LSpush

context

dit document beschrijft kort de werking van LSPush

werking

1. run LSPush op asset die je wilt scannen
2. kopieer bestand naar \\\LS\c$\Program Files (x86)\Lansweeper\Service\import
   na succesvolle import verdwijnt het bestand uit die map.
3. dit bestand is niet standaard leesbaar, maar kan (na hernoemen naar .zip extentie) probleemloos geopend worden in 7zip. Het is een XML-bestand.
4. kijk asset na in LS

Utility kan je starten vanuit

- geplande taak
- GPO
- DOS:

```
lspush <AdresLSServer> /showresult
```

Warning: Bij upload naar LSServer moet verkeer op tcp/9524 op LSServer doorgelaten worden

geplande taak

lspush. exe zonder opties:

`command: lspush.exe`

- %temp%/lspush bevat het bestand.
- als lspush meerdere keren draait, wordt het bestand en de timestamp bijgewerkt.
- troubleshooting tips:
  - controleer de Exit code in task scheduler (success: 0x0)
  - controleer of het bestand werd aangemaakt/bijgewerkt.

lspush. exe met opties

`command: lspush.exe <LansweeperServerName/IP>`

- er wordt geen tijdelijk bestand aamgemaakt. Alle scaninfo wordt in geheugen geladen
- op 't eind wordt alle info naar Lansweeper server bestuurd op tcp/9524
- meerdere keren uitvoeren, werkt LastSeen and Last LSPush Scan waarden bij in LS (ScanTime tab)
- troubleshooting tips:
  - controleer de Exit code in task scheduler
  - controleer of de computer de Lansweeper server kan bereiken:

    ```
    telnet <LansweeperServer/IP> 9524
    ```

  - controleer firewall logs als computer en LS server op verschillende subnets zitten.
  - controleer Last Run Time timestamp in TaskScheduler met LastSeen / LSPush Last Scan timestamp in Lansweeper. Die zouden moeten overeen komen.

meer info

- LSpush voor Windows scanning

lansweeper, lspush, agent scanning