WindowLogger für MS-Terminalserver

1. Einleitung

Viele Administratoren oder Betreiber von Terminalservern haben ein Interesse daran, die Aktivitäten von Terminalserverbenutzern nachvollziehen zu können. Dabei ist es nicht nötig jede Aktion eines Benutzers zu registrieren. Es ist eigentlich ausreichend die An- und Abmeldung von Benutzern sowie das Öffnen und Schliessen von Fenstern (einschliesslich des Fenstertitels) zu protokollieren. So kann beispielsweise nachvollzogen werden, wann ein bestimmter Benutzer eine Internetsite besucht, ein Programm gestartet oder eine Datei gelöscht hat.
Um eine zu hohe Belastung des Terminalservers zu vermeiden, wird nicht etwa das Gesamtsystem einem Subclassing unterzogen, sonder in einem Zeittakt von ca. 300 ms ein Snapshot jeder Sitzung erstellt und das Ergebnis in einer Datenbank abgelegt.

2. Software Architektur

Die vorliegende Software setzt sich aus 3 Komponenten zusammen.

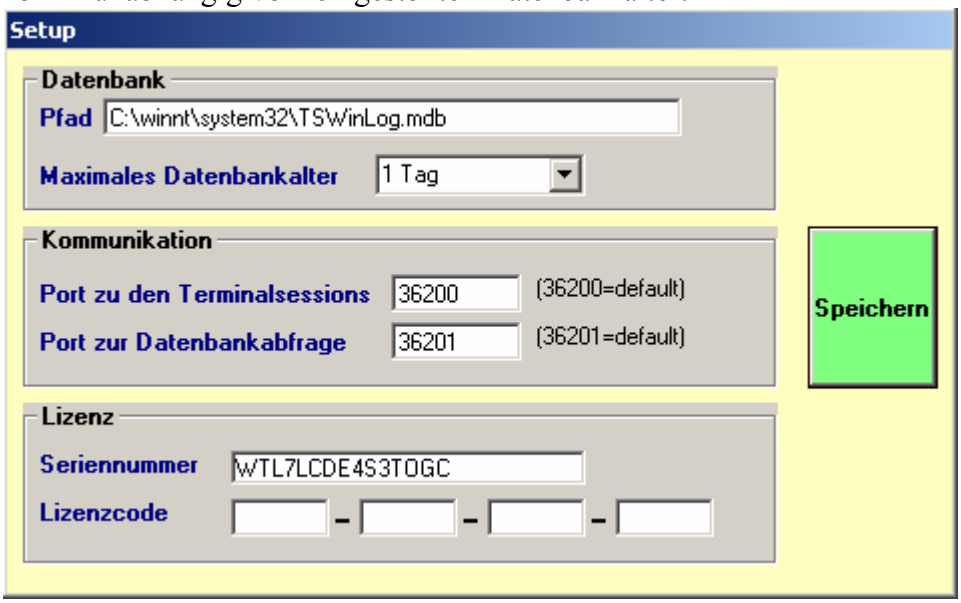
a) Serverkomponente: Eine Dienstkomponente, die die Informationen der Clients empfängt und in die Datenbank einträgt.
b) Clientcomponente: Ein Hintergrundprozess, der in jeder Session (einschließlich Konsole) gestartet wird
c) Auswertekomponente: Ein GUI für die Datenbankauswertung

3. Installation

Im Archiv befinden sich 3 Installer (für jede Komponente ein Installer).
Bitte entpacken Sie zunächst das Archiv an einem temporären Ort. Folgende Vorgehensweise ist dann anzuwenden:

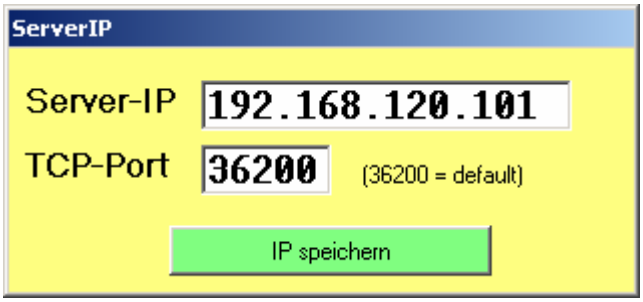
a) Ausführen von von ***SetupSvr.exe***. Hierdurch wird der erforderliche Dienst installiert. In der Setupmaske geben Sie bitte den Pfad zur Datenbank (%windir%\system32\TSWinlog.mdb ist voreingestellt), das maximale Dataenbankalter (sind Einträge älter als die Systemzeit abzüglich der eingetragenen Datenbankalters werden sie gelöscht) und die Ports für die Kommunikation an. Die bei der Installation erzeugte Seriennummer wird angezeigt und die Eingabefelder für den Lizenzcode sind noch leer. Speichern Sie mit leerem Lizenzcode läuft die Software in der DEMO-Version, d.h. die Datenbankeinträge werden nicht älter als

15min unabhängig vom eingestellten Datenbankalter.



Eine Messagebox informiert über die Dienstinstallation.

b) Führen Sie den Installer ***SetupCli.exe*** aus. Es wird der Clientprozess für alle Sessions installiert.



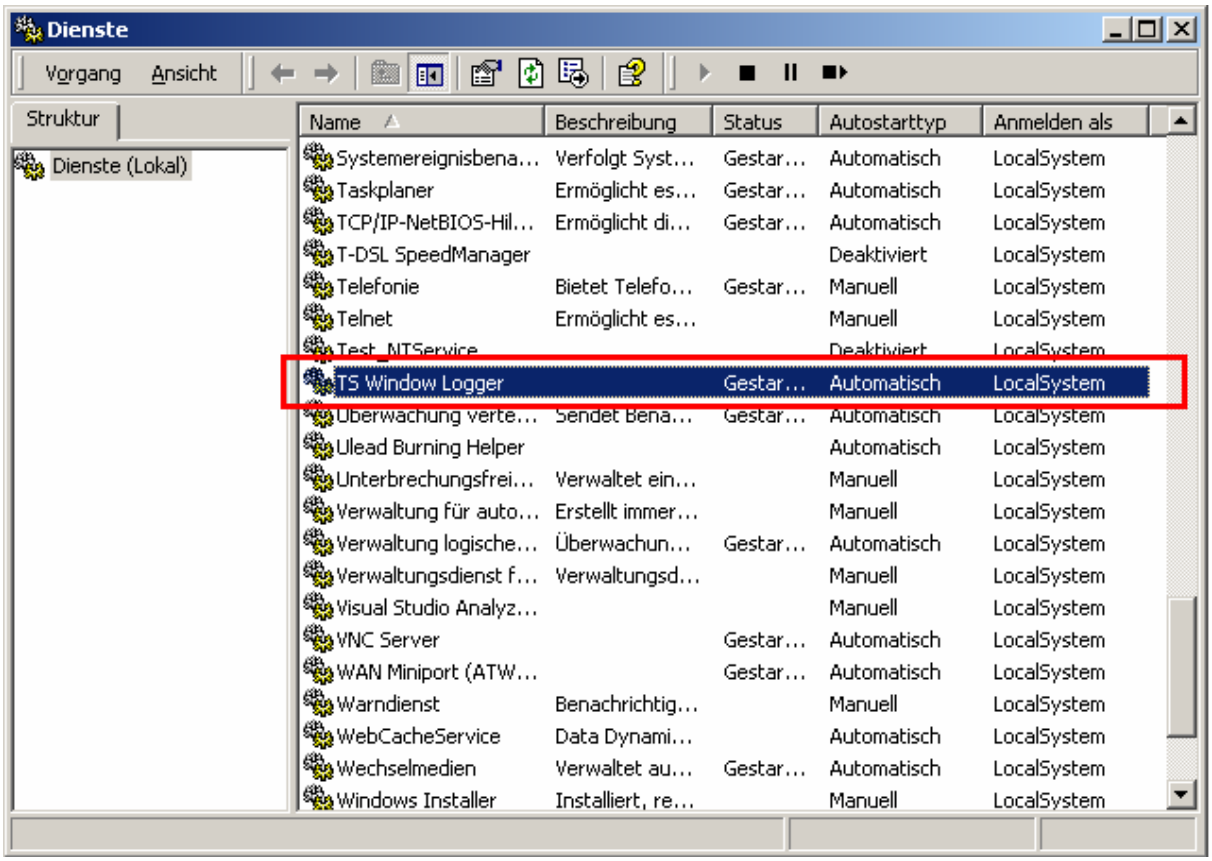
Im Eingabefenster tragen Sie bitte die IP-Adresse ihres Servers(oder wenn Sie mehrere Server verwenden sollten, die Adresse des Servers auf der Sie gerade den Dienst installiert haben. Die Dienstkomponente muß nur auf einem Server installiert werden.) Der Port muß dem der Serverinstallation entsprechen!

c) Führen Sie den Installer ***SetupReport.exe*** auf allen Maschinen, wo Sie Auswertung abfragen möchten, aus.

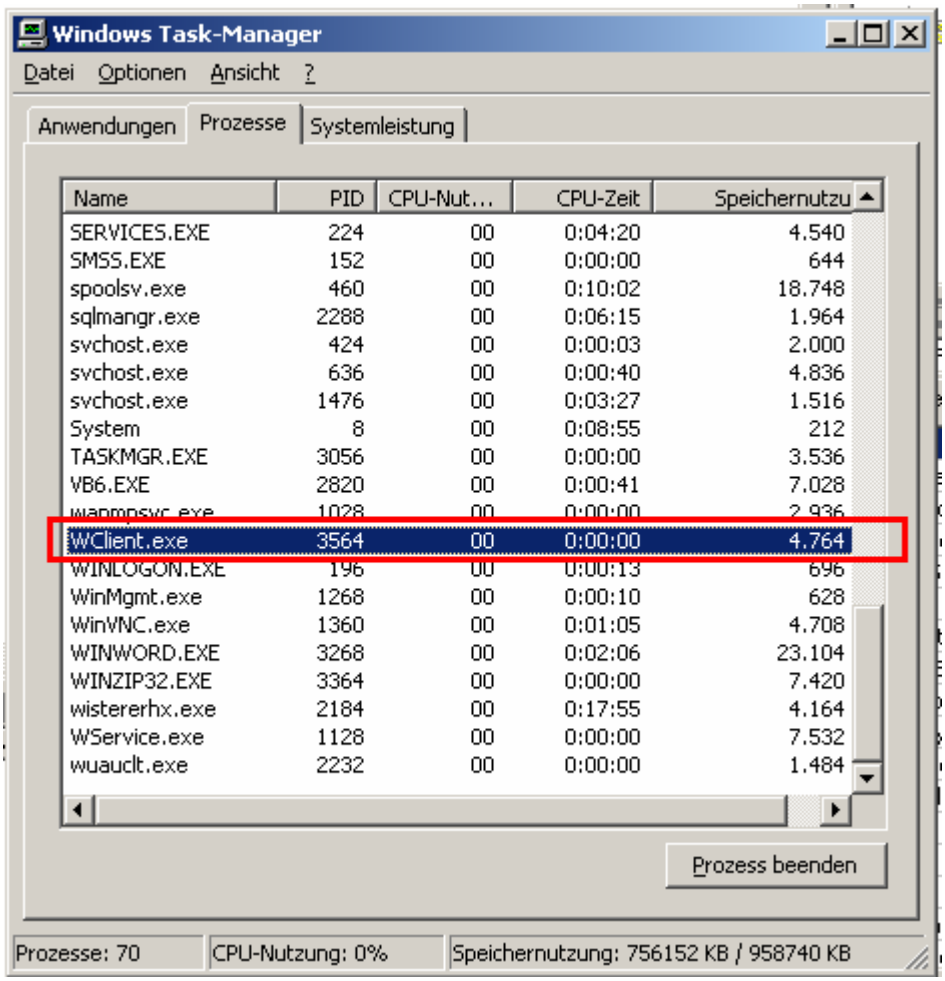
d) Starten Sie den(die) Server neu.

4. Test der Installation

Nach dem Neustart des(der) Server(s) öffnen Sie auf dem Server, der die Serviceinstallation erhalten hat, die Diensteverwaltung. Dort muß sich der Dienst **„TS Window Logger“** im Zustand **„gestartet“** befinden.



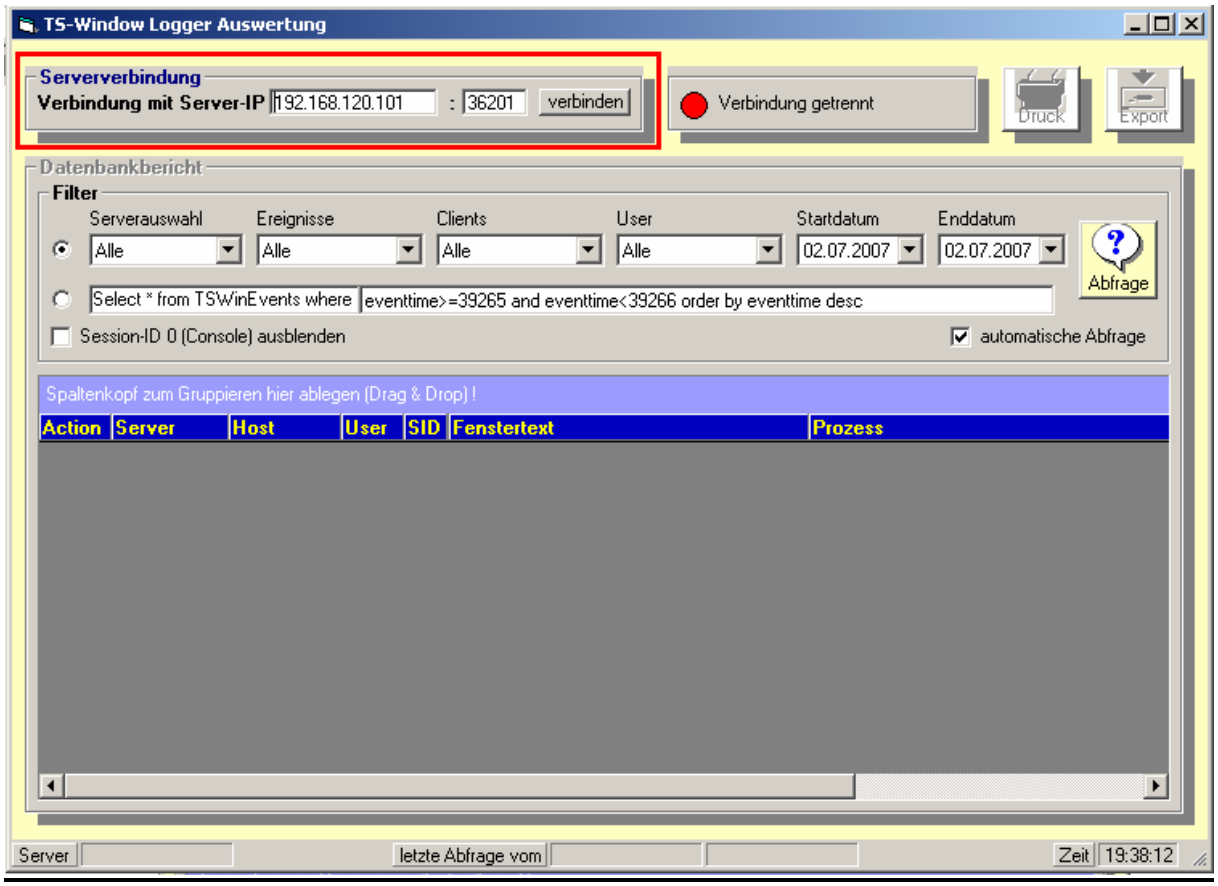
In der Konsole des(r) Server(s) sowie in jeder Terminalsession muß ein Prozess **WClient.exe** zu finden sein. Dies kann man schnell mit dem Taskmanager überprüfen.



An-, Abmeldevorgänge, Öffnen und Schließen von Fenstern oder das Ändern des Fenstertitels werden nun in der Datenbank gespeichert.

5. Auswertung der gesammelten Daten

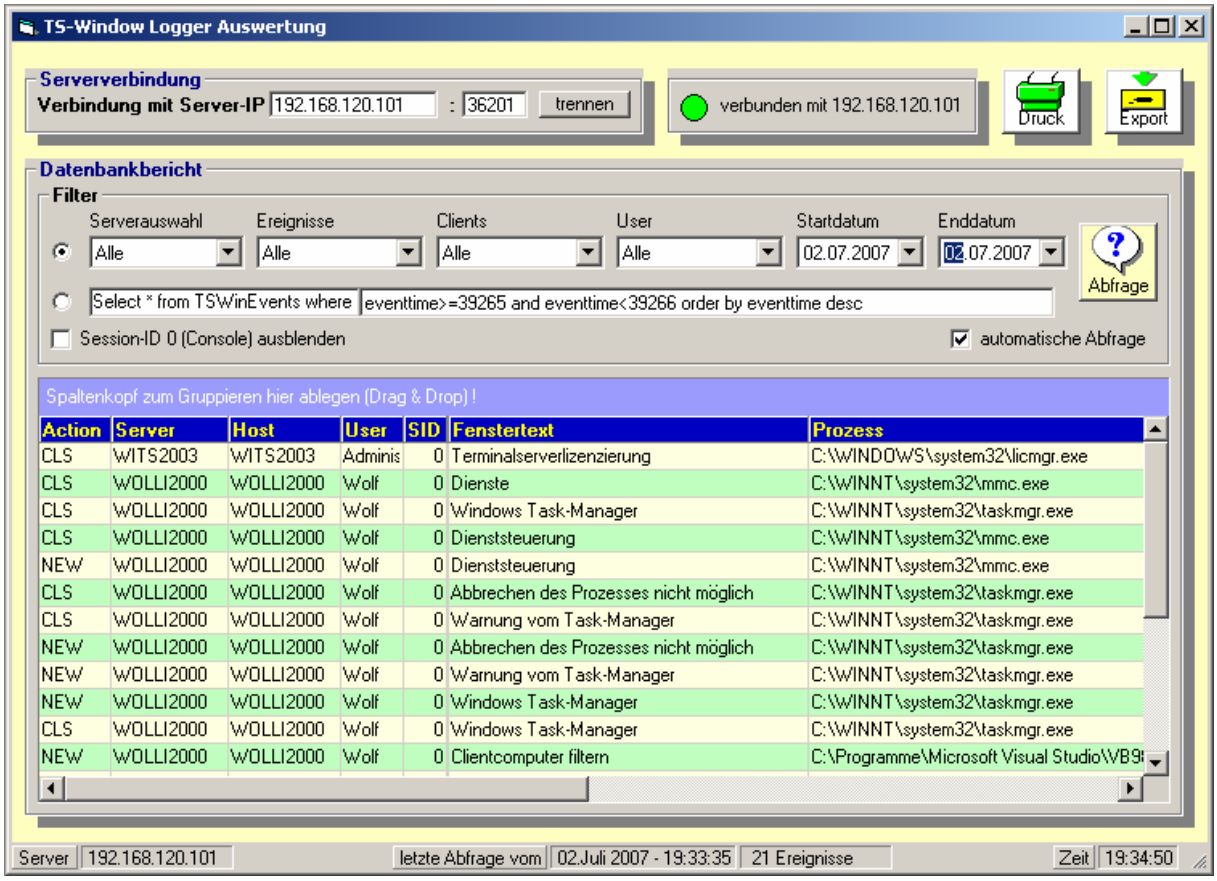
Durch Ausführen von Report.exe erscheint das Datenbank-GUI.
Hier muß zunächst die TCP/IP-Verbindung zur Datenabank hergestellt werden. Also IP-Adresse und Port eingeben und den Button verbinden clicken.



Ist die Verbindung hergestellt wird dies angezeigt, der Frame Datenbankbericht ist freigegeben und es kann der Button Abfrage geclickt werden.
Die möglichen Filtereinstellungen erklären sich eigentlich selbst.
Der Schlüssel im Datenbankfeld Action erklärt sich wie folgt:

LGI	--->	Ein Benutzer hat sich neu eingeloggt
NEW	--->	Ein Fenster wurde neu geöffnet
CHG	--->	Die Titelzeile des Fensters wurde verändert
CLS	--->	Ein Fenster wurde geschlossen
LGO	--->	Ein Benutzer hat sich abgemeldet

Über die Button Druck und Export kann der Bericht in seiner momentanen Darstellung ausgegeben werden.



6. Einstellungen von Dienst und Clients verändern

Sollen Einstellungen an der Dienstkomponente verändert werden, so ist der Dienst zunächst über den Dienstemanager zu beenden.
Dann führen Sie bitte *C:\%windir%\system32\Wservice.exe –edit* aus. Die Setupmaske, wie oben beschrieben, erscheint erneut. Speichern Sie die Einstellungen, der Dienst wird dann sofort neu gestartet.
Sollen an den Clients Einstellungen geändert werden, beenden Sie zunächst alle Prozesse Wclient.exe über den Taskmanager.
Starten Sie dann mit *C:\%windir%\system32\Wclient.exe –edit* den Clienten neu. Die TCP/IP –Maske erscheint und Änderungen können gespeichert werden. Der Client ist danach neu gestartet.

7. Lizenzierung

Wie bereits oben erwähnt läuft die Software ohne gültigen Lizenzcode im DEMO-Modus und kann nur Ereignisse, die weniger als 15 Minuten zurückliegen speichern. Diese Datenbankbereinigung ist ein dynamischer Prozess der jede Minute einmal durchgeführt wird.
Alle Ereignisse, die älter als 15 Minuten, bezogen auf die momentane Systemzeit, sind, werden gelöscht.
Zum Erwerb eines Lizenzcodes senden sie bitte eine Email mit der Seriennummer und einer Rechnungsanschrift an service@wolf-it-service.de . Der Lizenzcode wird einmal je Dienstkomponente benötigt. Die Anzahl der Clients ist unbegrenzt.
Den zur Zeit gültigen Nettopreis entnehmen Sie bitte meiner Website www.wolf-it-service.de .

8. Updates

Updates zur Software erscheinen in loser Folge auf meiner Website www.wolf-it-service.de und sind kostenlos.

Für weitere Fragen stehe ich Ihnen gern per email, Telefon oder Telefax zur Verfügung.