How to change the SSL certificate in VoipNow

This article describes how to change the SSL certificate used by your VoipNow 3 or higher HTTP server.

Requirements

Before you start, make sure that the following requirements are met:

- You have the latest VoipNow version (e.g. VoipNow 3 or higher)
- You have access and basic knowledge for using a SSH client (e.g. Putty).

Change the server's SSL certificate

STEP 1: Generate private key and request certificate.

Log in as root using a SSH client, create a certificate request, and send it to your CA authority:

```
[root@server ~]# openssl req -nodes -newkey rsa:2048 -keyout /root/new.key -out /root/certrequest.csr
```

This command will generate a **2048-bit key** file. Then it will ask basic information about the entity being certified. The Private Key file generated with above command will not have a secret pass-phrase.

When you will receive the message:

"Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:"

DO NOT SUBMIT ANY PASSWORD, just press enter.

STEP 2: Save and keep your new key because you will need it later.

Send the `certrequest.csr` to to your CA authority and they will send back to you a new certificate. After you receive the certificate, copy it on your server in your root directory. Let us assume that the certificate name is `newcert.crt`.

STEP 3: Make a backup copy of the existing certificate.

Create a backup copy of the existing httpd.pem. If something goes wrong you can restore the certificate from backup:

```
[root@server ~]# cp /etc/voipnow/certs/http.pem /etc/voipnow/certs/http.pem.backup
```

VoipNow 3.0.7

If you are still using VoipNow 3.0.x, replace `/etc/voipnow/certs/http.pem` with `/usr/local/voipnow/admin/conf/voipnow.pem`

Install the new certificate

The `newcert.crt` contains the the primary certificate received from the CA authority.

The `voipnow.key` file contain the private key generated earlier.

If an intermediate certificate was provided by your CA authority, it should be concatenated into the same file as the primary certificate. Let's consider `intermediate_cert.crt` as the intermediate certificate for our example.

STEP 1: Copy the key to the proper location and rename the key:

```
[root@server ~]# cat /root/new.key /root/newcert.crt > /etc/voipnow/certs/http.pem
```

If you have an intermediate certificate, use this command:

```
[root@server ~]# cat /root/new.key /root/newcert.crt /root/intermediate_cert.crt > /etc/voipnow/certs/http.pem
```

VoipNow 3.0.7

If you are still using VoipNow 3.0.x, replace `/etc/voipnow/certs/http.pem` with `/usr/local/voipnow/admin/conf/voipnow.pem`

STEP 2: Change the permission and the ownership of `http.pem`:

```
[root@server ~]# chmod 400 /etc/voipnow/certs/http.pem
[root@server ~]# chown httpsa:httpsa /etc/voipnow/certs/http.pem
```

VoipNow 3.0.7

If you are still using VoipNow 3.0.x, replace `/etc/voipnow/certs/http.pem` with `/usr/local/voipnow/admin/conf/voipnow.pem`

Test installation of new certificate

Restart VoipNow HTTP service using:

```
[root@server ~]# /etc/init.d/voipnow restart
```

If everything goes well and VoipNow service starts without errors verify if the certificate is installed as should using SSL checker.

Related articles

- How to install a LetsEncrypt SSL certificate in VoipNow
- How to avoid the SSL Poodle attack
- How to change the SSL certificate in VoipNow
- Where can I find the VoipNow certificates
- How to change my 4PSA DNS Manager HTTP server SSL certificate