Renew FileWave Server Self-signed Certificate

Description

For simplicity, we should recommend Renewing with an Official SSL certificate or Let's Encrypt Setup for FileWave Server (Debian)

> Using a self-signed certificate is strongly discouraged for a production server.

Information

A self-signed certificate may not be trusted by devices out of the box. Instead, the device requires a local copy to be able to trust the certificate. Prior to FileWave 13, this has only affected Mobile devices: Renew MDM self signed SSL certificate on iOS

However, FileWave uses the certificate for additional security for non MDM communication and initial installation or upgrading to FileWave 13 from a release of 12 or lower.

> Renewal though requires additional steps to ensure device communication is not lost.

Directions

The 'fwcontrol' command for creating certificates is now a 2 step process, where 'fqdn' should be the Fully Qualified Domain Name of your FileWave Server, e.g. demo.filewave.ch:

```
sudo fwcontrol server generateSelfSignedCert --create --cn=fqdn [--country COUNTRY] [--state STATE] [--locality LOCALITY] [--organization ORGANIZATION] [--ou ORGANIZATIONAL_UNIT] [--email EMAIL] [--ignore_name_mismatch]
sudo fwcontrol server generateSelfSignedCert --install
```

Bracketed options are not required, but may be specified.

Step 1

Certificate Generation

Using demo.filewave.ch as an example:

```
sudo fwcontrol server generateSelfSignedCert --create --cn=demo.filewave.ch. --country Switzerland
```

This first step generates a new certificate, but unlike before, it does not overwrite the current active certificate. Instead, this certificate is in a 'pending' state. You should see the following warning when creating the certificate:

```
WARNING: Self-signed certificates are NOT recommended! If you install one, clients in version 13 or greater will no longer allow connections with the FileWave Server unless you put the new self-signed certificate in their trust store.
A self-signed certificate has been successfully created and is now pending for later installation on the server.

IMPORTANT!
- Before installing it, you must deploy it to the trust store of any device whose FileWave Client is in version 13 or greater, otherwise these clients will no longer be able to connect to the server!
To do so, you can create a fileset with a copy of /usr/local/filewave/certs/server.crt.pending to be deployed in the trust store folder.
- Once you are ready to install the new self-signed certificate and if you understand the risks, please run this command again with option --install.
running restart apache command
```

Instead a new certificate key/crt pair of files may be seen in the following server folder and will show as 'pending', along with the original key/crt pair:

```
/usr/local/filewave/certs/server.crt
/usr/local/filewave/certs/server.crt.pending
/usr/local/filewave/certs/server.key
/usr/local/filewave/certs/server.key.pending
```

As indicated by the Important message, all clients will require a copy of this certificate to communicate with the server. During transition, it is important that both original and new certificate are installed on devices. Copy the server.crt.pending and rename appropriately for deployment. e.g. server.2019.04.30.crt

Mobile Devices

Installing the new certificate on Mobile devices is as before, except a profile needs to be made with this new certificate as well as the current certificate:

Renew MDM self signed SSL certificate with iOS devices

Computers

Installing the new certificate on Computers is the same as the process for Upgrading to FileWave 13, but this new certificate needs to be added to a Fileset manually. This could either be the current FileWave Upgrade Fileset or a new Fileset. Location of the file is either:

macOS:

macOS Client/Booster Trust Store

```
/private/var/FileWave/trust_store
```

Windows:

Windows Client/Booster Trust Store

```
C:\ProgramData\FileWave\FWClient\trust_store
```

⚠ Set the certificate 'Verification' to 'Ignore At Verify' to ensure it is never removed

⚠ If the new certificate should become live on the server prior to the clients receiving this Fileset, those devices will no longer be manageable through FileWave and a manual process will be required to locally instal the certificate.

Whichever option is chosen, a method should be designed to monitor the installation process. Only once all devices are updated, should the 'pending' certificate become the active server certificate.

Options for monitoring could include:

- Fileset Reports
- Custom Fields

A Custom Field could take the following form (assuming the example file name of 'server.2019.04.30.crt'):

macOS Example Custom Field

```
#!/bin/bash

server_cert=$(find /var/FileWave/trust_store -name "server.*.crt")

if [[ "$server_cert" != "" ]]
then
    echo Yes
else
    echo No
fi

exit 0
```

Step 2

This second step enables the 'pending' certificate as the active certificate, replacing the original server certificate file.

```
sudo fwcontrol server generateSelfSignedCert --install
```

Once all clients have the new certificate within their respective trust stores, the 'pending' server certificate may now become active. When this update of the certificate occurs, any other elements requiring the server certificate should also be updated as this time.

DEP

The server certificate is stored as an 'Anchor certificate' within any created DEP profile. As with any certificate change, once the

certificate is renewed, new DEP profiles should be created; do not duplicate.

Custom PKG/MSI

The Custom Client Installer also needs to include the certificate. The following links allow for uploading the current server certificate within the 'Options'

- macOS Custom Client Builder
- Windows Custom Client Builder

Details highlighted on: Self-Signed Certificates Going Forward

---

Revision #8
★Created 10 July 2023 23:19:44 by Josh Levitsky
✎Updated 23 April 2024 14:40:05 by Josh Levitsky