Exercise 3: Fix SSL certificates so all peripherals use the Hub CA

1. Take a snapshot of peripheral 1
    1. Recommend shutting down first
2. On the peripheral, rename /root/ssl-build to /root/ssl-build.old
3. Copy the CA information from the Hub to the Peripheral

    1.
       ```
       # mkdir -m 700 /root/ssl-build
       ```

    2.
       ```
       # cd /root/ssl-build
       ```

    3.
       ```
       # scp root@suma-hub.example.com:/root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY .
       ```

    4.
       ```
       # scp root@suma-hub.example.com:/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT .
       ```

    5.
       ```
       # scp root@suma-hub.example.com:/root/ssl-build/rhn-ca-openssl.cnf .
       ```
4. Recreate the server certificate using the Hub CA

    1.
       ```
       # rhn-ssl-tool --gen-server --dir="/root/ssl-build" --set-country="US" --set-state="UT" --set-city="Pleasant Grove" --set-org="SUSE" --set-org-unit="Tech Summit" --set-hostname="suma-p1.example.com" --set-cname="suma-p1.example.com"
       ```
    2. CA Password = suse1234
5. Replace certificates on SUMA Peripheral

    1.
       ```
       # mgr-ssl-cert-setup --root-ca-file=/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT --server-cert-file=/root/ssl-build/suma-p1/server.crt --server-key-file=/root/ssl-build/suma-p1/server.key
       ```

    2.
       ```
       # spacewalk-service stop
       ```

    3.
       ```
       # systemctl restart postgresql.service
       ```

    4.
       ```
       # spacewalk-service start
       ```
6. Verify that the Issuer of the certificate is suma-hub.example.com by viewing the certificate of suma-p1.example.com in the browser.
    1. You may need to “Remove Exception” in order to “Accept the Risk and Continue” in order to view the new certificate.
7. Fix SSL on Branch server
    1. Go to branch-store1.store1.example.com.
    2. Run “zypper ref” to see failure with SSL.
    3. To get the new CA certificate, simply run the highstate on the Branch server.

      1. # venv-salt-call state.apply

   4. Verify issue is resolved.

8. Replace server certificate on Branch server

   1. Note the Issuer of the certificate of branch-store1.store1.example.com in a browser (it should be suma-hub.example.com)

   2. To fix, repeat steps 2 and 3 to copy down certificate files from suma-p1.example.com to the branch-store1.store1.example.com

9. Use salt to rerun configure-proxy.sh

   1. On the Peripheral, copy cert files from /root/ssl-build to /srv/salt/branch/configure_branch/master-certs

   2. On the Branch, remove /root/.BRANCH_SETUP_COMPLETE

   3. On the Peripheral, run salt ‘branch-store1*’ state.apply branch.configure_branch

      1. You can use ‘test=TRUE’ to perform a dry run first

   4. View the Branch certificate again in the browser to confirm the Issuer is correct