

IBM Power Systems - IBM i

# S28 - La mise en œuvre de SSL afin de sécuriser les connexions avec un IBM i



Dominique GAYTE- dgayte@notos.fr 04 67 86 09 08 - 06 30 17 02 55

www.notos.fr

© IBM France 2013

## NoToS

Expertise autour de l'IBM i
 Plus de 20 ans d'expérience sur AS/400
 Regard moderne
 PHP sur IBM i
 DB2 Web Query

Développement de progiciels







Fourni des solutions et des services autour de IBM i, PHP et de Zend

NOLO





#### Le contexte

- Connexion classiques aux IBM i sont non sécurisées
  - Emulation écran, FTP
  - ID et mot de passe circulent en clair
- Un simple test !
  - FTP vers un IBM i
  - Traces avec IP Tools (par exemple)
  - ID et PWD en clair
  - En TELNET (PC5250) à peine plus complexe
    - EBCDIC

#### FTP

| 😡 IP Tools 1 9  | 9 3 0 By Frwan I   | / Run&s · XPMUSE   | R   |   |   |   |   | X   |  |   |  |  |   |
|---|--|--|---|---|---|---|---|---|--|---|--|--|---|
| File Edit View  | Capture Tools Help   |  |   |   |   |   | لعالع   | -   |  |   |  |  |   |
|   | 2.168.1.36   |  | <u> </u>  |   |   |   |   |   |  |   |  |  |   |
| •         • | Source<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168. | Destination<br>192.168.1.3<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>1 | ▼rot       Len         TCP       48         TCP       40         TCP       40         TCP       54         TCP       40         TCP       54         TCP       40         TCP       54         TCP       40         TCP       40 | <ul> <li>Src Port</li> <li>3917</li> <li>21</li> <li>3917</li> <li>21</li> <li>3917</li> <li>21</li> <li>3917</li> <li>21</li> <li>21</li> <li>3917</li> <li>21</li> <li>21</li> <li>3917</li> <li>21</li> <li>21</li> <li>3917</li> <li>3917</li> <li>21</li> <li>21</li> <li>3917</li> <li>3917</li> <li>3917</li> <li>21</li> <li>21</li> <li>3917</li> <li>3917</li> <li>21</li> <li>21</li> <li>50</li> <li>6 R. C</li> <li>× M. \$0.</li> <li>P + US cof r</li> <li>ip</li> </ul> | Dest Port           21           3917           21           3917           21           3917           21           3917           21           3917           21           3917           21           3917           21           3917           21           3917           21           3917           21           21           3917           21           SEP qse           SEP qse | <ul> <li>⊢IP</li> <li>Version:4</li> <li>Header len::20</li> <li>Total len::54</li> <li>-D:\$52C3</li> <li>Fragmentation</li> <li>-TTL:28</li> <li>Protocol \$06 (T</li> <li>-Checksum:\$24</li> <li>-Source IP:192:</li> <li>-Dest. IP:192:16</li> <li>= -TCP</li> <li>- src_port:3917</li> <li>- dest_port:21</li> <li>- seq_number:33</li> <li>- deta_offset:5</li> <li># flags (PUSH)</li> <li>- window:5544</li> <li>- checksum:\$88</li> <li>- wrgent_pointer:5</li> <li>FTP</li> <li>- USER qsecoff</li> </ul> | CCP)<br>87<br>168.1.36<br>8.1.3<br>368191244<br>28<br>00<br>11:46:17.886<br>11:46:17.886<br>11:46:1.351<br>11:46:21.351<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361<br>11:46:21.361 | 0 By Erwan L.<br>ure Tools Help<br>132<br>0 Urce<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>32.168.1.36<br>192.168.1.3<br>192.168.1.3<br>192.168.1.3<br>192.168.1.36<br>192.168.1.36<br>192.168.1.3<br>192.168.1.36<br>192.168.1.3<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>192.168.1.36<br>1 | / RunAs : XPMUSER<br>Destination<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1921681.3<br>1 | Prot.         Len.           TCP         48           TCP         44           TCP         40           TCP         40           TCP         40           TCP         40           TCP         40           TCP         40           TCP         51           TCP         40           TCP         40           TCP         51           TCP         40           TCP         40 | Src Port<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>3917<br>21<br>21<br>3917<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>21<br>21<br>3917<br>3917<br>21<br>21<br>21<br>21<br>21<br>21<br>21<br>21<br>21<br>21 | DestPort<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>3917<br>21<br>21<br>21<br>3917<br>3917<br>21<br>21<br>21<br>3917<br>3917<br>21<br>21<br>21<br>3917<br>3917<br>21<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>3917<br>21<br>395<br>395<br>395<br>395<br>395<br>395<br>395<br>395<br>395<br>395 | Version:4<br>Header len:20<br>Total len:51<br>ID:\$52E5<br>B fragmentation<br>TTL:128<br>Protocol:\$06 (TCP)<br>Checksum:\$2468<br>Source IP:192.168.1.36<br>Dest IP:192.168.1.3<br>Dest IP:192.168.1.3<br>TCP<br>src_port3917<br>dest_port21<br>seq_number:3868191265<br>data_offset5<br>B flags (PUSH)<br>window:65423<br>checksum:\$E3FD<br>urgent_pointer\$10<br>FTP<br>PASS toto |
|   |  |  |   |   |   |   | Frames : 20, Bytes  | : 1032, Bytes / sec. : 1  | 9, Frames / sec. : 0   |   | ip   | proto 6 and port 21  | 1 //  |
|   |  |  |   |   |   |   |   |   |  |   |  |  |   |



# Telnet

| = <u>192</u>         | .168.1.36                      |                                    | • (     |                 | 9 🚳 😂 💁 🐂 🔤 🦛 🖓 🥮 1 | ■■ <mark>*</mark> № ⊗ <u>0</u>   |
|----------------------|--------------------------------|------------------------------------|---------|-----------------|---------------------|--|
| ime                  | Source                         | Destination                        | Prot. L | en. Src Port    | Dest Port           | United States St |
| :07:53.442           | 192.168.1.3                    | 192.168.1.36                       | TCP 4   | 0 8476          | 3936                | Header len.:20   |
| 2:07:53.442          | 192.168.1.36                   | 192.168.1.3                        | TCP 4   | 8 3937          | 23                  | Total len :72  |
| 2:07:53.442          | 192.168.1.3                    | 192.168.1.36                       | TCP 4   | 4 23            | 3937                | - ID:\$E8E3  |
| :07:53.442           | 192.168.1.36                   | 192.168.1.3                        | TCP 4   | 0 3937          | 23                  | + fragmentation  |
| :07:53.442           | 192.168.1.3                    | 192.168.1.36                       | TCP 4   | 6 23            | 3937                | TTI 128  |
| :07:53.442           | 192.168.1.36                   | 192.168.1.3                        | TCP 4   | 6 3937          | 23                  | Protocol \$06 (TCP)  |
| :07:53.442           | 192.168.1.3                    | 192.168.1.36                       | TCP 7   | 1 23            | 3937                | Checksum \$8E54  |
| 2:07:53.442          | 192.168.1.36                   | 192.168.1.3                        | TCP 1   | 38 3937         | 23                  | Source IP:192 168 1 36   |
| 2:07:53.442          | 192.168.1.3                    | 192.168.1.36                       | TCP 5   | 2 23            | 3937                | Dect IP:192.168.1.3  |
| 2:07:53.452          | 192.168.1.36                   | 192.168.1.3                        | TCP 5   | 2 3937          | 23                  |  |
| 2:07:53.452          | 192.168.1.3                    | 192.168.1.36                       | TCP 1   | 15 23           | 3937                | are port 2027  |
| 2:07:53.452          | 192.168.1.3                    | 192.168.1.36                       | TCP 5   | 44 23           | 3937                | dest port22  |
| 2:07:53.452          | 192.168.1.36                   | 192.168.1.3                        | TCP 4   | 0 3937          | 23                  | uest_portza  |
| 2:08:03.567          | 192.168.1.23                   | 192.168.1.255                      | UDP 7   | 8 137           | 137                 | seq_number.155266612   |
| 2:08:04.328          | 192.168.1.23                   | 192.168.1.255                      | UDP 7   | 8 137           | 137                 | ack_number.4030763506  |
| 2:08:05.069          | 192.168.1.23                   | 192.168.1.255                      | TOP 7   | 6  3/<br>0 0007 | 137                 | data_onset:5   |
| 08:08:965            | 192.168.1.36                   | 192.168.1.3                        | TOP 7   | 2 3937          | 23                  | H-flags (POSH)   |
| 00.00.365            | 192.100.1.3                    | 102.100.1.30                       | TCP 5   | 0.3 2.3         | 3337                | window:64907   |
| 0.00.03.005          | 192.100.1.30                   | 132.100.1.3<br>200.000.000         |         | 0 5337<br>29 67 | 23                  | Checksum:\$FEF5  |
| 2.00.10.700          | 192.100.1.1                    | 200.200.200.200<br>255 255 255 255 |         | 20 07<br>29 67  | 00                  | urgent_pointer:\$UU  |
| 30: 0003<br>40: ∎4⊡6 | 0738 F111 063<br>D5D7 E6C4 FFE | 5 E4E2 C5D9 F1                     |         | ·; 5 5<br>[     |                     | USER1  |
| mes : 46, Bytes :    | 6133, Bytes / sec. : 180       | ), Frames / sec. : 1               |         |                 |                     | RAW IP   |
|                      |                                |                                    | ľ       | NONPWI          |                     |  |
|                      |                                |                                    |         |                 | NoToS               |  |

|   | C1 | A               |     |
|---|----|-----------------|-----|
|   | C2 | В               |     |
|   | C3 | С               |     |
| ĺ | C4 | D               | ĺ   |
| ĺ | C5 | E               | İ   |
| ĺ | C6 | F               |     |
| ĺ | C7 | G               | İ   |
|   | C8 | Н               |     |
|   | C9 |                 |     |
|   | CA |                 |     |
|   | CB |                 |     |
|   | CC | non-displayable |     |
|   | CD |                 |     |
|   | CE | non-displayable |     |
|   | CF |                 |     |
|   | D0 | }               |     |
|   | D1 | J               |     |
|   | D2 | K               |     |
|   | D3 | L               |     |
|   | D4 | М               |     |
|   | D5 | N               |     |
|   | D6 | 0               |     |
|   | D7 | Р               |     |
|   | D8 | Q               |     |
|   | D9 | R               |     |
|   | DA |                 |     |
|   | DB |                 |     |
|   | DC |                 |     |
|   | DD |                 |     |
| Î | DE |                 |     |
|   | DF |                 |     |
|   | E0 | Ι               |     |
|   | E1 |                 |     |
|   | E2 | S               |     |
|   | E3 | Т               |     |
|   | E4 | U               |     |
| Î | E5 | V               |     |
| Î | E6 | W               |     |
|   | E7 | Х               |     |
|   | E8 | Y               | 50. |
|   | E9 | Z               |     |



# SSL : Secure Socket Layer

- C'est un protocole de sécurisation des échanges sur Internet – A utiliser à partir de V3.0
- TLS (*Transport Layer Security*) est la nouvelle version
   TLS 1.0 équivalent de SSL 3.1
- Création d'un « tunnel » dans lequel les informations circulent cryptées
- Possibilité de s'assurer de l'identité du serveur et du client
- S'appuie sur des certificats émis par des autorités de certification (CA)



#### Les protocoles

- Généralement des protocoles spécifiques sont utilisés
  - HTTPS, FTPS...
  - SSH, SFTP (implémentation particulière sur IBM i)
  - Sur des ports spécifiques

| modèle OSI                 | pile de protocoles                       |
|----------------------------|--|
| 7 - couche application     | HTTP, SMTP, FTP, SSH, IRC, SNMP, SIP     |
| 6 - couche de présentation |  |
| 5 - couche de session      | TLS, SSL,SSH-user, NetBIOS               |
| 4 - couche de transport    | TLS, SSL,TCP, UDP, SCTP, RTP, DCCP       |
| 3 - couche réseau          | IPv4, IPv6, ARP, IPX                     |
| 2 - couche de liaison      | Ethernet, 802.11 WiFi, Token ring, FDDI, |
| 1 - couche physique        | Câble, fibre optique, ondes radio        |

NOLO

#### IBM

## SSL dans l'IBM i

- V7R1 TR 6 : support de TLS 1.2
- Tous les outils en standard
  - DCM Digital Certificate Manager
    - 5770SS1 option 34 en V7R1
  - Serveur Web d'administration
    - Administration générale via le Web
  - IBM Web Administration for i
    - Administration des serveurs Web
- IBM i Access for Windows et System i Navigator

NOLON

- Toutes les fonctions supportent SSL
- IBM Portable Utilities for i
  - 5733SC1
  - SSH, SFTP



#### Les certificats

#### Emis par une autorité de certification

- CA Certificate Autority
- Soit officielles (accréditées)
  - CyberTrust, Verisign...
  - Vendent les certificats et assurent leurs validités
- Soit privées (locales)
  - Certificats émis sont gratuits
  - Mais non reconnus comme surs, il faudra les définir comme étant de confiance sur les postes clients

 L'IBM i peut être une CA et émettre tous les certificats dont nous auront besoin

- Idéal dans le cas d'une utilisation interne



# Les certificats (2)

- Caractéristiques
  - Longueur de clé
  - Common name
  - Numéro de série
- Contenus dans des magasins de certificats
  - Dans l'IFS de l'IBM i
    - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB (System)
  - Dans Client Access
  - Dans Windows





# Organisation avec une CA locale dans l'IBM i

- 1. Créer une CA locale sur l'IBM i
- 2. Créer les certificats et les associer aux applications
- 3. Configurer les applications
- 4. Eventuellement, configurer les clients afin de faire confiance à la CA locale de l'IBM i
  - 1. Web
  - 2. IBM i Client (Telnet, FTP...) SSL d'un autre IBM i



#### DCM

- Outil de gestion des certificats
- Interface Web
  - port 2001 de l'IBM i
  - Le serveur d'administration doit être démarré



Notos



#### Création de la CA locale

Create a Certificate Authority (CA)

Certificate type: Certificate Authority (CA) Certificate store: Local Certificate Authority (CA)

The system will create a certificate with a private key and store the certificate in the Local Certificate Authority (CA) certificate store.

| Key size:                           | 4096 🗸 (bits)           |             |                                    |
|-------------------------------------|-------------------------|-------------|------------------------------------|
| Certificate store password:         | •••••                   | (required)  |                                    |
| Confirm password:                   | •••••                   | (required)  |                                    |
|                                     | Certificate Inf         | formation   |                                    |
| Certificate Authority (CA) name:    | NoToS                   |             | (required)                         |
| Organization unit:                  | DSI                     |             | ]                                  |
| Organization name:                  | NoToS                   |             | (required)                         |
| Locality or city:                   | BEAULIEU                |             | ]                                  |
| State or province:                  | 34160                   |             | (required:minimum of 3 characters) |
| Country or region:                  | FR (required)           |             |                                    |
| Validity period of Certificate Auth | nority (CA) (2-7300): 7 | 7300 (days) |                                    |
|                                     |                         | NOTOS.      |                                    |



# Création de la CA locale (2)

 Eventuellement définir les applications acceptant la CA locale (trust)

| Install Local C | A Certificate |
|-----------------|---------------|
|-----------------|---------------|

Certificate type: Certificate Authority (CA) Certificate store: Local Certificate Authority (CA)

A certificate for your Certificate Authority (CA) was cr

You must install the Certificate Authority (CA) certificat the certificate in your browser. Your web browser will (

#### Install certificate

After installing the certificate, select Continue so you car

Continue Cancel

#### Certificate Authority (CA) Policy Data

Your Certificate Authority (CA) was created with the default policy data shown below.

Allow creation of user certificates: O Yes O No

Validity period of certificates that are issued by this Certificate Authority (CA) (1-2000): 1000 (days)

Days until Certificate Authority (CA) expires: 3000

Continue Cancel

Message The applications you selected will trust this Certificate Authority (CA).



## Création de la CA locale (3)

#### View Certificate Authority (CA)

Certificate type: Certificate Authority (CA) Certificate store: Local Certificate Authority (CA)

| Certificate label: LOCAL_CERTIFICATE_AUTH | IORITY_1017A0R1(18) |                             |                           |  |  |
|---|---------------------|-----------------------------|---------------------------|--|--|
| Subject:                                  |                     |                             |                           |  |  |
| Common name                               |                     | CA NoToS                    |                           |  |  |
| Organization unit                         |                     | DSI                         |                           |  |  |
| Organization name                         |                     | NoToS                       |                           |  |  |
| Locality or city                          |                     | BEAULIEU                    |                           |  |  |
| State or province                         |                     | 34160                       |                           |  |  |
| Zip or postal code                        |                     |                             |                           |  |  |
| Country or region                         |                     | FR                          |                           |  |  |
| Additional information:                   |                     |                             |                           |  |  |
| Private key                               | Yes                 |                             |                           |  |  |
| Certificate Authority (CA) enabled        | Yes                 |                             |                           |  |  |
| Signed certificate                        | Yes                 |                             |                           |  |  |
| Serial number                             | 515C3032            |                             |                           |  |  |
| Validity period                           | 04/02/13 0          | 3:35:46 - 06/20/21 03:35:46 | :5:46 - 06/20/21 03:35:46 |  |  |
| Private key information:                  |                     |                             |                           |  |  |
| Key length                                | 4096                |                             |                           |  |  |
| Storage location                          | Stored in           | tware                       |                           |  |  |
| lssuer:                                   |                     |                             |                           |  |  |
| Common name                               |                     | CA NoToS                    |                           |  |  |
| Organization unit                         |                     | DSI                         |                           |  |  |
| Organization name                         |                     | NoToS                       |                           |  |  |
| Locality or city                          |                     | BEAULIEU                    |                           |  |  |
| State or province                         |                     | 34160                       |                           |  |  |
| Zip or postal code                        |                     |                             |                           |  |  |
| Country or region                         |                     | FR                          |                           |  |  |



#### Création de certificats

#### Se connecter sur le magasin System

| Certificate Store and Password        |   |  |  |  |  |  |
|---------------------------------------|---|--|--|--|--|--|
| Enter the certificate store password. |   |  |  |  |  |  |
| Certificate type:                     | Server or client                                |  |  |  |  |  |
| Certificate store:                    | *SYSTEM   |  |  |  |  |  |
| Certificate store path and filenau    | me: /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB |  |  |  |  |  |
| Certificate store password:           | • • • • • • • •                                 |  |  |  |  |  |
| Continue Reset Password               | Cancel  |  |  |  |  |  |
|                                       |   |  |  |  |  |  |

Noto

Créer un certificat Server certifié par la CA locale



# Création de certificats (2)

#### Pour Client Access

| Create Certificate   | Create Certificate      |                                    |  |  |  |  |  |  |
|--|-------------------------|------------------------------------|--|--|--|--|--|--|
| Certificate type: Server or client<br>Certificate store: *SYSTEM             |                         |                                    |  |  |  |  |  |  |
| Use this form to create a certificate in the certificate store listed above. |                         |                                    |  |  |  |  |  |  |
| Key size:  | 2048 🗸 (bits)           |                                    |  |  |  |  |  |  |
| Certificate label:   | CA400                   | (required)                         |  |  |  |  |  |  |
| Cer  | Certificate Information |                                    |  |  |  |  |  |  |
| Common name:   | CA400                   | (required)                         |  |  |  |  |  |  |
| Organization unit:   | DOI                     |                                    |  |  |  |  |  |  |
| Organization name:   | NoToS                   | (required)                         |  |  |  |  |  |  |
| Locality or city:  | BEAULIEU                |                                    |  |  |  |  |  |  |
| State or province:   | 34160                   | (required minimum of 3 characters) |  |  |  |  |  |  |
| Country or region:   | FR (required)           |                                    |  |  |  |  |  |  |

Notos

# Association à une application

#### Associer le certificat aux applications (ici Client Access)

|   | Application                     | Туре   | Assigned certificate |
|---|---------------------------------|--------|----------------------|
| ✓ | Central Server                  | Server | None assigned        |
| ✓ | Database Server                 | Server | None assigned        |
| ✓ | Data Queue Server               | Server | None assigned        |
|   | Network Print Server            | Server | None assigned        |
| ✓ | Remote Command Server           | Server | None assigned        |
| ✓ | Signon Server                   | Server | None assigned        |
|   | IBM i TCP/IP Telnet Server      | Server | None assigned        |
|   | IBM i TCP/IP Telnet Client      | Client | None assigned        |
|   | Serveur i5/OS DDM/DRDA - TCP/IP | Server | None assigned        |
|   | Client i5/OS DDM/DRDA - TCP/IP  | Client | None assigned        |
|   | Cluster Security                | Server | None assigned        |
| ✓ | Host Servers                    | Server | None assigned        |
| ✓ | File Server                     | Server | None assigned        |
| ✓ | Serv gestion centralisée        | Server | None assigned        |
|   | IBM Tivoli Directory Server     | Server | None assigned        |





#### Pour les serveurs Web

Le Common name doit être le constituant principal de l'URL

#### Pour le site mante.notos.fr

| Create Certificate      | ;   |                                    |
|-------------------------|---|------------------------------------|
| Certificate type: Ser   | ver or client                                     |                                    |
| Certificate store: *S   | SYSTEM  |                                    |
| Use this form to create | a certificate in the certificate store listed abo | we.                                |
| Key size:               | 2048 🗸 (bits)                                     |                                    |
| Certificate label:      | WEB   | (required)                         |
| Ce                      | rtificate Information                             |                                    |
| Common name:            | mante.notos.fr. ×                                 | (required)                         |
| Organization unit:      | DOI   | ]                                  |
| Organization name:      | NoToS   | (required)                         |
| Locality or city:       | BEAULIEU  | ]                                  |
| State or province:      | 34160   | (required:minimum of 3 characters) |
| Country or region:      | FR (required)                                     |                                    |

Notos

#### Pour les serveurs Web (2)

Associer à l'application correspondant au site Web sélectionné

|   | IBM i TCP/IP FTP Client       | Client | None assigned |
|---|-------------------------------|--------|---------------|
|   | IBM i TCP/IP POP Server       | Server | None assigned |
| ✓ | QIBM_HTTP_SERVER_APACHEDFT    | Server | None assigned |
|   | QIBM_HTTP_SERVER_ADMIN        | Server | None assigned |
|   | QIBM_HTTP_SERVER_TESTSSL      | Server | None assigned |
|   | QIBM_HTTP_SERVER_ADMIN1       | Server | None assigned |
|   | QIBM_DIRECTORY_SERVER_QUSRDIR | Server | None assigned |
|   | QIBM_HTTP_SERVER_WQLWI77      | Server | None assigned |

Cancel Continue





# Configuration de Client Access

- Dans System i Navigator
  - Sur la connexion choisie, Propriétés, onglet Utilisation de la fonction SSL

Notos

- Si option installée !

| opriétés de Mante   | ? X  |
|---|--|
| Système d'administration Services d'annuaires   | Maintenance Modules d'extension  |
| Fonction SSL     ✓     Utiliser la fonction SSL pour la connexi   | on   |
| /érification de la conn   | iexion SSI   |
| Autorité d'accréditation i5/OS<br>Pour que System i Access Express puisse s<br>serveur signés ou créés par l'autorité d'acc<br>dernière doit être téléchargée sur ce PC. R<br>péressaire de télécharger les autres autori | e fier aux certificats de<br>créditation i5/OS, cette<br>Remarque : Il n'est pas<br>tés d'accréditation fournies |
| Pour utiliser l'autorité d'accréditation i5/O   | )S, cliquez sur  |
|   |  |
|   |  |
|   |  |
|   | OK Annuler Aide  |



# Magasin de certificat de CA/400

- Cliquer sur Téléchargement afin de redescendre le certificat de la CA locale dans le magasin de CA/400
- Le mot de passe par défaut du magasin est ca400

| Invite de mot d  | le passe de  | la base de données de clés   |                 | ? 🛛             |                                     |    |  |
|--|--------------|------------------------------|-----------------|-----------------|-------------------------------------|----|--|
| Pour que les certificats utilisés par l'autorité d'accréditation IBM i soient<br>sécurisés, les droits associés aux certificats seront placés dans la base<br>de données de clés SSL.<br>Indiquez le mot de passe pour la base de données de clés sur le PC. |              |                              |                 |                 |                                     |    |  |
| Base de donnée   | es de clés : | U:\Users\Public\Documents\It | M\Ulient Acces: | s\cwbssidt.     |                                     |    |  |
| Mot de passe :   |              | ****                         | Attributs de re | démarrage       |                                     | 23 |  |
| _  | _            |                              | i L'a           | autorité d'acci | réditation i5/OS a été téléchargée. |    |  |
|  |              |                              | _               | _               | ОК                                  |    |  |

NOIO

# Magasin de certificat de CA/400 (2)

#### Redémarrer IBM i Navigator



Remarquer l'icone avec un cadenas



Notos



# Magasin de certificat de CA/400 (4)

- Ce magasin est constitué de trois fichiers
  - cwbssldf.kdb c'est la base de données de clés
  - cwbssljavaca.jck c'est le fichier de clé utilisé par JDBC
  - cwbssldf.sth contient le mot de passe du magasin
- Ils pourront être copiés sur les postes de travail lors d'un déploiement des postes clients





# Magasin de certificat de CA/400 (5)

# Utilitaire de gestion des clés – IBM Key Management

| IBM Key Management - [C:\Users\Public\Documents\IBM\Client Access\\cwbssldf.kdb]     Fichier de base de données de clés     Informations sur la base de données de clés     Type de base de données :     CMS     Nom de fichier :     C:\Users\Public\Documents\IBM\Client Access\\cwbssldf.kdb     Libellé de jeton :     Contenu de la base de données de clés     Certificats de signataire     Ajouter     192.168.1.3 CA - Saturday, November 10, 2012 11:40:16 |  |  |  |  |  |
|---|--|--|--|--|--|
| Eichier de base de données de clés Créer Afficher Ajde     Informations sur la base de données de clés     Type de base de données :   CMS   Nom de fichier :   C:Users\Public\Documents\IBM\Client Access\\cwbssldf.kdb Libellé de jeton :    Contenu de la base de données de clés   Certificats de signataire     Ajouter     192.168.1.3 CA - Saturday, November 10, 2012 11:40:16  |  |  |  |  |  |
| Informations sur la base de données de clés         Type de base de données :       CMS         Nom de fichier :       C:\Users\Public\Documents\UBM\Client Access\\cwbssldf.kdb         Libellé de jeton :       Contenu de la base de données de clés         Certificats de signataire       Ajouter         192.168.1.3 CA - Saturday, November 10, 2012 11:40:16       Supprimer   |  |  |  |  |  |
| Informations sur la base de données de clés  Type de base de données : CMS  Nom de fichier : C:\Users\Public\Documents\IBM\Client Access\\cwbssldf.kdb Libellé de jeton :  Contenu de la base de données de clés  Certificats de signataire  Ajouter  192.168.1.3 CA - Saturday, November 10, 2012 11:40:16  Supprimer  |  |  |  |  |  |
| Type de base de données :       CMS         Nom de fichier :       C:UJsers\Public\Documents\IBM\Client Access\\cwbssldf.kdb         Libellé de jeton :   |  |  |  |  |  |
| Nom de fichier :     C:\Users\Public\Documents\IBM\Client Access\\cwbssldf.kdb       Libellé de jeton :   |  |  |  |  |  |
| Libellé de jeton :<br>Contenu de la base de données de clés<br>Certificats de signataire  Ajouter 192.168.1.3 CA - Saturday, November 10, 2012 11:40:16  Supprimer  |  |  |  |  |  |
| Contenu de la base de données de clés Certificats de signataire  192.168.1.3 CA - Saturday, November 10, 2012 11:40:16  Supprimer   |  |  |  |  |  |
| Contenu de la base de données de clés           Certificats de signataire         Ajouter           192.168.1.3 CA - Saturday, November 10, 2012 11:40:16         Supprimer   |  |  |  |  |  |
| Certificats de signataire     Ajouter       192.168.1.3 CA - Saturday, November 10, 2012 11:40:16     Supprimer   |  |  |  |  |  |
| 192.168.1.3 CA - Saturday, November 10, 2012 11:40:16   |  |  |  |  |  |
| 403 460 4 2 CA Thursdoy Nevember 30, 3043 46(44)50  |  |  |  |  |  |
| 192.168.1.3 CA - Tuesday, October 16, 2012 17:02:18 Afficher/Editer   |  |  |  |  |  |
| Entrust.net Certification Authority (2048)  |  |  |  |  |  |
| Entrust.net Client Certification Authority Extraire   |  |  |  |  |  |
| Entrust.net Global Client Certification Authority   |  |  |  |  |  |
| Entrust.net Global Secure Server Certification Authority Remplin Remplin  |  |  |  |  |  |
| Entrustinet secure server cerunication Authority MANTE CA. Worknessen 2013 16:30-57   |  |  |  |  |  |
| RsA secure server certification authority   |  |  |  |  |  |
| Thawte Personal Basic CA  |  |  |  |  |  |
| Thavie Personal Freemail CA   |  |  |  |  |  |
| Thawte Personal Premium CA  |  |  |  |  |  |
| Thawte Premium Server CA  |  |  |  |  |  |
| Thawte Server CA  |  |  |  |  |  |
| VeriSign Class 1 Public Primary Certification Authority   |  |  |  |  |  |
|   |  |  |  |  |  |
| L'action demandée a abouti  |  |  |  |  |  |

| Informations de clé pour [MAN   | NTE CA - Wednesday, April 03, 2013 16:30:57]  | 23 |
|---|---|----|
| MANTE CA  | - Wednesday, April 03, 2013 16:30:57  |    |
| -   |   |    |
| Taille de clé :<br>Propriétés de certificat :   | 4096  |    |
| Version :   | X509 V3   |    |
| Numéro de série :   | 51 5C 30 32   |    |
| Emis vers :   |   | _  |
| CN=CA NoToS, OU=DSI,  | .O=NoToS, L=BEAULIEU, ST=34160, C=FR  |    |
| Emis par :  |   |    |
| CN=CA NoToS, OU=DSI,  | , O=NoToS, L=BEAULIEU, ST=34160, C=FR   |    |
| Validité :<br>Empreinte digitale (SHA1 I<br>00:F1:EB:AF:E4:75:08:F0:<br>Algorithme de signature :<br>Autres noms de sujet :<br>Adresse électronique : | Valide entre le 2 avril 2013 et le 20 juin 2021<br>Digest) :<br>3C:A6:44:F2:75:8D:4E:0A:46:7B:59:5C<br>SHA1withRSA (1.2.840.113549.1.1.5) |    |
| Adresse IP :  |   |    |
| Nom DNS :   |   |    |
| r   | <u>A</u> fficher les détails  |    |
| ☑ Définir le certificat en tant   | t que certificat racine digne de confiance  |    |
|   | Ōĸ  |    |

# TELNET

- Associer un certificat au serveur TELNET
  - Celui de CA/400 ou un autre



 Faire reconnaitre la CA Locale à l'application si ce n'est déjà fait (Define CA trust list)



 Redémarrer le serveur Telnet (avec System i Navigator. Attention à la perte de tous les écrans 5250 !)

NOIO

- Configurer les émulations écran et les démarrer



#### Session 5250

#### Configuration sur le port 992

| Configuration de PC5250   | 8 23  |
|---|---|
| Nom de système : MANTE  | ✓ Propriétés  |
| D poste de travail<br>C Utiliser le nom de l'ordinateur<br>Utiliser le nom utilisateur Wii<br>Indiquer un ID poste de trav<br>Tronquer :<br>C Caractères de début | rr Ajouter un préfixe pour désigner une imprimante ou un écran<br>ndows Eviter les noms en double sur ce poste de travail<br>vail Eviter les noms en double avec d'autres postes de travail |
| − Type d'émulation  | Taille :     24x80        Configuration     Association d'imprimante  |
| ☐ Ignorer mire de connexion<br>☐ Reconnexion automatique<br>Page de codes hôte :<br>Numéro de port :  | 1147 France (Euro)       992       OK     Annulation  |



| Informations relatives à la Connexion Certificat clie | a sécurité de niveau session<br>nt |                         | 83  |
|---|------------------------------------|-------------------------|-----|
| Protocole de sécurité :                               |                                    |                         |     |
| TLS1.0  |                                    |                         |     |
| Niveau de chiffrement d                               | e sécurité :                       |                         |     |
| TLS_RSA_WITH_AES                                      | 128_CBC_SHA                        |                         |     |
| Informations concerna                                 | nt les certificats de serveur —    |                         |     |
| CA400   |                                    |                         |     |
|   | Extraire                           | Affichage du certificat |     |
|   |                                    |                         |     |
|   |                                    | ОК А                    | ide |

**NoToS** 



# Configuration du serveur TELNET

- CHGTELNA (Allow Secure Socket Layer ... ALWSSL)
- SSL optionnel : \*YES
- SSL obligatoire : \*ONLY

| Change TELM                              | IET Attributes (   | (CHGTELNA)   |
|--|--|--|
| Indiquez vos choix, puis appuyez         | sur ENTREE.  |  |
| Autostart server                         | <u>*YES</u><br>*CALC<br>*CALC<br>*VT100<br>*MULTINAT<br>*CCSID | *YES, *NO, *SAME<br>1-200, *SAME, *CALC<br>0-2147483647, *SAME, *CALC<br>*SAME, *VT100, *NVT<br>1-65533, *SAME, *MULTINAT<br>Nom, *SAME, *CCSID, *DFT<br>Nom, *LIBL, *CURLIB |
| Incoming ASCII/EBCDIC table .<br>Library | <u>*CCSID</u><br><u>*YES</u>                                   | Nom, *SAME, *CCSID, *DFT<br>Nom, *LIBL, *CURLIB<br>*YES, *NO, *ONLY, *SAME   |
| F3=Exit F4=Invite F5=Réaffich            | ner F12=An <u>nul</u> e  | Fin<br>Finer F13=Mode d'emploi invite  |
| E24-Outroo touchoo                       |  |  |
|  | Notos  |  |

## Netstat \*CNN

| <b>3년</b> Session B - [24 x 80]           |                  |                |             |                 |          |
|---|------------------|----------------|-------------|-----------------|----------|
| Fichier Edition Vue Communication Actio   | ons Fenêtre Aide |                |             |                 |          |
| 🖸 🖻 📭 📭 🖼 🔳 📾 🐁                           | Ы 🕹 🛃 🌰 🍕        | ≥              |             |                 |          |
|   | Work with        | <br>IPv4 Conne | ction Statu | S               |          |
|   |                  |                |             | Système:        | S1017A0R |
| Type options, press E                     | nter.            |                |             |                 |          |
| 3=Enable debug 4=                         | End 5=Dis        | play detail    | s 6=Disab   | le debug        |          |
| 8=Display jobs                            |                  |                |             |                 |          |
|   | -                |                |             |                 |          |
| Remote                                    | Remote           | Local          |             |                 |          |
| Opt Address                               | Port             | Port           | Idle Time   | State           |          |
| _ 192.168.1.20                            | 36819            | as-data >      | 000:19:26   | Established     |          |
| _ 192.168.1.20                            | 36821            | as-rmtc >      | 000:18:04   | Established     |          |
| _ 192.168.1.20                            | 36823            | as-data >      | 000:19:25   | Established     |          |
| _ 192.168.1.20                            | 36825            | as-rmtc >      | 000:19:17   | Established     |          |
| _ 192.168.1.20                            | 36831            | telnet         | 000:07:58   | Established     |          |
| _ 192.168.1.20                            | 36832            | telnet- >      | 000:00:00   | Established     |          |
| _ 192.168.1.20                            | 36926            | cifs           | 000:05:37   | Established     |          |
|   |                  |                |             |                 |          |
|   |                  |                |             |                 |          |
|   |                  |                |             |                 |          |
|   |                  |                |             |                 |          |
|   |                  |                |             |                 | _ ·      |
|   |                  |                |             |                 | Fin      |
| F4=Prompt F10=D1sp                        | lay connect      | ion totals     | F14=D1spl   | ay port numbers | 5        |
| F15=Subset F16=Repe                       | at position      | n to           | F1/=Posit   | 10n to F24=M    | ore keys |
|   |                  |                |             |                 |          |
|   | MW               |                |             |                 | 097003   |
| 1902 - Le démarrage de la session a about | ti               |                |             |                 | //       |

**Notos** 

#### **FTP**

#### Idem Telnet

#### Client FTPS

Statut : Connexion à 192.168.1.3:990... Connexion établie, initialisation TLS... Statut : Vérification du certificat... Statut : Certificat inconnu Statut : Connexion TLS/SSL établie, attente du message d'accueil... 220-QTCP at MANTE.NOTOS.BEAULIEU. Réponse : Le certificat du serveur est inconnu. Examinez le certificat avec attention avant de 220 Connection will close if idle more than 5 minutes. Réponse : faire confiance au serveur. Chaîne de certificats : 0 🔻 Détails Valable du : 02/04/2013 Valable jusqu'à : 29/12/2015 Numéro de série : 51:5c:37:7e:0b:4b:f8 Algorithme de la dé publique : RSA avec 2048 bits Gestionnaire de Sites 23 Empreinte (MD5) : b3:90:56:d4:a5:9d:31:b7:2c:26:04:1b:56:5f:17 Sélectionnez une entrée : b5:19:08:20:a7:7e:95:99:de:39:f9:5f:18:3f:10 Empreinte (SHA-1) : Général Avancé Paramètres de transfert Jeu de caractères Mes Sites Hôte : 192.168.1.3 Émetteur du certificat 192,168,1,3 Port : Objet du certificat Mante Nom commun : CA400 Nom commun : CA NoToS Protocole : FTP - Protocole de Transfert de Fichiers Ŧ Nouveau site NoToS Organisation : NoToS Organisation : Unité : DOI Unité : DSI Chiffrement : Connexion FTP implicite sur TLS FR FR Pavs: Pavs: État ou province : 34160 État ou province : 34160 Demander le mot de passe Type d'authentification : Ŧ Localité : BEAULIEU Localité : BEAULIEU Identifiant : dgayte Détails de session Mot de passe : Hôte : 192.168.1.3:990 Chiffrement : AES-128-CBC Compte : MAC: SHA1 Commentaires : Approuver ce certificat et l'associer à la connexion ? . Toujours faire confiance à ce certificat lors des prochaines sessions. Nouveau Site Nouveau Dossier Nouveau Favori Renommer OK Annuler Copier Supprimer OK Connexion Annuler

Notos

Statut :

Déconnecté du serveur



#### Serveur Web

 Configurer le serveur Web dans IBM Web Administration for i – HTTPxxx:2001/HTTPAdmin

NOLO

- Attribuer un certificat à l'application dans DCM
- Intégrer le certificat de la CA locale dans le magasin Windows



# Configuration du serveur Web

- Dans Security
  - Activer SSL
  - Associer une application

| <u>APACHEDFT</u> > Security   |  |  |  |  |
|---|--|--|--|--|
| Security 📀  |  |  |  |  |
| Authentication Control Access   |  |  |  |  |
| SSL Proxy SSL Proxy Advanced  |  |  |  |  |
| SSL with Certificate Authentication Control Certificate Access SSL Advanced |  |  |  |  |
|   |  |  |  |  |
|   |  |  |  |  |
| Client certificates when establishing the connection: ③                     |  |  |  |  |
| Do not request client certificate for connection                            |  |  |  |  |
| O Accept client certificate if available before making connection           |  |  |  |  |
| O Require client certificate for connection                                 |  |  |  |  |

- Dans General Server Configuration
  - Attribuer un port (443?)

| Server IP addresses and ports to listen on: 😨 |                  |     |       |  |  |  |
|---|------------------|-----|-------|--|--|--|
| IP address Port Protocol                      |                  |     |       |  |  |  |
| Example                                       | All IP addresses | 80  | http  |  |  |  |
| 0   | *                | 443 | https |  |  |  |
| Add   |                  |     |       |  |  |  |

NOLO

# Attribution du certificat à l'application

| 0 | IBM i TCP/IP FTP Server    | CA400         |
|---|----------------------------|---------------|
| 0 | IBM i TCP/IP POP Server    | None assigned |
| 0 | QIBM_HTTP_SERVER_APACHEDFT | WEB           |
| 0 | OIBM HTTP SERVER ADMIN     | None assigned |

| ծubject:           |                 |  |  |  |
|--------------------|-----------------|--|--|--|
| Common name        | mante.notos.fr. |  |  |  |
| Organization unit  | DOI             |  |  |  |
| Organization name  | NoToS           |  |  |  |
| Locality or city   | BEAULIEU        |  |  |  |
| State or province  | 34160           |  |  |  |
| Zip or postal code |                 |  |  |  |
| Country or region  | FR              |  |  |  |

#### Additional information:

| Private key        | Yes                                   |
|--------------------|---------------------------------------|
| Signed certificate | Yes                                   |
| Serial number      | 515C396E0AFF80                        |
| Validity period    | 04/02/13 04:15:10 - 12/29/15 03:15:10 |

**NoToS** 

# Le magasin de certificat de Windows

#### Deux problèmes

1. Problème de sécurité

| 8 | Le certificat de sécurité de ce site Web présente un problème.  |  |  |  |  |
|---|---|--|--|--|--|
|   | Le certificat de sécurité présenté par ce site Web a été émis pour une autre adresse de site Web.   |  |  |  |  |
|   | Les problèmes de certificat de sécurité peuvent indiquer une tentative de duperie ou d'interception des<br>données que vous envoyez sur le serveur. |  |  |  |  |
|   | Nous vous recommandons de fermer cette page Web et de quitter ce site.  |  |  |  |  |
|   | Ø Cliquez ici pour fermer cette page Web.   |  |  |  |  |
|   | Poursuivre avec ce site Web (non recommandé).   |  |  |  |  |
|   | Informations  |  |  |  |  |

#### 2. Erreur de certificat



Notos

Certificat non valide

X

Ce problème peut indiquer une tentative de duperie ou d'interception des données que vous envoyez sur le serveur.

Nous vous recommandons de fermer cette page Web.

À propos des erreurs de certificat

Afficher les certificats

© IBM France 2013



×



#### Problème de sécurité

- Il faut que le certificat de la CA soit placé dans le magasin de certificat de Windows
- Dans « Autorité de certification racines de confiance »
- A partir de DCM
  - Copier le certificat en local
  - L'installer dans le magasin Windows

| Certificat  | Assistant Importation de certificat  | Avertissement de sécurité   |
|---|--|---|
| Général Détails Chemin d'accès de certification   | Magasin de certificats<br>Les magasins de certificats sont des zones système où les certificats sont stockés.                                      | Vous êtes sur le point d'installer un certification (CA) demandant à rep  |
| Vous ne pouvez pas faire confiance à ce certificat<br>racine de l'autorité de certification. Pour activer la<br>confiance, installez ce certificat dans le magasin<br>d'autorités de certification de la racine de confiance. | Windows peut sélectionner automatiquement un magasin de certificats, ou vous<br>pouvez spécifier l'emplacement du certificat.                      | CA NoToS<br>Windows ne peut pas valider que le<br>NoToS", Vous devriez confirmer so   |
| Délivré à :         CA NOTOS           Délivré par :         CA NOTOS           Valide du         02/04/2013 au         20/06/2021  | Placer tous les certificats dans le magasin suivant     Magasin de certificats :     Autorités de certification racines de confiance     Parcourir | Le numéro suivant va vous aider à d<br>Aperçu (sha1) : 00F1EBAF E475D8F0<br>Avertissement :<br>Si vous installez ce certificat racine,<br>approuver tout certificat émis par c<br>L'installation d'un certificat avec ur<br>de sécurité. Si vous cliquez sur "Oui |
| Installer le certificat Dédaration de l'émetteur<br>En savoir plus sur les <u>certificats</u>   | En savoir plus sur les <u>magasins de certificats</u>  | Voulez-vous installer cette certificat  |
| ОК  | < Précédent Suivant > Annuler  |   |



Install Local CA Certificate on

Your PC

# Le magasin de certificat de Windows

- À partir de MMC
- Installer le composant Certificats

| Fichier Action Affichage Favoris Fenêtre ?                          |                                       |  |                          |                       | - 5         |
|---|---------------------------------------|--|--------------------------|-----------------------|-------------|
| 🔿 📶 🧹 🕒 🗙 🗊 🗟 🔽 📰   |                                       |  |                          |                       |             |
| Racine de la console  | Délivré à                             | Délivré par  | Date d'expirati          | Rôles prévus          | Actions     |
| Certificats - Utilisateur actuel           Personnel                | AAA Certificate Services              | AAA Certificate Services                               | 01/01/2029               | Authentification du   | Certificats |
| <ul> <li>Autorités de certification racines de confiance</li> </ul> | AddTrust External CA Root             | AddTrust External CA Root<br>Baltimore CyberTrust Root | 30/05/2020<br>13/05/2025 | Authentification du   | Autre       |
| Certificats   | CA NoToS                              | CA NoToS   | 20/06/2021               | <tout></tout>         | CA NoToS    |
| Contrance de l'entreprise Autorités de certification intermédiaires | CA_ARARCPRD                           | CA_ARARCPRD  | 31/10/2022               | <tout></tout>         | Autre       |
| Objet utilisateur Active Directory                                  | Certum CA                             | Certum CA  | 11/06/2027               | Authentification du   |             |
| Éditeurs approuvés  | Class 1 Public Primary Certificat     | Class 1 Public Primary Certificatio                    | 02/08/2028               | Messagerie électro    |             |
| Certificats non autorisés   | 🔄 Class 2 Primary CA                  | Class 2 Primary CA                                     | 07/07/2019               | Messagerie électro    |             |
| Autorités de certification racine tierce partie                     | 🔄 🖾 Class 3 Public Primary Certificat | Class 3 Public Primary Certificatio                    | 03/08/2028               | Authentification du   |             |
| Personnes autorisées  | 🔄 Class 3 Public Primary Certificat   | Class 3 Public Primary Certificatio                    | 02/08/2028               | Messagerie électro    |             |
| Autres personnes  | Class 3 Public Primary Certificat     | Class 3 Public Primary Certificatio                    | 08/01/2004               | Messagerie électro    |             |
| Demandes d'inscription de certificat                                | COMODO Certification Authority        | COMODO Certification Authority                         | 01/01/2031               | Authentification du   |             |
| Racines de confiance de carte à puce                                | Copyright (c) 1997 Microsoft C        | Copyright (c) 1997 Microsoft Corp.                     | 31/12/1999               | Enregistrement des    |             |
|   | 🔄 DigiCert Assured ID Root CA         | DigiCert Assured ID Root CA                            | 10/11/2031               | Authentification du   |             |
|   | DigiCert High Assurance EV Ro         | DigiCert High Assurance EV Root                        | 10/11/2031               | Authentification du   |             |
|   | DT Soft Ltd                           | VeriSign Class 3 Code Signing 200                      | 04/11/2012               | Signature du code     |             |
|   | Entrust.net Certification Author      | Entrust.net Certification Authority                    | 24/07/2029               | Authentification du   |             |
|   | Entrust.net Secure Server Certifi     | Entrust.net Secure Server Certifica                    | 25/05/2019               | Authentification du   |             |
|   | Equifax Secure Certificate Auth       | Equifax Secure Certificate Authority                   | 22/08/2018               | Messagerie électro    |             |
|   | Equifax Secure Global eBusiness       | Equifax Secure Global eBusiness C                      | 21/06/2020               | Messagerie électro    |             |
|   | 🔄 GeoTrust Global CA                  | GeoTrust Global CA                                     | 21/05/2022               | Authentification du   |             |
|   | GeoTrust Primary Certification        | GeoTrust Primary Certification Au                      | 17/07/2036               | Authentification du   |             |
|   | 🔄 GlobalSign Root CA                  | GlobalSign Root CA                                     | 28/01/2028               | Authentification du   |             |
|   | Go Daddy Class 2 Certification        | Go Daddy Class 2 Certification Au                      | 29/06/2034               | Authentification du   |             |
|   | GTE CyberTrust Global Root            | GTE CyberTrust Global Root                             | 14/08/2018               | Messagerie électro    |             |
|   | http://www.valicert.com/              | http://www.valicert.com/                               | 26/06/2019               | Messagerie électro    |             |
|   | IGC/A                                 | IGC/A  | 17/10/2020               | Authentification du 🖕 |             |
|   | •                                     |  |                          | · · · · · ·           |             |

NO O

 Les certificats de CA peuvent être déployés automatiquement avec les GPO de l'AD



#### Les serveurs utilisant SSL

- Interface d'administration
  - Peut être configurée pour ne fonctionner qu'en SSL
  - Administration (port 2001 => 2005)
  - DCM
  - IBM Web Administration for i
- POP, SMTP
- TIVOLI
- LDAP
- DRDA, DDM



IBM Power Systems - IBM i

# S28 - La mise en œuvre de SSL afin de sécuriser les connexions avec un IBM i



Dominique GAYTE- dgayte@notos.fr 04 67 86 09 08 - 06 30 17 02 55

www.notos.fr

© IBM France 2013