oVirt 4.3.x Host Certificate Renewal Guide (Minimal Downtime)

Author: Christopher Cross

This document outlines the manual, step-by-step procedure for renewing expired oVirt host certificates when Virtual Machine (VM) migration is failing due to SSL/TLS errors. This technique avoids the traditional host maintenance mode by generating and applying new certificate materials directly, resulting in minimal VM downtime limited only to a brief pause during service restarts.

Prerequisites

Requirement	Description
Operating System	Rocky Linux 8, 9, or 10 on both the Engine and Hosts.
Access	Root SSH access to the oVirt Engine (`[ENGINE_FQDN]`) and all affected Hosts (`[AFFECTED_HOST_FQDN]`).
System Identity	Know the exact Fully Qualified Domain Name (FQDN) for the oVirt Engine and each affected Host.
Engine CA Paths	Confirmed location of Engine Certificate Authority (CA) materials:
	- CA Certificate: `/etc/pki/ovirt-engine/ca.pem`
	- CA Private Key: `/etc/pki/ovirt-engine/private/ca.pem`
Text Editor	The default Linux text editor, **vi**, or another preferred text editor.

Phase 1: Create Certificate Signing Request (CSR) on the Host

In this phase, a new private key and a Certificate Signing Request (CSR) are generated directly on the affected host, ensuring the new private key remains secure on the host machine.

On the Affected oVirt Host ([AFFECTED_HOST_FQDN])

1. **Generate a new 2048-bit Private Key:**

```
Shell
openssl genrsa -out /tmp/[AFFECTED_HOST_FQDN].key 2048
```

2. **Generate the Certificate Signing Request (CSR):** The Subject Distinguished Name (DN) must adhere to the format expected by the oVirt Engine, replacing `[YOUR_ORGANIZATION_NAME]` with your organization's domain or identifier and `[AFFECTED_HOST_FQDN]` with the host's actual FQDN.

```
Shell
openssl req -new -key /tmp/[AFFECTED_HOST_FQDN].key -out
/tmp/[AFFECTED_HOST_FQDN].req -subj
"/O=[YOUR_ORGANIZATION_NAME]/CN=[AFFECTED_HOST_FQDN]" -extensions v3_req
-config <(cat /etc/pki/tls/openssl.cnf <(printf
"[v3_req]\nsubjectAltName=DNS:[AFFECTED_HOST_FQDN]"))
```

3. **Copy the CSR to the oVirt Engine:** Transfer the generated request file (`.req`) to the engine machine using `scp`. Replace `[ENGINE_FQDN]` with the FQDN of your oVirt Engine.

```
Shell
scp /tmp/[AFFECTED_HOST_FQDN].req root@[ENGINE_FQDN]:/tmp/
```

Phase 2: Sign the CSR on the oVirt Engine

The oVirt Engine uses its internal Certificate Authority (CA) to sign the CSR, establishing the host certificate as a trusted asset within the environment.

On the oVirt Engine ([ENGINE_FQDN])

1. **Navigate to the PKI directory:**

```shell
cd /etc/pki/ovirt-engine/
```

2. **Sign the CSR and generate the host certificate:** This command generates the new certificate (`.cer`), sets a 10-year validity period, and includes necessary extensions (Subject Alternative Name (SAN), Key Usage, Extended Key Usage). Replace `[AFFECTED_HOST_FQDN]` with the host's FQDN.

```shell
openssl x509 -req -in /tmp/[AFFECTED_HOST_FQDN].req -CA ca.pem -CAkey
private/ca.pem -CAcreateserial -out /tmp/[AFFECTED_HOST_FQDN].cer -days 3650
-extfile <(printf
"subjectAltName=DNS:[AFFECTED_HOST_FQDN]\nkeyUsage=critical,digitalSignature,ke
yEncipherment\nextendedKeyUsage=serverAuth,clientAuth")
```

3. **Copy the Signed Certificate back to the Host:** Transfer the signed certificate (`.cer`) back to the affected host using `scp`. Replace `[AFFECTED_HOST_FQDN]` with the host's FQDN.

```shell
scp /tmp/[AFFECTED_HOST_FQDN].cer root@[AFFECTED_HOST_FQDN]:/tmp/
```

Phase 3: Apply New Certificates and Restart Services

This phase involves backing up existing certificates, replacing them with the new files, correcting permissions, and restarting core host services.

On the Affected oVirt Host (`[AFFECTED_HOST_FQDN]`)

1. **Backup Existing Certificates: CRITICAL:** Create a dated backup of the existing certificates and keys to facilitate a quick rollback if necessary.

```shell
mkdir -p /root/certs_backup_$(date +%F)
cp /etc/pki/vdsm/certs/vdsmcert.pem /root/certs_backup_$(date +%F)/
```

```
cp /etc/pki/vdsm/keys/vdsmkey.pem /root/certs_backup_$(date +%F)/
cp /etc/pki/vdsm/libvirt-spice/server-cert.pem /root/certs_backup_$(date +%F)/
cp /etc/pki/vdsm/libvirt-spice/server-key.pem /root/certs_backup_$(date +%F)/
cp /etc/pki/libvirt/clientcert.pem /root/certs_backup_$(date +%F)/
cp /etc/pki/libvirt/clientkey.pem /root/certs_backup_$(date +%F)/
```

2. **Replace Expired Certificates with New Files:** Copy the new certificate (`.cer`) and private key (`.key`) to their appropriate system locations. Replace `[AFFECTED_HOST_FQDN]` with the host's FQDN.

```
Shell
cp /tmp/[AFFECTED_HOST_FQDN].cer /etc/pki/vdsm/certs/vdsmcert.pem
cp /tmp/[AFFECTED_HOST_FQDN].key /etc/pki/vdsm/keys/vdsmkey.pem
cp /tmp/[AFFECTED_HOST_FQDN].cer /etc/pki/vdsm/libvirt-spice/server-cert.pem
cp /tmp/[AFFECTED_HOST_FQDN].key /etc/pki/vdsm/libvirt-spice/server-key.pem
cp /tmp/[AFFECTED_HOST_FQDN].cer /etc/pki/libvirt/clientcert.pem
cp /tmp/[AFFECTED_HOST_FQDN].key /etc/pki/libvirt/clientkey.pem
```

3. **Fix Permissions and SELinux Context:** Incorrect permissions on private key files will prevent services from starting. **SELinux context is essential** after manual file copies.

    a. **Set Permissions (Crucial for Libvirt):**

```
Shell
chmod 600 /etc/pki/vdsm/keys/vdsmkey.pem
chmod 600 /etc/pki/vdsm/libvirt-spice/server-key.pem
chmod 600 /etc/pki/libvirt/clientkey.pem
chmod 644 /etc/pki/vdsm/certs/vdsmcert.pem
chmod 644 /etc/pki/vdsm/libvirt-spice/server-cert.pem
chmod 644 /etc/pki/libvirt/clientcert.pem
```

    b. **Restore SELinux Context (Essential):**

```
Shell
restorecon -Rv /etc/pki/vdsm/
restorecon -Rv /etc/pki/libvirt/
```

4. **Restart VDSM and Libvirt Services:** ⚠️ **WARNING:** VMs currently running on this host will experience a brief momentary pause (a soft stop, not a crash) during these restarts.

```shell
systemctl restart libvirtd
systemctl restart vdsmd
```

5. **Verify Host Status:** Check the oVirt Administration Portal. The host status should transition to **Up**. VM migration should now function correctly.

Phase 4: Fix SPICE Console Connectivity

If VM console connections (SPICE) continue to fail, it typically indicates that the client machine used to access the console does not trust the host's new certificate, which is signed by the oVirt Engine's CA.

On Your Client Machine (The machine used to access the Admin Portal)

1. **Download the oVirt Engine CA Certificate:** Open a web browser and navigate to the following URL, replacing `[ENGINE_FQDN]` with the FQDN of your oVirt Engine:

   `https://[ENGINE_FQDN]/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`

   Download the file (usually named `ca.pem`).

2. **Install the CA Certificate into the Operating System Trust Store:**

   a. **Windows:** Right-click the `.pem` file, select **Install Certificate**, and place it in the **Trusted Root Certification Authorities** store for the local machine. b. **Linux/macOS:** Import the certificate into the operating system's trust store using the appropriate utility for your distribution (e.g., `update-ca-certificates` on Debian/Ubuntu, or keychain access on macOS).

3. **Clear Console Viewer Cache:** Ensure all instances of the console viewer application (e.g., `virt-viewer` or `remote-viewer`) are closed and restarted.

Once the CA certificate is installed on the client machine, the SPICE client will be able to validate the host's certificate signature, and the console connection should succeed.