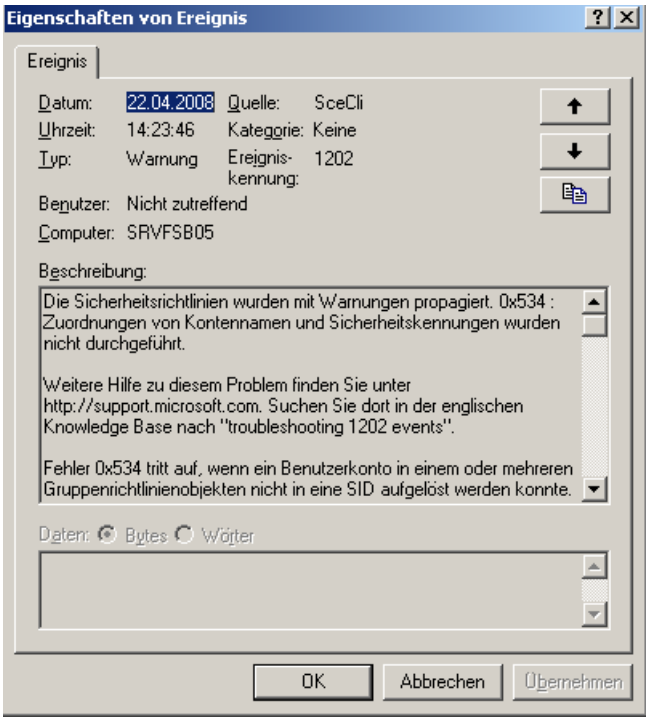
EventLog – 1202

So gesehen bei einem Kunden. Die Loesung ist trivial und dank Google kommt man dem Fehler auch leicht auf die Spur. Witzig finde ich nur, wie es dazu kommen kann, denn dieser Account wurde von dem Kunden und den Consultants nie bewusst erstellt.

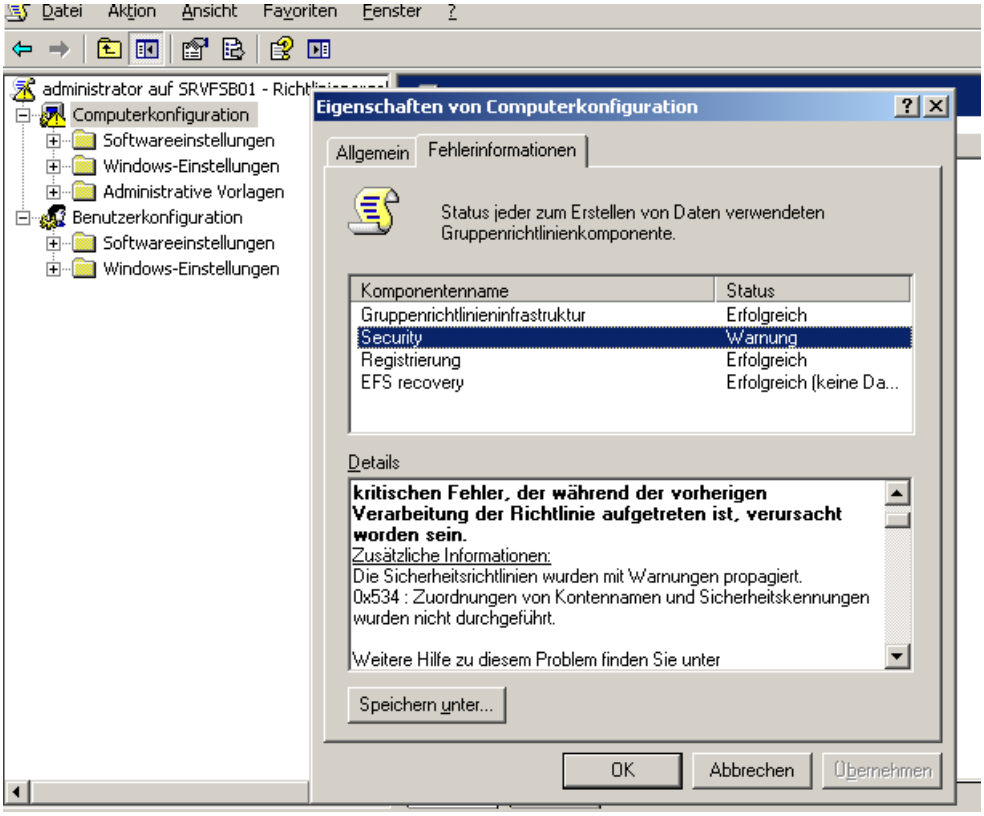
Die Ereignisanzeige mit gefuellten Eintraegen alle 5 Minuten.

Warnung	22.04.2008	14:48:55	SceCli	Keine	1202
Warnung	22.04.2008	14:43:53	SceCli	Keine	1202
Warnung	22.04.2008	14:38:52	SceCli	Keine	1202
Warnung	22.04.2008	14:33:50	SceCli	Keine	1202
Warnung	22.04.2008	14:28:48	SceCli	Keine	1202
Warnung	22.04.2008	14:23:46	SceCli	Keine	1202
Warnung	22.04.2008	14:18:44	SceCli	Keine	1202
Warnung	22.04.2008	14:13:42	SceCli	Keine	1202
Warnung	22.04.2008	14:08:40	SceCli	Keine	1202
Warnung	22.04.2008	14:03:38	SceCli	Keine	1202
Warnung	22.04.2008	13:58:36	SceCli	Keine	1202
Warnung	22.04.2008	13:53:35	SceCli	Keine	1202
Warnung	22.04.2008	13:48:33	SceCli	Keine	1202
Warnung	22.04.2008	13:43:31	SceCli	Keine	1202
Warnung	22.04.2008	13:38:29	SceCli	Keine	1202
Warnung	22.04.2008	13:33:27	SceCli	Keine	1202
Warnung	22.04.2008	13:28:25	SceCli	Keine	1202
Warnung	22.04.2008	13:23:23	SceCli	Keine	1202
Warnung	22.04.2008	13:18:21	SceCli	Keine	1202
Warnung	22.04.2008	13:13:19	SceCli	Keine	1202
Warnung	22.04.2008	13:08:17	SceCli	Keine	1202
Warnung	22.04.2008	13:03:16	SceCli	Keine	1202
Warnung	22.04.2008	12:58:14	SceCli	Keine	1202



RSOP.MSC ausführen

RSOP zeigt Detailinformationen an, wo es hakt.



KB Artikel raussuchen

Registry patchen

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{827D319E-6EAC-11D2-A4EA-00C04F7 9F83A}

c. On the **Edit** menu, click **Add Value**, and then add the following registry value:

Value name: ExtensionDebugLevel
Data type: DWORD
Value data: 2

d. Quit Registry Editor.

Winlogon.Log

Protokolliert werden die Debuginformationen in der Datei Winlogon.log

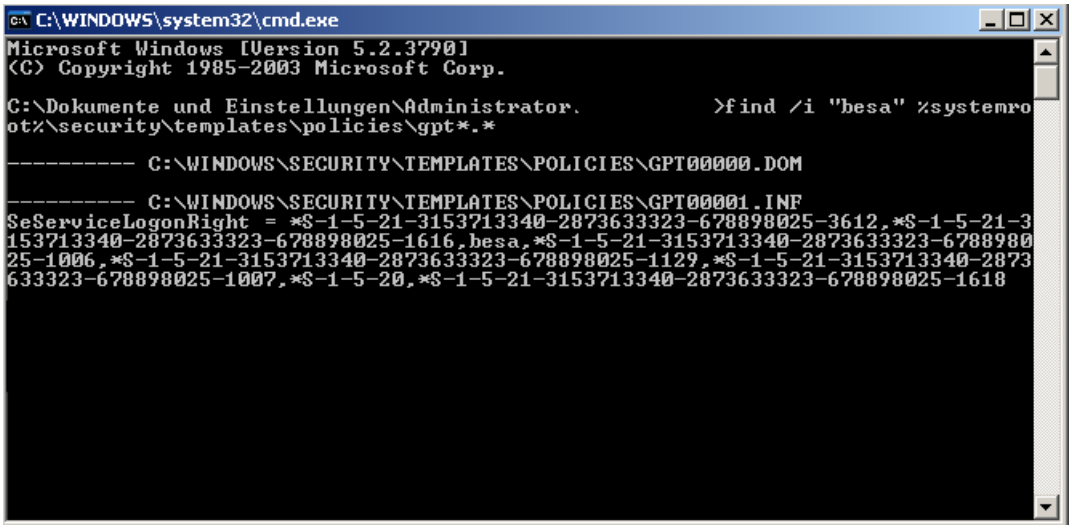
```
----Benutzerrechte werden konfiguriert...
        Konfigurieren von S-1-5-19.
        Konfigurieren von S-1-5-20.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1007.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1126.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1615.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1618.
        Konfigurieren von S-1-5-32-544.
        Konfigurieren von S-1-5-32-551.
        Konfigurieren von S-1-5-32-549.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1614.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1001.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1005.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1006.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1125.
        Konfigurieren von S-1-1-0.
        Konfigurieren von S-1-5-11.
        Konfigurieren von S-1-5-32-554.
        Konfigurieren von S-1-5-32-548.
        Konfigurieren von S-1-5-32-550.
        Konfigurieren von S-1-5-9.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1118.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-3612.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1616.
        Konfigurieren von besa.
Fehler 1332: Zuordnungen von Kontennamen und Sicherheitskennungen wurden nicht durchgeführt.
        besa wurde nicht gefunden.
        Konfigurieren von S-1-5-21-3153713340-2873633323-678898025-1129

        Konfiguration der Benutzerrechte wurde mit einem oder mehreren Fehlern abgeschlossen.
```

Da gibt es einen Account namens BESA – wohl angelehnt an BESADMIN? Von Blackberry RIM.

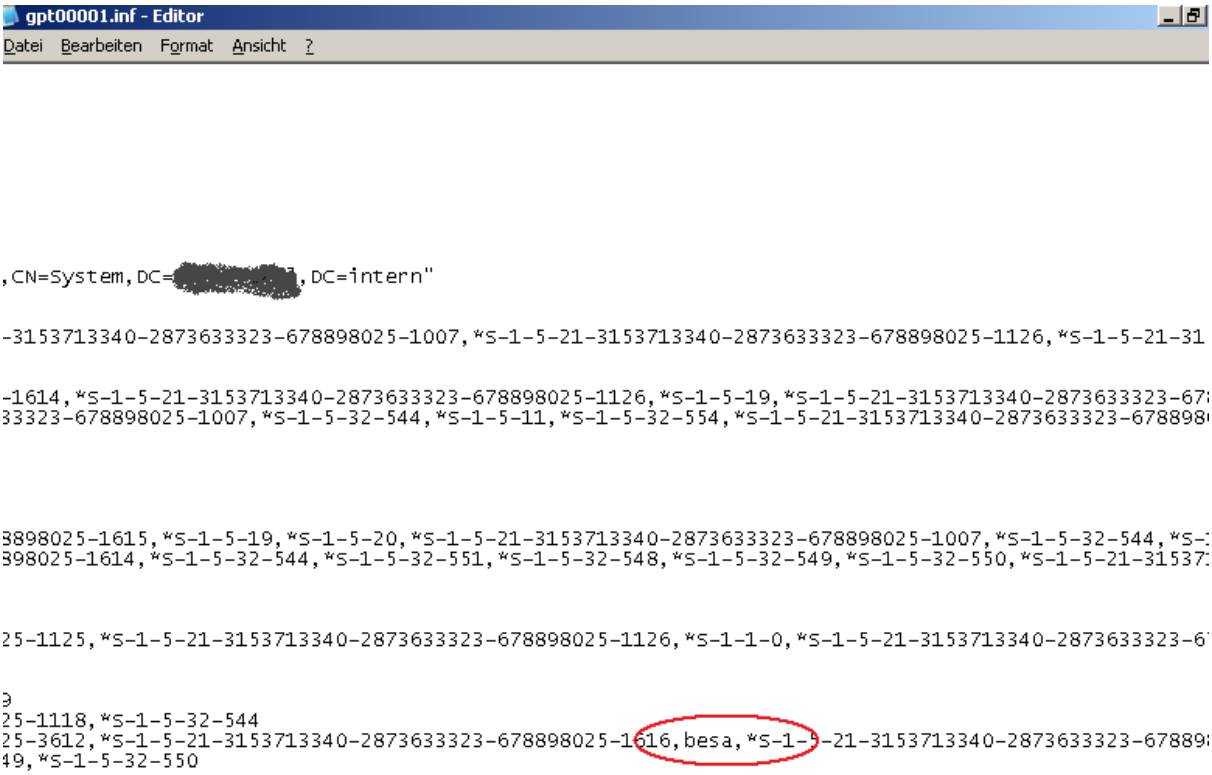
Ermitteln wo der Account zu finden ist

c:\>find /i “*account name*” %SYSTEMROOT%\security\templates\policies\gpt*.*



Ermitteln des GPT und öffnen der Datei

In diesem Fall GPT00001.INF



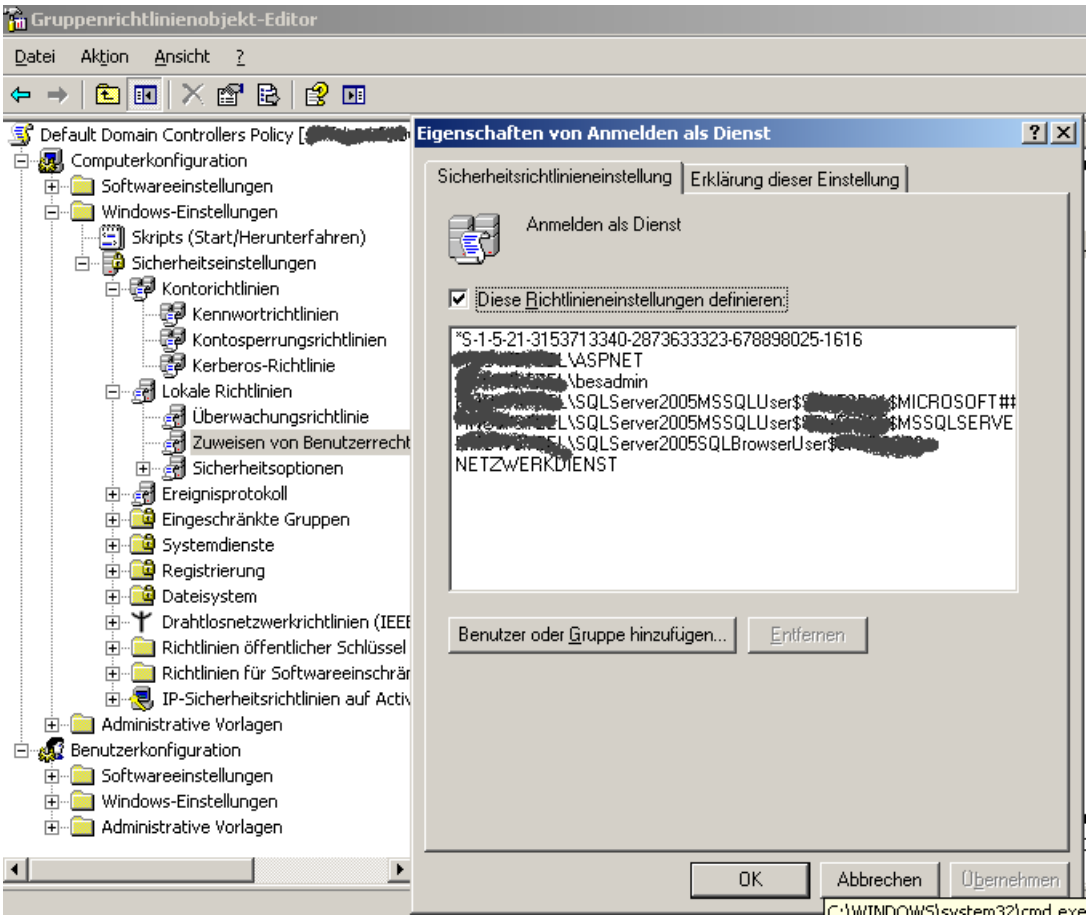
Ermitteln, in welcher Gruppenrichtlinie die Einstellung existiert

GPOPath={6AC1786C-016F-11D2-945F-00C04FB984F9}\MACHINE

Zuordnen der GUID zu einer Gruppenrichtlinie

GPOTOOL /VERBOSE oder bei wenigen Gruppenrichtlinien haendisch ueber den Manager

Entfernen des verwaisten Accounts



Danach hat der Spuk ein Ende.

Interessant ist auch noch, dass diese Fehlermeldung auch auf einem Domaenencontroller einer Subdomain auftaucht. In diesem Fall hiess der verwaiste Account WSUS, was wohl von dem wirklich existierenden Account WSUSADMIN stammen koennte?.