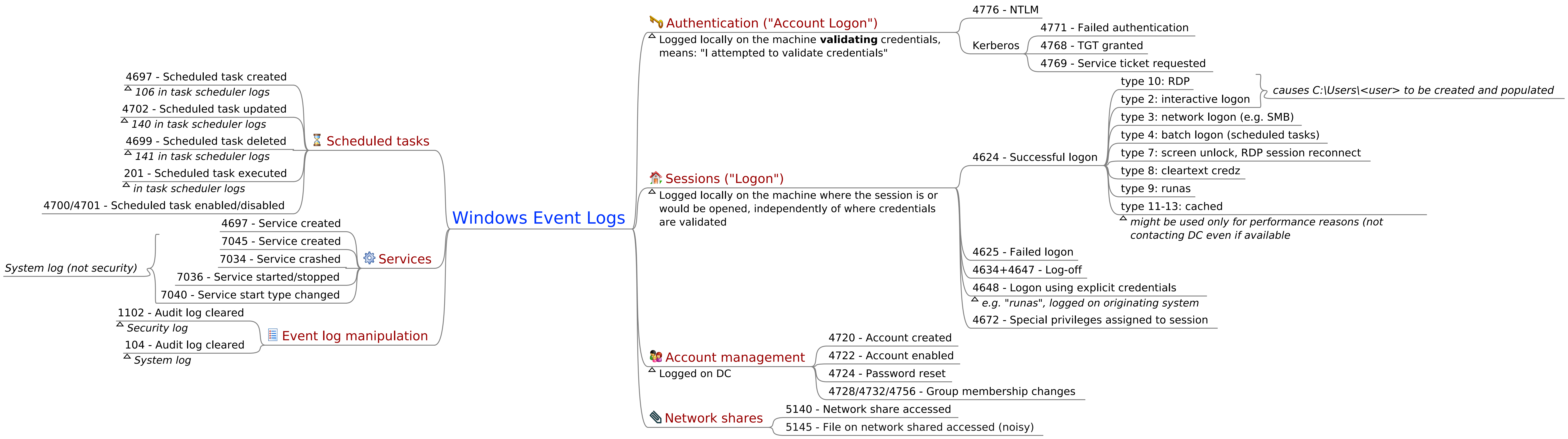

Windows Event Logs

- Authentication ("Account Logon")
  - Logged locally on the machine **validating** credentials, means: "I attempted to validate credentials"
  - 4776 - NTLM
  - Kerberos
    - 4771 - Failed authentication
    - 4768 - TGT granted
    - 4769 - Service ticket requested
- Sessions ("Logon")
  - Logged locally on the machine where the session is or would be opened, independently of where credentials are validated
  - 4624 - Successful logon
    - type 10: RDP
    - type 2: interactive logon
      - *causes C:\Users\<user> to be created and populated*
    - type 3: network logon (e.g. SMB)
    - type 4: batch logon (scheduled tasks)
    - type 7: screen unlock, RDP session reconnect
    - type 8: cleartext credz
    - type 9: runas
    - type 11-13: cached
      - *might be used only for performance reasons (not contacting DC even if available*
  - 4625 - Failed logon
  - 4634+4647 - Log-off
  - 4648 - Logon using explicit credentials
    - *e.g. "runas", logged on originating system*
  - 4672 - Special privileges assigned to session
- Account management
  - Logged on DC
  - 4720 - Account created
  - 4722 - Account enabled
  - 4724 - Password reset
  - 4728/4732/4756 - Group membership changes
- Network shares
  - 5140 - Network share accessed
  - 5145 - File on network shared accessed (noisy)
- Scheduled tasks
  - 4697 - Scheduled task created
    - *106 in task scheduler logs*
  - 4702 - Scheduled task updated
    - *140 in task scheduler logs*
  - 4699 - Scheduled task deleted
    - *141 in task scheduler logs*
  - 201 - Scheduled task executed
    - *in task scheduler logs*
  - 4700/4701 - Scheduled task enabled/disabled
- Services
  - 4697 - Service created
  - 7045 - Service created
  - 7034 - Service crashed
  - 7036 - Service started/stopped
  - 7040 - Service start type changed
  - *System log (not security)*
- Event log manipulation
  - 1102 - Audit log cleared
    - *Security log*
  - 104 - Audit log cleared
    - *System log*