Article Number: 000157711

Print

Isilon: PowerScale: OneFS: How to replace or renew the SSL certificate that is used for the Isilon web administration interface

Summary: Steps to renew or replace the SSL Certificate for OneFS web administration interface.

Audience Level: Customer

Article Content

Instructions

Introduction

This article explains how to replace or renew the Secure Sockets Layer (SSL) certificate for the Isilon web administration interface. The following procedures include options to complete a self-signed certificate replacement or renewal, or to request an SSL replacement or renewal from a Certificate Authority (CA).

Requisite tools or skills

To complete this task, you must have the URL for accessing the Isilon web administration interface. (The examples in this article use https://isilon.example.com:8080/.) You should also be comfortable running commands from the command line.

Pre-requisites

Reference information

The following lists include the default locations for the *server.crt* and *server.key* files in OneFS 7.0.x and OneFS 8.0.0.*x*. In the procedures that follow, update the steps to match this information for the version of OneFS that is installed.

OneFS 7.0.*x* and later

- SSL certificate: */usr/local/apache24/conf/ssl.crt/server.crt*
- SSL certificate key: */usr/local/apache24/conf/ssl.key/server.key*

OneFS 8.0.1.*x* and later

1. Obtain the list of certificates from running below command:

   ```
   isi certificate server list
   ```
2. Save a backup of the original certificate and key (only for OneFS 7.0.x to 8.0.0.x).
   1. Open an SSH connection on any node in the cluster and log in using the "root" account.
   2. Run the following commands to create a backup location and save the original key and certificate:

      ```
      mkdir -p /ifs/data/Isilon_Support/original_ssl_backup
      cp /usr/local/apache24/conf/ssl.crt/server.crt /ifs/data/Isilon_Support/original_ssl_backup
      cp /usr/local/apache24/conf/ssl.key/server.key /ifs/data/Isilon_Support/original_ssl_backup
      ```

Procedure

1. Create a local working directory.

   ```
   mkdir /ifs/local
   cd /ifs/local
   ```

   Verify if you want to just renew an existing certificate or if you want to create a certificate from scratch.

   Renew an existing self-signed Certificate.

This creates a renewal certificate that is based on the existing (stock) **ssl.key.** Run the following command to create a two-year certificate. Increase or decrease the value for -days to generate a certificate with a different expiration date:

```
cp /usr/local/apache2/conf/ssl.key/server.key ./ ; openssl req -new -days 730 -nodes -x509 -key server.key -out
server.crt
```

Answer the system prompts to complete the process to generate a self-signed SSL certificate, entering the appropriate information for your organization.

For example:

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (eg, city) []:Seattle
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Isilon
Organizational Unit Name (eg, section) []:Support
Common Name (e.g. server FQDN or YOUR name) []:isilon.example.com
Email Address []:support@example.com
```

When finished entering the information, the server.csr and server.key files appear in the /ifs/local directory.

- (Optional) Verify the integrity and attributes of the certificate:

  ```
  openssl x509 -text -noout -in server.crt
  ```

  Go to "**Add the certificate to the cluster.**" section of this KB after this step.

Create a certificate and key.

This procedure shows how to create a new private key and SSL certificate. Run the following command to create an RSA 2048-bit private key:

```
openssl genrsa -out server.key 2048
```

Create a certificate signing request:

```
openssl req -new -nodes -key server.key -out server.csr
```

Enter the appropriate information for your organization.

```
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

- (Optional) Generate a CSR for a Certificate Authority which includes Subject-Alternative-Names. If additional DNS is needed, it can be added by using a comma, (For example: **DNS:**example.com**,DNS:**www.example.com)

  ```
  openssl req -new -nodes -key server.key -out server.csr -reqexts SAN -config <(cat /etc/ssl/openssl.cnf <(printf "
  [SAN]\nsubjectAltName=DNS:example.com"))
  ```

When prompted, type the information to be incorporated into the certificate request. When finished entering the information, the server.csr and server.key files appear in the /ifs/local directory.

Verify if you want to self-sign the certificate or get it signed by a Certificate Authority.

Self-Sign the SSL Certificate.

To self-sign the Certificate with the key, run the below command which creates a new self-signed certificate which is valid for 2 years:

```
openssl x509 -req -days 730 -in server.csr -signkey server.key -out server.crt
```

Verify that the Key matches the certificate, both the commands should return the same md5 value:

```
openssl x509 -noout -modulus -in server.crt | openssl md5
openssl rsa -noout -modulus -in server.key | openssl md5
```

Go to "**Add the certificate to the cluster.**" section of this KB after this step.

Get a CA to Sign the Certificate.

If a CA is signing the certificate, ensure that the new SSL certificate is in x509 format, and includes the entire certificate trust chain.

It is common for CAs to return the new SSL certificate, the intermediate certificate, and the root certificate in separate files.

If the CA has done this, you **must** manually create the PEM formatted certificate.

Order matters when creating the PEM formatted certificate. Your cert must be the top of the file, followed by the intermediate certificates, and the root certificate must be at the bottom.

Here is an example of what the PEM formatted file looks like:

```
-----BEGIN CERTIFICATE-----
<The contents of your new TLS certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<The contents of the intermediate certificate>
<Repeat as necessary for every intermediate certificate provided by your CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<The contents of the root certificate file>
-----END CERTIFICATE-----
```

An easy way to create the PEM formatted file from the CLI is to cat the files (remember, the order of the files matter):

```
cat CA_signed.crt intermediate.crt root.crt > onefs_pem_formatted.crt
```

Copy the onefs_pem_formatted.crt file to /ifs/local and rename it to server.crt.

Note: If a .cer file is received, rename it to a .crt extension.

- (Optional) Verify the integrity and attributes of the certificate:

  ```
  openssl x509 -text -noout -in server.crt
  ```

Add the certificate to the cluster.

- **FOR OneFS 7.0.X TO 8.0.1.X**

  1. Install the new certificate and key on each node:

     ```
     isi services -a isi_webui disable
     chmod 640 server.key
     chmod 640 server.crt
     isi_for_array -s 'cp /ifs/local/server.key /usr/local/apache2/conf/ssl.key/server.key'
     isi_for_array -s 'cp /ifs/local/server.crt /usr/local/apache2/conf/ssl.crt/server.crt'
     isi services -a isi_webui enable
     ```

- **FOR OneFS 8.0.1.X AND LATER**

  1. Import the new certificate and key into the system:

     ```
     isi certificate server import /ifs/local/server.crt /ifs/local/server.key
     ```

  2. Verify that the certificate imported successfully:

     ```
     isi certificate server list -v
     ```

  3. Set the imported certificate as default:

- For OneFS 8.0 and 8.1, the command is:

  ```
  isi certificate server modify --id=<id_of_cert_to_set_as_default> --default
  ```

- For OneFS 8.2 and later, the command is:

  ```
  isi certificate settings modify --default-https-certificate=<id_of_cert_to_set_as_default>
  ```

4. Use the below command to confirm that the imported certificate is being used as default by verifying status of "Default HTTPS Certificate":

   ```
   isi certificate settings view
   ```

5. If there is an unused or outdated cert, delete this with the command:

   ```
   isi certificate server delete --id=<id_of_cert_to_delete>
   ```

6. View the new imported cert with command:

   ```
   isi certificate server view --id=<id_of_cert>
   ```

   Note: Ports 8081 and 8083 still use the certificate from the local directory for SSL. Follow the below steps if you want to use the new certificates for port 8081/8083.

   ```
   isi services -a isi_webui disable
   chmod 640 server.key
   chmod 640 server.crt
   isi_for_array -s 'cp /ifs/local/server.key /usr/local/apache2/conf/ssl.key/server.key'
   isi_for_array -s 'cp /ifs/local/server.crt /usr/local/apache2/conf/ssl.crt/server.crt'
   isi services -a isi_webui enable
   ```

Verification

There are two methods for verifying the updated SSL certificate.

- ### From a web browser

  1. Browse to **https://<common name>:8080**, where <common name> is the hostname that is used to access the Isilon web administration interface (for example, *isilon.example.com*).
  2. View the security details for the web page. The steps to do this vary by browser. In some browsers, click the padlock icon in the address bar to view the security details for the web page.
  3. In the security details for the web page, verify that the subject line and other details are correct. An output similar to the following is displayed, where <yourstate>, <yourcity>, and <your company> are the state, city, and name of your organization:

     ```
     Subject: C=US, ST=<yourstate>, L=<yourcity>, O=<yourcompany>,
     CN=isilon.example.com/emailAddress=support@example.com
     ```

- ### From a command line

  1. Open an SSH connection on any node in the cluster and log in using the "root" account.
  2. Run the following command:

     ```
     echo QUIT | openssl s_client -connect localhost:8080
     ```

  3. An output similar to the following is displayed, where <yourstate>, <yourcity>, and <your company> are the state, city, and name of your organization:

     ```
     Subject: C=US, ST=<yourstate>, L=<yourcity>, O=<yourcompany>,
     CN=isilon.example.com/emailAddress=support@example.com
     ```

Additional Information

Note:

Event alert also triggers on Isilon as below:

```
SW_CERTIFICATE_EXPIRING: X.509 certificate default is nearing expiration:

Event: 400170001
Certificate 'default' in '**' store is nearing expiration:
```

Isilon does not auto-renew the certificate itself as it has to be renewed manually by following the steps on this KB.

Videos

Article Properties

Affected Product

PowerScale OneFS

Product

Isilon

Last Published Date

15 Dec 2022

Version

12

Article Type

How To