Request Information				
Requestor	Jan Francis Lictao			
Implementing Team	Server Operation			
Ticket Number/s				
Change Classification	x	Major		Minor
After the fact	x	Yes		No
Emergency		Yes	x	No
Proposed Change Date	ATF			
Proposed Change Start/End Time	ATF			
Proposed Change Verification Time	ATF			

Objective of the change
Creating and installing Certificates to fulfill the PCIDSS compliance requirement.

Technical/Operational Impact of the change		
Negative: Required downtime as reboot is needed after the installation of certificate.	Beneficial: Certificate for ESXi host are valid.	Neutral: Compliance with PCIDSS requirements.

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	GL2-PESX-HV01	172.22.8.1	Virtualization
G2	GL2-PESX-HV02	172.22.8.2	Virtualization
Jaka	JKA-PESX-HV01	172.17.1.11	Virtualization

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
Server Operation	Rovie Salvatiera	0917-627-4325

Test Environment implementation and Verification Summary
Tested in 172.22.8.4 ESXi Host test server.

Test Environment Results Summary
Test ESXi host server has a valid certificate.

Configuration Change Template

Baseline File	3.1.135 DELL EMC - ESXi
Baseline Version	2.0

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
VMware self-signed certificates.	Create CSR and signed by our own CA then install to the ESXi host.	Addition tab for Certificates.	Certificates

Physical Implementation Procedures / Advisory
No physical implementation will be facilitated.

Backup Procedures
1. Login to ESXi Host via ssh and enter the super user account. 2. Navigate to /etc/vmware/ssl. cd /etc/vmware/ssl 3. Copy the existing certificate and key. mv rui.crt rui.crt.bak cp rui.key rui.key.bak

Technical Configuration Procedures
1. Login to the ESXi Host via SSH using root account. 2. Navigate to /etc/vmware/ssl. 3. Edit the openssl.conf and enter the following 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 = GL2-PESX-HV01.openaccess.bpo

4. Press :wq! to save the changed configurations.
5. Generate now the Certificate Signing Request.
   openssl req -new -key /etc/vmware/ssl/rui.key -config openssl.cnf \-out /etc/vmware/ssl/rui.csr

6. After generating the CSR file, copy it to the CA server (Kalliope) via SCP.
7. Save the CSR file to /root/ca/intermediate/csr
   scp /etc/vmware/ssl/rui.csr jlictao@10.1.0.250:/root/ca/intermidiate/csr

8. In CA server, navigate to /root/ca/intermediate and edit the openssl.conf. Add the FQDN of the requesting server to the last line then save it after editing.

   vi openssl.conf

   [nameSan]
   DNS.1 = GL2-PESX-HV01.openaccess.bpo
9. 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

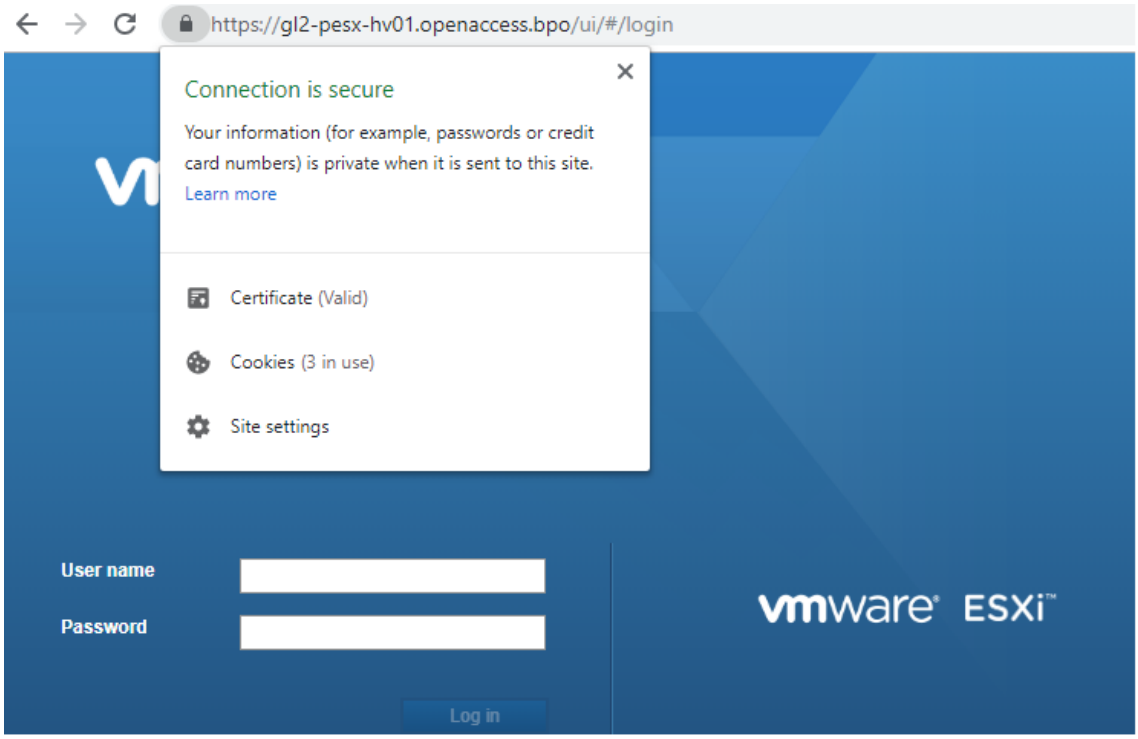
   Enter the intermediate key the press Y.

10. Copy the signed certificate to the ESXi host from the CA server.

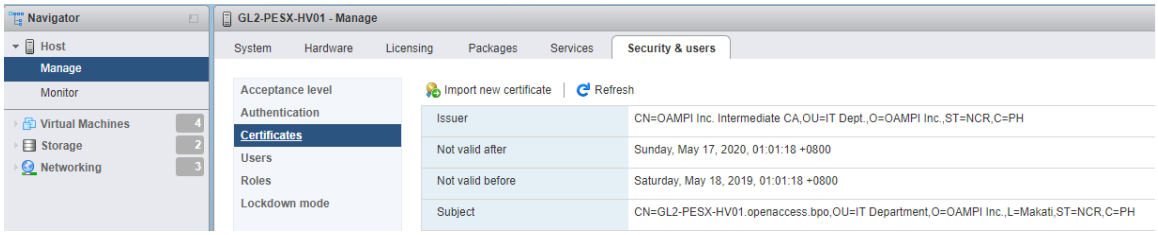
    scp /root/ca/intermidiate/certs/rui.crt root@172.22.8.1:/etc/vmware/ssl
11. Reboot the ESXi Host.
12. Follow the same procedure to the other ESXi host.

Verification Procedures

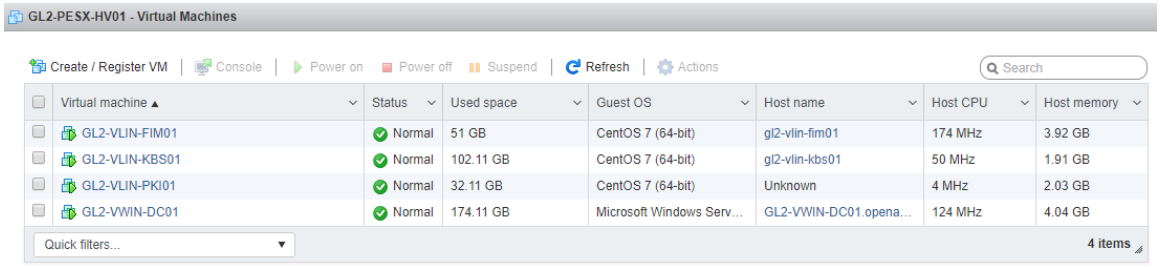
1. After rebooting the ESXi host, log in to the web client using https.



2. Enter root login credentials and navigat to Host > Manage > Security > Certificates.



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



Back-out Procedures
1. Run the command below to the ESXi host. `/sbin/generate-certificate`