SSL certificates: Erneuern der TLS/SSL-Zertifikate

Sprachen:	**Deutsch** English
UCS	UCS 4

Die Kommunikation zwischen den verschiedenen Rechnern einer UCS-Domäne erfolgt größtenteils TLS/SSL-verschlüsselt. Bei der TLS/SSL-Verschlüsselung werden ein Root-Zertifikat und für jeden Rechner ein Rechnerzertifikat benötigt. Das Root-Zertifikat hat nur einen bestimmten Gültigkeitszeitraum, ebenso wie die mit dem Root-Zertifikat erstellten Rechnerzertifikate. Ist dieser Zeitraum abgelaufen, funktionieren Dienste, die ihre Kommunikation mit TLS/SSL verschlüsseln (z.B. LDAP, UMC) nicht mehr. Es ist deshalb notwendig, die Gültigkeit der Zertifikate regelmäßig zu prüfen und ggf. neue Rechnerzertifikate zu erstellen.

Die folgende Befehle müssen auf einem UCS Master durchgeführt werden.

Die Überprüfung, wie lange ein Rechnerzertifikat noch gültig ist, kann mit univention-certificate erfolgen:

Code:

```
univention-certificate dump -name ucs01.intra.example.org
[...]
Validity
Not Before: Jun 19 10:40:13 2016 GMT
Not After : Jun 18 10:40:14 2018 GMT
[...]
```

Hierbei ist immer der FQDN des Rechnernamens (Rechnername + Domain) anzugeben. Eine Liste aller verfügbaren Zertifikate erhält man mit

Code:

```
univention-certificate list
```

Normalerweise haben die Zertifikate aller Rechner einer UCS-Domäne das gleiche Gültigkeitsintervall (Standard sind 5 Jahre ab Erstellung). Wenn das Root-Zertifikat abläuft, wird auch die ganze Zertifikatskette als ungültig betrachtet. Daher müssen alle Zertifikate erneuert werden, sobald das Root-Zertifikat droht sein Gültigkeit zu verlieren. Um neue Zertifikate zu erstellen, ist folgendermaßen vorzugehen:

Sicherung der alten Zertifikate:

Code:

```
cp -a /etc/univention/ssl /etc/univention/ssl$(date --iso)
```

Erneuern der Zertifikate

Erneuerung des Root-Zertifikats, als Passwort ist der Inhalt der Datei **/etc/univention/ssl/password** anzugeben:

Code:

```
cd /etc/univention/ssl/ucsCA
openssl x509 -in CAcert.pem -out NewCAcert.pem -days "$(ucr get ssl/default/days)" \
    -passin file:/etc/univention/ssl/password \
    -signkey private/CAkey.pem
mv NewCAcert.pem CAcert.pem
```

Achtung: Bei UCS Systemen in einer Version älter als 2.0 lautet das Verzeichnis "/etc/univention/ssl/udsCA" statt "/etc/univention/ssl/ucsCA".

Erneuerung aller Rechnerzertifikate:

Code:

```
eval "$(ucr shell)"
cd /etc/univention/ssl
for i in *.$domainname; do univention-certificate renew -name $i -days "$(ucr get ssl/default/days)";
done
```

Kopieren der Zertifikate

Kopieren der neuen Zertifikate auf die anderen Rechnersysteme (jedes UCS/UCC System, außer UCS Backups - hier am Beispielrechner ucs03):

Code:

```
eval "$(ucr shell)"
cd /etc/univention/ssl/
scp ucsCA/CAcert.pem root@ucs03:/etc/univention/ssl/ucsCA/
scp -r ucs03.$domainname root@ucs03:/etc/univention/ssl/
scp -r ucs03.$domainname/* root@ucs03:/etc/univention/ssl/ucs03/
```

Dieser Schritt ist auf UCS Backups nicht zwingend erforderlich, denn dort erfolgt das Kopieren auch

automatisch per cron.

Um das neu erstellte Zertifikat allen Benutzern über die zentrale Verwaltungs-Webseite des UCS Masters zugänglich zu machen, kann der folgende Befehl verwendet werden:

cp /etc/univention/ssl/ucsCA/CAcert.pem /var/www/ucs-root-ca.crt

Nach dem Aktualisieren der Zertifikate werden die neuen Informationen noch nicht in der Univention Management Console (UMC) und im entsprechenden Monitoring-Check angezeigt.
Diese würden erst bei der nächsten regulären Prüfung aktualisiert, da der dafür angelegte Cronjob nur einmal am Tag ausgeführt wird.
Um die Gültigkeit der Zertifikate sofort prüfen zu können müssen die entsprechenden Univention Configuration Registry Variablen (ssl/validity/days) ausgewertet werden. Dies kann durch den Aufruf des folgenden Skriptes erfolgen:

/usr/sbin/univention-certificate-check-validity

Alle Dienste, die TLS/SSL-Verschlüsselung benutzen, müssen neu gestartet werden.
Alternativ kann ein Neustart des Systems durchgeführt werden, wenn nicht bekannt ist, welche Dienste mit TLS/SSL in Verbindung stehen.

SAML SSO

Seit UCS 4.1 sind UCS Master und alle UCS Backup auch **SAML Identity provider** und jedes UCS System in der Domäne, auf dem die Univention Management Console (UMC) läuft ist ein **SAML Service provider**. Die SAML Implementierung in UCS verwendet ebenfalls TLS-Verschlüsselung sowie ein Zertifikat, das auf den DNS Alias **ucs-sso.$domainname** ausgestellt ist - dieses muss ebenfalls ersetzt werden.

Auf jedem SAML Identity provider (UCS Master und alle UCS Backups) muss folgendes ausgeführt werden:

Code:

```
eval "$(ucr shell domainname)"
cp "/etc/univention/ssl/ucs-sso.${domainname}/cert.pem"
"/etc/simplesamlphp/ucs-sso.${domainname}-idp-certificate.crt"
cp "/etc/univention/ssl/ucs-sso.${domainname}/private.key"
"/etc/simplesamlphp/ucs-sso.${domainname}-idp-certificate.key"
service univention-saml restart
```

Auf jedem SAML Service provider (jedes UCS System, das Mitglied der Domäne ist) muss das neue Zertifikat eingerichtet werden:

Code:

```
eval "$(ucr shell ucs/server/sso/fqdn)"
rm /usr/share/univention-management-console/saml/idp/*.xml
ucr set
umc/saml/idp-server="https://${ucsserverssofqdn}/simplesamlphp/saml2/idp/metadata.php" ¦¦
echo 'Failed!'
/etc/init.d/univention-management-console-web-server restart
univention-run-join-scripts --force --run-scripts 92univention-management-console-web-server.inst
```

Cyrus

Auf Rechnern, auf denen der cyrus-Mailserver läuft, sind zusätzlich die Dateien cert.pem und private.key nach /var/lib/cyrus/ zu kopieren:

Code:

```
cp /etc/univention/ssl/"$(hostname -f)"/cert.pem /var/lib/cyrus/
cp /etc/univention/ssl/"$(hostname -f)"/private.key /var/lib/cyrus/
```

Im Anschluß muß Besitzer- und Gruppezugehörigkeit der kopierten Dateien auf dem Mailserver angepasst werden

```
chown cyrus:mail /var/lib/cyrus/cert.pem
chown cyrus:mail /var/lib/cyrus/private.key
```

AD-Connector

Wird der UCS AD-Connector eingesetzt, sollten die Zertifikate auch auf dem AD-System aktualisiert werden.
Hierfür können die neuen Zertifikate für das AD-Connector System über die UMC zum Download bereitgestellt werden:

```
cp /etc/univention/ssl/<FQDN des AD-Systems>/{cert.pem,private.key}
/var/www/univention-ad-connector/
chgrp www-data /var/www/univention-ad-connector/{cert.pem,private.key}
```

Anschließend können die Zertifikate wie in der AD-Connector Dokumentation beschrieben auf dem AD-System abgelegt werden.

RADIUS

Wird die RADIUS App (freeradius) eingesetzt, sind zusätzlich die Dateien cert.pem und private.key nach /etc/freeradius/ssl zu kopieren:

```
cp /etc/univention/ssl/"$(hostname -f)"/cert.pem /etc/freeradius/ssl/
cp /etc/univention/ssl/"$(hostname -f)"/private.key /etc/freeradius/ssl/
```

Im Anschluß muß Besitzer- und Gruppezugehörigkeit der kopierten Dateien auf dem Mailserver angepasst werden

```
chown root:freerad /etc/freeradius/ssl/cert.pem
chown root:freerad /etc/freeradius/ssl/private.key
```

Unique solution ID: #1000
Author: Janis Meybohm
Last update: 2017-08-08 17:46