invisAD-setup - action #55340

Nach Installation von xrdp funktioniert openVPN nicht mehr

2019-08-11 09:48 - EDV_Lotse

Status:	Closed	**Start date:**	2019-08-11
Priority:	Normal	**Due date:**	2020-06-01
Assignee:	EDV_Lotse	**% Done:**	100%
Category:	Feature	**Estimated time:**	0.00 hour
Target version:	14.2		

Description

Nach optionaler Installation von Xrdp bringt openVPN-client eine Fehlermeldung:

Tue Jul 30 19:46:27 2019 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
Tue Jul 30 19:46:27 2019 TLS Error: TLS handshake failed
Tue Jul 30 19:46:27 2019 SIGUSR1[soft,tls-error] received, process restarting

Serverseitig sieht die Fehlermeldung etwas informativer aus:

Aug 10 12:11:05 inviz openvpn[2623]: 194.95.66.31:51446 VERIFY ERROR: depth=0, **error=CRL has expired:** C=DE, ST=Nordrhein-Westfalen, L=Bonn, O=donum vitae Regionalverband Bonn/Rhein-Si>
Aug 10 12:11:05 inviz openvpn[2623]: 194.95.66.31:51446 OpenSSL: error:1417C086:SSL routines:tls_process_client_certificate:certificate verify failed
Aug 10 12:11:05 inviz openvpn[2623]: 194.95.66.31:51446 TLS_ERROR: BIO read tls_read_plaintext error
Aug 10 12:11:05 inviz openvpn[2623]: 194.95.66.31:51446 TLS Error: TLS object -> incoming plaintext read error
Aug 10 12:11:05 inviz openvpn[2623]: 194.95.66.31:51446 TLS Error: TLS handshake failed

Bei Installation von Xrdp werden RSA Keys erzeugt:

```
if [ ! -e /etc/xrdp/rsakeys.ini ]; then
xrdp-keygen xrdp /etc/xrdp/rsakeys.ini
if [ $? -ne 0 ] || [ ! -e /etc/xrdp/rsakeys.ini ]; then
echo "Could not generate rsakeys.ini, please check manually!"
fi
fi
```

/etc/xrdp/xrdp.ini:

```
...
; security layer can be 'tls', 'rdp' or 'negotiate'
; for client compatible layer
security_layer=negotiate
; minimum security level allowed for client
; can be 'none', 'low', 'medium', 'high', 'fips'
crypt_level=high
; X.509 certificate and private key
; openssl req -x509 -newkey rsa:2048 -nodes -keyout key.pem -out cert.pem -days 365
certificate=
key_file=
; set SSL protocols
; can be comma separated list of 'SSLv3', 'TLSv1', 'TLSv1.1', 'TLSv1.2'
ssl_protocols=TLSv1, TLSv1.1, TLSv1.2
; set TLS cipher suites
#tls_ciphers=HIGH
```

Frage: wie kann xrdp Funktionalität von openVPN verhindern?

Problem ist wie in den Kommentaren beschrieben der Ablauf der CRL. Siehe auch:
https://community.openvpn.net/openvpn/wiki/CertificateRevocationListExpired

Die Empfehlung dort: "In order to fix this, regenerate the CRL with a new nextUpdate value. If you don't want your CRLs expire put that value far enough into the future. "

Related issues:

Related to invisAD-setup - action #63631: We should publish the CRL expiratio...	**Closed**	**2020-02-20**

History

#1 - 2019-08-12 10:50 - EDV_Lotse

- Status changed from New to In Progress

- % Done changed from 0 to 50

Nachdem ich mit dem Befehl

/usr/bin/inviscerts crl

certificate revocation list erneuert habe, funktioniert openVPN wieder.

Frage #1: die Zusammenhang mit xrdp ist immer noch unklar, weil openVPN aleine ohne CRL-Erneuerung funktioniert einwandfrei

Frage #2: wie kann man die Sache komfortabler gestalten, wenn nach 6 Monaten CRL-Frist wieder ausläuft:

- im Portal ähnlich wie Zertifikatsfristen visuell kontrollieren
- eine Warnungsemail an Admin verschicken

#2 - 2019-08-12 11:30 - flacco

- Category set to Feature

- Assignee set to EDV_Lotse

- Target version set to 14.2

Hallo Dimitri

EDV_Lotse wrote:

> Frage #1: die Zusammenhang mit xrdp ist immer noch unklar, weil openVPN aleine ohne CRL-Erneuerung funktioniert einwandfrei

Das verstehe ich beim besten Willen auch nicht. Normalerweise muss eine Software, die eine "Certificat Revocation List" nutzt deren "Ablaufdatum" nicht als Grund ansehen den Dienst einzustellen. Das Ablaufdatum ist, wenn ich es richtig verstehe nicht bindend, sondern hat nur den Character einer Warnung.

> Frage #2: wie kann man die Sache komfortabler gestalten, wenn nach 6 Monaten CRL-Frist wieder ausläuft:
>
> - im Portal ähnlich wie Zertifikatsfristen visuell kontrollieren
> - eine Warnungsemail an Admin verschicken

Das sind gute Ideen. Schaue ich mir an.

#3 - 2019-08-13 06:42 - flacco

- % Done changed from 50 to 60

Das Script getcertinfo ermittelt jetzt, wann spätestens die nächste CRL-Auffrischung ansteht und schreibt dies nach /var/spool/results/certs/crlstatus.

Dies muss jetzt noch vom invis-Portal ausgelesen und angezeigt werden.

#4 - 2019-08-16 19:09 - ingogoeppert

- Description updated

#5 - 2019-08-17 16:24 - flacco

Das CRL-Update Interval ist in easy-rsa auf 6 Monate voreingestellt. Default-Wert in der klassischen openSSL Konfiguration ist der Wert sogar auf 30 Tage gesetzt.

Ich denke, dass 6 Monate eigentlich OK sind. Noch länger führt das Ganze ad absurdum. Mit Warnung per Mail und Anzeige im Portal sollte das auch zu beherrschen sein.

#6 - 2020-05-20 06:33 - flacco

- Related to action #63631: We should publish the CRL expiration date via invis portal added

#7 - 2020-05-24 08:32 - flacco

- % Done changed from 60 to 70

Der Status der Certificate Revocation List (CRL) wird jetzt im invis-Postal angezeigt.

#8 - 2020-05-24 09:03 - flacco

- Status changed from In Progress to Feedback

- % Done changed from 70 to 90

Um hier mal zu einem Abschluss zu kommen. Ich vermute, dass es ein Zufall war, dass die CRL am gleichen Tag abgelaufen ist, an dem du xrdp installiert hast. Es kann eigentlich keinen Zusammenhang geben.

Das xrdp während der Installation ein Server-Zertifikat generiert ist normal, schließlich müssen RDP-Verbindungen ja verschlüsselt werden. Du solltest in Erwägung ziehen dafür ein eigenes Zertifikat mittels easyrsa zu erzeugen, es wäre dann mit unserer eigenen CA signiert. Damit ließen sich Zertifikatswarnungen auf der Client-Seite verhindern.

invis:~ # easyrsa --subject-alt-name="DNS:host.example.loc" build-server-full host.example.loc nopass

Können wir das Ticket schließen?

#9 - 2020-05-25 06:22 - flacco

- Due date set to 2020-06-01

#10 - 2020-05-30 09:59 - flacco

- Status changed from Feedback to Closed

- % Done changed from 90 to 100

Keine Rückmeldung - Wird geschlossen.