liquidware

Stratusphere™ TechBrief

Placing Signed SSL Certificates on the Appliances

Overview

> **Note:** This document applies to Stratusphere versions 6.6.0-2 and earlier. For instructions on how to place signed SSL certificates on appliances starting with Stratusphere 6.6.1, refer to the 6.6.1 version of this document.

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.

If you are using a version of Stratusphere Hub, Database, and Collector older than 5.6.0, 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 console users as per the platform i.e., `<username>` as `friend` on VMware, Citrix, and Nutanix, `ec2-user` on AWS, `azureuser` on Azure, 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, an SCP client such as Windows 10 Command Prompt and 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 your favorite SCP client such as WinSCP or FileZilla or similar to download certificate requests and upload the SSL Certificate files.
5. 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. You will then use the new certificate to complete the process.

Scenarios

1. Ad Hoc: Import and Install a PFX Certificate
2. Traditional: Generate a Request, Import & Install an SSL certificate.

Scenario 1: Ad Hoc: Import and Install a PFX Certificate

This scenario applies when the IT or Security department created a certificate without using a request generated by a Stratusphere appliance. It walks the user through the steps to import the certificate, apply the right permissions, and then install it in the appropriate locations.

Instructions for the Stratusphere Hub & Collector Appliances

1. Use your favorite SCP client, such as WinSCP, to upload the PFX file to `/home/<username>/` (replace `<username>` with `friend/ec2-user/azureuser`) on the Hub or Collector using credentials for the `<username>` on your platform i.e., `<username>` as `friend` on VMware, Citrix, and Nutanix, `ec2-user` on AWS, and `azureuser` on Azure.
2. Use your favorite SSH client, such as Windows 10 Command Prompt or PuTTY, to connect and log in using the credentials for `<username>` and run `sudo bash` to change to `root` user. When prompted, enter the password for your `<username>`.
3. Export the certificate from the PFX file by running the following command on the command line (replace `<username>` as appropriate along with the OFX file name YOURCERTNAME):

```
openssl pkcs12 -in /home/<username>/YOURCERTNAME.pfx -clcerts -nokeys -out
/home/<username>/ssl.crt.new
```

4. Export the private key file from the PFX file:

```
openssl pkcs12 -in /home/<username>/YOURCERTNAME.pfx -nocerts -nodes -out
/home/<username>/ssl.key.new
```

5. Remove the passphrase from the private key (if needed):

```
openssl rsa -in /home/<username>/ssl.key.new -out /home/<username>/ssl.key.new
```

6. Back up the working or existing certificate and key:

```
cp /etc/lwl/ssl/ssl.crt /etc/lwl/ssl/ssl.crt.backup
cp /etc/lwl/ssl/ssl.key /etc/lwl/ssl/ssl.key.backup
```

7. Copy the new certificate and key into the same location:

```
cp /home/<username>/ssl.crt.new /etc/lwl/ssl/ssl.crt
cp /home/<username>/ssl.key.new /etc/lwl/ssl/ssl.key
```

8. Update ownership, permissions, and the security context of the certificate and key:

```
chown root:root /etc/lwl/ssl/ssl.crt
chmod 644 /etc/lwl/ssl/ssl.crt
chmod 640 /etc/lwl/ssl/ssl.key
restorecon -RF /etc/lwl/ssl
```

9. Restart the Web Server to load the newly added SSL Certificate.

   On versions up to 6.1.1, use the following command:

```
/etc/init.d/httpd restart
```

   On versions 6.1.3, 6.1.4, use the following command:

```
/etc/init.d/lwl-httpd24 restart
```

   On versions 6.5.0 and higher, use the following command:

```
systemctl restart httpd
```

10. Check that httpd is running:

    On versions up to 6.1.1, use the following command:

```
/etc/init.d/httpd status
```

On versions 6.1.3, 6.1.4, use the following command:

```
/etc/init.d/lwl-httpd24 status
```

On versions 6.5.0 and higher, use the following command:

```
systemctl status httpd
```

11. If httpd restarted successfully after the cert was replaced, the Stratusphere Web UI should be accessible. Check that your browser shows the correct certificate.

Instructions for the Stratusphere Database Appliances

1. Use your favorite SCP client, such as WinSCP, to upload the PFX file to `/home/<username>/` (replace `<username>` with `friend/ec2-user/azureuser`) on the Database using credentials for the `<username>` on your platform i.e., `<username>` as `friend` on VMware, Citrix, and Nutanix, `ec2-user` on AWS, and `azureuser` on Azure.
2. Use your favorite SSH client, such as Windows 10 Command Prompt or PuTTY, to connect and log in using the credentials for `<username>` and run `sudo bash` to change to `root` user. When prompted, enter the password for your `<username>`.
3. Export the certificate from the PFX file by running the following command on the command line (replace `<username>` as appropriate along with the OFX file name YOURCERTNAME):

```
openssl pkcs12 -in /home/<username>/YOURCERTNAME.pfx -clcerts -nokeys -out
/home/<username>/server.crt.new
```

4. Export the private key file from the PFX file:

```
openssl pkcs12 -in /home/<username>/YOURCERTNAME.pfx -nocerts -nodes -out
/home/<username>/server.key.new
```

5. Remove the passphrase from the private key (if needed):

```
openssl rsa -in /home/<username>/server.key.new -out /home/<user-
name>/server.key.new
```

6. Back up the working or existing certificate and key:

```
cp /var/lib/pgsql/current/data/server.crt /var/lib/p-
gsql/current/data/server.crt.backup
cp / var/lib/pgsql/current/data/server.key / var/lib/p-
gsql/current/data/server.key.backup
```

7. Copy the new certificate and key into the same location:

```
cp /home/<username>/server.crt.new / var/lib/pgsql/current/data/server.crt
cp /home/<username>/server.key.new / var/lib/pgsql/current/data/server.key
```

8. Update ownership, permissions, and the security context of the certificate and key:

```
chown postgres:postgres / var/lib/pgsql/current/data/server.crt
chmod 400 / var/lib/pgsql/current/data/server.crt
chown postgres:postgres / var/lib/pgsql/current/data/server.key
chmod 400 / var/lib/pgsql/current/data/server.key
```

9. Restart the Postgres Database Server to load the newly added SSL Certificate.

   On versions prior to 6.5.0, use the following command:

```
/etc/init.d/postgresql<PRESS-TAB-KEY> restart
```

   On versions 6.5.0 and higher, use the following command:

```
systemctl restart postgresql-12
```

10. Check whether the Postgres Database Server is running:

    On versions prior to 6.5.0, use the following command:

    ```
    /etc/init.d/postgresql-<PRESS-TAB-KEY> status
    ```

    On versions 6.5.0 and higher, use the following command:

    ```
    systemctl status postgresql-12
    ```

    If postgresql-12 service restarted successfully, then new certificate was accepted.

Scenario 2: Traditional: Generate a Request, Import, and Install an SSL Certificate

In this scenario, Stratusphere administrators will execute a script which prompts the end user for relevant inputs to create a certificate request. After entering information for the generation of the certificate request, the end user must download the certificate request file, send it to the Certifying Authority (CA) to receive the certificate back, and then place it back on the appliance to install it.

Instructions for the Stratusphere Hub Appliance

1. Use your favorite SSH client, such as Windows 10 Command Prompt or PuTTY, to connect and log in to the Stratusphere Hub appliance console using the credentials for `<username>` on your platform i.e., `<username>` as `friend` on VMware, Citrix, and Nutanix, `ec2-user` on AWS, and `azureuser` on Azure. The default password is `sspassword`.
2. Switch to the `root` user by executing the `sudo bash` command. When prompted, enter the password for your `<username>`. The default password is `sspassword`.
3. Change to the following folder using the command:

    ```
    cd /home/friend
    ```

4. Enter the following commands to generate a new key and backup the original:

```
openssl genrsa 2048 > /etc/lwl/ssl/ssl.key.2048
cp /etc/lwl/ssl/ssl.key /etc/lwl/ssl/ssl.key.original
```

5. Press **CTRL+C** on your keyboard to copy the information below into a text editor like Notepad:

```
[req]
default_bits        = 2048
distinguished_name  = req_distinguished_name
req_extensions      = req_ext
[req_distinguished_name]
countryName         = Country Name (2 letter code)

stateOrProvinceName = State or Province Name (full name)

localityName        = Locality Name (eg, city)

organizationName    = Organization Name (eg, company)

commonName          = Common Name (e.g. server FQDN or YOUR name)

[req_ext]

subjectAltName      = @alt_names

[alt_names]

DNS.1               = insert your alternate dns here

DNS.2               = insert your alternate dns here

DNS.3               = insert your alternate dns here
```

6. Within Notepad, edit the lines under `[alt_names]` for `DNS.1` through `DNS.3` and enter additional DNS names for the Hub. This step is necessary to address compatibility errors on Google Chrome related to missing `Subject Alternative Name` and/or `NET::ERR_CERT_COMMON_NAME_INVALID` errors. After the DNS alternate names are updated, copy the entire contents of Notepad to your clipboard by pressing **CTRL+C**.

7. In the SSH Client's command prompt used in #3 above, execute the following command to open a text editor like vi.

```
vi /etc/lwl/ssl/name.req.config
```

This opens a blank text configuration file that needs to be populated with what is copied to the clipboard.

8. Perform the following to save the contents to the file:
   a. Press the `I` key to go into insert mode.
   b. Right-click your mouse to paste the clipboard contents from Notepad within the vi editor.
   c. Press the **ESC** key to exit insert mode.
   d. Type `:wq!` to write and quit the vi editor.
9. Execute the following command in the command prompt to generate a certificate request on the Stratusphere Hub using the existing SSL Key.

```
openssl req -key /etc/lwl/ssl/ssl.key.2048 -config /etc/lwl/ssl/name.req.config
-out hubcertrequest.csr -new -sha256
```

10. When prompted for a common name, provide your Hub's fully qualified DNS name.

```
common name: <hubdnsname.domain.com>
```

The certificate request is generated in the following location:

```
/home/friend/hubcertrequest.csr
```

11. Enter the following to change ownership of the file so that it is accessible to the `<username>` for the platform, such as `friend`, `ec2-user` or `azureuser` user. Here is an example for the `friend` user:

```
chown friend:friend /home/friend/hubcertrequest.csr
```

12. Use your favorite SCP client, such as WinSCP or similar software, to connect to the appliance using its IP or DNS address, with SCP protocol and connecting to Port 22 using the credentials of the platform `<username>` (e.g., `friend` or `ec2-user` or `azureuser` user) to download this certificate request from `/home/friend/hubcertrequest.csr` file to your local desktop.

13. 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, call the SSL Certificate file `hubsslcert.crt`. When you see references to `hubsslcert.crt` in this document, you should substitute the actual name of the SSL Certificate file you received from your security provider or Certifying Authority.

    Important: Pause here until you receive your SSL certificate from your provider, then complete the process using the following instructions.

14. Use your favorite SCP client, such as WinSCP or similar software, to connect to the appliance using its IP or DNS address, with SCP protocol and connecting to Port 22 using the credentials of the platform `<username>` (e.g., `friend` or `ec2-user` or `azureuser` user) to upload the `hubsslcert.crt` SSL Certificate file to your Stratusphere Hub or Collector in the `/home/friend/hubsslcert.crt` location.

15. 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
```

16. 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 -RF /etc/lwl/ssl
```

17. Restart the Web Server to load the newly added SSL Certificate.

    On versions up to 6.1.1, use the following command:

```
/etc/init.d/httpd restart
```

On versions 6.1.3 to 6.1.5, use the following command:

```
/etc/init.d/lwl-httpd24 restart
```

On versions 6.5.0 and higher, use the following command:

```
systemctl restart httpd
```

18. Using your browser of choice, log in to 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 the Stratusphere Database Appliance

1. Use your favorite SSH client, such as Windows 10 Command Prompt or PuTTY, to connect and log in to the Stratusphere Database appliance console using the credentials for `<username>` on your platform i.e., `<username>` as `friend` on VMware, Citrix, and Nutanix, `ec2-user` on AWS, and `azureuser` on Azure. The default password is `sspassword`.
2. Switch to the `root` user by executing the `sudo bash` command. When prompted, enter the password for your `<username>`.
3. Change to the following folder using the command:

```
cd /home/friend
```

4. 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/p-
gsql/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 dbcer-
trequest.csr -new -sha256
```

6. When prompted for common name, make sure you provide your database's fully qualified DNS name.

```
common name: <dbdnsname.domain.com>
```

7. The certificate request is generated in the following location:

```
/home/friend/dbcertrequest.csr
```

8. Enter the following to change ownership of the file so that it is accessible to the `<username>` for the platform, such as `friend`, `ec2-user` or `azureuser` user. Here is an example for the `friend` user:

```
chown friend:friend /home/friend/dbcertrequest.csr
```

9. 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 the User ID `friend` and the password `sspassword` as credentials within the program. Use the SCP protocol with WinSCP (Port 22).

10. 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, call the SSL Certificate file `server.crt`. When you see references to `server.crt` in this document, you should substitute the actual name of the SSL Certificate file you received from your security provider or Certifying Authority.

> **Important:** Pause here until you receive your SSL certificate from your provider, then complete the process using the following instructions.

11. Use WinSCP or FileZilla or similar software to upload the `server.crt` SSL Certificate file to your Stratusphere database in the `/home/friend/server.crt` location. In WinSCP or FileZilla, use the User ID `friend` and the password `sspassword` as credentials within the program. Use the SCP protocol with WinSCP (Port 22).

12. 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/p-
gsql/current/data/server.crt.orig
```

13. 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/p-
gsql/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
chown postgres:postgres /var/lib/pgsql/current/data/server.key
chmod 400 /var/lib/pgsql/current/data/server.key
```

14. Restart the database server to load the newly added SQL Certificate:

    On versions prior to 6.5.0, use the following command:

```
/etc/init.d/postgresql<PRESS-TAB-KEY> restart
```

    On versions 6.5.0 and higher, use the following command:

```
systemctl restart postgresql-12
```

Instructions for the Stratusphere Collector Appliance

1. Use your favorite SSH client, such as Windows 10 Command Prompt or PuTTY, to connect and log in to the Stratusphere Hub appliance console using the credentials for `<username>` on your platform i.e., `<username>` as `friend` on VMware, Citrix, and Nutanix, `ec2-user` on AWS, and

`azureuser` on Azure. The default password is `sspassword`.

2. Switch to the `root` user by executing the `sudo bash` command. When prompted, enter the password for your `<username>`. The default password is `sspassword`.
3. Change to the following folder using the command:

```
cd /home/friend
```

4. Enter the following commands to generate a new key and backup the original:

```
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
```

6. When prompted for common name, provide your Collector's fully qualified DNS name.

```
common name: <coldnsname.domain.com>
```

The certificate request is generated in the following location:

```
/home/friend/colcertrequest.csr
```

7. Enter the following to change ownership of the file so that it is accessible to the `<username>` for the platform, such as `friend`, `ec2-user` or `azureuser` user. Here is an example for the `friend` user:

```
chown friend:friend /home/friend/colcertrequest.csr
```

8. Use WinSCP or FileZilla or similar software download this certificate request `/home/-friend/colcertrequest.csr` file to your local desktop. In WinSCP or FileZilla, use the 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.

10. For these instructions, call the SSL Certificate file `colsslcert.crt`. When you see references to `colsslcert.crt` in this document, you should substitute the actual name of the SSL Certificate file you received from your security provider or Certifying Authority.

> **Important:** Pause here until you receive your SSL certificate from your provider, then complete the process using the following instructions.

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

12. 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
```

13. 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 -RF /etc/lwl/ssl
```

14. Restart the Collector to load the newly added SSL Certificate.

    On versions up to 6.1.1, use the following command:

```
/etc/init.d/httpd restart
```

On versions 6.1.3 to 6.1.5, use the following command:

```
/etc/init.d/lwl-httpd24 restart
```

On versions 6.5.0 and higher, use the following command:

```
systemctl restart httpd
```