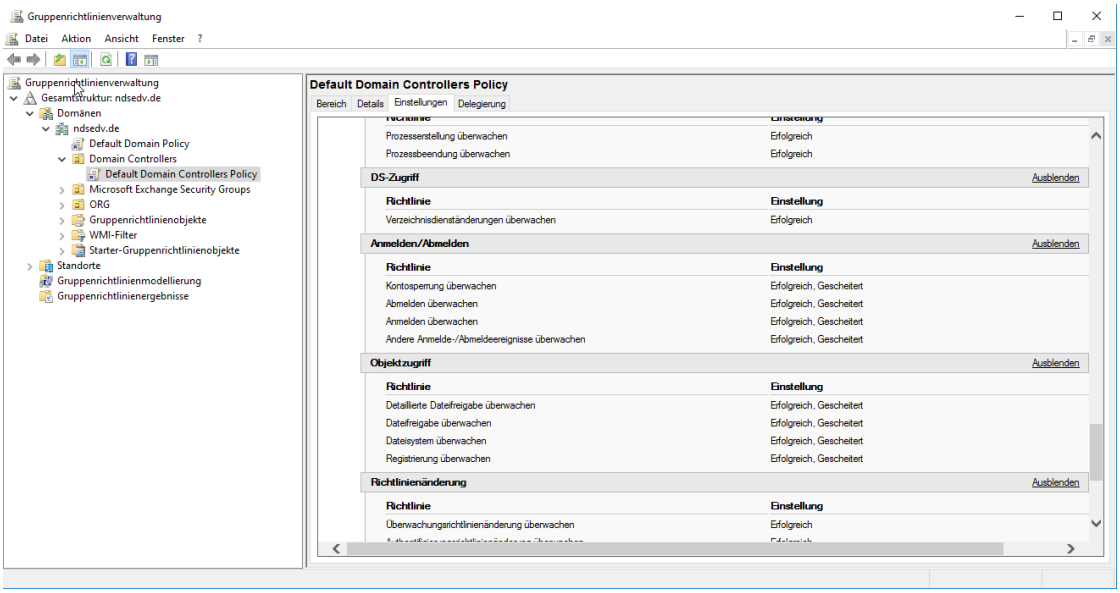
# Anmeldeversuche überwachen

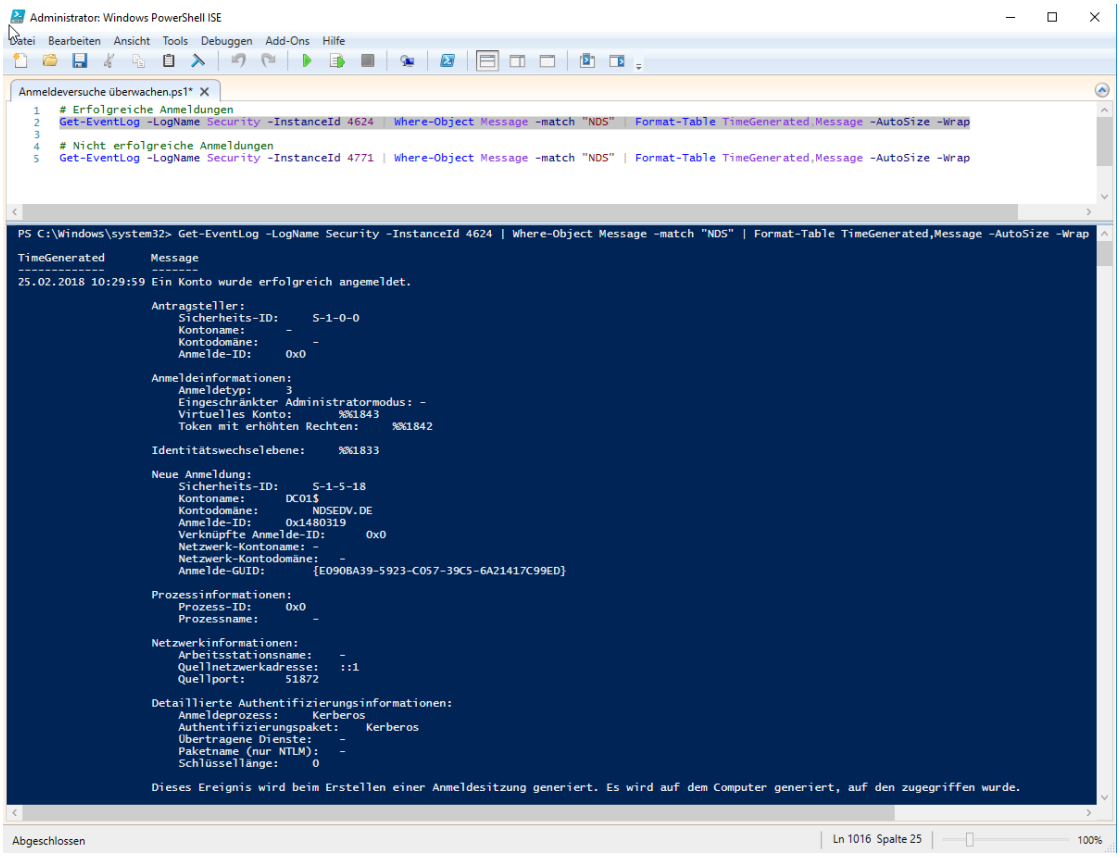
Zur Überwachung der An- und Abmeldeversuche muss die Default Domain Controller Policy entsprechend angepasst werden. Natürlich besteht auch die Möglichkeit eine neue Richtlinie anzulegen.




Logeinträge in der Ereignisanzeige sind der Dreh- und Angelpunkt einer Analyse, wenn es darum geht, ein Anliegen des Sicherheitsbeauftragten nach zu kommen. Die Powershell kann uns helfen, die Auswertung von Ereignissen zu beschleunigen.

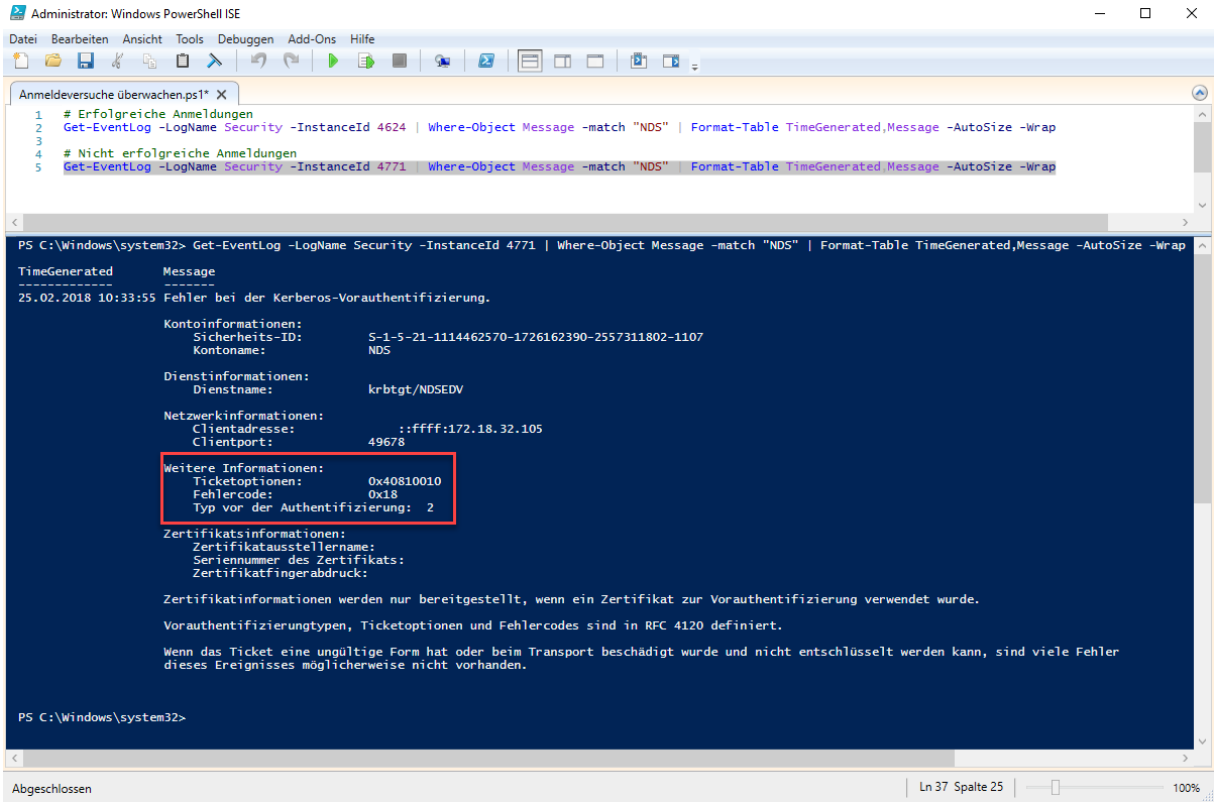
Erfolgreiche Anmeldungen werden mit der Event-ID 4624 registriert.

## Erfolgreiche Anmeldung an die Domäne:



## Anmeldeversuche überwachen

Nicht erfolgreiche Anmeldungen werden mit der Event-ID 4771 registriert. Bei nicht erfolgreichen Anmeldungen ist noch wichtig zu beachten, was der Grund für die Falschanmeldung war. In diesem Fall war ein falsches Passwort der Grund für die Ablehnung der Anmeldung. Gekennzeichnet mit dem Fehlercode 0x18.




```
# Erfolgreiche Anmeldungen
Get-EventLog -LogName Security -InstanceId 4624 | Where-Object Message -match "NDS" | Format-Table TimeGenerated,Message -AutoSize -Wrap

# Nicht erfolgreiche Anmeldungen
Get-EventLog -LogName Security -InstanceId 4771 | Where-Object Message -match "NDS" | Format-Table TimeGenerated,Message -AutoSize -Wrap
```

### Weitere Abfragen:

```
# Erfolgreiche Anmeldungen
wevtutil qe Security "/q:*[System[(EventID=4624)]]" /f:text

# System Shutdown
wevtutil qe System "/q:*[System[(EventID=1074)]]" /f:text

# Letzten 5 Security Logs
wevtutil qe Security /c:5 /rd:true /f:text

# Listet alle Security Logs auf
powershell -c "& {import-modue eventlog;get-eventlog -logname Security;}"

# Fehlerhafte RDP Anmeldungen letzten 500
wevtutil qe security /c:500 /rd:true /f:text|findstr 4625
```

**Erstellt von Jörn Walter** **25.02.2018**

## Anmeldeversuche überwachen

### Result Codes die zurückgegeben werden können:

| Result code | Kerberos RFC description | Notes on common failure codes |
|---|---|---|
| 0x1 | Client's entry in database has expired | |
| 0x2 | Server's entry in database has expired | |
| 0x3 | Requested protocol version # not supported | |
| 0x4 | Client's key encrypted in old master key | |
| 0x5 | Server's key encrypted in old master key | |
| 0x6 | Client not found in Kerberos database | Bad user name, or new computer/user account has not replicated to DC yet |
| 0x7 | Server not found in Kerberos database | New computer account has not replicated yet or computer is pre-w2k |
| 0x8 | Multiple principal entries in database | |
| 0x9 | The client or server has a null key | Administrator should reset the password on the account |
| 0xA | Ticket not eligible for postdating | |
| 0xB | Requested start time is later than end time | |
| 0xC | KDC policy rejects request | Workstation restriction |
| 0xD | KDC cannot accommodate requested option | |
| 0xE | KDC has no support for encryption type | |
| 0xF | KDC has no support for checksum type | |
| 0x10 | KDC has no support for padata type | |

| | | |
|---|---|---|
| 0x11 | KDC has no support for transited type | |
| 0x12 | Clients credentials have been revoked | Account disabled, expired, locked out, logon hours. |
| 0x13 | Credentials for server have been revoked | |
| 0x14 | TGT has been revoked | |
| 0x15 | Client not yet valid - try again later | |
| 0x16 | Server not yet valid - try again later | |
| 0x17 | Password has expired | The user’s password has expired. |
| 0x18 | Pre-authentication information was invalid | Usually means bad password |
| 0x19 | Additional pre-authentication required* | |
| 0x1F | Integrity check on decrypted field failed | |
| 0x20 | Ticket expired | Frequently logged by computer accounts |
| 0x21 | Ticket not yet valid | |
| 0x21 | Ticket not yet valid | |
| 0x22 | Request is a replay | |
| 0x23 | The ticket isn't for us | |
| 0x24 | Ticket and authenticator don't match | |
| 0x25 | Clock skew too great | Workstation’s clock too far out of sync with the DC’s |
| 0x26 | Incorrect net address | IP address change? |
| 0x27 | Protocol version mismatch | |
| 0x28 | Invalid msg type | |
| 0x29 | Message stream modified | |

| | | |
|---|---|---|
| 0x2A | Message out of order | |
| 0x2C | Specified version of key is not available | |
| 0x2D | Service key not available | |
| 0x2E | Mutual authentication failed | may be a memory allocation failure |
| 0x2F | Incorrect message direction | |
| 0x30 | Alternative authentication method required* | |
| 0x31 | Incorrect sequence number in message | |
| 0x32 | Inappropriate type of checksum in message | |
| 0x3C | Generic error (description in e-text) | |
| 0x3D | Field is too long for this implementation | |

**Logon Types:**

| Logon type | Logon title | Description |
|---|---|---|
| **2** | Interactive | A user logged on to this computer. |
| **3** | Network | A user or computer logged on to this computer from the network. |
| **4** | Batch | The batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention. |
| **5** | Service | A service was started by the Service Control Manager. |
| **7** | Unlock | This workstation was unlocked. |
| **8** | NetworkCleartext | A user logged on to this computer from the network. The user’s password was passed to the authentication |

| | | |
|---|---|---|
| | | package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext). |
| **9** | NewCredentials | A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections. |
| **10** | RemoteInteractive | A user logged on to this computer remotely using Terminal Services or Remote Desktop. |
| **11** | CachedInteractive | A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials. |

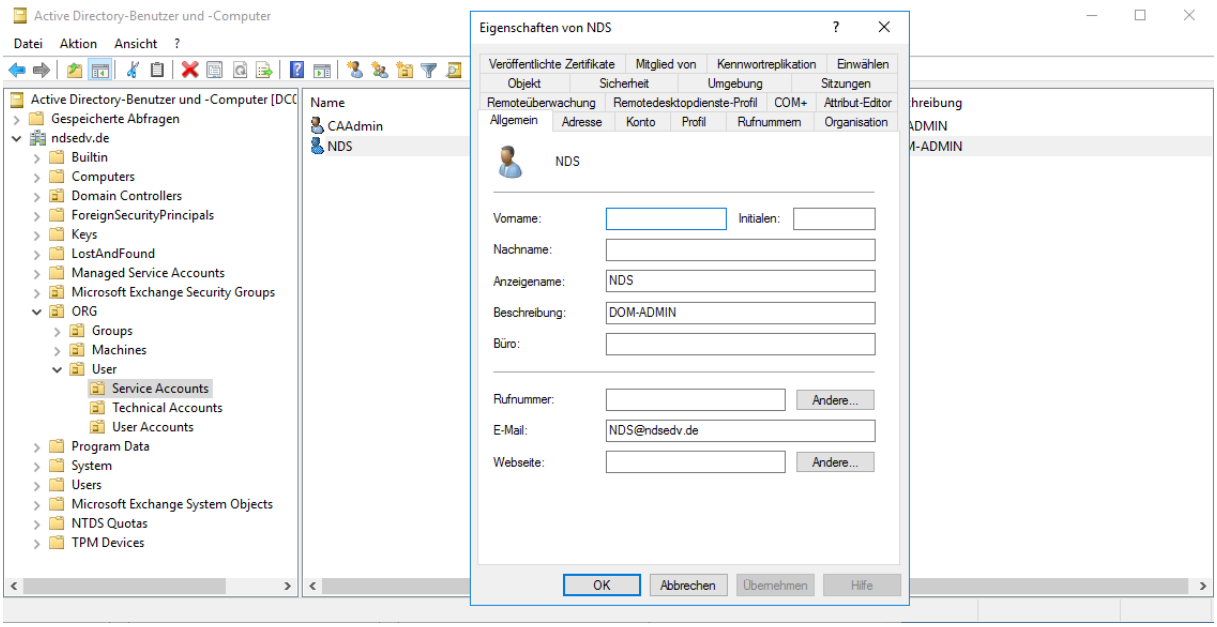
| **Level** | **Description** |
|---|---|
| Level 1 | Critical |
| Level 2 | Error |
| Level 3 | Warning |
| Level 4 | Information |

**Batch Datei zur Ausführung über den Taskplaner:**

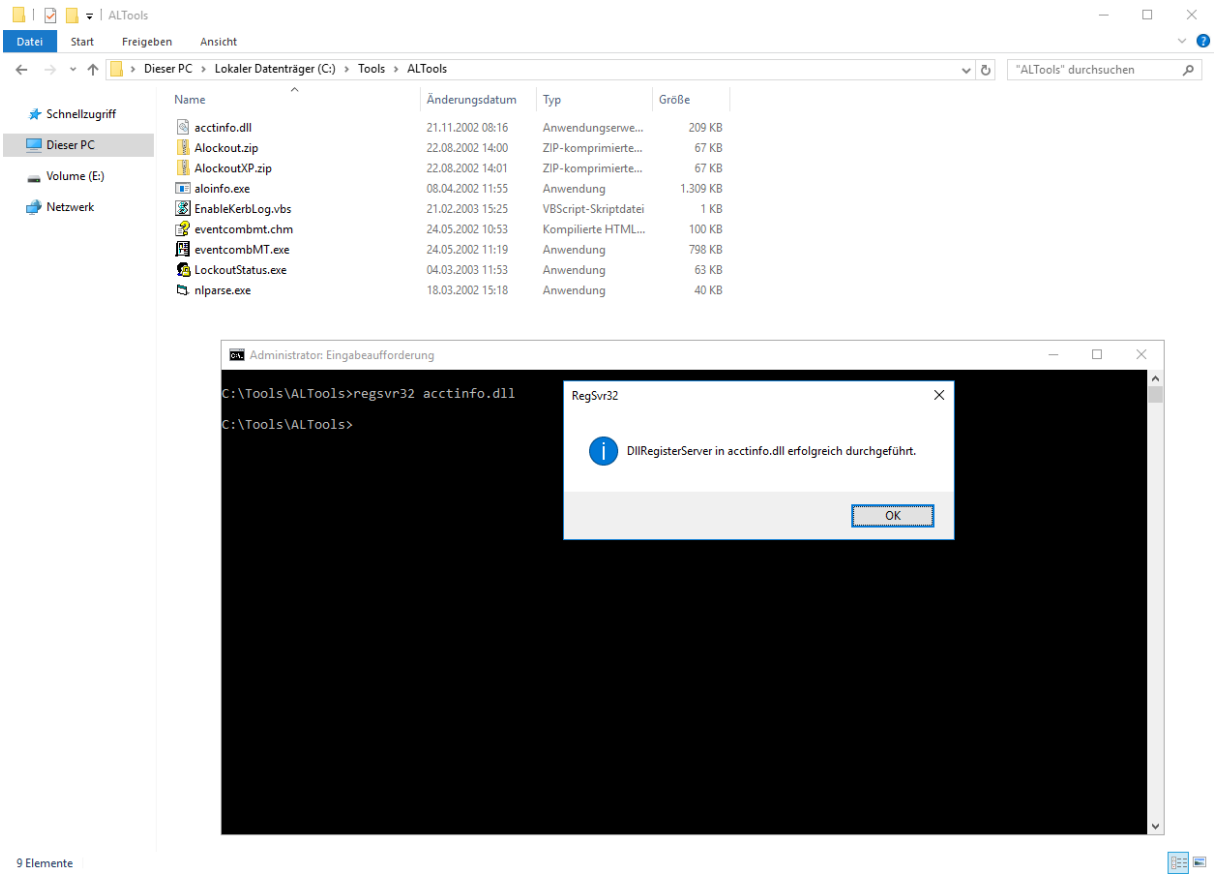
```
del C:\Temp\logon.txt

wevtutil qe Security "/q:*[System [(EventID=4624)]]" /f:text /rd:true /c:1 > C:\Temp\Logon.txt

notepad C:\Temp\logon.txt
```

# Anmeldeversuche überwachen

Unnützes Wissen: acctinfo.dll – eine 15 Jahre alte DLL.



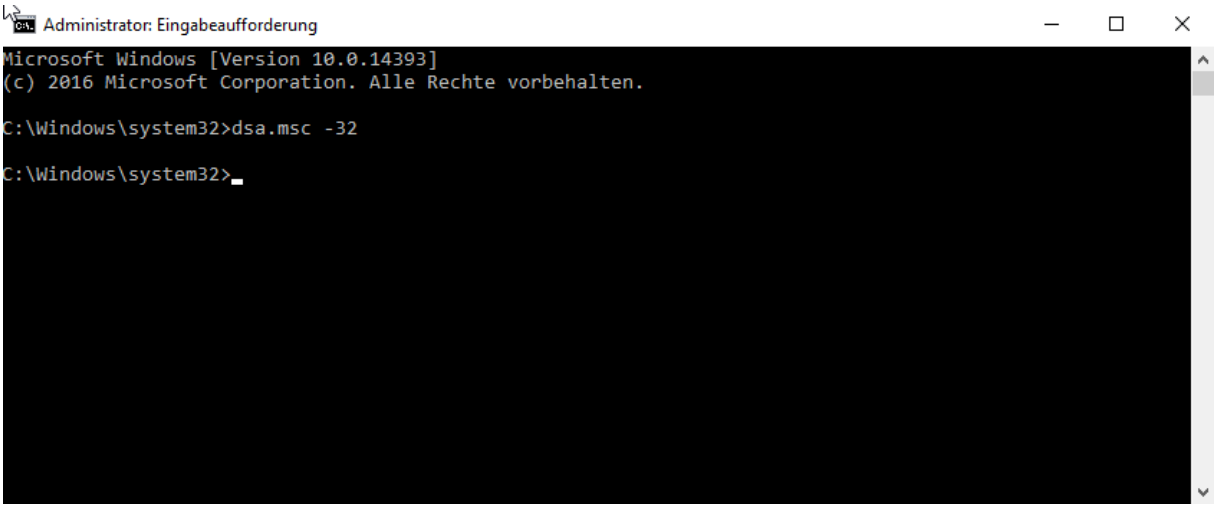

Registrieren der acctinfo.ddl:




**Erstellt von Jörn Walter** **25.02.2018**

## Anmeldeversuche überwachen

Die Konsole in der 32-Bit Version öffnen:




Die letzte Anmeldung ist nun etwas schicker einzusehen sowie die letzte Passwortänderung: