AUDITLGN

LOGIN/LOGOUT AUDIT (VERS. 1.20)

1. Description:

- The audit module AUDITLGN.NLM is designed for registration of the following events:
  - USER LOGIN to a NetWare server.
  - USER LOGOUT of a NetWare server.
  - NIGHT CONTROL – Control of stations logged on to the server at night (at midnight). It allows to find users who don't turn off their computer for the night
- The module registers all logon events with a NORMAL status (similarly to MONITOR.NLM program).

If the interval between log on and logoff is shorter then 0.2 seconds an event can be not registered in the system.

- The module can control status of maximum of 200 (or 2000) users logged on to the server.
- The program enables to present maximum of 77 users logged on to the server at one screen.
- AUDITLGN is dedicated for servers working on the NetWare platform version 5.0, 5.1, 6.0 and 6.5.

2. Installation of AUDITLGN program on NetWare server:

Module AUDITLGN.NLM should be copied to a controlled server to SYSTEM folder on SYS volume.

3. Start AUDITLGN.NLM module:

The program can be started from a server console level immediately or automatically as a command line in AUTOEXEC.NCF file:

AUDITLGN /a /ppath **/m /n /X**

where:
/a - active connections screen is enable (default is disable).

/m - monthly log is enable (default is disable). For every month is created a separate log file that is named **AUDTyymm.LOG**, where yy – short form of year, mm – month.

/**n** - night control is enable (default is disable). It is created a separate log file containing a list of stations which are logged on to the server at midnight of every day.

/ppath - set the path for log fil.
path - path for log file: e.g. DATA:LOGS/AUDIT
(!! without char "/" or "\" at the end of line)
in this example log file will be: DATA:LOGS/AUDIT/AUDT0610.LOG
default path: SYS:ETC

/X – a start of the program with the /X option causes the additional audit records are created in an XML format. For every event a separate file is created. Files are written on the SYS volume in the ETC/XMLLOG folder.

Without /X option there is created only a standard event log - AUDITLGN.LOG in a structure as below:

LOGIN: 012 20060219 09:19:57 ADMIN1   IP 192.168.0.121
LOGOUT: 012 20060219 09:44:35 ADMIN1   IP 192.168.0.121

example:
auditlgn /a /m   /pDATA:LOGS/AUDIT

Default the AUDITLGN.LOG - event log is created on the SYS volume in the ETC folder.

The XML structure of files is following:

Login of the ADMIN1 user to the SERVER1 server:

```
<?xml version="1.0" encoding="Windows-1250" ?>
- <XMLLOG>
    <SERVER>Server SERVER1</SERVER>
    <EVENT>User Login</EVENT>
    <DATE>20060219 09:19:57</DATE>
    <CONN_NR>012</CONN_NR>
    <USER>ADMIN1</USER>
    <ADDRESS_TYPE>IP</ADDRESS_TYPE>
    <ADDRESS>192.168.0.121</ADDRESS>
  </XMLLOG>
```

Logout of the ADMIN1 user from the SERVER1 server :

```
<?xml version="1.0" encoding="Windows-1250" ?>
- <XMLLOG>
    <SERVER>Server SERVER1</SERVER>
    <EVENT>User Logout</EVENT>
    <DATE>20060219 09:44:35</DATE>
    <CONN_NR>012</CONN_NR>
    <USER>ADMIN1</USER>
    <ADDRESS_TYPE>IP</ADDRESS_TYPE>
    <ADDRESS>192.168.0.121</ADDRESS>
  </XMLLOG>
```

To finish a running AUDITLGN module it should be entered a command: *unload auditlgn*.

4. Screen of AUDITLGN program:

A main screen of the program after its start (with option /a) (Fig. 1)

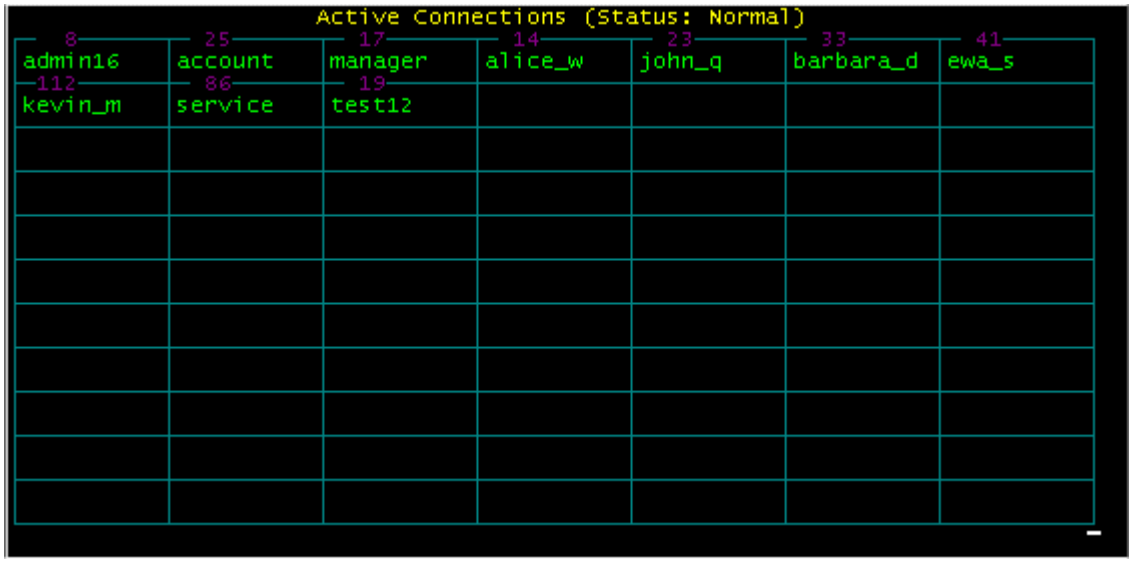

Fig. 1

If you have any Comments and Suggestions please send them to:djack@djack.com.pl

---

http://www.djack.com.pl