Aufnahme ins Backup

Windows – Part 1

Im Service *Backup & Restore* ist Kanalverschlüsselung (TLS) Standard. Um TLS nutzen zu können, erstellen Sie mit OpenSSL ein *Certificate Request*, welches später von uns signiert zurückgeschickt wird:

1. **OpenSSL installieren**

   OpenSSL für Windows herunterladen:

   a) `https://www.openssl.org/community/binaries.html` oder

   b) `http://slproweb.com/products/Win32OpenSSL.html`

   ("light" - Version reicht, gibt's auch als 64bit). Unter Umständen muss noch das 'Microsoft Visual C++ 2008 Redistributable Package' installiert werden (auch hier gibt es Versionen für 32bit und 64bit). Link zum Microsoft Download Center gibt es auch unter (b). Sie müssen OpenSSL nicht auf Ihrem Server installieren. Das Certificate Request können Sie auch auf Ihrem Arbeitsplatz-PC erstellen (Windows, Linux, Mac etc).

   Folgen Sie dem Installer, und installieren Sie am besten nach `C:\openssl` (Leerzeichen in Ordnernamen machen das Leben kompliziert).

2. **Certificate Request erstellen**

   Öffnen Sie eine Konsole (Powershell oder cmd.exe). Wenn es bei

   ```
   C:\openssl\bin > .\openssl version
   ```

   eine Warnung gibt, weil die Datei 'openssl.cnf' nicht gefunden wird, sollte man die Umgebungsvariable `OPENSSL_CONF` setzen:

   ```
   C:\openssl\bin > set OPENSSL_CONF=C:\openssl\bin\openssl.cfg
   ```

   (unter cmd.exe) bzw.

   ```
   PS C:\openssl\bin > $env:OPENSSL_CONF = 'C:\openssl\bin\openssl.cfg'
   ```

   (in der Powershell)

   Zur Erstellung des Requests nun folgenden Befehl absetzen (in einer Zeile):

   ```
   C:\openssl\bin > .\openssl req -newkey rsa:2048 -keyout <subdomain>.<hostname>.key
                    -keyform PEM -out <subdomain>.<hostname>.req -outform PEM -nodes
   ```

   Dabei sind:
   `<subdomain>` z.B. bei dem FQDN (DNS-Namen) dns1.luis.uni-hannover.de ist die subdomain = luis
   `<hostname>` z.B. dem FQDN (DNS-Namen) dns1.luis.uni-hannover.de ist der hname = dns1

Beispiel: Für den Server `dns1.luis.uni-hannover.de` sähe die Zeile so aus:

```
C:\openssl\bin > .\openssl req -newkey rsa:2048 -keyout luis.dns1.key
                 -keyform PEM -out luis.dns1.req -outform PEM -nodes
```

Angaben:

```
Country Name (2 letter code) [AU]: DE
State or Province Name (full name) [Some-State]:Niedersachsen
Locality Name (eg, city) []:Hannover
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Leibniz Universitaet Hannover
Organizational Unit Name (eg, section) []:  <Institutskuerzel>
Common Name (e.g. server FQDN or YOUR name) []:  <hostname>.<subdomain>.uni-hannover.de
Email Address []:  <name>@<subdomain>.uni-hannover.de
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: (frei lassen)
An optional company name []: (frei lassen)
```

Bei `Common Name` geben Sie bitte den FQDN an. Die letzten beiden 'Extra'-Attribute (`password` und `optional company name`) werden nur mit Enter bestätigt (also leer lassen).

3. **Request-Datei hochladen**

   Es werden mit dem openssl-Befehl zwei Dateien erstellt. Die Certificate Request Datei (.req) laden Sie bitte über unser Webformular hoch:

   www.luis.uni-hannover.de/de/services/speichersysteme/backup-restore/backup-anmeldung

   Wenn Sie (optional) Datenverschlüsselung nutzen wollen, können Sie dies im Feld 'Weitere Angaben' des Webformulars vermerken.

   Den privaten Schlüssel (.key) schicken Sie uns bitte **nicht** zu! Der private Schlüssel darf nur Administratoren der im Zertifikat genannten Server zugänglich sein. Bitte kontaktieren Sie uns umgehend, wenn die im Zertifikat enthaltenen Daten nicht mehr korrekt sind oder wenn eine unbefugte Person Kontrolle über den privaten Schlüssel hatte.

   Das Absenden des Webformulars erzeugt bei uns ein Ticket, welches vom Backup & Restore Team bearbeitet wird. Wir prüfen Ihre Angaben und schicken Ihnen das Zertifikat sowie Informationen zum Download und zur Installation der Bacula Client Software zu.