TechBrief

Stratusphere™ How to Place Signed SSL Certificates on the Appliances

Overview

This document provides instructions on how to place signed SSL certificates on the Stratusphere Hub, Database, and Collector appliances. Apart from getting rid of the alarming warning each time the Stratusphere Hub Web UI is accessed, placing a signed SSL certificate provides verifiable identification and security compliance to administrator & users accessing the Web UI of Stratusphere.

These instructions apply to Stratusphere Hub, Database, and Collector version 5.6.0 and higher. If using an older version of Stratusphere please upgrade to the latest version or contact Support@Liquidware.com for additional information to upgrade.

Preparation

1. Procure any change controls required to make changes to the production Stratusphere Hub & Database appliances.
2. Acquire credentials of the '`friend`' and '`root`' users to access the console of the Stratusphere Hub, Database, and Collector appliances.
3. Procure access to the local console of the Stratusphere Hub, Database, and Collector Appliances depending on the hypervisor on which the Hub is housed. Alternatively, PuTTY can also be used to access the console of the Hub, Database, and Collector provided SSH (TCP/22) access is allowed to the appliances.
4. Download and install WinSCP or FileZilla or similar software to download and upload certificate request and SSL Certificate files.
5. Please be aware that you will need to start the initial steps to prepare the SSL certificate request, pause in the middle of the instructions as you submit the request to the Certifying Authority (CA), and then **receive your certificate** (this may take minutes, hours, or even days depending on your CA), and use the new certificate to complete the process.

Instructions for Stratusphere Hub Appliance

Start with these initial few steps to prepare the certificate request:

1. On the Stratusphere Hub appliance local console, log in using User ID: '`friend`' and Password: '`sspassword`' first.
2. Switch to '`root`' user using the following command and enter the password when prompted (default: '`sspassword`'):
   - `su -`
3. Change to the following folder using the command:
   - `cd /home/friend`
4. Please enter the following commands:
   - `openssl genrsa 2048 > /etc/lwl/ssl/ssl.key.2048`
   - `cp /etc/lwl/ssl/ssl.key /etc/lwl/ssl/ssl.key.original`
5. Generate a certificate request on the Stratusphere Hub using the existing SSL Key.
   - `openssl req -key /etc/lwl/ssl/ssl.key.2048 -out hubcertrequest.csr -new -sha256`

   When prompted for common name, make sure you provide your Hub's fully qualified DNS name.
   - `common name: <hubdnsname.domain.com>`
6. You will find the certificate request generated in the following location: `/home/friend/hubcertrequest.csr`
7. Change ownership of the file so that it accessible using the '`friend`' user.
   - `chown friend:friend /home/friend/hubcertrequest.csr`
8. Use WinSCP or FileZilla or similar software to download this certificate request '`/home/friend/hubcertrequest.csr`' file to your local desktop. In WinSCP or FileZilla, use User ID: 'friend' and Password: '`sspassword`' as credentials within the program. Use the SCP protocol with WinSCP (Port 22).
9. Provide this certificate request file to your security provider or Certifying Authority and request that they provide the SSL Certificate specifically in **base64 / PEM** format. For these instructions we will call it '`hubsslcert.crt`' – this is the actual SSL Certificate you will receive back from your security provider or Certifying Authority.

Pause here until you receive your SSL certificate from your provider. After receiving your SSL Certificate from your provider, complete the process with the remaining instructions:

10. Use WinSCP or FileZilla or similar software to upload this '`hubsslcert.crt`' SSL Certificate file to your Stratusphere Hub in the '`/home/friend/hubsslcert.crt`' location. In WinSCP or FileZilla, use User ID: '`friend`' and Password: '`sspassword`' as credentials within the program. Use the SCP protocol with WinSCP (Port 22).

11. On the Stratusphere Hub local console, while still logged in as the root user, make a copy the original SSL certificate as a backup:
    - `cp /etc/lwl/ssl/ssl.crt /etc/lwl/ssl/ssl.crt.orig`
12. Place the new key and certificate in place of the original and modify the file permissions as follows:
    - `cp /etc/lwl/ssl/ssl.key.2048 /etc/lwl/ssl/ssl.key`
    - `mv /home/friend/hubsslcert.crt /etc/lwl/ssl/ssl.crt`
    - `chown root:root /etc/lwl/ssl/ssl.crt`
    - `chmod 644 /etc/lwl/ssl/ssl.crt`
    - `chmod 640 /etc/lwl/ssl/ssl.key`
    - `restorecon –r /etc/lwl/ssl`
13. Restart the Web Server to load the newly added SSL Certificate:
    - `/etc/init.d/httpd restart`
14. Using your browser of choice, log into the Stratusphere Hub Web UI. Ensure that the UI Login page shows with no certificate related warning. Also verify the information within the certificate provided by the browser address bar.

Instructions for Stratusphere Database Appliance

Start with these initial few steps to prepare the certificate request:

1. On the Stratusphere Database appliance local console, log in using User ID: '`friend`' and Password: '`sspassword`' first.
2. Switch to '`root`' user using the following command and enter the password when prompted (default: '`sspassword`'):
   - `su -`
3. Change to the following folder using the command:
   - `cd /home/friend`
4. Please enter the following commands:
   - `openssl genrsa 2048 > /var/lib/pgsql/current/data/server.key.2048`
   - `cp /var/lib/pgsql/current/data/server.key /var/lib/pgsql/current/data/server.key.original`
5. Generate a certificate request on the Stratusphere Database using the existing SSL Key.
   - `openssl req -key /var/lib/pgsql/current/data/server.key.2048 -out dbcertrequest.csr -new -sha256`

   When prompted for common name, make sure you provide your Hub's fully qualified DNS name.
   - `common name: <dbdnsname.domain.com>`
6. You will find the certificate request generated in the following location: `/home/friend/dbcertrequest.csr`
7. Change ownership of the file so that it accessible using the '`friend`' user.
   - `chown friend:friend /home/friend/dbcertrequest.csr`
8. Use WinSCP or FileZilla or similar software to download this certificate request '`/home/friend/dbcertrequest.csr`' file to your local desktop. In WinSCP or FileZilla, use User ID: '`friend`' and Password: '`sspassword`' as credentials within the program. Use the SCP protocol with WinSCP (Port 22).
9. Provide this certificate request file to your security provider or Certifying Authority and request that they provide the SSL Certificate specifically in **base64 / PEM** format. For the purpose of these instructions, we will call the actual certificate file received from your Certifying Authority `server.crt`.

Pause here until you receive your SSL certificate from your provider. After receiving your SSL Certificate from your provider, complete the process with the remaining instructions:

10. Use WinSCP or FileZilla or similar software to upload this '`server.crt`' SSL Certificate file to your Stratusphere Database in the '`/home/friend/server.crt`' location. In WinSCP or

FileZilla, use User ID: '`friend`' and Password: '`sspassword`' as credentials within the program. Use the SCP protocol with WinSCP (Port 22).

11. On the Stratusphere Database local console, while still logged in as the root user, make a copy the original SSL certificate as a backup:
    - `cp /var/lib/pgsql/current/data/server.crt /var/lib/pgsql/current/data/server.crt.orig`
12. Place the new key and certificate in place of the original and modify the file permissions as follows:
    - `cp /var/lib/pgsql/current/data/server.key.2048 /var/lib/pgsql/current/data/server.key`
    - `mv /home/friend/server.crt /var/lib/pgsql/current/data/server.crt`
    - `chown postgres:postgres /var/lib/pgsql/current/data/server.crt`
    - `chmod 400 /var/lib/pgsql/current/data/server.crt`
    - `chmod 400 /var/lib/pgsql/current/data/server.key`
13. Restart the database server to load the newly added SSL Certificate:
    - `/etc/init.d/postgresql<PRESS-TAB-KEY> restart`

Instructions for Stratusphere Collector Appliance

Start with these initial few steps to prepare the certificate request:

1. On the Stratusphere Collector appliance local console, log in using User ID: '`friend`' and Password: '`sspassword`' first.
2. Switch to '`root`' user using the following command and enter the password when prompted (default: '`sspassword`'):
   - `su -`
3. Change to the following folder using the command:
   - `cd /home/friend`
4. Please enter the following commands:
   - `openssl genrsa 2048 > /etc/lwl/ssl/ssl.key.2048`
   - `cp /etc/lwl/ssl/ssl.key /etc/lwl/ssl/ssl.key.original`
5. Generate a certificate request on the Stratusphere Collector using the existing SSL Key.
   - `openssl req -key /etc/lwl/ssl/ssl.key.2048 -out colcertrequest.csr -new -sha256`

   When prompted for common name, make sure you provide your Collector's fully qualified DNS name.
   - `common name: <coldnsname.domain.com>`
6. You will find the certificate request generated in the following location: `/home/friend/colcertrequest.csr`
7. Change ownership of the file so that it accessible using the 'friend' user.
   - `chown friend:friend /home/friend/colcertrequest.csr`
8. Use WinSCP or FileZilla or similar software to download this certificate request '`/home/friend/colcertrequest.csr`' file to your local desktop. In WinSCP or FileZilla, use User ID: '`friend`' and Password: '`sspassword`' as credentials within the program. Use the SCP protocol with WinSCP (Port 22).
9. Provide this certificate request file to your security provider or Certifying Authority and request that they provide the SSL Certificate specifically in **base64 / PEM** format. For these instructions we will call it '`colsslcert.crt`' – this is the actual SSL Certificate you will receive back from your security provider or Certifying Authority.

Pause here until you receive your SSL certificate from your provider. After receiving your SSL Certificate from your provider, complete the process with the remaining instructions:

10. Use WinSCP or FileZilla or similar software to upload this '`colsslcert.crt`' SSL Certificate file to your Stratusphere Hub in the '`/home/friend/colsslcert.crt`' location. In WinSCP or FileZilla, use User ID: '`friend`' and Password: '`sspassword`' as credentials within the program. Use the SCP protocol with WinSCP (Port 22).

11. On the Stratusphere Collector local console, while still logged in as the root user, make a copy the original SSL certificate as a backup:
    - `cp /etc/lwl/ssl/ssl.crt /etc/lwl/ssl/ssl.crt.orig`
12. Place the new key and certificate in place of the original and modify the file permissions as follows:
    - `cp /etc/lwl/ssl/ssl.key.2048 /etc/lwl/ssl/ssl.key`
    - `mv /home/friend/colsslcert.crt /etc/lwl/ssl/ssl.crt`
    - `chown root:root /etc/lwl/ssl/ssl.crt`
    - `chmod 644 /etc/lwl/ssl/ssl.crt`
    - `chmod 640 /etc/lwl/ssl/ssl.key`
    - `restorecon –r /etc/lwl/ssl`
13. Restart the Collector to load the newly added SSL Certificate:
    - `/etc/init.d/httpd restart`