KB LEVEL: **SVR**	**KB ARTICLE** ***How to Generate SSL Certificate for ESXi Host***	**KB NUMBER:** **01**

KB Category:	**Internal**		
Author:	Jan Francis Lictao	Date:	**May 25, 2019**

Problem Description:	Accessing VMware web client is not secured due to invalid certificate.
Symptoms and Cause of the issue:	Existing SSL Certificate is not valid due to untrusted CA Root.

Servers:
GL2-PESX-HV01.openaccess.bpo
GL2-PESX-HV02.openaccess.bpo
JKA-PESX-HV01.openaccess.bpo

Procedures:
Step 1: Perform backup by accessing the ESXi host server via SSH or remote console using VMware web client. Navigate to ***/etc/vmware/ssl*** then copy the existing certificate and key.

```
cd /etc/vmware/ssl
mv rui.crt rui.crt.bak
cp rui.key rui.key.bak
```

Step 2: Edit the ***openssl.conf*** on the same directory and add the lines below.

```
vi openssl.conf
        [req]
        distinguished_name = req_distinguished_name
        prompt = no
        [req_distinguished_name]
        C = PH
        ST = NCR
        L = Makati
        O = OAMPI Inc.
        OU = IT Department
        CN = (server_name)
```

Then press :wq! to save the configuration.

Step 3: Generate now the Certificate Signing Request by executing the command below.

```
openssl req -new -key /etc/vmware/ssl/rui.key -config openssl.cnf \-out
/etc/vmware/ssl/rui.csr
```

Step 4: After generating the CSR file, copy it to the CA server (Kalliope) via SCP. Save the CSR file to /root/ca/intermediate/csr

```
scp /etc/vmware/ssl/rui.csr jlictao@10.1.0.250:/root/ca/intermidiate/csr
```

Step 5: In CA server, navigate to ***/root/ca/intermediate*** and edit the ***openssl.conf***. Add the FQDN of the requesting server to the last line as **Subject Alternative Name** then save.

```
cd /root/ca/intermediate
vi openssl.conf
```

```
[ nameSan ]
DNS.1 = GL2-PESX-HV01.openaccess.bpo
```

Step 6: Sign the CSR using the command below.

```
openssl ca -config intermediate/openssl.cnf \-extensions server_cert -days 365 -notext -md sha256 \-in intermediate/csr/rui.csr \-out intermediate/certs/rui.crt
```

Enter the intermediate key then press Y.

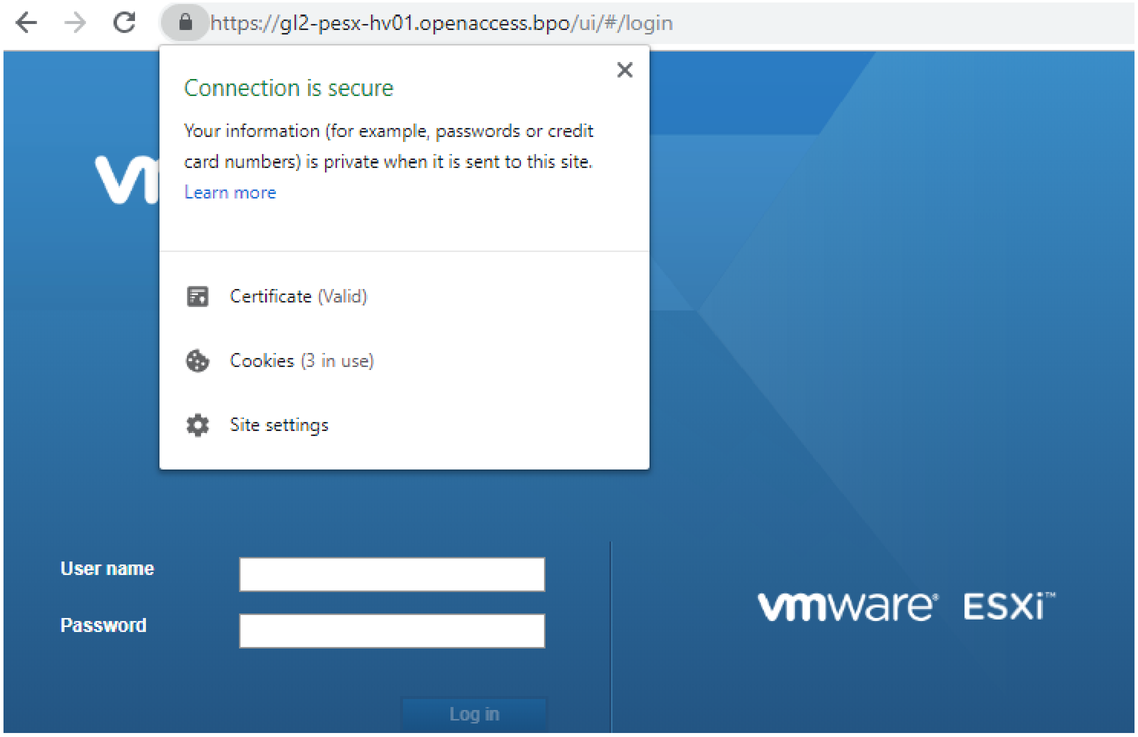
Step 7: Copy the signed certificate to the ESXi host from the CA server.

```
scp /root/ca/intermidiate/certs/rui.crt root@172.22.8.1:/etc/vmware/ssl
```

Step 8: Reboot the ESXi host server.

Verification Steps:

Step 1: After rebooting the ESXi host server, login into the VMware web client using https.

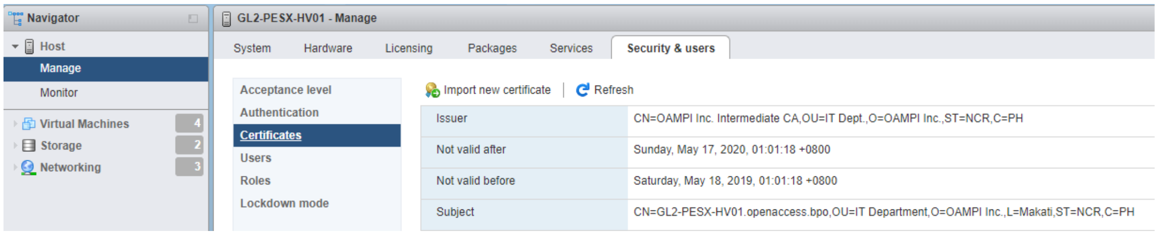


https://gl2-pesx-hv01.openaccess.bpo/ui/#/login

Connection is secure

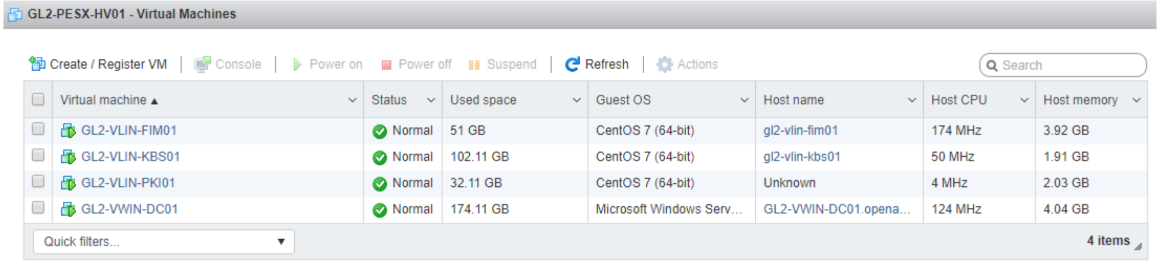
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Step 2: Enter the root login credential then navigate to Host > Manage > Security > Certificates. And you can see the newly deployed secured self-signed SSL certificate.



Issuer	CN=OAMPI Inc. Intermediate CA,OU=IT Dept.,O=OAMPI Inc.,ST=NCR,C=PH
Not valid after	Sunday, May 17, 2020, 01:01:18 +0800
Not valid before	Saturday, May 18, 2019, 01:01:18 +0800
Subject	CN=GL2-PESX-HV01.openaccess.bpo,OU=IT Department,O=OAMPI Inc.,L=Makati,ST=NCR,C=PH

Step 3: Verify all Virtual Machines resides on the ESXi host if running and working properly.



□	Virtual machine ▲	Status	Used space	Guest OS	Host name	Host CPU	Host memory
□	GL2-VLIN-FIM01	✓ Normal	51 GB	CentOS 7 (64-bit)	gl2-vlin-fim01	174 MHz	3.92 GB
□	GL2-VLIN-KBS01	✓ Normal	102.11 GB	CentOS 7 (64-bit)	gl2-vlin-kbs01	50 MHz	1.91 GB
□	GL2-VLIN-PKI01	✓ Normal	32.11 GB	CentOS 7 (64-bit)	Unknown	4 MHz	2.03 GB
□	GL2-VWIN-DC01	✓ Normal	174.11 GB	Microsoft Windows Serv...	GL2-VWIN-DC01.opena...	124 MHz	4.04 GB