Nastavenie zabezpeenej komunikácie (SSL/TLS)

Systém D2000 je možné nakonfigurova tak, aby komunikácia medzi serverom a klientami prebiehala zabezpeeným šifrovaným komunikaným kanálom. Zabezpeenie je implementované protokolom **Transport Layer Security** (TLS v1.3).

Pre aktiváciu zabezpeenej komunikácie je potrebné vykona nasledujúce kroky:

1. Pre server je nutné získa/vygenerova šifrovací kú a certifikát. Certifikát je potrebné distribuova klientským procesom.

Kú a certifikát je možné vygenerova napr. pomocou utility **openssl** (https://slproweb.com/products/Win32OpenSSL.html).

Generovanie šifrovacieho kúa

```
openssl genrsa -out server.pem 4096
```

Generovanie certificate signing request

```
openssl req -new -key server.pem -out server.csr
```

Generovanie self-signed certifikátu

```
openssl x509 -req -days 730 -in server.csr -signkey server.pem -out server.crt
```

2. Nastavi TLS podporu v registroch pre kernel

```
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Server\TLS_CertFile = c:\<cesta>\server.
crt
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Server\TLS_KeyFile = c:\<cesta>\server.pem
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Server\TLS_RequiredLevel = <level>
```

Nastavenie vyžadovanej úrovne zabezpeenia pripájajúceho sa klienta <level>:

- **None** - kernel dovolí pripoji sa klientovi aj bez zabezpeenia aj so zabezpeením
- **TLSNoPeerAuth** - kernel dovolí pripojenie len od klienta, ktorý komunikuje zabezpeene (ale nemusí by overený certifikátom)

3. Nastavi TLS podporu v registroch pre klientov

```
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Client\TLS_TrustedCerts = c:
\<cesta>\server.crt
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Client\TLS_RequiredLevel = <level>
```

TLS_TrustedCerts: nastavenie serverového certifikátu - cesta k serverovému certifikátu. Je možné zada aj viacero certifikátov oddelených bodkoiarkou (;). To je použitené pre redundantné systémy alebo v procese výmeny certifikátov, ke môže by nakonfigurovaný starý aj nový serverový certifikát.

TLS_RequiredLevel: Nastavenie vyžadovanej úrovne zabezpeenia pripájajúceho sa klienta:

- **None** - klient sa pripojí na kernel aj v prípade, že kernel podporuje zabezpeenú komunikáciu, aj v prípade, že nepodporuje
- **TLSNoPeerAuth** - klient sa pripojí len na kernel podporujúci zabezpeenú komunikáciu (ale nemusí by overený certifikátom, t.j. neporovnáva sa certifikát so zoznamom *TLS_TrustedCerts*)
- **TLSPeerAuth** - klient sa pripojí len na kernel podporujúci zabezpeenú komunikáciu, ktorého certifikát je v zozname *TLS_TrustedCerts*

4. Pre použitie TLS musí by klient štartovaný okrem obvyklých parametrov (/S, /RD prípadne /RF) **aj s parametrom /C<*názov_aplikácie*>**

Dôvodom je, aby už pred pripojením sa k aplikanému serveru vedel názov aplikácie a naítal parametre TLS z registrov (vi bod 3).
Alternatívou je nastavenie parametra *DefaultApplication* v registry.
Pozn: odporúame nastavenie *DefaultApplication* v registry kvôli tomu, aby nebolo nutné zadáva parameter /C<názov_aplikácie> nielen vo všetkých skratkách na ploche, ale aj pri runom spúšaní aplikácií.

Klient pripájajúci sa na server s použitím TLS to vypíše do logu. Ak je vyžadované aj overenie certifikátu a certifikát je korektne overený, v logu je slovo VERIFIED:

[2022-09-23 07:48:11.289]I CLIENT - Connecting to D2000 Server [localhost] TCP/IP|TLS...
[2022-09-23 07:48:11.348]I CLIENT - Connection established to D2000 Kernel V22.00.074 s380 [TCP/IP localhost:3119][TLSv1.3 VERIFIED].
ConnectionSqId = 1

Kernel pripájajúci klienta cez TLS takisto túto informáciu zapíše do logu:

[2022-09-23 07:48:10.598]I BACKEND - RegistrateProces request from DispPC.HIP V22.00.074 s380 [TCP/IP 127.0.0.1:50481][TLSv1.3]. ClientName: DispPC.HIP
[2022-09-23 07:48:10.600]I SERVER - RegistrateProces OK. ClientName: DispPC.HIP Id: 7652 ComputerName: PC1PHUM1v SAS: 0

Výmena kúov a certifikátov

D2000 Server naítava konfiguráciu TLS pri každom pripájaní klienta, takže je možné zmeni poas behu D2000 Servera konfiguráciu (vítane výmeny súborov s certifikátom a so súkromným kúom) bez reštartu D2000 Servera.

Blog

O nastavovaní TLS si môžete preíta blog:

- Bezpenos - Konfigurácia TLS (za 15 minút)

Súvisiace stránky:

Procesy systému D2000
Štartovacie parametre procesov