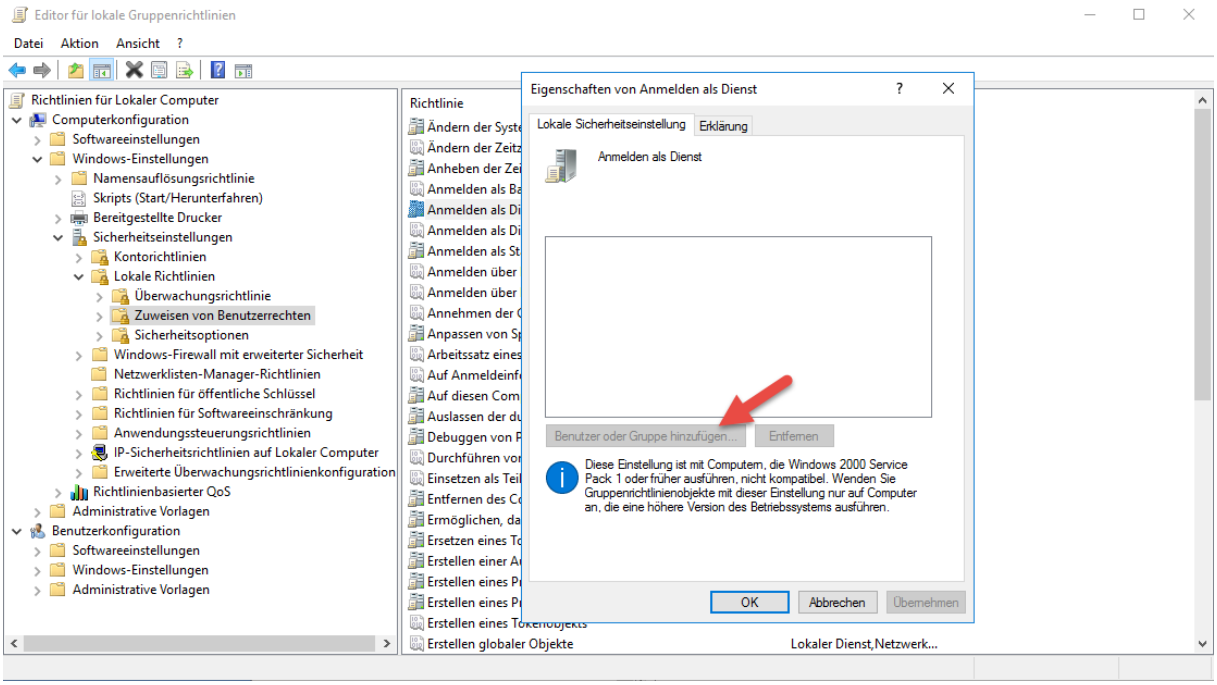
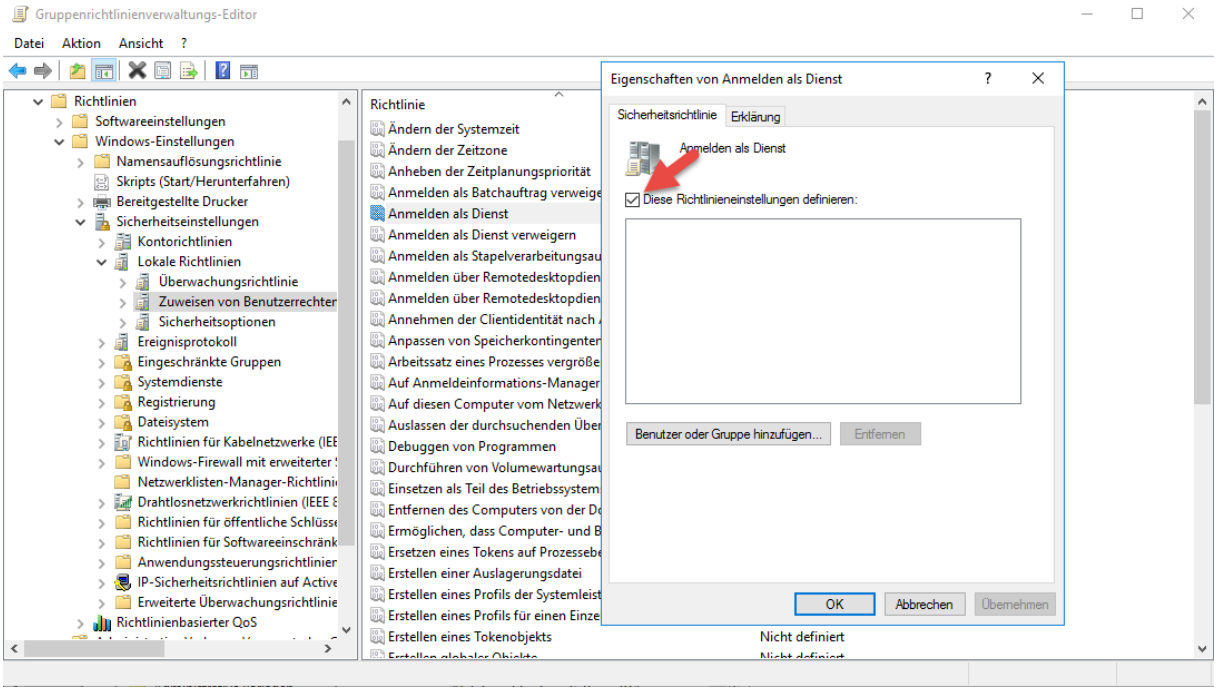
NTRIGHTS – Set Local Security

Wie hier zu sehen ist, werden die meisten Einstellungen über Gruppenrichtlinien gesteuert. Aus diesem Grund können auch keine weiteren Veränderungen vorgenommen werden.

Der Button ist ausgegraut, weil…

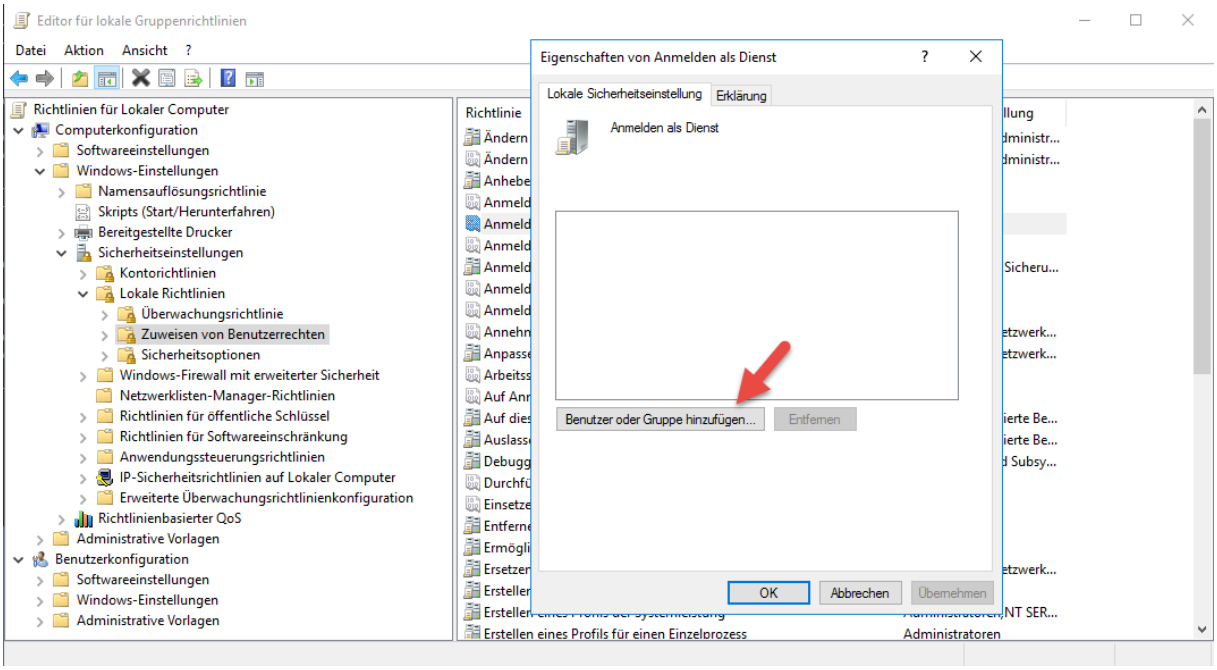


…die Richtlinie aktiviert ist.



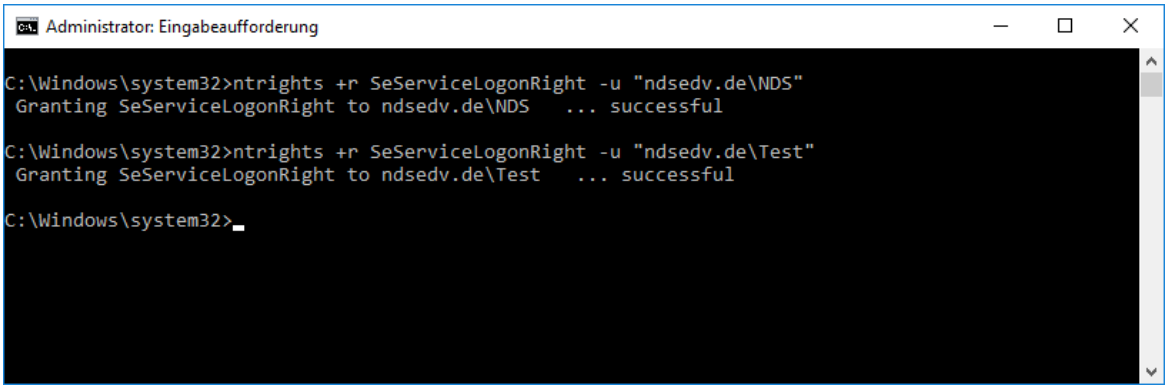
NTRIGHTS – Set Local Security

Deaktivieren wir diese wieder, ist ein Hinzufügen von Objekten wieder möglich.



Änderungen an den lokalen Sicherheitseinstellungen sind trotzdem möglich, auch dann wenn diese über eine Gruppenrichtlinie gesteuert werden. Dazu nutzen wir das Tool aus dem Ressource Kit 2003.

```
ntrights +r SeServiceLogonRight -u "ndsedv.de\NDS"
ntrights +r SeServiceLogonRight -u "ndsedv.de\Test"
```



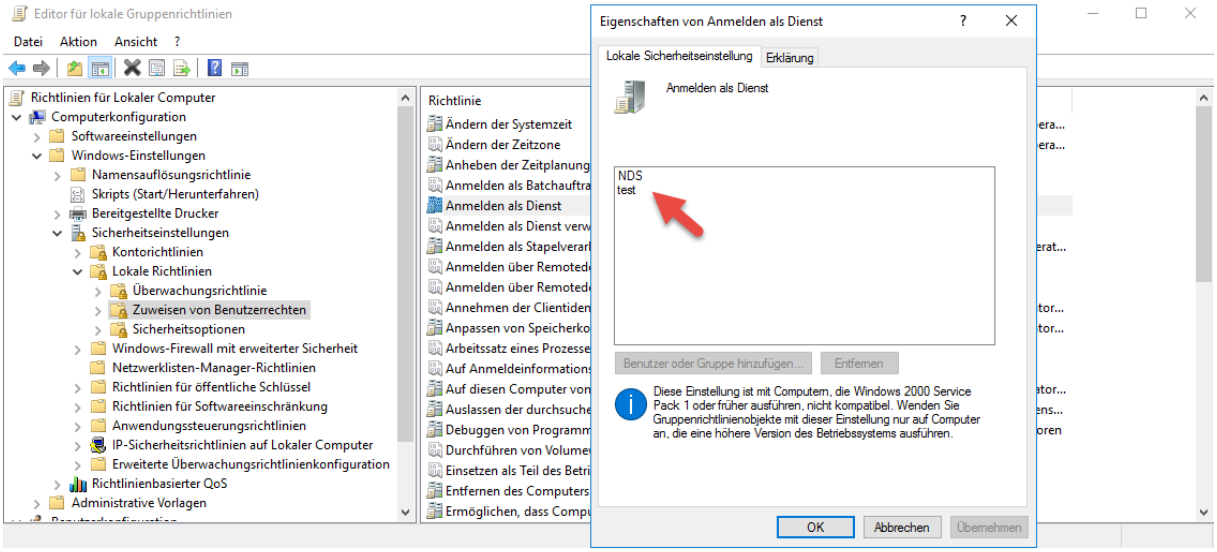
Syntax:

```
NTRIGHTS +r Right -u UserOrGroup [-m \\Computer] [-e Entry]
```

```
NTRIGHTS -r Right -u UserOrGroup [-m \\Computer] [-e Entry]
```

NTRIGHTS – Set Local Security

Der User NDS und Test wurden erfolgreich hinzugefügt:



NTRIGHTS – Set Local Security

Logon Privileges	**Constant Name**
Log on as a batch job	SeBatchLogonRight
Deny logon as a batch job	SeDenyBatchLogonRight
Log on locally	SeInteractiveLogonRight
Deny local logon	SeDenyInteractiveLogonRight
Logon as a service	SeServiceLogonRight
Deny logon as a service	SeDenyServiceLogonRight
Access this Computer from the Network	SeNetworkLogonRight
Deny Access to this computer via network	SeDenyNetworkLogonRight
Allow logon through RDP/Terminal Services	SeRemoteInteractiveLogonRight
Deny logon through RDP/Terminal Services	SeDenyRemoteInteractiveLogonRight
System Admin Privileges	**Constant Name**
Generate security audits	SeAuditPrivilege
Manage auditing and security log	SeSecurityPrivilege
Backup files and directories	SeBackupPrivilege
Add workstations to the domain	SeMachineAccountPrivilege
Shut down the system	SeShutdownPrivilege
Force shutdown from a remote system	SeRemoteShutdownPrivilege
Create a pagefile	SeCreatePagefilePrivilege
Increase quotas	SeIncreaseQuotaPrivilege
Restore files and directories	SeRestorePrivilege
Change the system time	SeSystemTimePrivilege
Take ownership of files/objects	SeTakeOwnershipPrivilege
Enable computer/user accountsto be trusted for delegati	SeEnableDelegationPrivilege
Remove computer from docking station	SeUndockPrivilege
Service Privileges	**Constant Name**
Create permanent shared objects	SeCreatePermanentPrivilege
Create a token object	SeCreateTokenPrivilege
Replace a process-level token	SeAssignPrimaryTokenPrivilege
Impersonate a client after authentication	SeImpersonatePrivilege
Increase scheduling priority	SeIncreaseBasePriorityPrivilege
Act as part of the operating system	SeTcbPrivilege
Profile a single process	SeProfileSingleProcessPrivilege
Load and unload device drivers	SeLoadDriverPrivilege
Lock pages in memory	SeLockMemoryPrivilege
Create global objects	SeCreateGlobalPrivilege
Misc Privileges	**Constant Name**
Debug programs	SeDebugPrivilege
Bypass traverse checking	SeChangeNotifyPrivilege
Synch directory service data	SeSyncAgentPrivilege
Edit firmware environment values	SeSystemEnvironmentPrivilege
Profile system performance	SeSystemProfilePrivilege

NTRIGHTS – Set Local Security

Das Ganze noch einmal mit entsprechender Verlinkung zu Microsoft:

Richtlinie	Feste Bezeichnung
Access Credential Manager as a trusted caller	SeTrustedCredManAccessPrivilege
Access this computer from the network	SeNetworkLogonRight
Act as part of the operating system	SeTcbPrivilege
Add workstations to domain	SeMachineAccountPrivilege
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege
Allow log on locally	SeInteractiveLogonRight
Allow log on through Remote Desktop Services	SeRemoteInteractiveLogonRight
Back up files and directories	SeBackupPrivilege
Bypass traverse checking	SeChangeNotifyPrivilege
Change the system time	SeSystemtimePrivilege
Change the time zone	SeTimeZonePrivilege
Create a pagefile	SeCreatePagefilePrivilege
Create a token object	SeCreateTokenPrivilege
Create global objects	SeCreateGlobalPrivilege
Create permanent shared objects	SeCreatePermanentPrivilege
Create symbolic links	SeCreateSymbolicLinkPrivilege
Debug programs	SeDebugPrivilege
Deny access to this computer from the network	SeDenyNetworkLogonRight
Deny log on as a batch job	SeDenyBatchLogonRight
Deny log on as a service	SeDenyServiceLogonRight
Deny log on locally	SeDenyInteractiveLogonRight
Deny log on through Remote Desktop Services	SeDenyRemoteInteractiveLogonRight
Enable computer and user accounts to be trusted for delegation	SeEnableDelegationPrivilege
Force shutdown from a remote system	SeRemoteShutdownPrivilege
Generate security audits	SeAuditPrivilege
Impersonate a client after authentication	SeImpersonatePrivilege
Increase a process working set	SeIncreaseWorkingSetPrivilege
Increase scheduling priority	SeIncreaseBasePriorityPrivilege
Load and unload device drivers	SeLoadDriverPrivilege
Lock pages in memory	SeLockMemoryPrivilege
Log on as a batch job	SeBatchLogonRight
Log on as a service	SeServiceLogonRight

NTRIGHTS – Set Local Security

Manage auditing and security log	SeSecurityPrivilege
Modify an object label	SeRelabelPrivilege
Modify firmware environment values	SeSystemEnvironmentPrivilege
Perform volume maintenance tasks	SeManageVolumePrivilege
Profile single process	SeProfileSingleProcessPrivilege
Profile system performance	SeSystemProfilePrivilege
Remove computer from docking station	SeUndockPrivilege
Replace a process level token	SeAssignPrimaryTokenPrivilege
Restore files and directories	SeRestorePrivilege
Shut down the system	SeShutdownPrivilege
Synchronize directory service data	SeSyncAgentPrivilege
Take ownership of files or other objects	SeTakeOwnershipPrivilege