24 Language: English subscribe

### ✓ Symptoms

- vCenter/PSC Services do not start due to expired certificate showing the following errors:  

```
Path: /var/log/vmware/vpxd-svcs/vpxd-svcs.log
ERROR com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl$RequestResponseProcessor opId=]
Server rejected the provided time range. Cause:ns0:InvalidTimeRange: The token authority rejected
an issue request for TimePeriod [startTime=Thu Jan 02 09:22:13 EST 2020, endTime=Fri Jan 03
09:22:13 EST 2020] :: Signing certificate is not valid at Thu Jan 02 09:22:13 EST 2020, cert
validity: TimePeriod [startTime=Wed Jan 06 20:44:39 EST 2010, endTime=Wed Jan 01 20:54:23 EST
2020]
```

Note: The endTime should be a date in the past if the certificate is expired.
- The following error is observed when logging into the Web Client:  

```
HTTP Status 400 - Bad Request Message BadRequest, Signing certificate is not valid
```
- Accessing WebClient or UI Client will show below error message if vmware-vpxd service is not running due to expired certificate  

```
503 Service Unavailable (Failed to connect to endpoint:
[N7Vmacore4Http20NamedPipeServiceSpecE:0x00007fb444041040] _serverNamespace = /
action = Allow _pipeName =/var/run/vmware/vpxd-webserver-pipe)
```

#### Additional Resources

#### Related Products:

VMware vCenter Server Appliance  
VMware vCenter Server

#### Related Versions:

VMware vCenter Server Appliance 6.7.x  
VMware vCenter Server Appliance 6.5.x  
VMware vCenter Server 7.0.x  
VMware vCenter Server 6.5.x  
VMware vCenter Server 6.7.x

#### Actions

Copy link to clipboard  
Print  
Language: English

#### Attachments

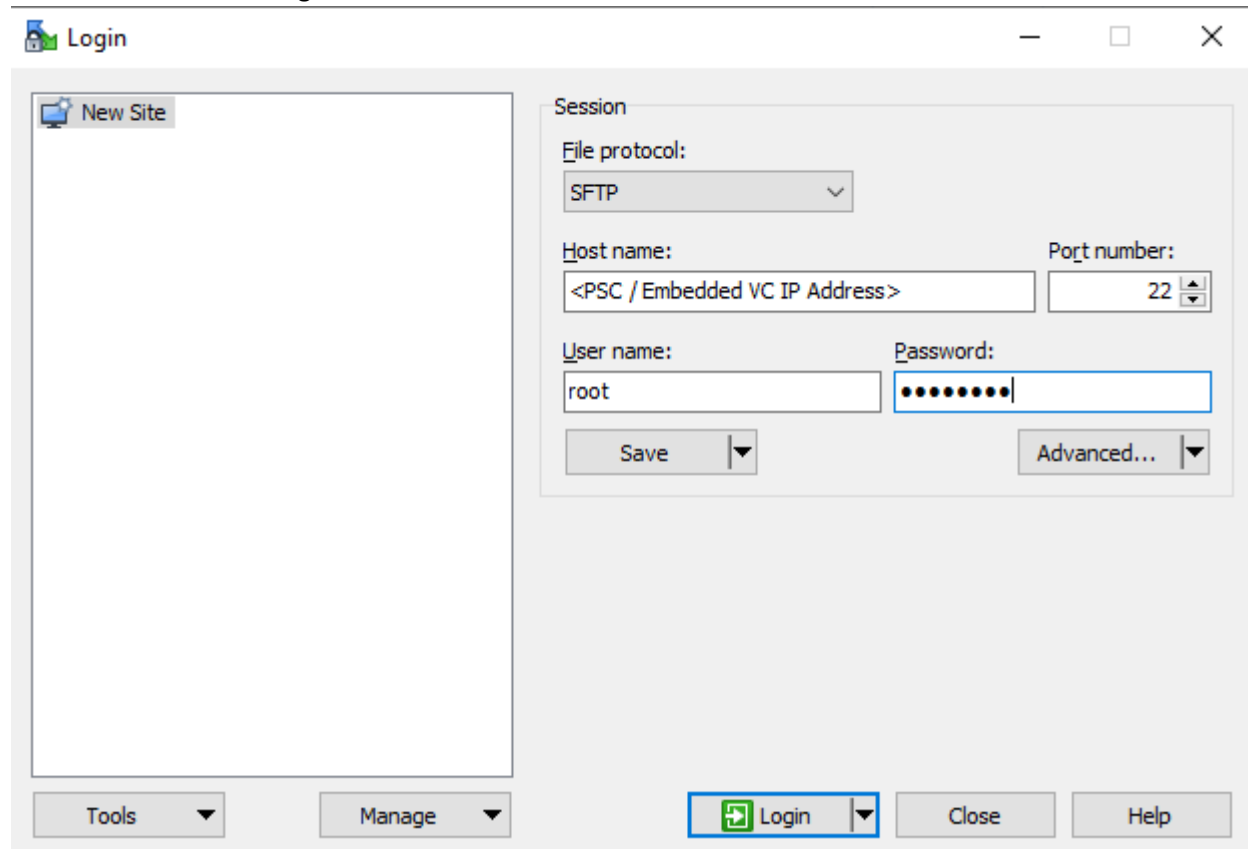
fixsts

2. Upload the script to VCSA using WinSCP

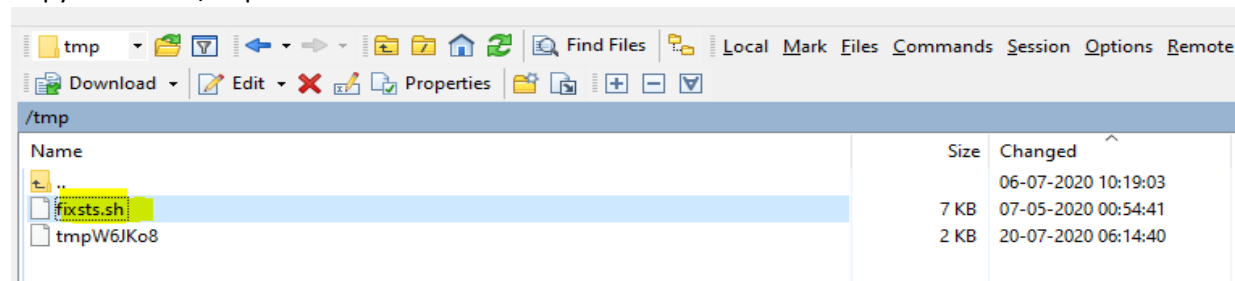
- a. Change Shell to Bash by following KB <https://kb.vmware.com/s/article/2107727>

```
root@vcsa1 [ ~ ]# chsh -s /bin/bash root
root@vcsa1 [ ~ ]#
```

- b. Connect to vCenter using root account



- c. Copy the file to /tmp



3. Change file permission using command **chmod +x fixsts.sh**

```
root@vcsal [ /tmp ]# chmod +x fixsts.sh
root@vcsal [ /tmp ]#
```

4. Execute the shell script “./fixsts.sh”, enter the SSO Administrator (Eg. [Administrator@vsphere.local](mailto:Administrator@vsphere.local)) password when prompted

```
root@vcsal [ /tmp ]# ./fixsts.sh
NOTE: This works on external and embedded PSCs
This script will do the following
1: Regenerate STS certificate

What is needed?
1: Offline snapshots of VCs/PSCs
2: SSO Admin Password
=====
Resetting STS certificate for vcsal started on Tue Jul 28 22:00:09 UTC 2020

Detected DN: cn=is-static45-62.isl.vmware.com,ou=Domain Controllers,dc=vsphere,d
c=local
Detected PNID: is-static45-62.isl.vmware.com
Detected PSC: is-static45-62.isl.vmware.com
Detected SSO domain name: vsphere.local
Detected Machine ID: c20f2099-2bfc-4ca3-b501-e9elafefe2a0
Detected IP Address: 10.109.45.62
Domain CN: dc=vsphere,dc=local
Detected Root's certificate expiration date: 2028 May 2
Detected today's date: 2020 Jul 28

Exporting and generating STS certificate
Status : Success
Using config file : certool.cfg
Status : Success

Enter password for administrator@vsphere.local:
Amount of tenant credentials: 1
Exporting tenant and trustedcertchain 1 to /var/tmp

Deleting tenant and trustedcertchain 1

Applying newly generated STS certificate to SSO domain
adding new entry "cn=TenantCredential-1,cn=vsphere.local,cn=Tenants,cn=IdentityManager,cn=Services,dc=vsphere,
dc=local"

adding new entry "cn=TrustedCertChain-1,cn=TrustedCertificateChains,cn=vsphere.local,cn=Tenants,cn=IdentityMan
ager,cn=Services,dc=vsphere,dc=local"

Replacement finished - Please restart services!
root@vcsal [ /tmp ]#
```

5. Restart the services on vCenter Server using service-control --stop --all && service-control --start --all

```
Replacement finished - Please restart services!  
root@vcsal [ /tmp ]# service-control --stop --all && service-control --start --all
```

6. Just in case, if services are not starting after executing service-control --start --all command, please verify the validity of other certificates in VECS store using following one-liner script.
- ```
for i in $(/usr/lib/vmware-vmafd/bin/vecs-cli store list); do echo STORE $i; /usr/lib/vmware-vmafd/bin/vecs-cli entry list --store $i --text | egrep "Alias|Not After"; done
```

#### Sample result:

```
root@vcsal [ ~ ]# for i in $(/usr/lib/vmware-vmafd/bin/vecs-cli store list); do echo STORE $i; /usr/lib/vmware-vmafd/bin/vecs-cli entry list --store $i --text | egrep "Alias|Not After"; done  
STORE MACHINE_SSL_CERT  
Alias : __MACHINE_CERT  
Not After : May 7 19:54:43 2020 GMT  
STORE TRUSTED_ROOTS  
Alias : 8446d49f3392ee614cd9eaa3a7b5334efb20407e  
Not After : Apr 4 06:20:48 2030 GMT  
Alias : 101834a76cc59244e8f3dc6dbf960a8d8a0c1798  
Not After : May 2 20:04:42 2028 GMT  
STORE TRUSTED_ROOT_CRLS  
Alias : fff3fdd5f1821cf9fd4cea7eela567b4d50537ce  
Alias : f58833b7e61741162c4852f43e2a4125d7096963  
STORE machine  
Alias : machine  
Not After : May 7 19:56:39 2020 GMT  
STORE vsphere-webclient  
Alias : vsphere-webclient  
Not After : May 7 19:56:40 2020 GMT  
STORE vpxd  
Alias : vpxd  
Not After : May 7 19:56:41 2020 GMT  
STORE vpxd-extension  
Alias : vpxd-extension  
Not After : May 7 19:56:41 2020 GMT  
STORE SMS  
Alias : sms_self_signed  
Not After : Apr 9 06:27:36 2030 GMT  
STORE BACKUP_STORE  
Alias : bkp__MACHINE_CERT  
Not After : May 7 19:54:43 2020 GMT  
Alias : bkp_machine  
Not After : Apr 9 06:11:54 2022 GMT  
Alias : bkp_vsphere-webclient  
Not After : Apr 9 06:11:54 2022 GMT  
Alias : bkp_vpxd  
Not After : Apr 9 06:11:55 2022 GMT  
Alias : bkp_vpxd-extension  
Not After : Apr 9 06:11:55 2022 GMT  
root@vcsal [ ~ ]# date  
Wed Jul 29 14:03:00 UTC 2020  
root@vcsal [ ~ ]#
```

7. Replace other expired certificates if any, using certificate-manager utility (Refer KB <https://kb.vmware.com/s/article/2097936> for more information).
- Select Option 3 in Certificate Manager if only STORE: MACHINE\_SSL\_CERT - Alias: \_\_MACHINE\_CERT is expired
  - Select Option 6 in Certificate Manager if only Solution User Certificates are expired (STORES - machine, vpxd, vpxd-extension or vsphere-webclient)
  - Select Option 8 in Certificate Manager if both MACHINE\_SSL\_CERT and Solution Users are expired
    - In above sample result, both MACHINE\_SSL\_CERT and Solution User certs are expired, hence need to proceed with Option 8 to reset the certificates with Default VMCA certs.

Sample screenshot for Option 8:

```
root@vcsal [ ~ ]# /usr/lib/vmware-vmca/bin/certificate-manager
*** Welcome to the vSphere 6.5 Certificate Manager ***

-- Select Operation --

1. Replace Machine SSL certificate with Custom Certificate
2. Replace VMCA Root certificate with Custom Signing
   Certificate and replace all Certificates
3. Replace Machine SSL certificate with VMCA Certificate
4. Regenerate a new VMCA Root Certificate and
   replace all certificates
5. Replace Solution user certificates with
   Custom Certificate
6. Replace Solution user certificates with VMCA certificates
7. Revert last performed operation by re-publishing old
   certificates
8. Reset all Certificates

Note : Use Ctrl-D to exit.
Option[1 to 8]: 8
Do you wish to generate all certificates using configuration file : Option[Y/N] ? : N

Please provide valid SSO and VC privileged user credential to perform certificate operations.
Enter username [Administrator@vsphere.local]:
Enter password:

Please configure certtool.cfg with proper values before proceeding to next step.

Press Enter key to skip optional parameters or use Default value.

Enter proper value for 'Country' [Default value : US] : US
Enter proper value for 'Name' [Default value : CA] : vcsal.test.com
Enter proper value for 'Organization' [Default value : VMware] : VMware
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] : VMware Engineering
Enter proper value for 'State' [Default value : California] : California
Enter proper value for 'Locality' [Default value : Palo Alto] : Palo Alto
Enter proper value for 'IPAddress' (Provide comma separated values for multiple IP addresses) [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :

Enter proper value for 'Hostname' (Provide comma separated values for multiple Hostname entries) [Enter valid Fully Qualified Domain Name (FQ
DN), For Example : example.domain.com] : vcsal.test.com
Enter proper value for VMCA 'Name' :vcsal.test.com
Continue operation : Option[Y/N] ? : Y
```

## Steps for Windows vCenter Server

1. Download the PowerShell script "**fixsts.ps1**" and Jar file "**vmware-identity-sso-config67u3g.jar**" from the KB <https://kb.vmware.com/s/article/79263>

"Signing certificate is not valid" X

← → ↻ 🏠 🔒 https://kb.vmware.com/s/article/79263 ⋮ 📌 ☆

# "Signing certificate is not valid" - Regenerating and replacing expired STS certificate using PowerShell script on vCenter Server 6.5/6.7 installed on Windows (79263)

Last Updated: 7/21/2020

Categories: Troubleshooting

👍 5

Language: English ▼

📄 subscribe

✓ Symptoms

- vCenter/PSC Services do not start due to expired certificate showing the following errors:  

```
Path: %ProgramData%/VMware/vCenterServer/vpxd-svcs/vpxd-svcs.log
ERROR com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl$RequestResponseProcessor opId=]
Server rejected the provided time range. Cause:ns0:InvalidTimeRange: The token authority rejected
an issue request for TimePeriod [startTime=Thu Jan 02 09:22:13 EST 2020, endTime=Fri Jan 03
09:22:13 EST 2020] :: Signing certificate is not valid at Thu Jan 02 09:22:13 EST 2020, cert
validity: TimePeriod [startTime=Wed Jan 06 20:44:39 EST 2010, endTime=Wed Jan 01 20:54:23 EST
2020]
```

Note: The endTime should be a date in the past if the certificate is expired.
- The following error is observed when logging into the Web Client:  

```
HTTP Status 400 - Bad Request Message BadRequest, Signing certificate is not valid
```
- Accessing WebClient or UI Client will show below error message if vmware-vpxd service is not running due to expired certificate

Additional Resources

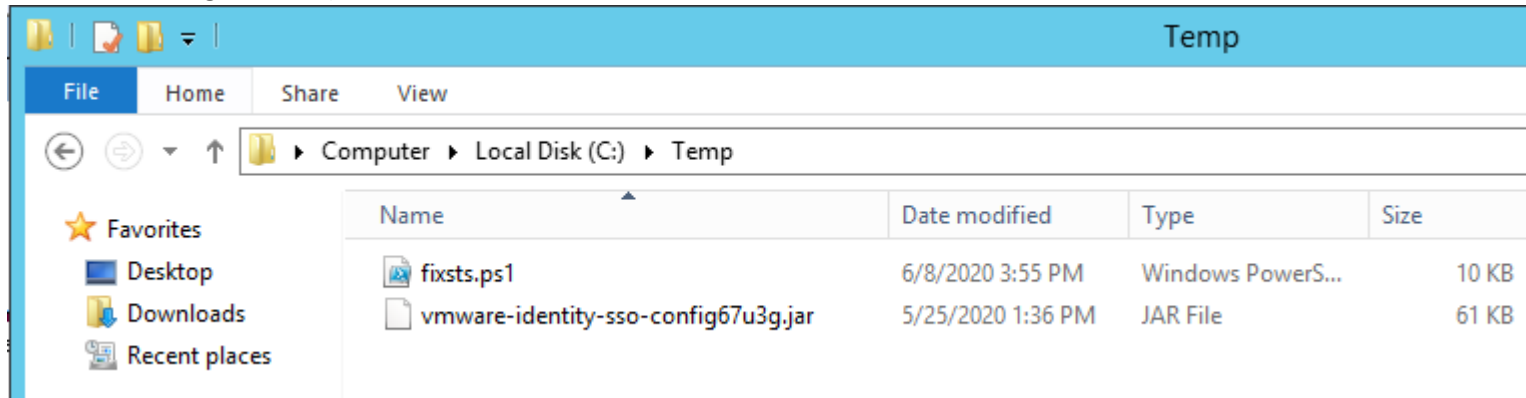
Related Products:  
VMware vCenter Server

Related Versions:  
VMware vCenter Server 6.5.x  
VMware vCenter Server 6.7.x

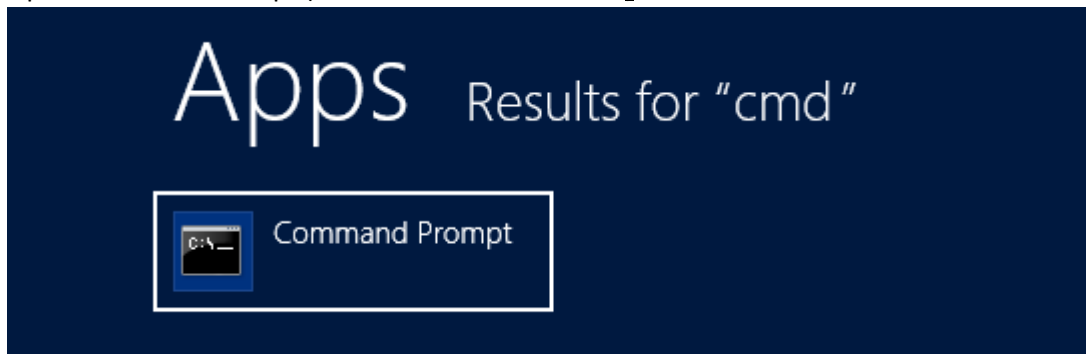
Actions  
📄 Copy link to clipboard  
🖨 Print  
🌐 Language: English ▼

Attachments  
🔗 vmware-identity-sso-config67u3g  
🔗 fixsts

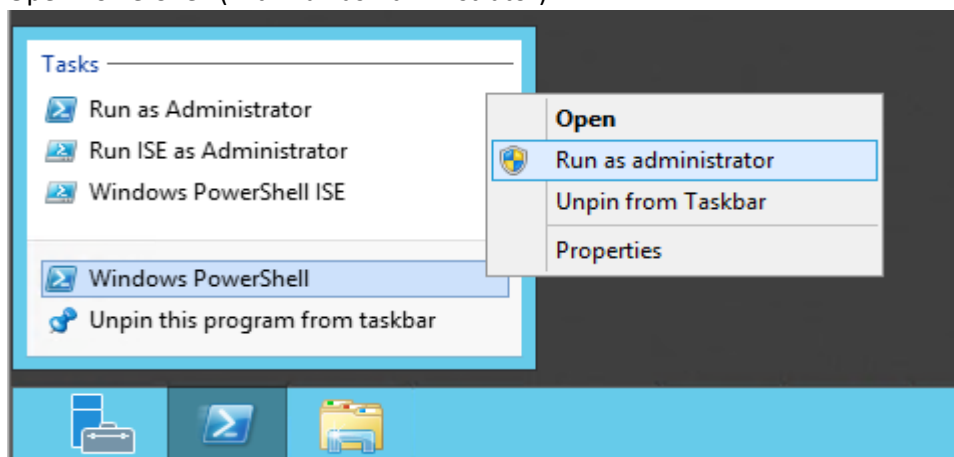
2. Copy the files **fixsts.ps1** & **vmware-identity-sso-config67u3g.jar** to C:\Temp folder in Windows vCenter Server (copying Jar file is not necessary if vCenter Server version is 6.7 U3g or above)



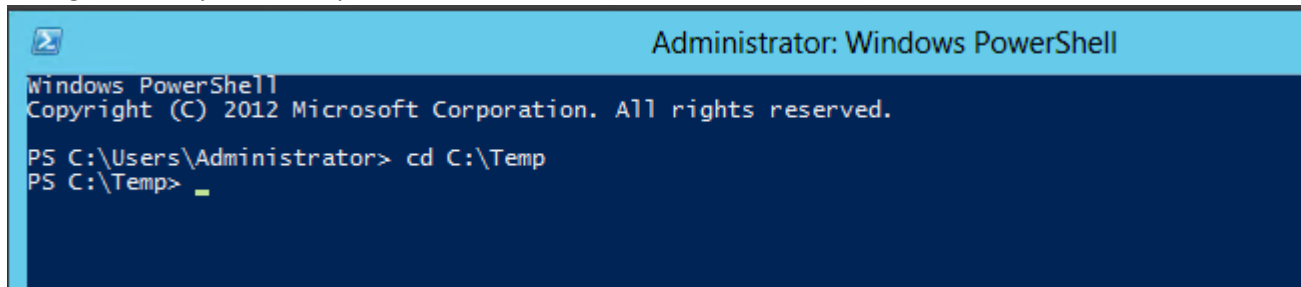
3. Open Command Prompt (with Run as Administrator)



4. Open PowerShell (with Run as Administrator)



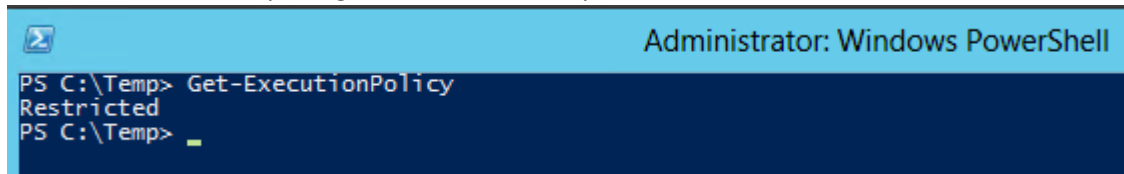
5. Change directory to C:\Temp



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

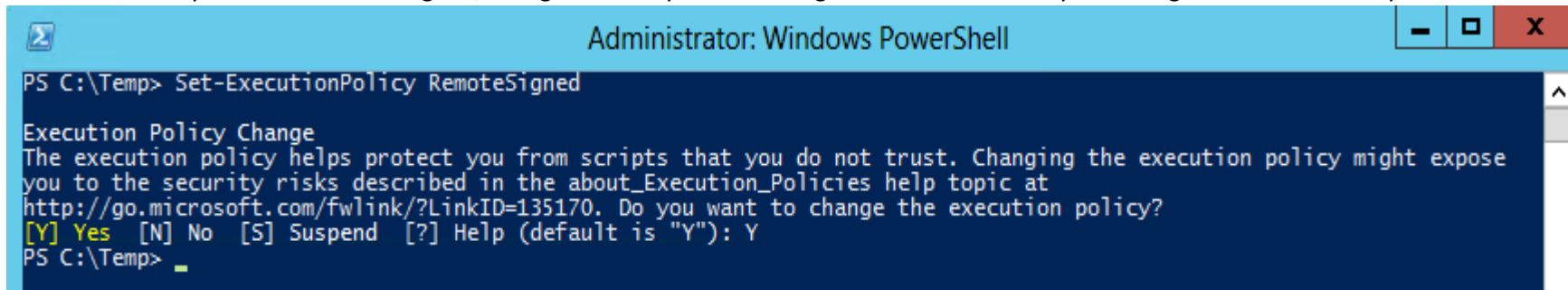
PS C:\Users\Administrator> cd C:\Temp
PS C:\Temp> _
```

6. Check execution Policy using Get-ExecutionPolicy



```
Administrator: Windows PowerShell
PS C:\Temp> Get-ExecutionPolicy
Restricted
PS C:\Temp> _
```

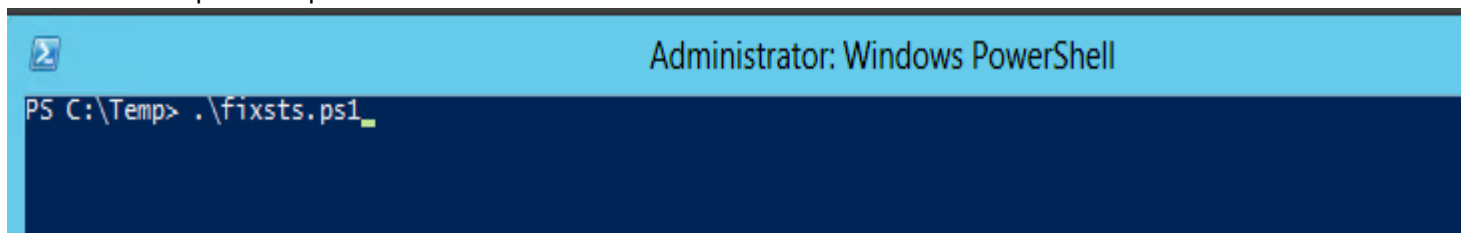
7. If Execution Policy is Restricted or AllSigned, change the Policy to RemoteSigned or Unrestricted by executing Set-ExecutionPolicy CmdLet to allow script execution



```
Administrator: Windows PowerShell
PS C:\Temp> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Temp> _
```

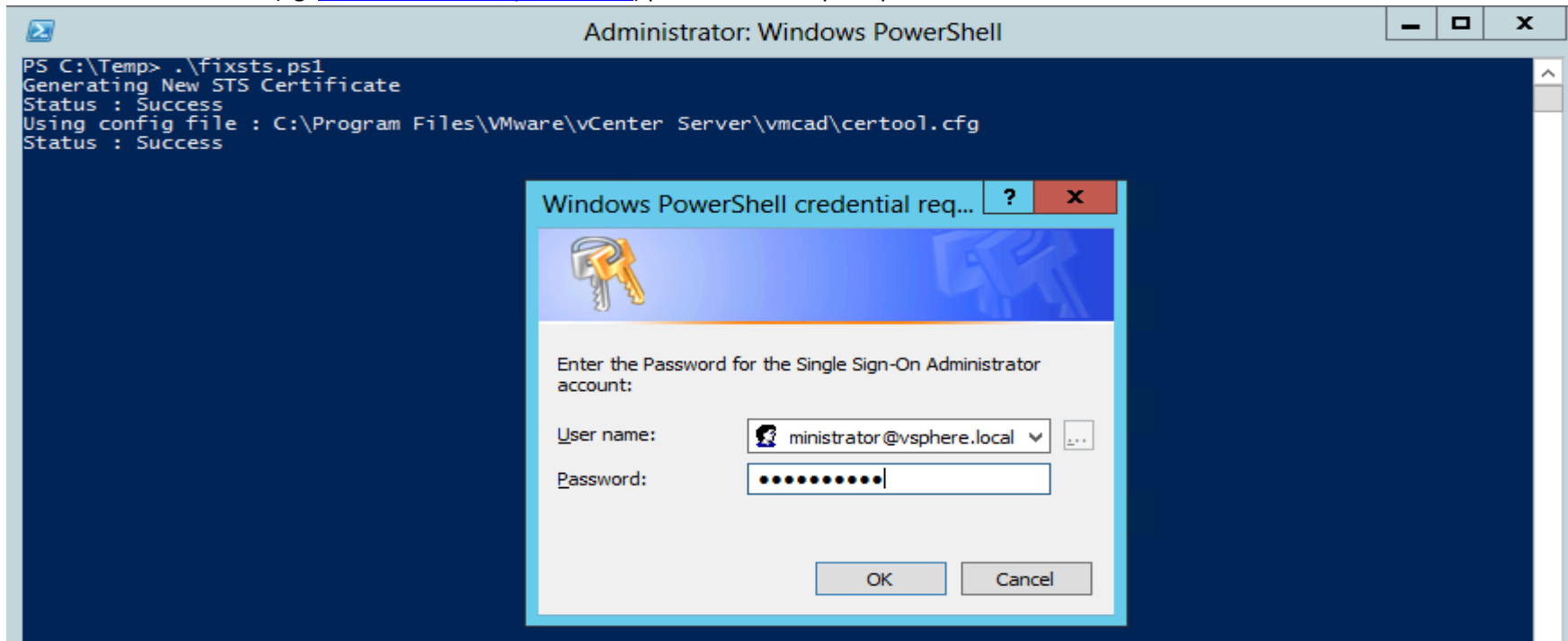
8. Execute the script "fixsts.ps1"



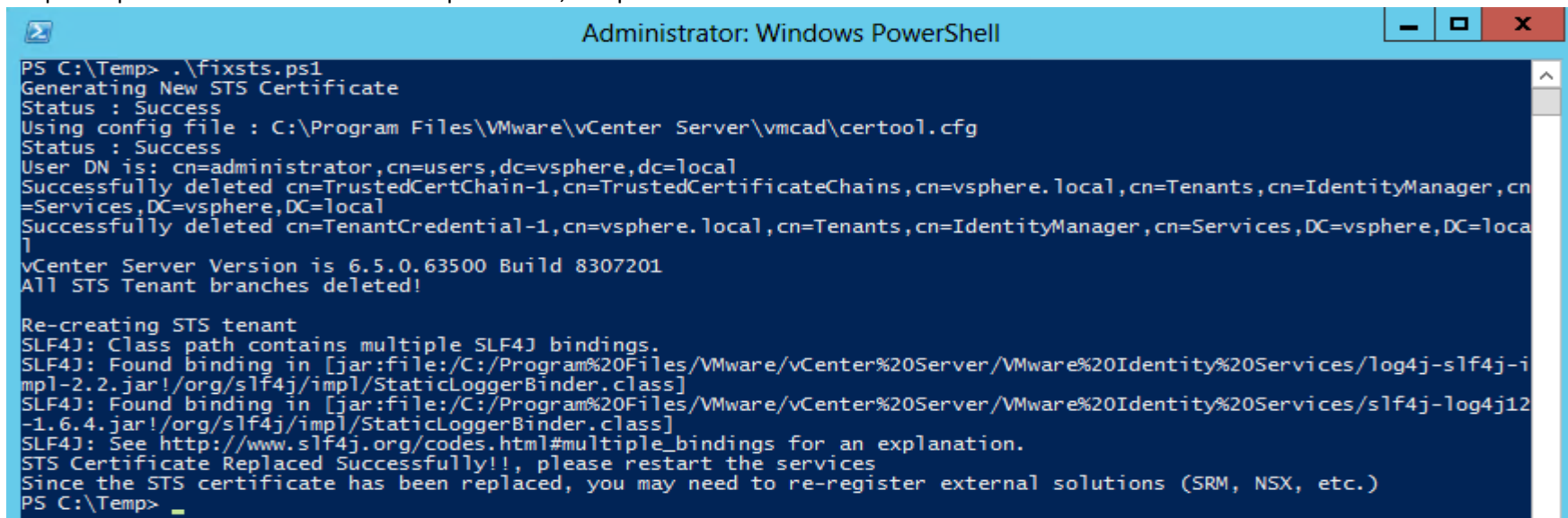
```
Administrator: Windows PowerShell
PS C:\Temp> .\fixsts.ps1_
```



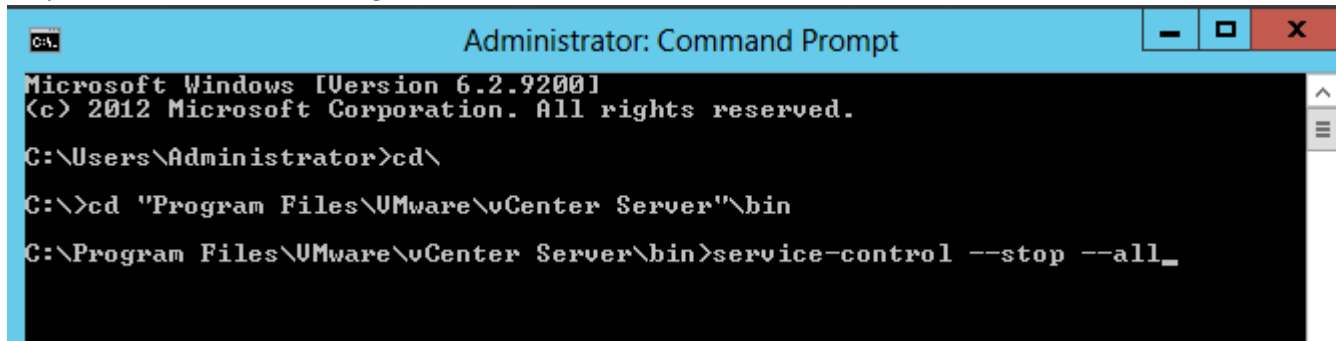
9. Enter SSO Administrator (Eg. [Administrator@vsphere.local](mailto:Administrator@vsphere.local)) password when prompted



10. Script will proceed with STS Certificate replacement, sample result in below screenshot



11. Stop and Start all Services using service-control

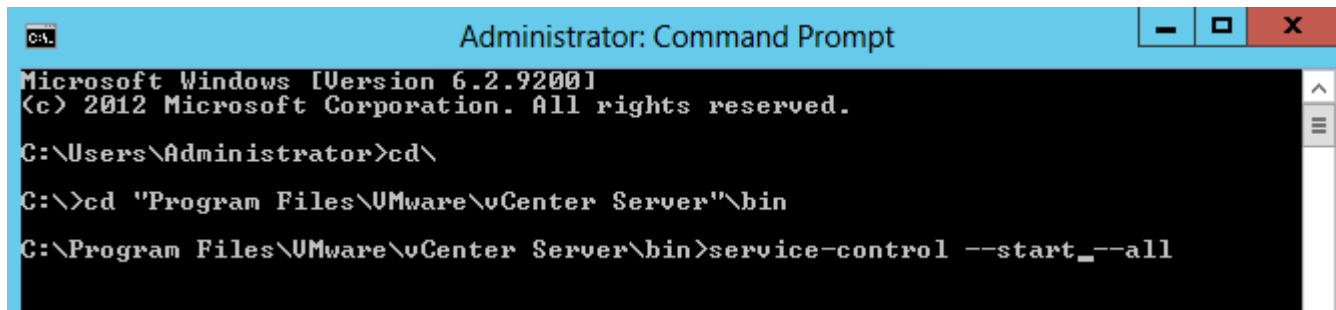


```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd\

C:\>cd "Program Files\VMware\VMware Server\bin"

C:\Program Files\VMware\VMware Server\bin>service-control --stop --all_
```



```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd\

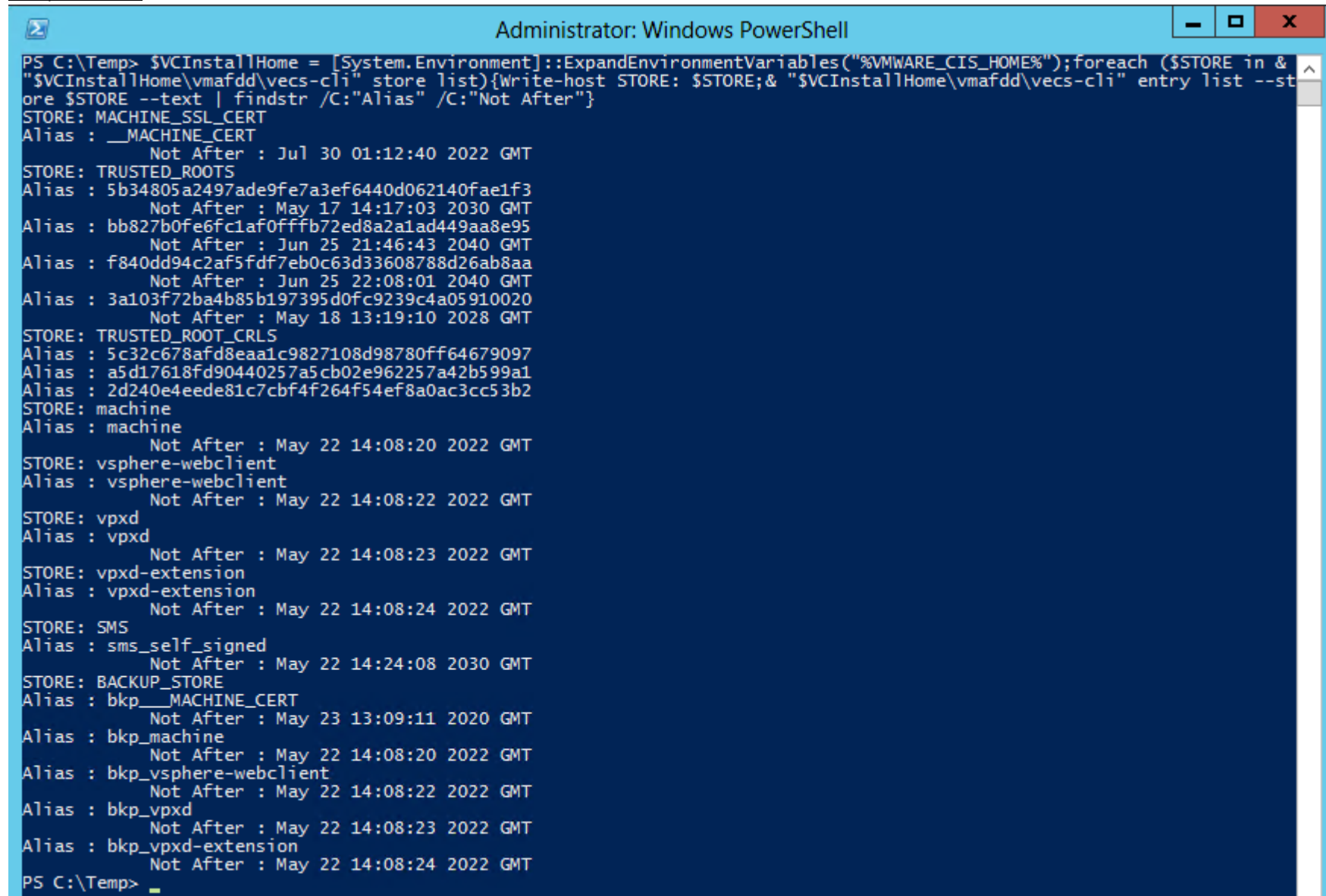
C:\>cd "Program Files\VMware\VMware Server\bin"

C:\Program Files\VMware\VMware Server\bin>service-control --start --all
```

12. Just in case, if services are not starting after executing `service-control -start --all` command, please verify the validity of other certificates in VECS store using following one-liner PowerShell script.

```
$VCInstallHome = [System.Environment]::ExpandEnvironmentVariables("%VMWARE_CIS_HOME%");foreach ($STORE in &
"$VCInstallHome\vmaddd\vecs-cli" store list){Write-host STORE: $STORE;& "$VCInstallHome\vmaddd\vecs-cli" entry
list --store $STORE --text | findstr /C:"Alias" /C:"Not After"}
```

Sample Result:



```
Administrator: Windows PowerShell
PS C:\Temp> $VCInstallHome = [System.Environment]::ExpandEnvironmentVariables("%VMWARE_CIS_HOME%");foreach ($STORE in &
"$VCInstallHome\vmafdd\vecs-cli" store list){Write-host STORE: $STORE;& "$VCInstallHome\vmafdd\vecs-cli" entry list --st
ore $STORE --text | findstr /C:"Alias" /C:"Not After"}
STORE: MACHINE_SSL_CERT
Alias : __MACHINE_CERT
Not After : Jul 30 01:12:40 2022 GMT
STORE: TRUSTED_ROOTS
Alias : 5b34805a2497ade9fe7a3ef6440d062140fae1f3
Not After : May 17 14:17:03 2030 GMT
Alias : bb827b0fe6fc1af0fffb72ed8a2a1ad449aa8e95
Not After : Jun 25 21:46:43 2040 GMT
Alias : f840dd94c2af5fdf7eb0c63d33608788d26ab8aa
Not After : Jun 25 22:08:01 2040 GMT
Alias : 3a103f72ba4b85b197395d0fc9239c4a05910020
Not After : May 18 13:19:10 2028 GMT
STORE: TRUSTED_ROOT_CRLS
Alias : 5c32c678afd8eaa1c9827108d98780ff64679097
Alias : a5d17618fd90440257a5cb02e962257a42b599a1
Alias : 2d240e4eede81c7cbf4f264f54ef8a0ac3cc53b2
STORE: machine
Alias : machine
Not After : May 22 14:08:20 2022 GMT
STORE: vsphere-webclient
Alias : vsphere-webclient
Not After : May 22 14:08:22 2022 GMT
STORE: vpxd
Alias : vpxd
Not After : May 22 14:08:23 2022 GMT
STORE: vpxd-extension
Alias : vpxd-extension
Not After : May 22 14:08:24 2022 GMT
STORE: SMS
Alias : sms_self_signed
Not After : May 22 14:24:08 2030 GMT
STORE: BACKUP_STORE
Alias : bkp__MACHINE_CERT
Not After : May 23 13:09:11 2020 GMT
Alias : bkp_machine
Not After : May 22 14:08:20 2022 GMT
Alias : bkp_vsphere-webclient
Not After : May 22 14:08:22 2022 GMT
Alias : bkp_vpxd
Not After : May 22 14:08:23 2022 GMT
Alias : bkp_vpxd-extension
Not After : May 22 14:08:24 2022 GMT
PS C:\Temp>
```

13. Replace other expired certificates if any, using certificate-manager utility (Refer KB <https://kb.vmware.com/s/article/2097936> for more information).
  - a. Select Option 3 in Certificate Manager if only STORE: MACHINE\_SSL\_CERT - Alias: \_\_MACHINE\_CERT is expired
  - b. Select Option 6 in Certificate Manager if only Solution User Certificates are expired (STORES - machine, vpxd, vpxd-extension or vsphere-webclient)
  - c. Select Option 8 in Certificate Manager if both MACHINE\_SSL\_CERT and Solution Users are expired

### Sample screenshot for Option 8:

```
C:\Program Files\VMware\oCenter Server\vmcad>certificate-manager

*** Welcome to the vSphere 6.5 Certificate Manager ***

-- Select Operation --

1. Replace Machine SSL certificate with Custom Certificate
2. Replace UMCA Root certificate with Custom Signing
   Certificate and replace all Certificates
3. Replace Machine SSL certificate with UMCA Certificate
4. Regenerate a new UMCA Root Certificate and
   replace all certificates
5. Replace Solution user certificates with
   Custom Certificate
6. Replace Solution user certificates with UMCA certificates
7. Revert last performed operation by re-publishing old
   certificates
8. Reset all Certificates

Note : Use Ctrl-Z and hit Enter to exit.
Option [1 to 8]: 8
Do you wish to generate all certificates using configuration file : Option [Y/N] ? : N

Please provide valid SSO and UC privileged user credential to perform certificate operations.
Enter username [Administrator@vsphere.local]:
Enter password:

Please configure certool.cfg with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] :
Enter proper value for 'Name' [Default value : CA] : WIN-KT2UQKEKLUT
Enter proper value for 'Organization' [Default value : VMware] :
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] :
Enter proper value for 'State' [Default value : Californial] :
Enter proper value for 'Locality' [Default value : Palo Alto] :
Enter proper value for 'IPAddress' <Provide comma separated values for multiple IP addresses> [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' <Provide comma separated values for multiple Hostname entries> [Enter valid Fully Qualified Domain Name(FQDN), For E
xample : example.domain.com] : WIN-KT2UQKEKLUT
Enter proper value for UMCA 'Name' :UMCA
Continue operation : Option [Y/N] ? : Y

You are going to reset by regenerating Root Certificate and replace all certificates using UMCA
Continue operation : Option [Y/N] ? : Y
```