Vorwort

Liebe Leserinnen, liebe Leser!

Datensicherheit ist ein absolutes „Muss“. Dies schuldet jede Daten verarbeitende Stelle den Menschen, deren Daten sie verarbeitet. Zum Schutz der informationellen Selbstbestimmung gehört es nicht nur, dass die gesetzlichen Befugnisnormen eingehalten werden, sondern auch, dass durch technische und organisatorische Sicherungen die Ziele der Integrität, Vertraulichkeit, Authentizität und Revisionssicherheit erreicht werden. Das schuldet jede Stelle sich selbst. Die Informationstechnik ist das Rückgrat jeder Behörde oder jeden Unternehmens. Deren Leistungsfähigkeit und Sicherheit und damit deren Produktivität hängen hiervon ab. Die Risiken des Datenklaus und der Datenvernichtung sind angesichts der zunehmenden Vernetzung der IT-Systeme hochaktuell.

Das Unabhängige Landeszentrum für den Datenschutz Schleswig-Holstein (ULD) verfolgt neben seinen Prüfungs- und Kontrollaufgaben das Ziel des präventiven Datenschutzes und der präventiven Datensicherheit. Prävention bedeutet Sensibilisierung, Beratung, Schulung und Audit. Wir wollen den Administratoren helfen, die verfügbaren Sicherheitsfunktionen der eingesetzten Systeme optimal zu nutzen. Hierzu fehlen oft die nötigen Kenntnisse. Mit unserer ***backUP***-Serie möchten wir spezielles Wissen vermitteln, wie Sicherheitsmaßnahmen richtig ein- und umgesetzt werden können. Die in Betriebssystemen vorgesehenen Sicherheitsfunktionen müssen, damit sie wirksam werden können, verstanden, implementiert, gepflegt und nachhaltig dokumentiert werden.

Microsoft hat in seinen Betriebssystemen Windows Server 2000 und 2003 neue Sicherheitsfunktionen mit den Gruppenrichtlinien bereitgestellt, die den Administratoren sehr viel Gestaltungsspielraum für die Absicherung ihrer Systeme bieten. Leider ist es aber Microsoft nicht gelungen, die Gruppenrichtlinien überschaubar und leicht anwendbar zu gestalten, sodass es viele Administratoren aufgeben, sich mit ihnen zu beschäftigen.

Das vorliegende ***backUP***-Magazin soll dieses Defizit beheben und die Administratoren unterstützen, sich dem Thema Gruppenrichtlinien zu nähern. Es soll insbesondere aufzeigen, welche administrativen Schritte notwendig sind, um die Gruppenrichtlinien in ihrer Gesamtheit einfach und schnell einsetzen zu können.

Die ***backUP***-Magazine sind eine Serviceleistung des Unabhängigen Landeszentrums für Datenschutz. Sie werden ergänzt und abgerundet durch die Spezialkurse der DATENSCHUTZAKADEMIE Schleswig-Holstein. Ich würde mich über Kritik und Anregungen zur Optimierung unserer ***backUP***-Magazine freuen und wünsche Ihnen viel Spaß und Erfolg bei der Verbesserung der Sicherheit Ihres Betriebssystems.

Kiel, im November 2006

Dr. Thilo Weichert

Landesbeauftragter für den Datenschutz

Inhaltsverzeichnis

1 Grundlagen

In diesem Kapitel erfahren Sie,

- wie das ***backUP***-Magazin zu benutzen ist,
- welche Voraussetzungen für den Einsatz der Gruppenrichtlinien erfüllt sein müssen,
- welche Bedeutung die Gruppenrichtlinien haben und
- welche Schwerpunktthemen in den einzelnen Kapiteln behandelt werden.

1.1 Einleitung

Die Praxis und die Ergebnisse der Fortbildungsveranstaltungen der DATENSCHUTZAKADEMIE[1] haben gezeigt, dass das Verständnis für den richtigen Umgang mit den Gruppenrichtlinienobjekten eine tiefgehende Hilfestellung verlangt. Microsoft hat dieses Instrument mit der Einführung des Betriebssystems Windows 2003 und der *Group Policy Management Console* (GPMC) weiterentwickelt, sodass in diesem ***backUP-***Magazin der Schwerpunkt auf die neuen Funktionen der Gruppenrichtlinien gelegt wird.

*Wir haben das Thema **„Windows Gruppenrichtlinien – Planen und effektiv anwenden“** in die Reihe der **backUP-**Magazine[2] aufgenommen, um den Administratoren einen umfassenden Einblick in die Administration der Gruppenrichtlinien unter Windows 2000/2003 zu verschaffen.*

Gedanken...gut!?

[1] Das Kursangebot ist im Jahresprogramm der DATENSCHUTZAKADEMIE Schleswig-Holstein abgedruckt und beim ULD erhältlich. Näheres unter <www.datenschutzzentrum.de/akademie/>.

[2] ***backUP*** Nr. 1: IT-Sicherheitskonzepte: Planung – Erstellung – Umsetzung
backUP Nr. 2: MS-Windows NT 4.0 – Sicherheitsmaßnahmen und Restrisiken
backUP Nr. 3: MS-Windows NT 4.0 – Resource Kit und Security-Tools
backUP Nr. 4: PC-Arbeitsplatz – So viel Datenschutz muss an jedem Arbeitsplatz sein!
backUP Nr. 5: MS-Windows 2000 – Sicherheitsmaßnahmen und Restrisiken
backUP Nr. 6: Windows Gruppenrichtlinien – Planen und effektiv anwenden

1.2 Hinweise für die Benutzung dieses *backUP*-Magazins

Dieses ***backUP***-Magazin soll als ein praktischer Ratgeber den IT-Betreuern die Arbeit mit den Windows 2000/2003 Gruppenrichtlinien erleichtern. Es werden nur die Funktionen ausführlich beschrieben, die die Sicherheitsaspekte für den Einsatz der IT-Systeme betreffen und eine effektive, wirtschaftliche, zentrale Verwaltung einer Vielzahl von IT-Systemen erlauben. Für eine weiterführende Administration sollten die im Anhang aufgelisteten Fachbücher und Web-Seiten oder die Windows 2000/2003-Hilfe zusätzlich herangezogen werden.

Es werden folgende Schreibweisen verwendet, um Schaltflächen, Befehle und Definitionen unterscheiden zu können:

- **Schaltflächen**, Verzeichnisnamen, Registerkarten usw. werden, wie bei HINZUFÜGEN, in Kapitälchen gesetzt.
- **Befehle**, wie `gpupdate /force`, werden in nicht proportionaler Schrift gesetzt.
- **Eigennamen**, wie *gpedit.msc,* werden kursiv dargestellt.
- **Internetadressen**, wie <www.gruppenrichtlinien.de>, und Verzeichnispfade, wie <E:\I386\Winnt32>, werden in eckige Klammern gesetzt.

Zur Verbesserung der Orientierung ist der Text in Funktionsabschnitte gegliedert, die durch entsprechende Symbole gekennzeichnet sind. Folgende Symbole finden Verwendung:

Weist auf Inhalte hin, die bei der Planung von Aufgaben nützlich sein können. Eine so gekennzeichnete Vorgehensweise sollte mit der Leitungsebene abgestimmt werden.

Kennzeichnet Hinweise, die für die Umsetzung von Sicherheitsmaßnahmen von entscheidender Bedeutung sind. Die beschriebenen Empfehlungen sollten in jedem Fall beachtet werden.

Achtung! Hier ist bei administrativen Maßnahmen Vorsicht geboten!

Die beschriebenen Sachverhalte sollten unbedingt überprüft und die dargestellten Sicherungsvorkehrungen oder Administrationshilfen beachtet werden.

Beschreibt im Detail die Arbeitsschritte, die für die Umsetzung einer Sicherheitsmaßnahme oder für die Einstellung einer technischen Funktion notwendig sind.

Beschreibt zusammenfassend in einer Checkliste die Sicherheitsmaßnahmen und die Informationen, die beim Einsatz von Windows 2000/2003 berücksichtigt werden sollten.

1.3 Systemtechnische Voraussetzungen

In der Netzwerkumgebung muss sich ein Windows 2000/2003 Domänen Controller mit einem Active Directory befinden, der die Benutzerkonten für die Authentifizierung am PC/Client verwaltet. Darüber hinaus ist zu beachten, dass das Active Directory so strukturiert wird, dass die Gruppenrichtlinien effektiv eingesetzt werden können. Nähere Einzelheiten zur Konfiguration eines Windows 2000/2003 Domänen Controllers und zum Design des Active Directory sind im ***backUP-***Magazin Nr. 5 **„**Windows 2000 Sicherheitsmaßnahmen und Restrisiken“ dargestellt.

Die Gruppenrichtlinien werden üblicherweise auf Windows 2000 Professional oder Windows XP Clients eingesetzt. Dabei ist zwischen den *Lokalen Richtlinien* und den Active Directory Gruppenrichtlinien zu unterscheiden, worauf im Folgenden noch näher eingegangen wird. Befinden sich in der Netzwerkumgebung Windows NT 4.0 oder sogar Windows 9x Clients, können die unter Windows NT 4.0 vorhandenen Systemrichtlinien auf dem Windows 2000/2003 Domänencontroller eingesetzt werden. Auch hierzu werden nachfolgend einige Hinweise gegeben. Ausschlaggebend für den Einsatz der Richtlinien ist das Betriebssystem auf dem Domänencontroller, wie sich aus der nachfolgenden Tabelle ergibt.

Domänencontroller	**Client**	**Richtlinien**
Windows NT 4.0 PDC	Windows 9x Windows NT 4.0 Workstation	Windows NT 4.0 Systemrichtlinien (poledit)
Windows 2000/2003 DC	Windows 9x Windows NT 4.0 Workstation	Windows NT 4.0 Systemrichtlinien (poledit)
Windows 2000/2003 DC	Windows 2000 Professional Windows XP	Lokale und Active Directory Gruppenrichtlinien

Über den DNS-Server findet der PC/Client Verweise auf die für das Active Directory notwendigen Dienste. Damit die Active Directory-Gruppenrichtlinien umgesetzt werden, ist es erforderlich, dass der DNS-Server unter den TCP/IP Einstellungen des Clients eingetragen wird. Fehlt die IP-Adresse des DNS Servers, werden die Active Directory-Gruppenrichtlinien nicht übernommen. Es treten darüber hinaus Probleme bei der Namensauflösung auf.

Vor dem Einsatz von Gruppenrichtlinien sollten Sie sich detailliert mit dem theoretischen Hintergrundwissen beschäftigen. Ihre ersten Schritte beim Einsatz von Gruppenrichtlinien sollten Sie in einer Übungsumgebung durchführen, die aus einem Domänencontroller und einem Client besteht. Auch bei größeren Änderungen im späteren Betrieb sollten Sie über eine dedizierte Testumgebung verfügen, um wesentliche Veränderungen an Ihrer IT-Infrastruktur testen und freigeben (lassen) zu können.

1.4 Die Bedeutung von Gruppenrichtlinien

Systemadministratoren komplexer IT-Systeme stehen vor einem elementaren Problem: Aktuelle Betriebssysteme bieten viele Einstellungsmöglichkeiten in Bezug auf Datenschutz und Datensicherheit. Ein manuelles Konfigurieren aller Einstellungen ist bei der üblicherweise hohen Anzahl an Arbeitsplatz- oder Server-Systemen weder wirtschaftlich noch praktikabel. Darüber hinaus schleichen sich bei einer solchen „Turnschuh"-Administration (das Laufen von Rechner zu Rechner) Fehler ein. Jegliche kleine Änderung sorgt sofort für ungleich höheren Aufwand.

Leider liefert Microsoft weder Server- noch Client-Betriebssysteme mit einer Standardkonfiguration aus, in der sämtliche Zusatzfunktionen für normale Anwender zunächst deaktiviert sind und erst durch die Systemverwalter aktiviert werden müssen. Komfort und universelle Anwendbarkeit wurden hier gegenüber Datensicherheit und Datenschutz höher bewertet. Für die aktuellen Betriebssysteme gilt deshalb leider immer noch, dass eine Standardinstallation weder sicher noch datenschutzkonform ist. So haben beispielsweise einfache Benutzer bei Standardinstallationen zu viele Möglichkeiten, administrativ in das System einzugreifen.

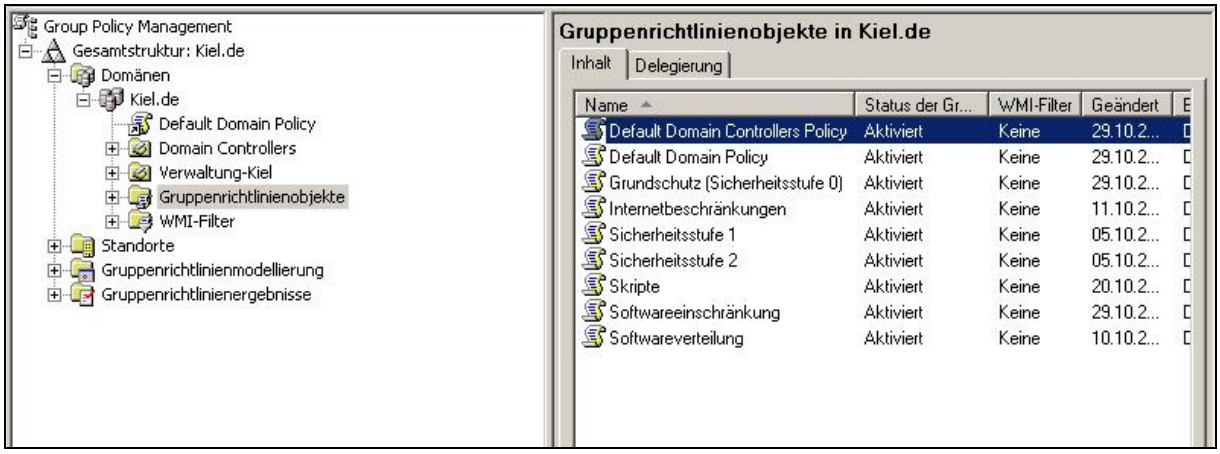
Microsoft hat mit dem Active Directory einen Verzeichnisdienst eingeführt, in dem die komplette IT-Infrastruktur einer Organisation abgebildet werden kann. In diesem Verzeichnisdienst gibt es für das zentrale Durchführen und Rücknehmen von administrativen Einstellungen einen neuen Mechanismus: die Gruppenrichtlinie (häufig auch Group-Policy, Group-Policy-Object oder GPO genannt).

Über Gruppenrichtlinien konfigurierte Einstellungen steuern Funktionen des Betriebssystems und teilweise auch das Verhalten einzelner Anwendungen. So lassen sich beispielsweise Einstellungen wie die Sichtbarkeit einzelner Menüpunkte in Microsoft Windows ebenso zentral vorgeben wie ein zentrales Verzeichnis für Dokumentvorlagen in Microsoft Word. Zusätzlich kann ein Systemverwalter beispielsweise auch die Installation von Softwarepaketen veranlassen.

Über den Gruppenrichtlinienobjekt-Editor lassen sich Einstellungen zentral verwalten, sodass direkte administrative Zugriffe auf die jeweiligen Rechner im lokalen Netz nicht notwendig sind.

Active Directory-Gruppenrichtlinie *Default Domain Policy*

Mit der *Group Policy Management Console* können Gruppenrichtlinien deutlich einfacher verwaltet werden.



Group Policy Management Console

Dieses ***backUP***-Magazin soll Ihnen helfen, von den ersten Schritten mit Gruppenrichtlinien bis zu ausgefeilten Szenarien die volle Bandbreite dieses mächtigen administrativen Werkzeugs zu nutzen.

Im folgenden **Kapitel 2** werden Sie grundlegende Informationen über den Aufbau und die Wirkungsweise von Gruppenrichtlinien finden. Wir erläutern Ihnen, welche administrativen Werkzeuge für die Arbeit mit Gruppenrichtlinien hilfreich sind und wie Sie mit diesen Hilfsmitteln effektiv arbeiten. Auch Lesern mit grundlegenden Kenntnissen von Gruppenrichtlinien empfehlen wir, dieses Kapitel zum Einstieg nochmals „querzulesen". Es enthält Details, die das Verständnis der nachfolgenden Kapitel erleichtern.

Sobald Sie Ihre ersten Erfahrungen mit Gruppenrichtlinien gemacht haben, werden Sie erkennen, dass gerade beim Zusammenspiel mehrerer Gruppenrichtlinien viel zu beachten ist. **Kapitel 3** erläutert Ihnen deswegen einfach und verständlich das „Wie" und „Wann" der Verarbeitung von Gruppenrichtlinien und gibt Ratschläge, die Ihnen bei der Fehlersuche helfen.

Die Arbeit mit Gruppenrichtlinien kann schnell unübersichtlich werden, wenn Sie das zugrundeliegende Active Directory nicht strukturieren. **Kapitel 4** zeigt Ihnen Mittel und Wege auf, wie Sie Ihr Active Directory gestalten sollten, damit Sie Gruppenrichtlinien effektiv einsetzen und nutzen können.

In **Kapitel 5** erhalten Sie mit dem Wissen und den Ratschlägen der vorherigen Kapitel dann weitere Hilfestellungen und lernen einzelne Funktionalitäten kennen, die es Ihnen ermöglichen, die volle Leistungsfähigkeit von Gruppenrichtlinien zu nutzen. Unter anderem lernen Sie, wie Sie mit Verknüpfungen die Übersicht behalten und durch Veränderung der Vererbung und zusätzlichem Filtern die Anwendung von Gruppenrichtlinien gezielter steuern können.

Kapitel 6 erklärt Ihnen dann, wo Sie die Funktionalitäten, die sie in Kapitel 5 kennen gelernt haben, im standardmäßig vorhandenen Verwaltungsprogramm für Gruppenrichtlinien wiederfinden.

Im **Kapitel 7** werden alle Funktionalitäten, die der Gruppenrichtlinienobjekt-Editor zur Verfügung stellt, zusammengefasst. Weiterhin werden die Möglichkeiten erläutert, wie Sie in diesem Editor die Ansicht filtern oder Richtlinien finden können.

Ihr in den vorherigen Kapiteln erworbenes Verständnis zu Gruppenrichtlinien können Sie dann in **Kapitel 8** anwenden. Hier erhalten Sie einen Überblick, welche Aspekte Sie im Bereich der Softwareverteilung und der Sicherheitseinstellungen über Gruppenrichtlinien steuern können.

Kapitel 9 erläutert aufbauend auf die vorherigen Kapitel den strukturellen Aufbau der administrativen Vorlagen und den Umgang mit Vorlagendateien.

Als Zusammenfassung und Verdeutlichung zeigen wir Ihnen in **Kapitel 10** anhand eines größeren Beispiels, wie Gruppenrichtlinien geplant und effektiv eingesetzt werden können.

Das **Kapitel 11** stellt Ihnen ergänzende Programme zur Unterstützung der täglichen administrativen Arbeit vor.

Im **Anhang** finden Sie dann Verweise auf Literatur, Downloadseiten und weiterführende Informationen.

2 Aufbau der Gruppenrichtlinien

In diesem Kapitel erfahren Sie,

- wie die Gruppenrichtlinien strukturell aufgebaut sind,
- welche Gruppenrichtlinien es gibt,
- welche Standard-Gruppenrichtlinien implementiert werden,
- welche Besonderheiten für die einzelnen Gruppenrichtlinien gelten und
- welche Bedeutung NT-Systemrichtlinien in einer Windows 2000/2003-Domäne haben.

2.1 Gruppenrichtlinien systematisch anwenden

Das Thema Gruppenrichtlinien wird in der Fachliteratur in Bezug auf die Beschreibung von einzelnen Richtlinien und den vielfältigen Administrationsmöglichkeiten ausführlich behandelt. Aber eine theoretische und vor allem praktische Auseinandersetzung mit

- der Struktur und dem Aufbau der Gruppenrichtlinien,
- der Wirksamkeit der einzelnen Gruppenrichtlinien auf unterschiedlichen Ebenen und den zahlreichen Ausnahmen,
- dem Zusammenhang der Active Directory-Struktur mit dem Einsatz der Gruppenrichtlinien und
- der systematischen Erarbeitung eines Konzeptes zum Einsatz der Gruppenrichtlinien

findet in den meisten Fällen nicht oder nur teilweise statt. Dem Systemadministrator fehlen in diesem Fall die Zusammenhänge, um die Gruppenrichtlinien systematisch planen und umsetzen zu können.

„Testen" Sie auf keinen Fall auf den Produktionsmaschinen, sondern immer erst in einer Testumgebung bestehend aus einem Client und einem Domänencontroller. Führen Sie vor dem „Test" mit den Gruppenrichtlinien unbedingt eine Datensicherung der Systemstatusdateien durch. Die Durchführung der Sicherung wird im ***backUP****-Magazin Nr. 5 beschrieben.*

Sie sollten die Grundlagen zu dem Thema Gruppenrichtlinien nicht nur theoretisch erarbeiten. Viele Zusammenhänge werden erst während der praktischen Umsetzung deutlich.

2.2 Einleitende Hinweise

In den ersten Kapiteln werden die Grundlagen der Gruppenrichtlinien dargestellt. Zur Darstellung der Theorie, der Abbildungen und der praktischen Beispiele werden zuerst

- die Standardkonfigurationen der Betriebssysteme (Windows Server 2003 Enterprise Edition als Serverbetriebssystem und Windows XP SP2 als Clientbetriebssystem),
- eine einfache Active Directory-Konfiguration (eine „Mini"-Domäne Kiel.de mit einer Organisationseinheit) und
- keine zusätzlichen Verwaltungswerkzeuge (z. B. die Gruppenrichtlinien-Verwaltungskonsole) und Tools

verwendet. So können zunächst die standardmäßigen und grundlegenden Funktionalitäten erklärt werden, bevor in den folgenden Kapiteln nach und nach

- das Active Directory für den Einsatz der Gruppenrichtlinien erweitert wird,
- die Gruppenrichtlinien-Verwaltungskonsole zum Einsatz kommt und
- zusätzliche Verwaltungsmöglichkeiten vorgestellt werden.

2.3 Struktureller Aufbau

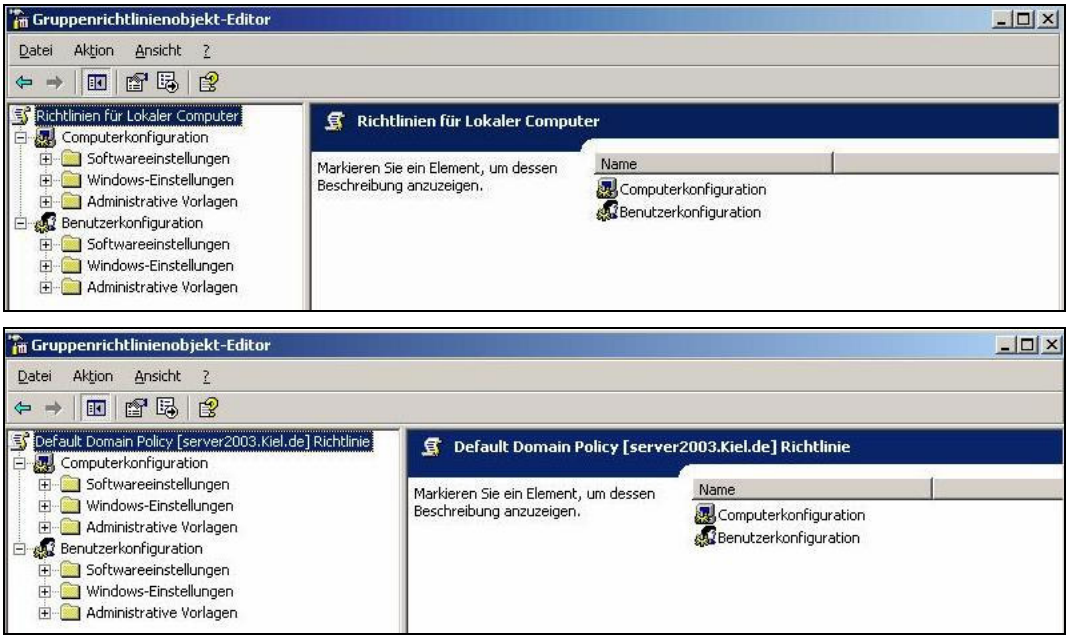
Wie die Bezeichnung Gruppenrichtlinien schon vermuten lässt, gibt es nicht nur eine Gruppenrichtlinie. Sowohl bei der Installation von Servern und Clients ab Windows 2000 als auch bei der Einrichtung des Active Directory werden standardmäßig mehrere Gruppenrichtlinien implementiert. Des Weiteren können auf unterschiedlichen Ebenen zusätzliche Gruppenrichtlinien eingerichtet bzw. verknüpft werden. Diese Richtlinien unterscheiden sich in Bezug auf den Einsatz, die Gültigkeit und Verwaltung zum Teil erheblich. Dennoch sind alle Gruppenrichtlinien gleich strukturiert und die Besonderheiten in der Wirksamkeit einzelner Richtlinien werden nicht gekennzeichnet. Auf diese Besonderheiten wird in den entsprechenden Kapiteln dieses ***backUP***-Magazins hingewiesen.

Sämtliche Gruppenrichtlinien werden im Gruppenrichtlinienobjekt-Editor bearbeitet und zeigen den gleichen strukturellen Aufbau:

- Jede Gruppenrichtlinie ist in die Knoten COMPUTERKONFIGURATION und BENUTZERKONFIGURATION unterteilt, die sich jeweils in die Knoten SOFTWARE-EINSTELLUNGEN, WINDOWS-EINSTELLUNGEN und ADMINISTRATIVE VORLAGEN untergliedern (siehe folgende Abbildung).
- Unterhalb dieser Struktur finden sich die einzelnen Richtlinien bzw. weitere Unterstrukturen, die die enthaltenen Richtlinien thematisch sortieren.

Diese Struktur ist für alle Gruppenrichtlinien einheitlich vorgegeben.

Eine Gruppenrichtlinie lässt sich anhand des strukturellen Aufbaus nicht von anderen unterscheiden. Nur die Titelzeile im Gruppenrichtlinienobjekt-Editor gibt den Hinweis darauf, um welche Gruppenrichtlinie es sich handelt:



Struktureller Aufbau der Gruppenrichtlinien

In Hinblick auf den Einsatz, die Gültigkeit und Verwaltung kann zwischen zwei Arten von Gruppenrichtlinien unterschieden werden:

- *Lokale Gruppenrichtlinien* und
- Active Directory-Gruppenrichtlinien.

Beide Arten werden in den nachfolgenden Kapiteln näher beschrieben.

*In den Abbildungen oben sind die beiden Gruppenrichtlinien **Lokaler Computer** und **Default Domain Policy** geöffnet.*

Während Ihrer administrativen Arbeit können Sie nur anhand der Titelzeile im Gruppenrichtlinienobjekt-Editor erkennen, welche Gruppenrichtlinie Sie gerade bearbeiten. Das birgt die Gefahr, dass Sie ungewollt Einstellungen in einer „falschen" Gruppenrichtlinie vornehmen und Sie sich im schlimmsten Falle als Administrator ausschließen.

Achten Sie daher bei der Konfiguration einer Gruppenrichtlinie darauf, dass Sie sich in der „richtigen" Gruppenrichtlinie befinden.

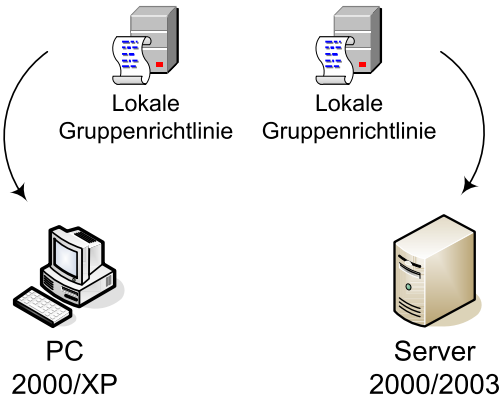
*Gruppenrichtlinien wirken **nicht**, wie der Name das vermuten lassen würde, auf Gruppenkonten.*

Alle Einstellungen, die in dem Knoten COMPUTERKONFIGURATION vorgenommen werden, finden auf alle Computerkonten Anwendung, auf die die entsprechende Gruppenrichtlinie wirkt (Lokal, Standort, Domäne oder Organisationseinheit).

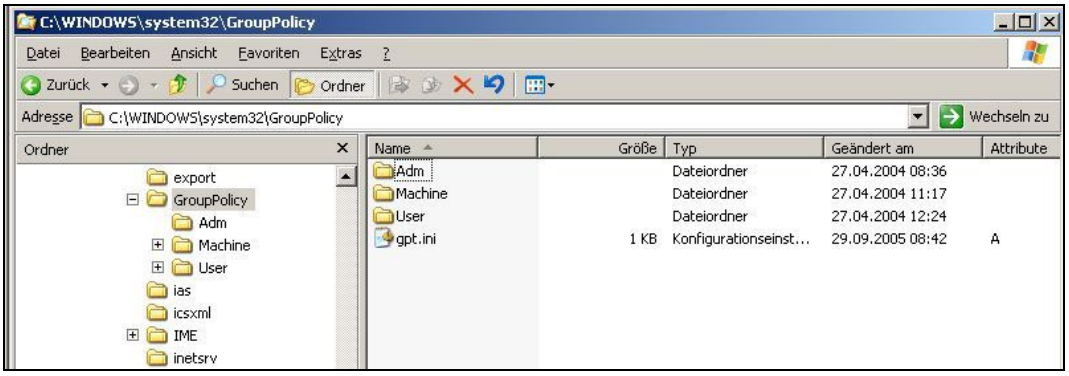
Alle Einstellungen, die in dem Knoten BENUTZERKONFIGURATION vorgenommen werden, finden auf alle Benutzerkonten Anwendung, auf die die entsprechende Gruppenrichtlinie wirkt (Lokal, Standort, Domäne oder Organisationseinheit).

2.4 Lokale Gruppenrichtlinien

Grundsätzlich wird bei der Installation jedes Server- oder Clientbetriebssystems ab Windows 2000 eine lokale Gruppenrichtlinie implementiert, die mit ihren Standardeinstellungen eine gewisse Grundsicherheit gewährleisten soll.



Diese Richtlinie wird im Dateisystem im Verzeichnis <Stammverzeichnis:\Windows\System32\GroupPolicy> gespeichert und unterteilt sich in die Unterverzeichnisse ADM, MACHINE und USER.

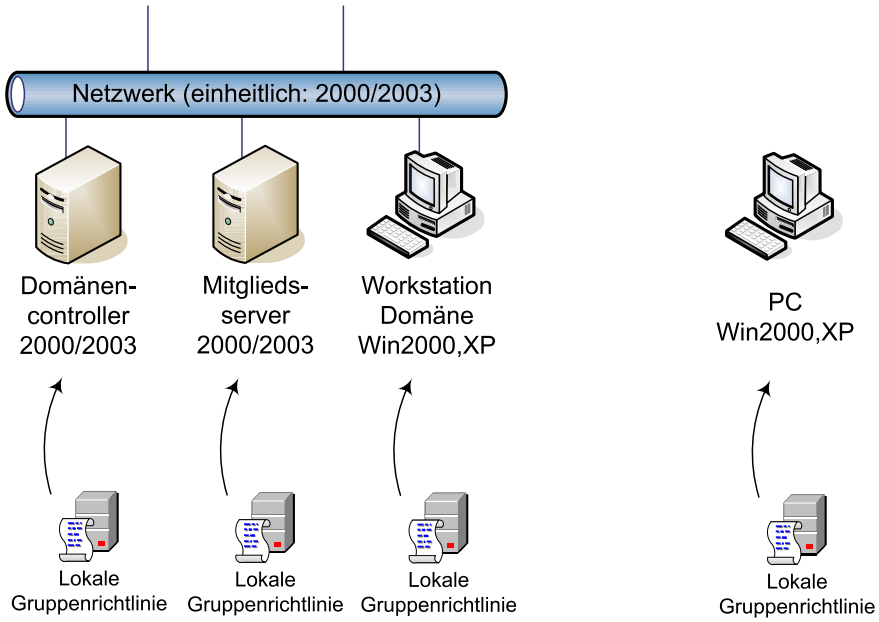


Speicherort der lokalen Richtlinie

Die *Lokale Gruppenrichtlinie* kann einzelnen Benutzerkonten nicht explizit zugewiesen werden. Alle Einstellungen, die in der lokalen Gruppenrichtlinie

- im Knoten COMPUTERKONFIGURATION vorgenommen werden, wirken standardmäßig auf das lokale Computerkonto und
- im Knoten BENUTZERKONFIGURATION vorgenommen wurden, wirken standardmäßig auf alle Benutzerkonten eines lokalen Computers,

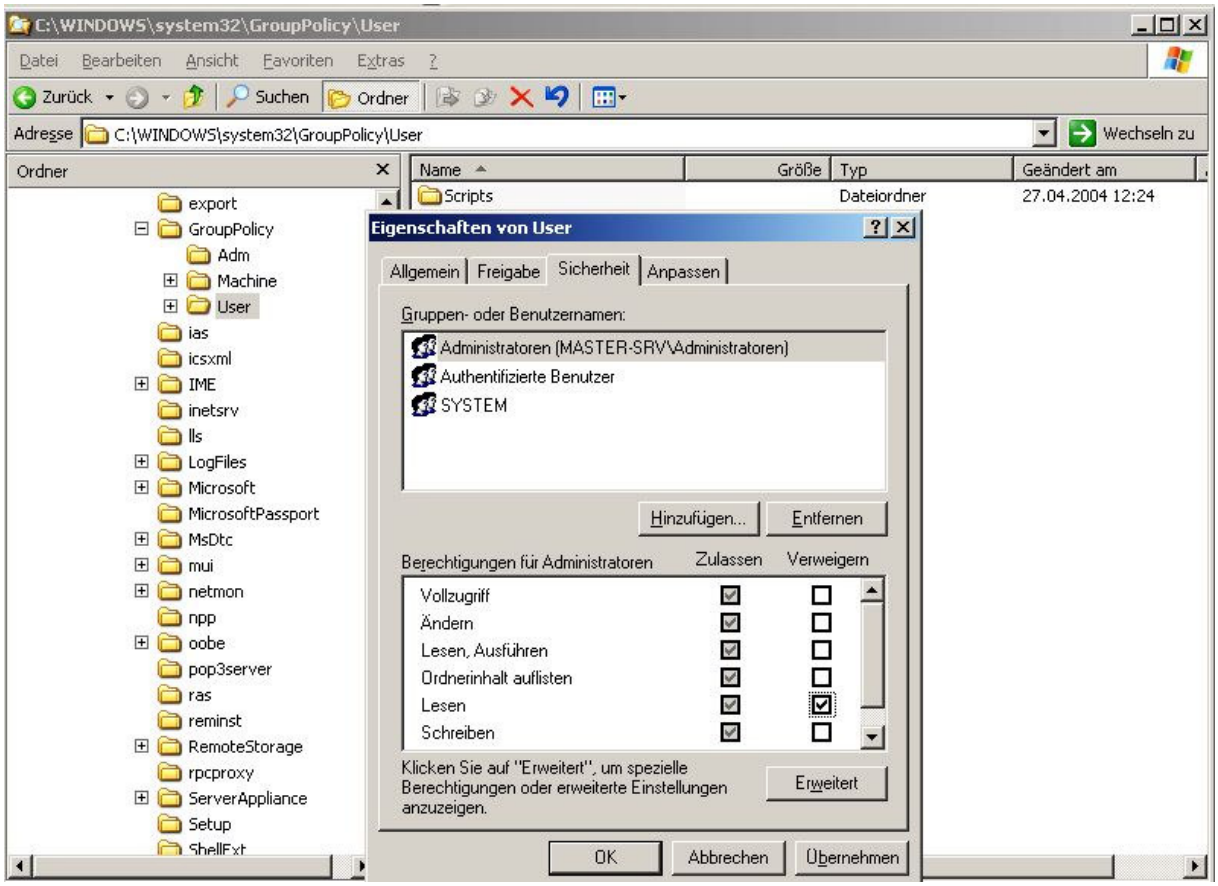
unabhängig davon, ob es sich um einen alleinstehenden Computer handelt oder ob er in einer Domäne als Domänencontroller, Mitgliedsserver oder Client konfiguriert ist.



*Die lokale Gruppenrichtlinie wirkt auf **alle** Benutzerkonten, davon betroffen ist auch das Administratorkonto! Das kann im ungünstigsten Fall dazu führen, dass Sie als Administrator keinen Zugriff mehr auf das System erhalten.*

*Um zu verhindern, dass die **Lokalen Richtlinien** auf den Administrator wirken, können Sie der Administratorgruppe den lesenden Zugriff auf das Verzeichnis MACHINE oder USER verweigern (siehe folgende Abbildung), je nachdem, ob Sie Einstellungen in der Computer- oder Benutzerverwaltung vorgenommen haben.*

Nachdem dem Administrator das lesende Recht verweigert wurde, kann er keine Einstellungen mehr an der Lokalen Richtlinie vornehmen. Soll er die Lokale Richtlinie bearbeiten, muss ihm das Recht kurzfristig wieder erteilt werden.



Rechtevergabe auf die lokale Gruppenrichtlinie

Die *Lokale Gruppenrichtlinie* kann mit dem Gruppenrichtlinienobjekt-Editor bearbeitet werden, der sich auf zwei unterschiedliche Arten aufrufen lässt:

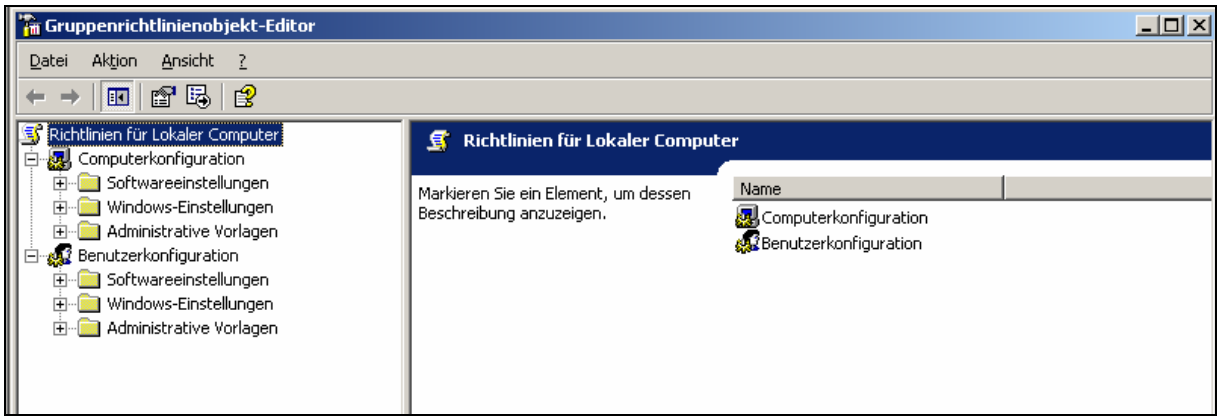
Erstellen einer Managementkonsole für die lokale Sicherheitsrichtlinie im Startmenü

1. *Wählen Sie START-AUSFÜHREN, geben den Befehl* `mmc` *ein und bestätigen Sie mit OK.*
2. *Wählen Sie DATEI und SNAP-IN HINZUFÜGEN/ENTFERNEN und betätigen danach die Schaltfläche HINZUFÜGEN.*
3. *Die verfügbaren Snap-Ins werden angezeigt. Wählen Sie GRUPPENRICHTLINIENEDITOR-OBJEKT (SERVER UND DOMÄNENCONTROLLER) oder GRUPPENRICHTLINIE (CLIENT) und bestätigen Sie das Snap-In für den lokalen Computer.*

4. *Schließen Sie die Auswahlliste und bestätigen Sie Ihre Auswahl mit OK. In dem importierten Gruppenrichtlinienobjekt-Editor können Sie nun die lokalen Richtlinien bearbeiten.*
5. *Wählen Sie DATEI-SPEICHERN UNTER und vergeben Sie Ihrer erstellten Managementkonsole einen aussagekräftigen Namen. Sie können sie danach über START-PROGRAMME-VERWALTUNG aufrufen.*

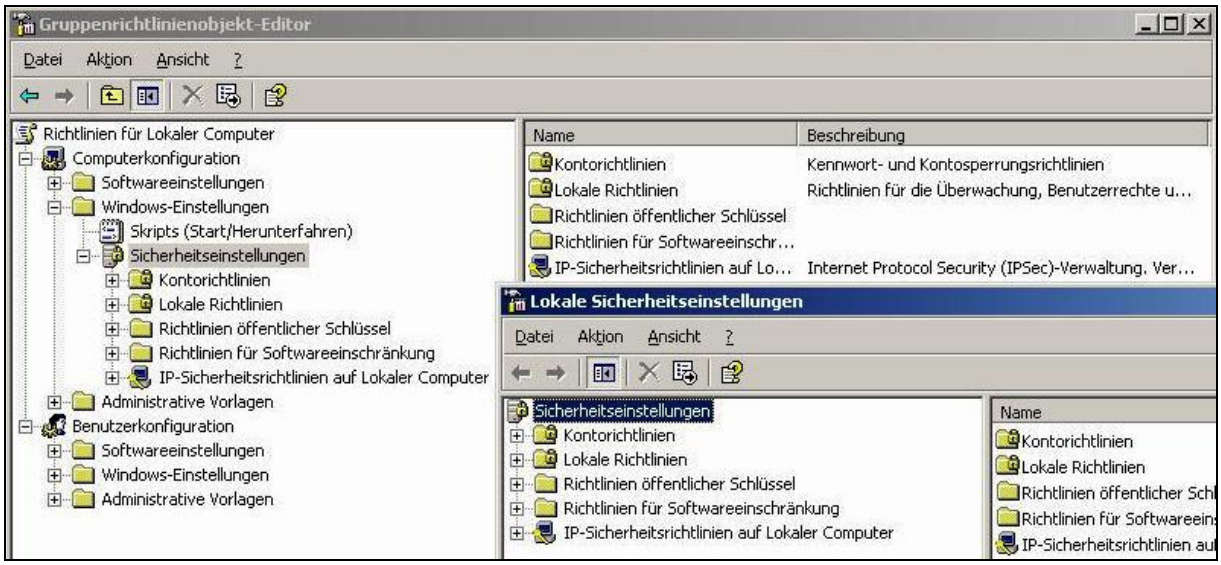
Aufrufen der lokalen Gruppenrichtlinie über Ausführen

1. *Wählen Sie START-AUSFÜHREN.*
2. *Geben Sie* `gpedit.msc` *ein, es öffnet sich der Gruppenrichtlinienobjekt-Editor.*



Lokale Gruppenrichtlinie (gpedit.msc)

Die im Startmenüpunkt VERWALTUNG (SERVER UND DOMÄNENCONTROLLER) bzw. unter SYSTEMSTEUERUNG-VERWALTUNG (CLIENTS) aufgeführten LOKALEN SICHERHEITSRICHTLINIEN zeigen einen Ausschnitt der gesamten lokalen Gruppenrichtrichtlinie. Sie berücksichtigen nur, wie unten abgebildet, die Richtlinien im Knoten COMPUTERKONFIGURATION-SICHERHEITSEINSTELLUNGEN.



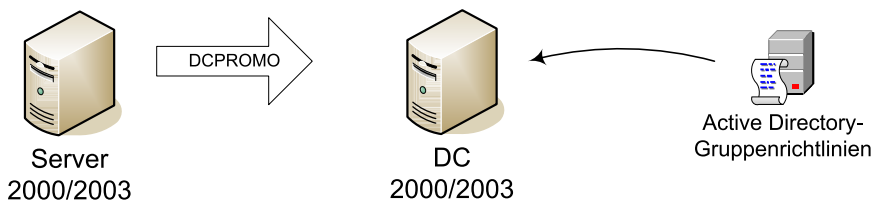
Lokale Sicherheitsrichtlinien

Da die Einstellungen in den *Lokalen Gruppenrichtlinien* standardmäßig auf alle lokalen Benutzerkonten wirken und sie von Active Directory-Gruppenrichtlinien überschrieben werden können (siehe Kapitel 3.2), beschränkt sich das Einsatzgebiet der *Lokalen Gruppenrichtlinie* auf Computer, die nicht Mitglied einer Domäne sind oder als Einzelplatz-PC eingesetzt werden.

Ist der Computer Mitglied in einer Domäne, sollten in der lokalen Richtlinie der Domänenmitglieder (Domänencontroller, Mitgliedsserver und Clients) keine weiteren Einstellungen vorgenommen werden.

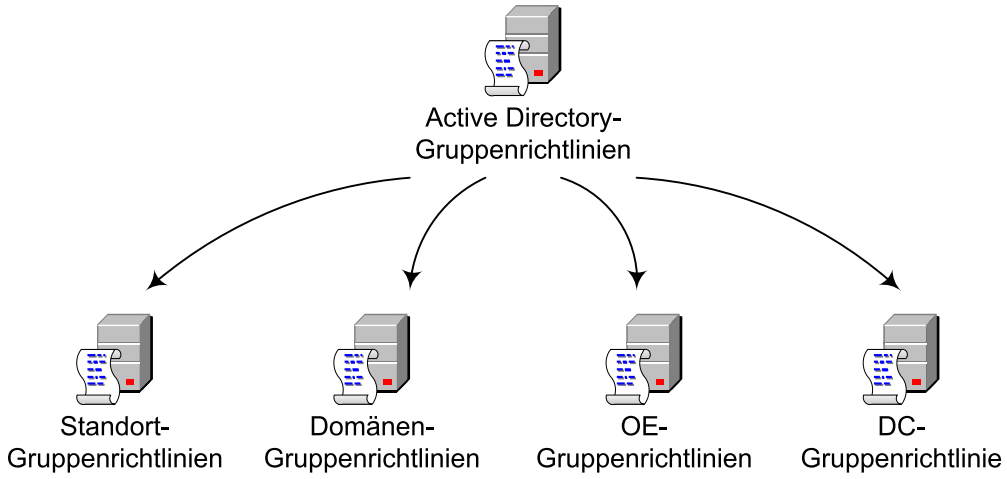
2.5 Active Directory-Gruppenrichtlinien

Die Active Directory-Gruppenrichtlinien sind Bestandteil einer Active Directory-Domäne. Sie werden in dem Moment in das Active Directory implementiert, in dem ein Server zu einem Domänencontroller heraufgestuft und eine neue Domäne erstellt wird.

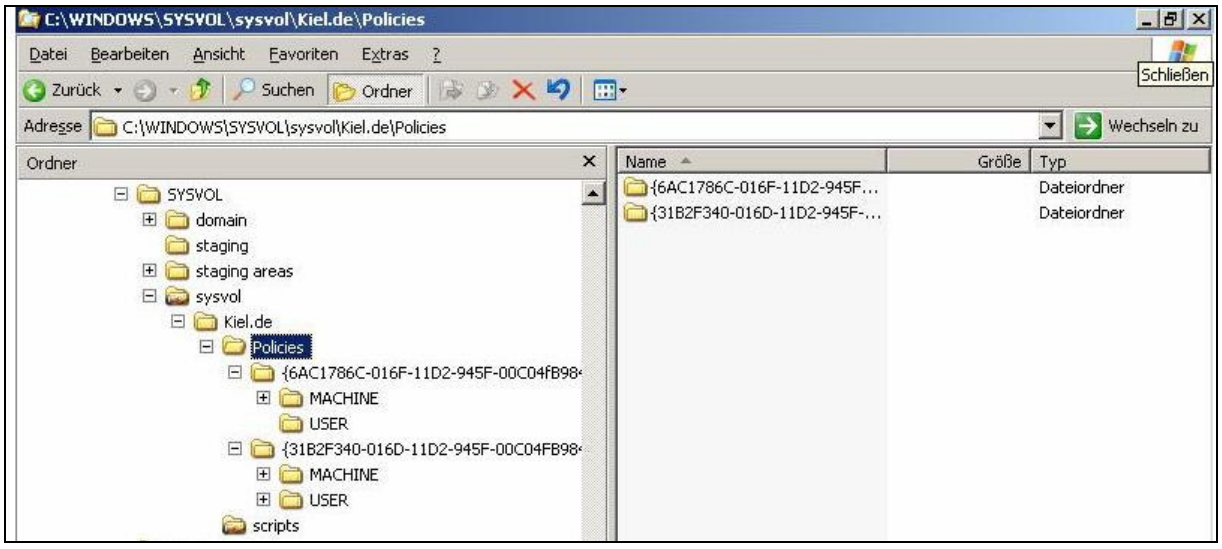


Zu den Active Directory-Gruppenrichtlinien gehören:

- Standort-Gruppenrichtlinien,
- Domänen-Gruppenrichtlinien,
- Organisationseinheiten (OE)-Gruppenrichtlinien
- und als eine besondere OE-Gruppenrichtlinie die Domänencontroller-Gruppenrichtlinie.



Active Directory-Gruppenrichtlinien werden standardmäßig in der Verzeichnisdatenbank im Verzeichnis SYSVOL auf dem Domänencontroller gespeichert.



Speicherort der Active Directory-Gruppenrichtlinien

Bei der Planung, Erstellung und Verwaltung der Active Directory-Gruppenrichtlinien sollte Folgendes berücksichtigt werden:

- Standardmäßig werden bei der Installation des Active Directory zwei Gruppenrichtlinien im Active Directory erstellt: Die Domänen-Gruppenrichtlinie (*Default Domain Policy*), die mit der entsprechenden Domäne verknüpft ist, und die Domänencontroller-Gruppenrichtlinie (*Default Domain Controller Policy*), die mit dem Active Directory-Container DOMAIN CONTROLLERS verknüpft ist.
- Es können weitere Active Directory-Gruppenrichtlinien im Active Directory erstellt werden. Sie können mit einem Standort, einer Domäne oder einer Organisationseinheit verknüpft werden.
- Active Directory-Gruppenrichtlinien wirken auf unterschiedlichen Ebenen im Active Directory. Die Abarbeitungsreihenfolge und die entsprechende Umsetzung der Gruppenrichtlinien werden im nächsten Kapitel behandelt.
- Je nach Verknüpfungsebene und der Aktivierung von Richtlinien in der Benutzer- bzw. Computerkonfiguration einer Gruppenrichtlinie wirken die Active Directory-Gruppenrichtlinien auf alle Benutzer- und/oder Computerkonten eines Standortes, einer Domäne oder einer Organisationseinheit. Diese Thematik ist für das Verständnis der Wirkungsweise der Gruppenrichtlinien wesentlich und wird in diesem und in den nächsten Kapiteln vertieft.

Active Directory-Gruppenrichtlinien werden mit Hilfe der Verwaltungsprogramme *Active Directory-Benutzer und -Computer* bzw. *Active Directory-Standorte und -Dienste* aufgerufen. Sofern die Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) installiert wurde, können die Active Directory-Gruppenrichtlinien auch über diese Konsole aufgerufen werden. Die GPMC wird im Kapitel 6 ausführlich beschrieben.

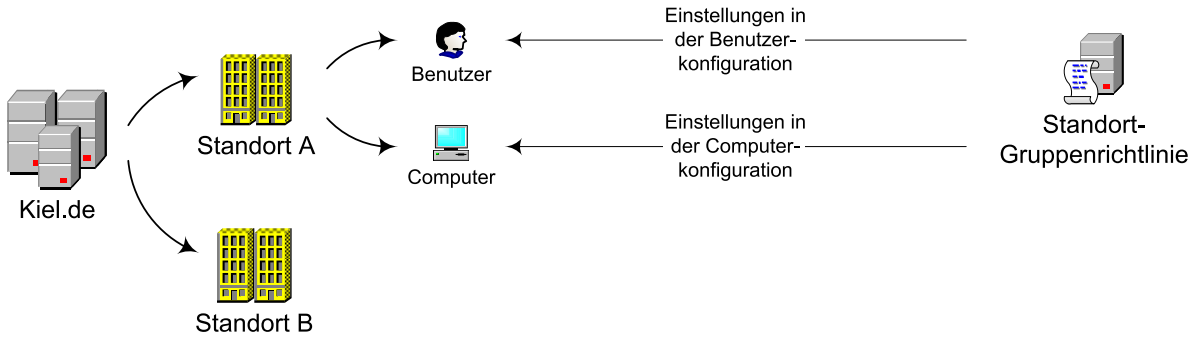
Standort-Gruppenrichtlinie

Eine Standort-Gruppenrichtlinie ist dann von Bedeutung, wenn Richtlinien für Computer umgesetzt werden sollen, die zu einem Standort[3] zusammengefasst wurden.

[3] backUP-Magazin Nr. 5, Kapitel 5.8

Alle Einstellungen, die in einer Standort-Gruppenrichtlinie

- im Knoten Computerkonfiguration vorgenommen werden, wirken standardmäßig auf alle Computerkonten des Standorts und
- im Knoten Benutzerkonfiguration vorgenommen wurden, wirken standardmäßig auf alle Benutzerkonten eines Standorts.

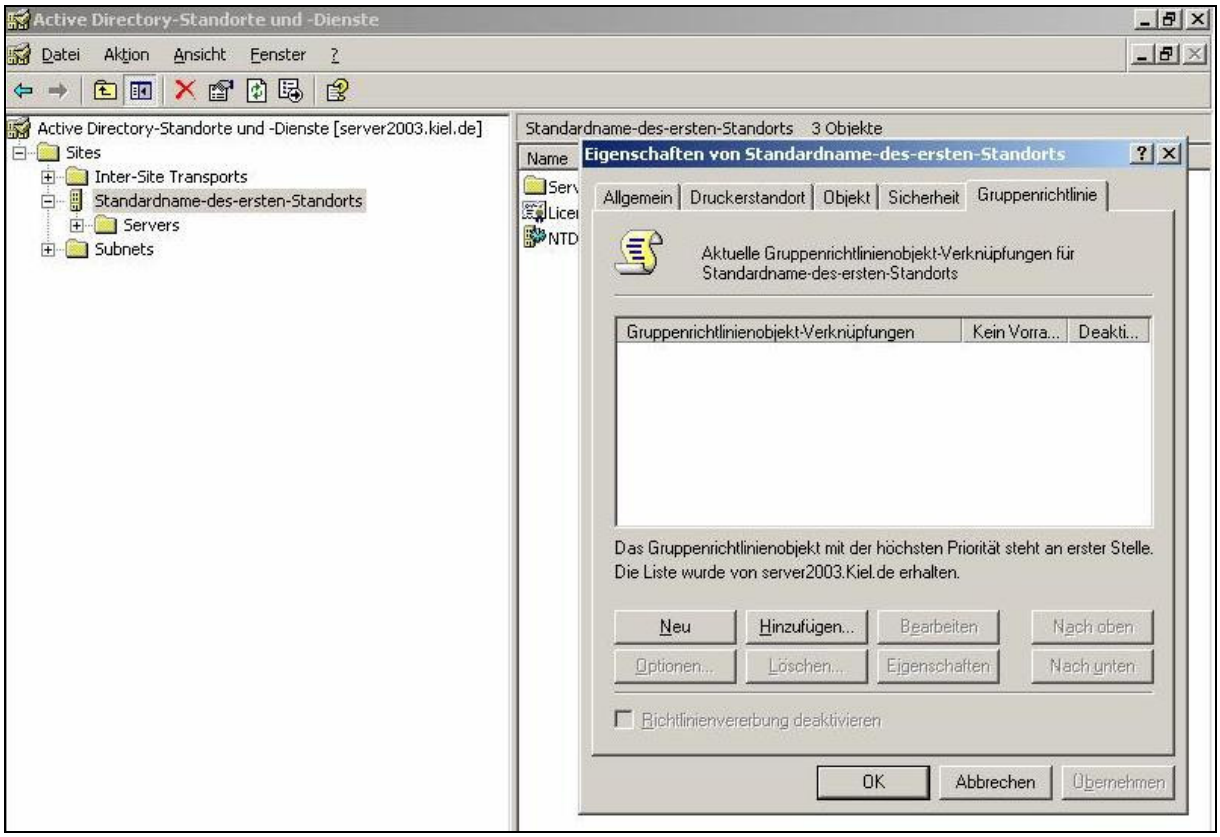


***Ausnahme**: Wenn in einem Standort Computer- und Benutzergruppen aus mehreren Domänen zusammengefasst wurden, wirkt die Standort-Gruppenrichtlinie domänenübergreifend, d. h. auf alle Computer- und Benutzerkonten in diesem Standort, unabhängig davon, zu welcher Domäne sie gehören (Ausnahme: bestimmte Einstellungen in der Standard-Richtlinie der Domäne, die im nächsten Abschnitt beschrieben wird).*

Aufrufen einer Standort-Gruppenrichtlinie!

1. *Wählen Sie START-PROGRAMME-VERWALTUNG.*
2. *Rufen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-STANDORTE UND -DIENSTE auf.*
3. *Markieren Sie den Knoten des Standorts, dessen Gruppenrichtlinie Sie öffnen möchten (in diesem Fall STANDARDNAME-DES-ERSTEN-STANDORTS) und drücken Sie die rechte Maustaste.*
4. *Wählen Sie EIGENSCHAFTEN und klicken Sie auf die Registerkarte GRUPPENRICHTLINIE.*

Standardmäßig wird mit der Installation eines Domänencontrollers keine Standort-Gruppenrichtlinie angelegt (siehe folgendeAbbildung). Soll eine Standort-Gruppenrichtlinie eingesetzt werden, muss sie im Active Directory erstellt und mit dem entsprechenden Standort verknüpft werden (siehe auch Kapitel 5.1).



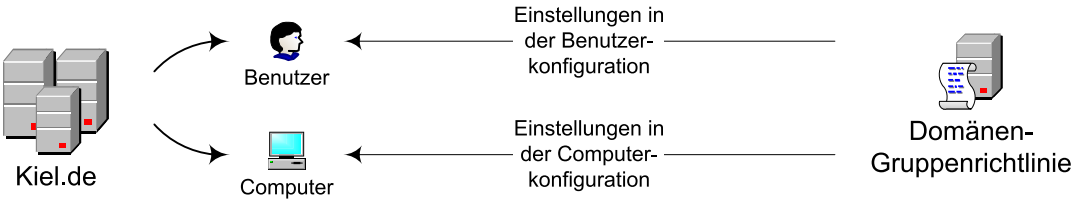
Standort-Gruppenrichtlinie (Active Directory)

Wenn in Ihrer Active Directory-Struktur nur ein Standort eingerichtet ist, hat die Standort-Gruppenrichtlinie die gleiche Wirkung wie eine Domänen-Gruppenrichtlinie. In diesem Fall sollten Sie die Einstellungen in der Domänen-Gruppenrichtlinie vornehmen.

Wenn in Ihrer Active Directory-Struktur mehrere Standorte eingerichtet sind, kann es sinnvoll sein, Standort-Gruppenrichtlinien einzusetzen. Sie müssen allerdings konzeptionell in der Gruppenrichtlinien-Struktur berücksichtigt werden.

Domänen-Gruppenrichtlinie

Eine Domänen-Gruppenrichtlinie soll gemeinsame Richtlinien für alle Computer und Benutzer einer Domäne bereitstellen. Sie wirkt daher auf alle der Domäne zugehörigen Computer- und Benutzerkonten. Jede Domäne ist als eigene Sicherheits- und Verwaltungseinheit zu sehen; daher kann die Domänen-Gruppenrichtlinie im Unterschied zur Standort-Gruppenrichtlinie nicht domänenübergreifend wirken.

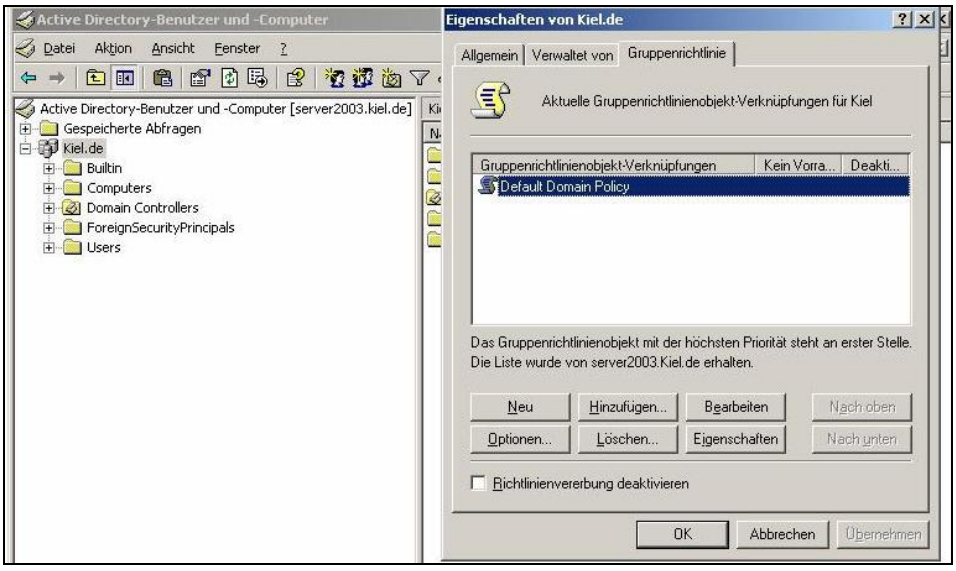


Im oben dargestellten Beispiel wurde eine Domänen-Gruppenrichtlinie erstellt und mit der Domäne Kiel.de verknüpft. Alle Einstellungen, die in der Benutzerkonfiguration der Gruppenrichtlinie vorgenommen wurden, wirken auf alle Benutzerkonten der Domäne und alle Einstellungen, die in der Computerkonfiguration der Gruppenrichtlinie vorgenommen wurden, wirken auf alle Computerkonten der Domäne.

Aufrufen der Standard-Gruppenrichtlinie für die Domäne!

1. *Wählen Sie START-PROGRAMME-VERWALTUNG.*
2. *Rufen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER auf.*
3. *Für den Aufruf der Domänen-Gruppenrichtlinie markieren Sie den Domänennamen (in diesem Beispiel KIEL.DE).*
4. *Drücken Sie die rechte Maustaste.*
5. *Wählen Sie EIGENSCHAFTEN und klicken Sie auf die Registerkarte GRUPPENRICHTLINIE.*

Mit der Installation eines Domänencontrollers wird eine Standard-Gruppenrichtlinie für die Domäne (*Default Domain Policy*) angelegt.



Domänen-Gruppenrichtlinie (Active Directory)

In dieser Domänen-Gruppenrichtlinie sind in dem Knoten *COMPUTERKONFIGURATION* standardmäßig einige Richtlinien aktiviert, die ein Grundsicherheitsniveau in der Domäne gewährleisten soll.

Besonderheiten der Gruppenrichtlinie für die Domäne:

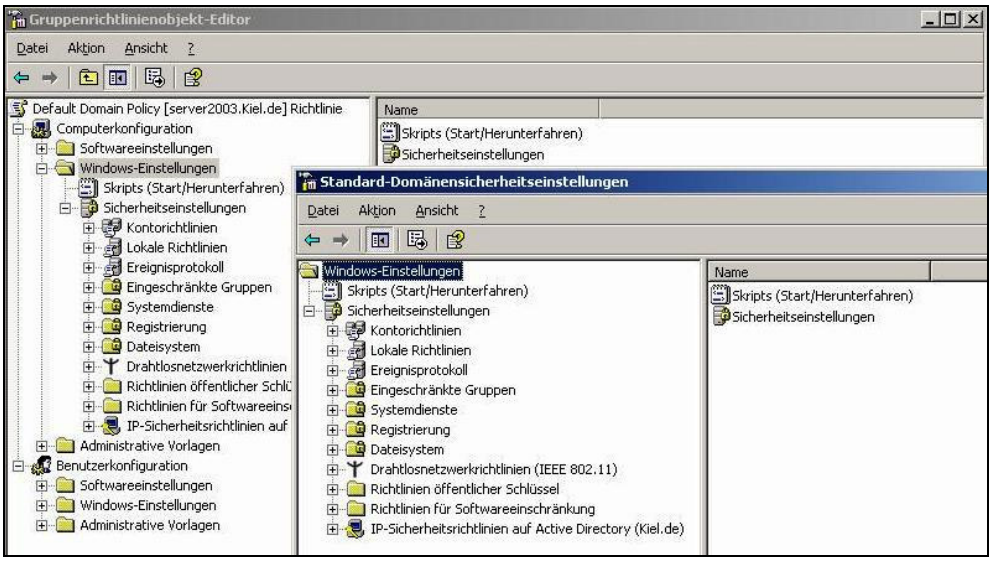
Einstellungen in den Kontorichtlinien (Kennwort-, Kontosperrungs- und Kerberos-Richtlinien) werden nur dann umgesetzt, wenn sie in einer Domänen-Gruppenrichtlinie vorgenommen wurden.

In den nachfolgenden Kapiteln wird auf diejenigen Richtlinien hingewiesen, auf die diese Besonderheit ebenfalls zutrifft.

Obwohl die Kontorichtlinien außer in einer Domänen-Gruppenrichtlinie auch in allen anderen Gruppenrichtlinien sichtbar sind und Sie diese konfigurieren können, werden diese Einstellungen in der Domäne nicht umgesetzt.

So können Sie z. B. in einer der Domäne untergeordneten Organisationseinheit eine Gruppenrichtlinie erstellen und in dieser die Standardlänge des Passwortes von 7 Zeichen auf 3 Zeichen ändern. Die Einstellung wird in der Domäne nicht umgesetzt. Trotzdem bleibt diese Einstellung nicht ohne Wirkung. In diesem Beispiel wird die Einstellung der Passwortlänge in der lokalen Gruppenrichtlinie aller Computerkonten geändert, die der Organisationseinheit zugeordnet sind, d. h. es sind nur die lokalen Benutzerkonten der entsprechenden Computer betroffen.

Die im Startmenüpunkt VERWALTUNG aufgeführten LOKALEN SICHERHEITSRICHTLINIEN FÜR DOMÄNEN zeigen einen Ausschnitt der gesamten Domänen-Gruppenrichtlinie. Sie berücksichtigen nur, wie unten abgebildet, die Richtlinien im Knoten COMPUTERKONFIGURATION-WINDOWS-EINSTELLUNGEN.



Sicherheitsrichtlinie für Domänen

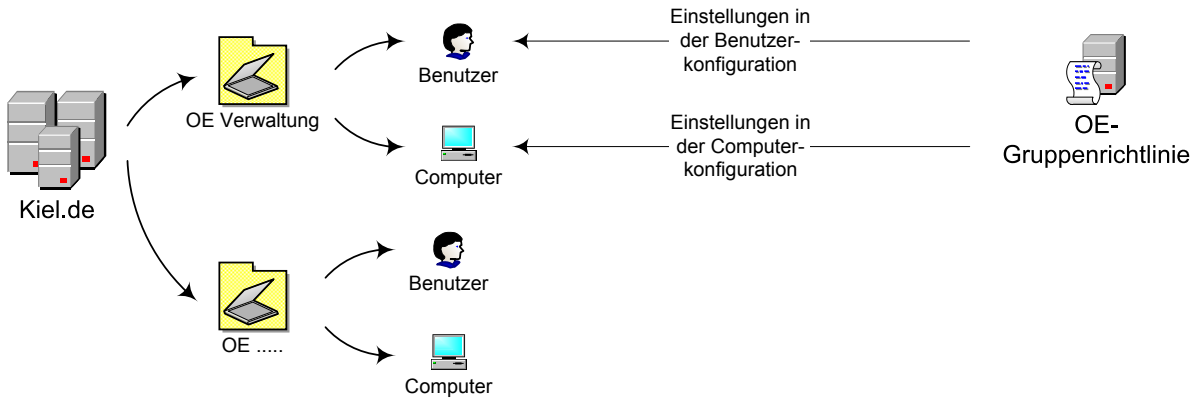
Organisationseinheiten (OE)-Gruppenrichtlinien

Die OE-Gruppenrichtlinien sind mit Organisationseinheiten verknüpft und stehen deshalb im unmittelbaren Zusammenhang mit dem strukturellen Aufbau des Active Directory.

Grundsätzlich wirken alle Einstellungen, die in einer OE-Gruppenrichtlinie

- im Knoten Computerkonfiguration vorgenommen werden, auf alle Computerkonten der OE und
- im Knoten Benutzerkonfiguration vorgenommen wurden, auf alle Benutzerkonten der OE.

Im unten dargestellten Beispiel wurde eine OE-Gruppenrichtlinie erstellt und mit der OE VERWALTUNG verknüpft. Alle Einstellungen, die in der Benutzerkonfiguration der Gruppenrichtlinie vorgenommen wurden, wirken auf alle Benutzerkonten der OE VERWALTUNG, aber nicht auf die Benutzerkonten der anderen Organisationseinheiten. Alle Einstellungen, die in der Computerkonfiguration der Gruppenrichtlinie vorgenommen wurden, wirken auf alle Computerkonten der OE VERWALTUNG, aber nicht auf die Computerkonten der anderen Organisationseinheiten.

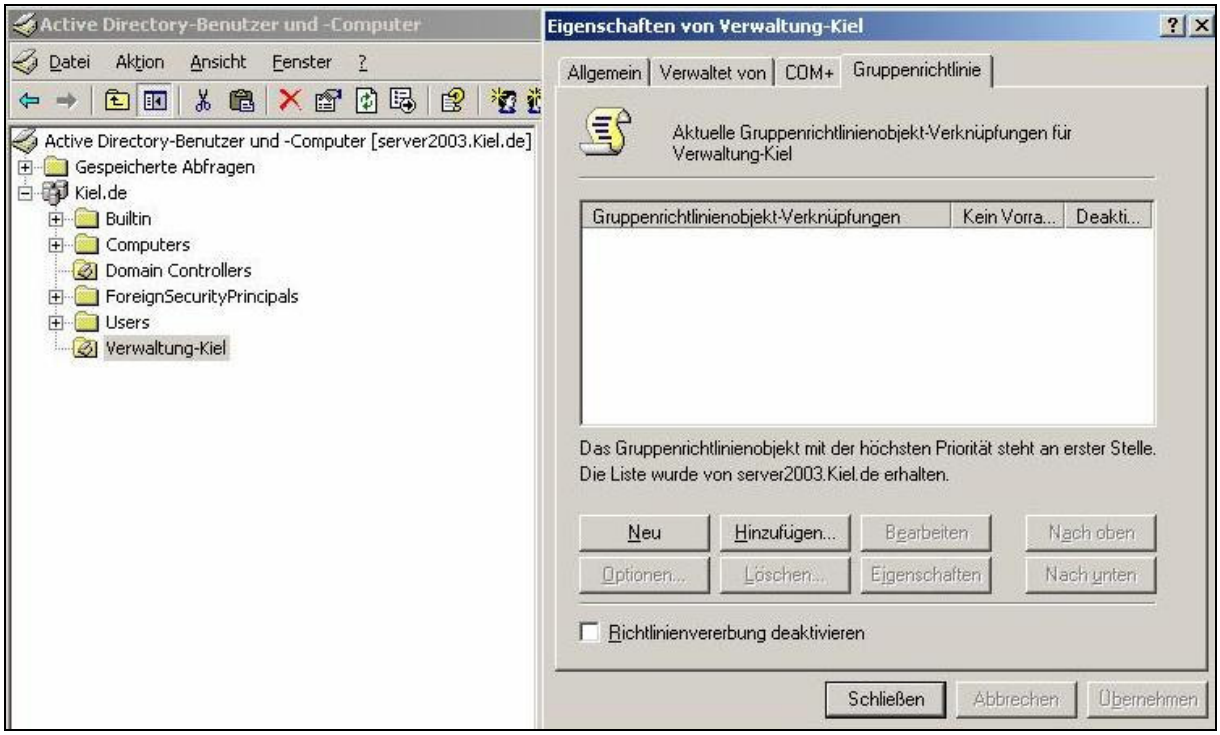


Aufrufen der Gruppenrichtlinie für eine Organisationseinheit!

1. *Wählen Sie START-PROGRAMME-VERWALTUNG.*
2. *Rufen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER auf.*
3. *Für den Aufruf einer Organisationseinheiten-Gruppenrichtlinie markieren Sie die entsprechende Organisationseinheit (in diesem Beispiel VERWALTUNG-KIEL).*

4. *Drücken Sie die rechte Maustaste.*
5. *Wählen Sie EIGENSCHAFTEN und klicken Sie auf die Registerkarte GRUPPENRICHTLINIE.*

Mit der Installation des Active Directory werden standardmäßig keine OE-Gruppenrichtlinien erstellt (eine Ausnahme bildet die Domänencontroller-Gruppenrichtlinie, die im nächsten Abschnitt angesprochen wird). Wenn nach dem oben beschriebenen Verfahren eine Gruppenrichtlinie für die OE aufgerufen werden soll, ist dort zunächst keine Gruppenrichtlinie sichtbar (siehe folgende Abbildung). Sollen Gruppenrichtlinien auf Organisationseinheiten wirken, müssen sie an dieser Stelle erstellt bzw. verknüpft werden.

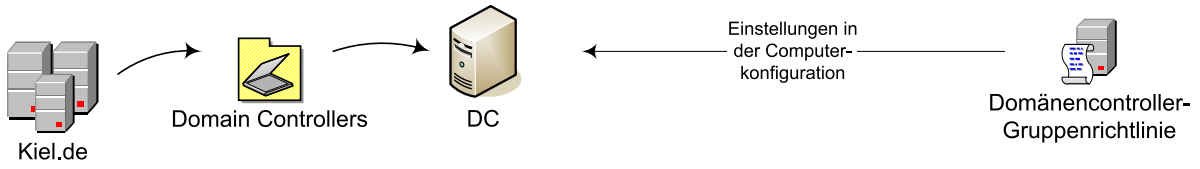


Organisationseinheiten (OE)-Gruppenrichtlinie

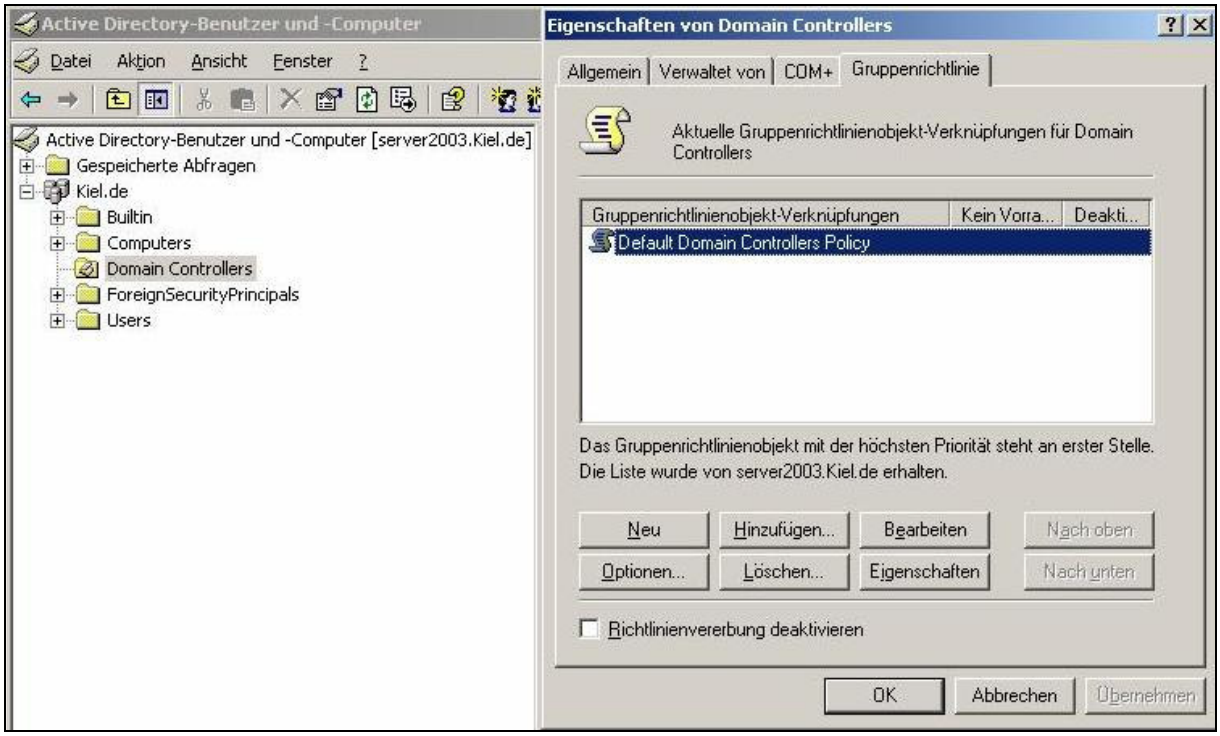
Die Entscheidung, ob und auf welcher Ebene OE-Gruppenrichtlinien eingesetzt werden, ist abhängig davon, nach welchen Kriterien das Active Directory strukturiert ist. Ein konzeptioneller Vorschlag zur Strukturierung des Active Directory und einen auf diese Struktur abgestimmten Einsatz von Gruppenrichtlinien werden im Kapitel 4 und in Form eines Beispiels im Kapitel 10 beschrieben.

Domänencontroller-Gruppenrichtlinie

Eine Domänencontroller-Gruppenrichtlinie soll gemeinsame Richtlinien für alle Domänencontroller einer Domäne bereitstellen. Bei der Domänencontroller-Gruppenrichtlinie *Default Domain Controllers Policy* handelt es sich um eine OE-Gruppenrichtlinie, die bei der Installation der Domäne standardmäßig erstellt und mit der Organisationseinheit DOMAIN CONTROLLERS verknüpft wird. Diese Gruppenrichtlinie definiert für alle Domänencontroller ein im Vergleich zu Mitgliedsservern erhöhtes Sicherheitsniveau.



In der Organisationseinheit DOMAIN CONTROLLERS befinden sich normalerweise, wie im oben dargestellten Beispiel, nur Domänencontroller und keine Benutzerkonten. Daher liegt die Hauptbedeutung der Domänencontroller-Gruppenrichtlinien in der Umsetzung der Richtlinien des Knotens Computerkonfiguration, die die Funktionen und den Betrieb des Domänencontrollers steuern. Die Wirkungsweise der Gruppenrichtlinien auf Benutzer- und Computerkonten wird im nächsten Kapitel näher erläutert.



Domänencontroller-Gruppenrichtlinie (Active Directory)

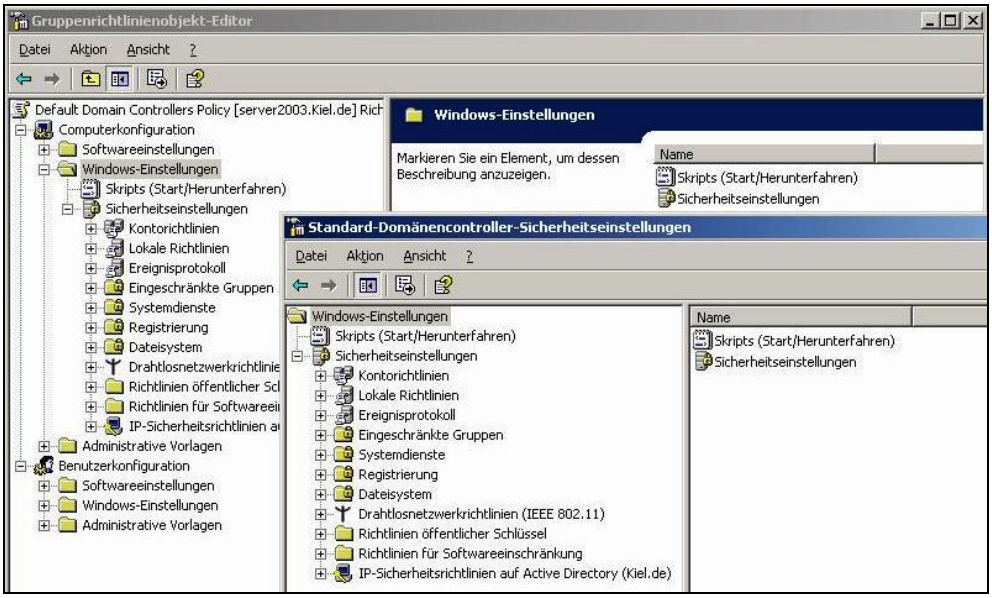
Aufrufen der Standard-Gruppenrichtlinie für den Domänencontroller!

1. *Wählen Sie START-PROGRAMME-VERWALTUNG.*
2. *Rufen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND –COMPUTER auf.*
3. *Für den Aufruf der Domänen-Controller-Gruppenrichtlinie markieren Sie den Container DOMAIN CONTROLLERS.*
4. *Drücken Sie die rechte Maustaste.*
5. *Wählen Sie EIGENSCHAFTEN und klicken Sie auf die Registerkarte GRUPPENRICHTLINIE.*

Besonderheiten der Gruppenrichtlinie für den Domänencontroller:

Eine besondere Bedeutung für die administrative Arbeit haben die Einstellungen in dem Knoten ÜBERWACHUNGSRICHTLINIEN (Computerkonfiguration) der Domänencontroller-Gruppenrichtlinie. Werden die Überwachungsrichtlinien in dieser Gruppenrichtlinie aktiviert, können die erzeugten Protokolle für die Domäne zentral verwaltet werden. Die Überwachungsrichtlinien werden im Kapitel 8.2.2 näher erläutert.

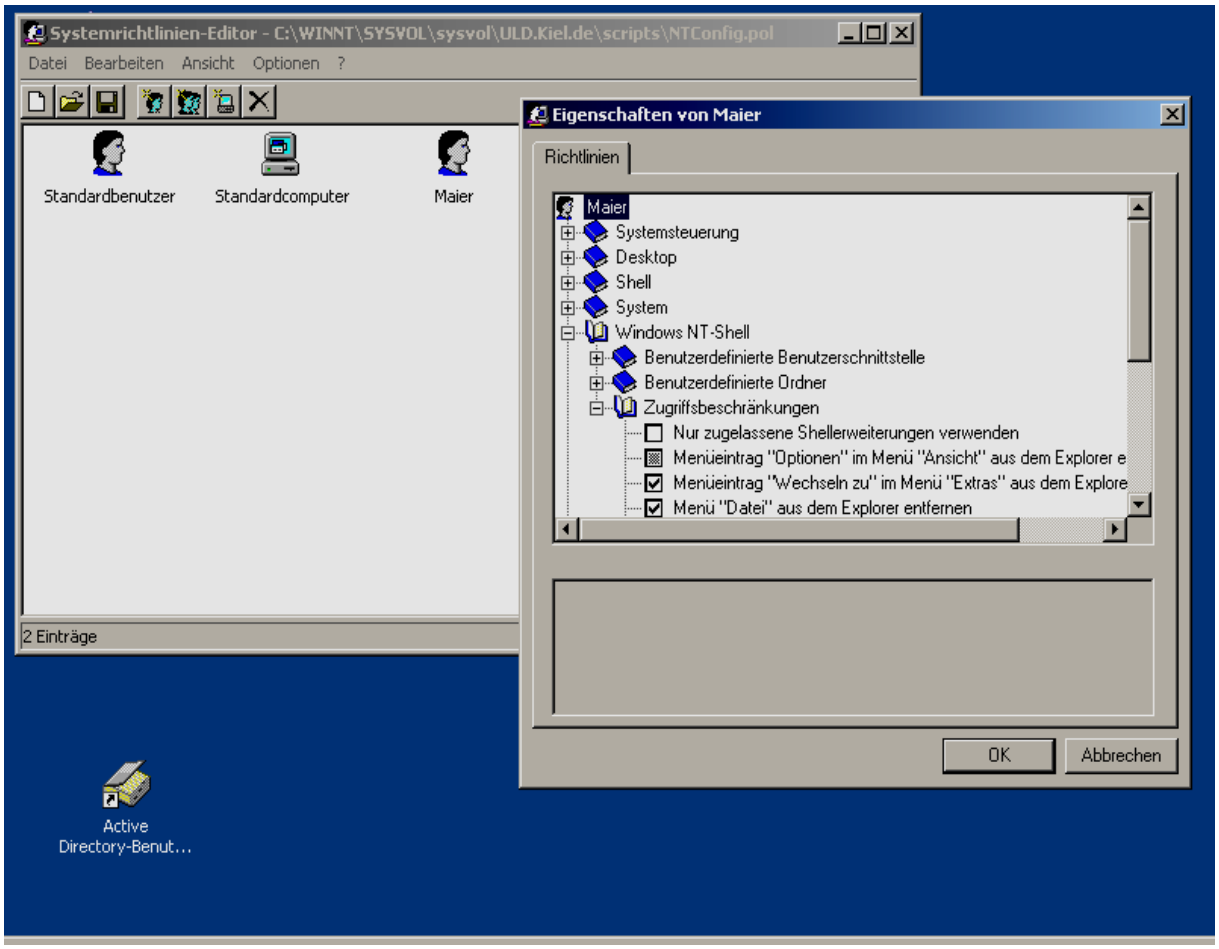
Die im Startmenüpunkt VERWALTUNG aufgeführte SICHERHEITSRICHTLINIE FÜR DOMÄNENCONTROLLER zeigt einen Ausschnitt der gesamten Domänencontroller-Gruppenrichtlinie. Sie berücksichtigt nur, wie unten abgebildet, die Richtlinien im Knoten COMPUTERKONFIGURATION-SICHERHEITSEINSTELLUNGEN.



Sicherheitsrichtlinie für Domänencontroller

2.6 Windows NT-Systemrichtlinien

An dieser Stelle werden nur die Funktionen der Windows NT-Systemrichtlinien dargestellt, die für den Einsatz in einer Windows 2000/2003 Domäne mit NT 4.0 Clients von Bedeutung sind.



Systemrichtlinien-Editor *POLEDIT.EXE*

Im Benutzermanager von Windows NT 4.0 lassen sich die Überwachungs- und Kennwortrichtlinien aktivieren. Mit dem Verwaltungsprogramm *poledit.exe* können zusätzlich eine Vielzahl von Systemrichtlinien aktiviert werden, die überwiegend die Funktionen auf dem Client reglementieren.

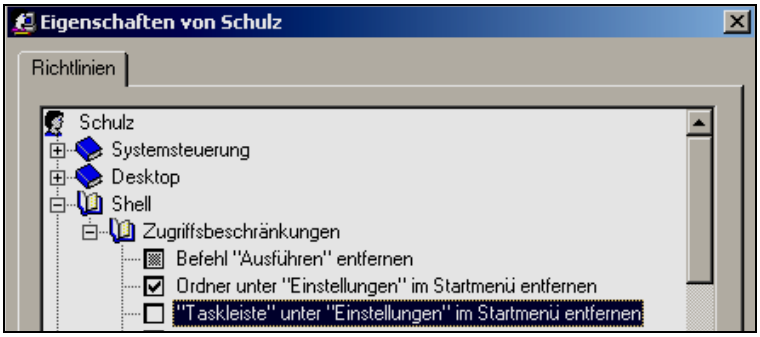
Die Active Directory-Gruppenrichtlinien finden nur begrenzt Anwendung auf NT 4.0 Clients. Daher ist in einer Windows 2000/2003 Domänenumgebung der Einsatz von *poledit.exe* nur dann erforderlich, wenn auf den Clients das Betriebssystem Windows NT 4.0 Workstation eingesetzt wird. So werden beispielsweise die Kennwort- und Kontosperrungsrichtlinien der

Active Directory-Domänen-Gruppenrichtlinie auch von NT 4.0 Clients berücksichtigt. Sollen darüber hinaus auch die Funktionen des NT 4.0 Clients eingeschränkt werden, greifen nur noch die Windows NT 4.0 Systemrichtlinien.

Standardmäßig ist auf einem Windows 2000 Domänen-Controller *poledit.exe* aufrufbar, während unter Windows 2003 die Installation nachgeholt werden muss.

Poledit.exe und die dazugehörigen adm-Dateien sind Bestandteil der Windows-Verwaltungsprogramme. Diese können über das Adminpak (START-AUSFÜHREN-adminpak.msi) installiert werden. Poledit.exe wird im Ordner <Stammverzeichnis\Windows> und die adm-Dateien im Ordner <Stammverzeichnis\Windows\inf gespeichert.

Die Funktionen des Systemrichtlinien-Editors sind im Vergleich zu den Gruppenrichtlinien überschaubar. Die unter einem Benutzerkonto aktivierten Systemrichtlinien werden dem Benutzerkonto zugeordnet und in dessen Benutzerprofil in der Datei NTUSER.DAT gespeichert. Die Umsetzung der Richtlinien erfolgt bei der nächsten Benutzeranmeldung.



Schalter Systemrichtlinien

Als Schalter für die Administration der Systemrichtlinien gibt es folgende Einstellungsvarianten:

 Richtlinie ist nicht aktiviert und wird nicht umgesetzt.

 Richtlinie ist aktiviert.

 Richtlinie war aktiviert und ist deaktiviert worden.

Aufrufen der Windows NT-Systemrichtlinien!

1. *Wählen Sie START-AUSFÜHREN.*
2. *Geben Sie* `poledit.exe` *ein.*

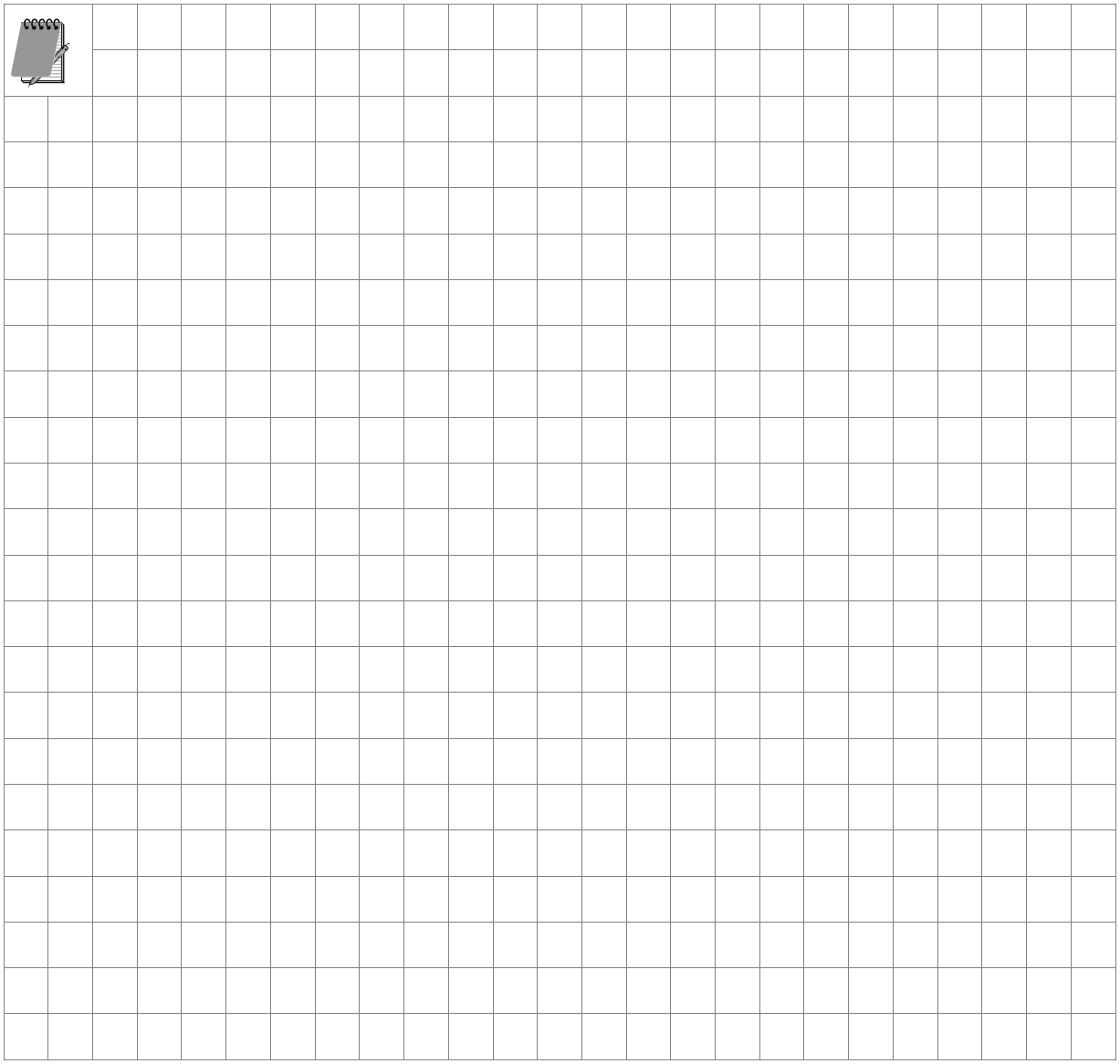
Erstellen einer Windows NT-Systemrichtlinie für ein Benutzerkonto!

1. *Rufen Sie den Systemrichtlinien-Editor unter START-AUSFÜHREN auf, indem Sie poledit.exe eingeben.*
2. *Wählen Sie unter dem Menü DATEI die Funktion NEUE RICHTLINIE aus. Anschließend öffnet sich eine neue Richtlinie, bestehend aus den Knoten COMPUTER und BENUTZER. Diese sind als Schablonen zu verstehen. Alle darin vorgenommenen Einstellungen wirken auf alle Computer- bzw. Benutzerkonten.*
3. *Um den Benutzern individuelle Systemrichtlinien zuzuordnen, wählen Sie das Menü BEARBEITEN und die Funktion BENUTZER HINZUFÜGEN aus. Klicken Sie auf DURCHSUCHEN. Es öffnet sich ein Fenster, indem Sie die Benutzerkonten des Domänencontrollers finden.*
4. *Nach Auswahl eines Benutzerkontos wird für dieses die Schablone BENUTZER übernommen. Es ist deshalb zu empfehlen, keine Einstellungen in den Schablonen vorzunehmen.*
5. *Klicken Sie auf das Symbol des neu angelegten Benutzers und aktivieren Sie die entsprechenden Systemrichtlinien.*
6. *Speichern Sie unter dem Menü DATEI und der Funktion SPEICHERN die Systemrichtlinie mit dem Namen ntconfig.pol in dem folgenden Ordner ab: <\Windows\sysvol\sysvol\<Domänenname>\scripts>.*

2.7 Sicherheitscheck

- *Beachten Sie, dass Windows **Lokale und Active Directory-Gruppenrichtlinien** unterstützt. Active Directory-Gruppenrichtlinien werden im Active Directory des Domänencontrollers administriert.*
- *Berücksichtigen Sie, dass die LOKALEN RICHTLINIEN auf **alle Benutzerkonten**, einschließlich des Administratorkontos, wirken. In einer Domänenumgebung ist der Einsatz der Lokalen Richtlinien nicht notwendig.*
- *Der Einsatz der **Kontorichtlinien** ist in dem Domänen-Gruppenrichtlinienobjekt zu administrieren.*
- *Für die Reglementierung der Clients und der Benutzerkonten ist es wichtig, dass Sie im Active Directory eine **Struktur** durch die Einrichtung von Organisationseinheiten (OE) schaffen, um die OE-Gruppenrichtlinien differenzierter einsetzen zu können.*

- *Jedes Gruppenrichtlinienobjekt besteht aus den Knoten Computer- und Benutzerkonfiguration. Die Umsetzung der Richtlinien der Computerkonfiguration erfolgt beim **Starten** des Computers, während die Richtlinien der Benutzerkonfiguration unmittelbar nach der **Anmeldung** des Benutzerkontos umgesetzt werden.*
- *In einem Netzwerk mit **Windows NT-Clients** können Sie für die PC die NT-Systemrichtlinien verwenden. Beachten Sie, dass die Datei **ntconfig.pol** mit diesem Namen in dem Ordner <\Windows\sysvol\sysvol\Domänenname\scripts> abgelegt wird.*



3 Wirkungsweise der Gruppenrichtlinien

In diesem Kapitel erfahren Sie,

- wie die Gruppenrichtlinien auf Benutzer- und Computerkonten wirken,
- in welcher Reihenfolge die Gruppenrichtlinien verarbeitet werden,
- wann Gruppenrichtlinien verarbeitet werden,
- in welchen Intervallen die Gruppenrichtlinien aktualisiert werden und
- wie Gruppenrichtlinien manuell aktualisiert werden können.

3.1 Wirkungsweise der Gruppenrichtlinien

Im vorherigen Kapitel wurde die Wirkungsweise der Gruppenrichtlinien auf Benutzer- und Computerkonten im Zusammenhang mit den unterschiedlichen Gruppenrichtlinien betrachtet. Zusammenfassend müssen folgende Hinweise in Bezug auf die Wirkungsweise der Gruppenrichtlinien berücksichtigt werden:

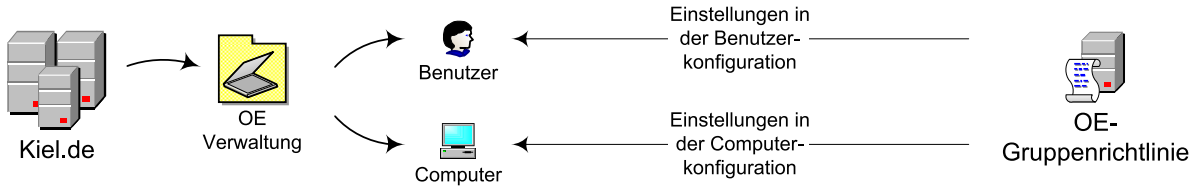
- Gruppenrichtlinien wirken nicht auf Gruppenkonten, sondern auf Benutzer- oder Computerkonten.
- *Lokale Gruppenrichtlinien* wirken auf das lokale Computerkonto und die lokalen Benutzerkonten.
- Active Directory-Gruppenrichtlinien wirken auf Benutzer- und Computerkonten der Domäne. Dabei spielt es eine Rolle, ob die Active Directory-Gruppenrichtlinie mit einem Standort, einer Domäne oder einer Organisationseinheit verknüpft ist.
- Einstellungen in dem Knoten Benutzerkonfiguration finden Anwendung auf Benutzerkonten und Einstellungen in dem Knoten Computerkonfiguration finden Anwendung auf Computerkonten.

Aus diesen Hinweisen lassen sich folgende Schlussfolgerungen ableiten:

- Wenn Einstellungen in der Benutzer- bzw. der Computerkonfiguration einer Gruppenrichtlinie vorgenommen werden, müssen sich auch tatsächlich Benutzer- bzw. Computerkonten in der Verwaltungseinheit befinden, mit der die entsprechende Gruppenrichtlinie verknüpft wird. Wenn z. B. eine Gruppenrichtlinie mit einer Organisationseinheit verknüpft wird und Richtlinieneinstellungen im Knoten Computerkonfiguration vorgenom-

men werden, dann muss auch ein Computerkonto in dieser Organisationseinheit vorhanden sein, auf das die Einstellungen wirken können.

- Werden Einstellungen in der Benutzerkonfiguration einer Gruppenrichtlinie vorgenommen und diese Gruppenrichtlinie mit einem Objekt verknüpft, in dem ein Benutzerkonto vorhanden ist (z. B. mit der Organisationseinheit VERWALTUNG in der Abbildung unten), dann wirken diese Einstellungen der Gruppenrichtlinie auf das entsprechende Benutzerkonto, egal an welchem Computer sich dieser Benutzer anmeldet.
- Werden Einstellungen in der Computerkonfiguration einer Gruppenrichtlinie vorgenommen und diese Gruppenrichtlinie mit einem Objekt verknüpft, in dem ein Computerkonto vorhanden ist (z. B. mit der Organisationseinheit VERWALTUNG in der Abbildung unten), dann wirken diese Einstellungen der Gruppenrichtlinie auf das entsprechende Computerkonto, egal welcher Benutzer sich an diesem Computer anmeldet.

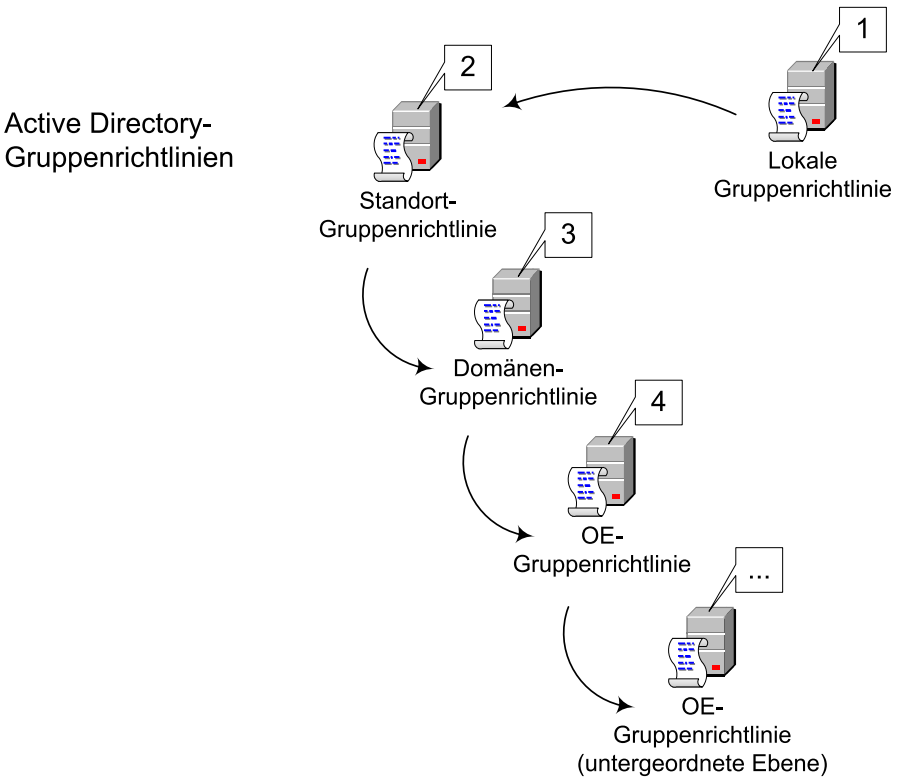


3.2 Reihenfolge bei der Verarbeitung der Gruppenrichtlinien

Wie kann bei den unterschiedlichen Gruppenrichtlinien, die auf den unterschiedlichen Ebenen wirken, sichergestellt werden, dass zum Schluss genau die Richtlinie wirkt, die gemäß der Planung wirken soll? Die Antwort liegt in einer fest vorgegebenen Hierarchie und Abarbeitungsreihenfolge.

Folgende Hinweise müssen in Bezug auf die Abarbeitungsreihenfolge der Gruppenrichtlinien berücksichtigt werden:

- Es gibt eine definierte Verarbeitungsreihenfolge der Gruppenrichtlinien.
- Abweichend von dieser Reihenfolge gibt es Ausnahmen bzw. können Ausnahmen definiert werden.
- Die Besonderheiten der unterschiedlichen Gruppenrichtlinien auf ihre Wirkungsweise und Gültigkeit müssen berücksichtigt werden.
- Die Gruppenrichtlinien werden nacheinander verarbeitet und wirken dabei kumulativ. Sie folgen dabei folgendem Schema:

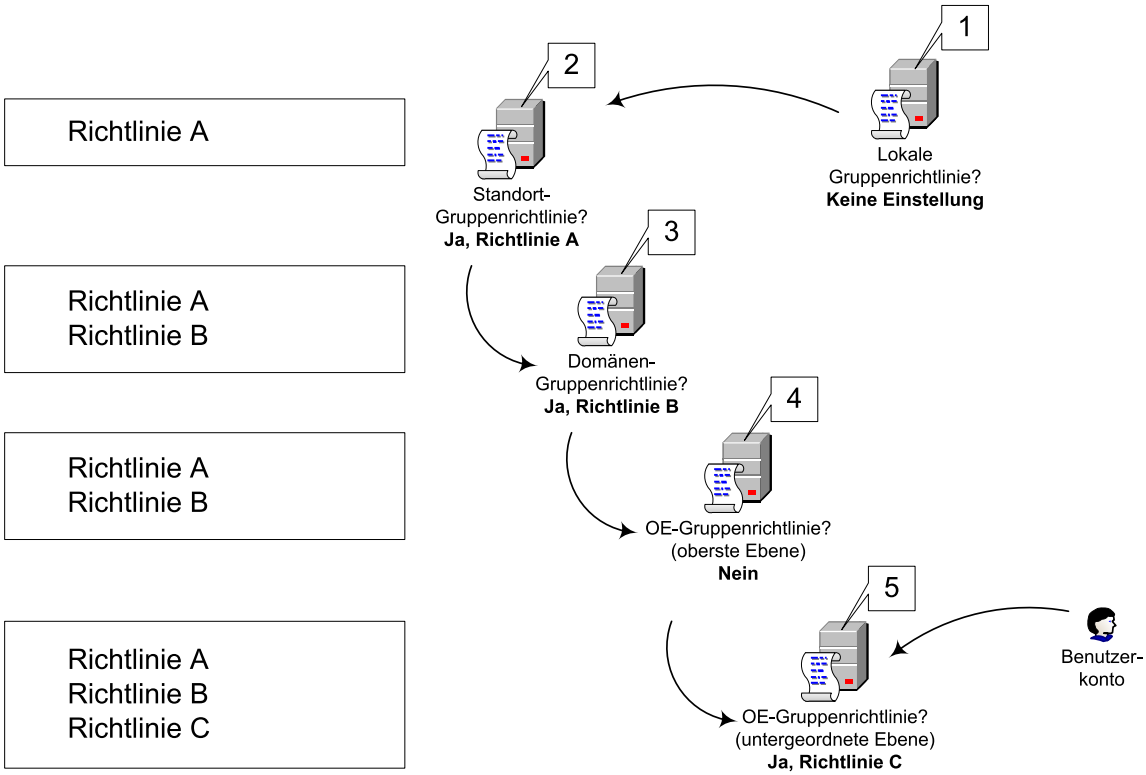


Zuerst wird die *Lokale Gruppenrichtlinie* verarbeitet, danach folgen die Active Directory-Gruppenrichtlinien in der oben angegebenen Reihenfolge. Falls unterhalb einer Organisationseinheit weitere Organisationseinheiten hierarchisch angeordnet wurden, werden Gruppenrichtlinien, die mit diesen untergeordneten Organisationseinheiten verknüpft werden, entsprechend ihrer Hierarchie verarbeitet. Im Kapitel 4 werden verschiedene Modelle zur Anordnung von Organisationseinheiten und die Vorbereitungen des Active Directory für den Einsatz von Gruppenrichtlinien vorgestellt.

Die Wirkungsweise und Gültigkeit der Gruppenrichtlinien sowie die Verarbeitungsreihenfolge sind für das Grundverständnis der Gruppenrichtlinien wesentlich. Daher soll an dieser Stelle die Verarbeitungsreihenfolge anhand eines Beispiels weiter verdeutlicht werden: In diesem Beispiel wird davon ausgegangen, dass jeweils eine Gruppenrichtlinie für den Standort, die Domäne, die Organisationseinheit und die untergeordnete Organisationseinheit eingerichtet wurde. Die aktivierten Richtlinien (im Knoten Benutzerkonfiguration) sollen auf ein Benutzerkonto angewendet werden, das sich in der untergeordneten Organisationseinheit befindet sowie dem Standort zugeordnet ist.

In folgenden Gruppenrichtlinien wurden Richtlinien in der Benutzerkonfiguration aktiviert:

- Standort-Gruppenrichtlinie: Richtlinie A
- Domänen-Gruppenrichtlinie: Richtlinie B
- OE-Gruppenrichtlinie: keine Richtlinie
- untergeordnete OE-Gruppenrichtlinie: Richtlinie C



Die Abbildung zeigt, dass die Gruppenrichtlinien in der definierten Reihenfolge verarbeitet werden und sich die einzelnen aktivierten Richtlinien der unterschiedlichen Gruppenrichtlinien auf diesem Weg aufsummieren. Das bedeutet, dass sich die Einstellungen der Gruppenrichtlinien auf die hierarchisch untergeordneten Gruppenrichtlinien vererben. Das Ergebnis der Abarbeitungsreihenfolge, die Summe der aktivierten Richtlinien A bis C, wirkt auf das entsprechende Benutzerkonto.

Wenn sich das Benutzerkonto nicht wie angenommen in der Organisationseinheit der untergeordneten Ebene befindet, sondern in der Organisationseinheit der obersten Ebene, dann wirkt auf dieses Benutzerkonto nur die Summe der aktivierten Richtlinien A und B.

Abweichend zu der oben dargestellten Abarbeitung der Gruppenrichtlinien sind nachfolgende Situationen denkbar, die direkt oder indirekt mit der Abarbeitung der Gruppenrichtlinien zusammenhängen:

- Die Vererbung soll auf bestimmten Ebenen deaktiviert werden.
- Die Vererbung darf im Verlauf der Abarbeitungsreihenfolge nicht unterbrochen oder deaktiviert werden.
- Die Abarbeitung der Gruppenrichtlinie soll für den Bereich Benutzer- oder Computerkonfiguration deaktiviert werden.
- Eine Gruppenrichtlinie soll z. B. in einer bestimmten Organisationseinheit nur auf eine bestimmte Benutzergruppe wirken oder auf eine bestimmte Benutzergruppe nicht angewendet werden.
- Ein Benutzer darf bei der Anmeldung an einem bestimmten Computer nur definierte Benutzereinstellungen erhalten und nicht die Einstellungen, die der Benutzer entsprechend der ihm zugewiesenen Gruppenrichtlinien eigentlich erhalten sollte (Loopback).

Ebenfalls können bei der Abarbeitung der Gruppenrichtlinien Situationen entstehen, in denen die Gruppenrichtlinien anscheinend nicht richtig verarbeitet werden, z. B. wenn zwei Gruppenrichtlinien miteinander konkurrieren und sich die hierarchisch übergeordnete Gruppenrichtlinie durchsetzt.

Die Problematik der oben beschriebenen Situationen wird im Kapitel 5 und Kapitel 9.3 (Loopback) aufgegriffen.

3.3 Verarbeitung und Aktualisierung der Gruppenrichtlinien

Bisher wurde nur die Abarbeitung der Gruppenrichtlinien dargestellt. Doch für den Gesamtzusammenhang ist es wichtig zu wissen,

- wann die Gruppenrichtlinien verarbeitet werden,
- in welchem Zeitraum die Gruppenrichtlinien aktualisiert werden,
- wo die Standardintervalle geändert werden können und
- wie Gruppenrichtlinien manuell aktualisiert werden.

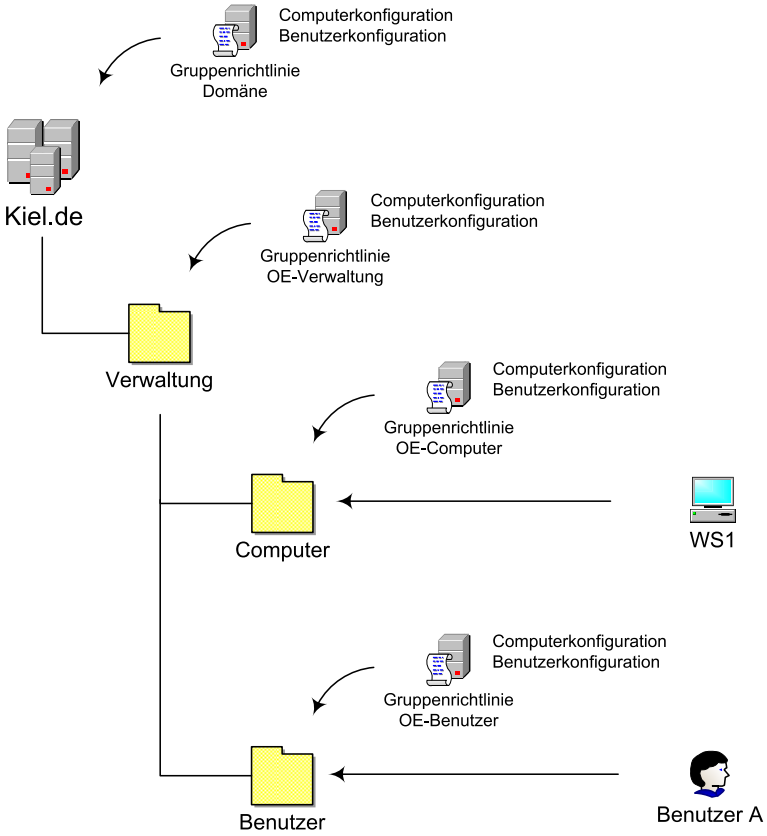
Verarbeitung von Gruppenrichtlinien

Bei der Verarbeitung spielt der strukturelle Aufbau einer Gruppenrichtlinie eine entscheidende Rolle.

Ein grundlegendes Strukturmerkmal ist die Unterteilung der Gruppenrichtlinien in die Knoten Computer- und Benutzerkonfiguration. Der Knoten COMPUTERKONFIGURATION enthält Richtlinien, die auf den Computer wirken sollen, unabhängig davon, welcher Benutzer sich anmeldet. Daher müssen diese Richtlinien verarbeitet werden, noch bevor sich ein Benutzer authentifizieren kann.

Erst unmittelbar nach der Anmeldung am System werden die Einstellungen im Knoten BENUTZERKONFIGURATION berücksichtigt, die dann auf das entsprechende Benutzerkonto wirken sollen.

Die Verarbeitung der Knoten Computer- und Benutzerkonfiguration erfolgt unabhängig voneinander. Die Richtlinien im Knoten COMPUTERKONFIGURATION werden beim Starten des Computers, die Richtlinien im Knoten BENUTZERKONFIGURATION werden unmittelbar nach dem Anmelden am System verarbeitet.



In der Abbildung oben ist ein Start- und Anmeldevorgang dargestellt, der das Zusammenspiel von Computer- und Benutzerkonfiguration bei der Verarbeitung der Gruppenrichtlinien veranschaulicht.

Die Darstellung spiegelt folgenden Vorgang wider:

- Der BENUTZER A startet den Computer WS1 und meldet sich an diesem Computer an.
- In den Gruppenrichtlinien der Domäne KIEL.DE und der Organisationseinheiten VERWALTUNG, BENUTZER und COMPUTER sind Einstellungen in den Knoten Computer- und Benutzerkonfiguration vorgenommen worden.

Wenn der BENUTZER A den Computer WS1 startet, werden die Computerkonfigurationen der Gruppenrichtlinien wie folgt verarbeitet:

- Zuerst wird die Computerkonfiguration der Domänen-Gruppenrichtlinie,
- danach die Computerkonfiguration der Gruppenrichtlinie OE-VEWALTUNG und
- zum Schluss die Computerkonfiguration der Gruppenrichtlinie OE-COMPUTER verarbeitet.

Wenn sich der BENUTZER A danach an dem Computer WS1 anmeldet, werden die Benutzerkonfigurationen der Gruppenrichtlinien folgendermaßen verarbeitet:

- Zuerst wird die Benutzerkonfiguration der Domänen-Gruppenrichtlinie,
- danach die Benutzerkonfiguration der Gruppenrichtlinie OE-VERWALTUNG und
- zum Schluss die Benutzerkonfiguration der Gruppenrichtlinie OE-BENUTZER verarbeitet.

Dabei ist in diesem Beispiel zu beachten, dass

- die Einstellungen in der Benutzerkonfiguration der Gruppenrichtlinie OE-COMPUTER nicht verarbeitet werden, da der BENUTZER A nicht der Organisationseinheit COMPUTER zugeordnet ist und
- die Einstellungen in der Computerkonfiguration der Gruppenrichtlinie OE-BENUTZER nicht verarbeitet werden, da der Computer WS1 nicht der Organisationseinheit BENUTZER zugeordnet ist.

Aktualisierung von Gruppenrichtlinien

Die Gruppenrichtlinien werden nicht nur beim Start- oder Anmeldevorgang, sondern zusätzlich regelmäßig im Hintergrund aktualisiert. Damit wird sichergestellt, dass Änderungen an den Gruppenrichtlinien allen betroffenen Clients, Mitgliedsservern und Domänencontrollern zeitnah zur Verfügung gestellt werden.

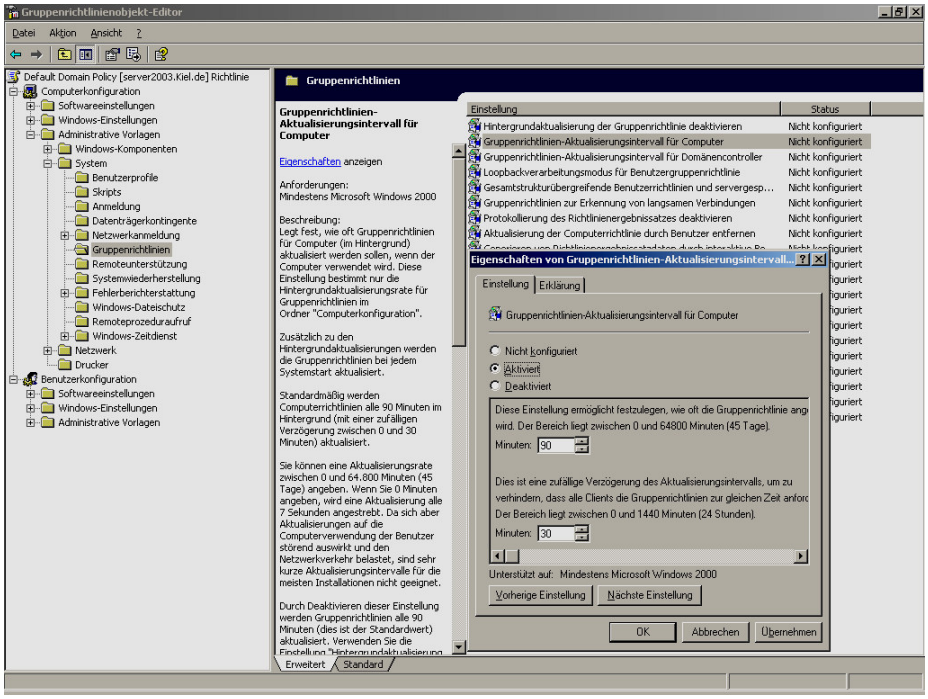
Die standardmäßigen Aktualisierungsintervalle betragen

- für Domänencontroller 5 Minuten und
- für Clients und Mitgliedsserver 90 Minuten mit einem zufälligen Verzögerungsintervall von bis zu 30 Minuten.

Das zufällige Verzögerungsintervall verhindert, dass alle Clients die Änderungen gleichzeitig anfordern und damit eine erhöhte Netzwerkbelastung erzeugen.

Diese standardmäßigen Aktualisierungsintervalle werden in Form von drei Gruppenrichtlinien implementiert und können für individuelle Anforderungen geändert werden:

1. Das Aktualisierungsintervall für Domänencontroller kann in der *Default Domain Policy* aufgerufen werden: COMPUTERKONFIGURATION/ADMINISTRATIVE VORLAGEN/SYSTEM/GRUPPENRICHTLINIEN/GRUPPENRICHTLINIEN-AKTUALISIERUNGSINTERVALL FÜR DOMÄNENCONTROLLER.



Gruppenrichtlinien-Aktualisierungsintervall für Computer (Standard)

2. Das Aktualisierungsintervall für Computereinstellungen kann in der *Default Domain Policy* aufgerufen werden: COMPUTERKONFIGURATION/ADMINISTRATIVE VORLAGEN/SYSTEM/GRUPPENRICHTLINIEN/ GRUPPENRICHTLINIEN-AKTUALISIERUNGSINTERVALL FÜR COMPUTER.
3. Das Aktualisierungsintervall für Benutzereinstellungen kann in der *Default Domain Policy* aufgerufen und geändert werden: BENUTZERKONFIGURATION/ADMINISTRATIVE VORLAGEN/ SYSTEM/GRUPPENRICHTLINIEN/GRUPPENRICHTLINIEN-AKTUALISIERUNGSINTERVALL FÜR BENUTZER.

In manchen Situationen kann es notwendig werden, die Gruppenrichtlinien manuell zu aktualisieren und nicht auf das Aktualisierungsintervall zu warten oder einen neuen Start- bzw. Anmeldevorgang zu starten.

Das Betriebssystem Windows 2000 (Server/Professional) stellt für eine manuelle Aktualisierung der Gruppenrichtlinien den Befehl *secedit* zur Verfügung.

Gruppenrichtlinien mit `secedit` aktualisieren!

1. *Gehen Sie an den Computer, auf dem die Gruppenrichtlinien aktualisiert werden sollen.*
2. *Wählen Sie START-AUSFÜHREN und rufen Sie den Befehlsinterpreter `cmd` auf.*
3. *Aktualisieren Sie **geänderte** Gruppenrichtlinien für den Knoten Computerkonfiguration mit dem Befehl `secedit /refreshpolicy machine_policy`.*
4. *Aktualisieren Sie **geänderte** Gruppenrichtlinien für den Knoten Benutzerkonfiguration mit dem Befehl `secedit /refreshpolicy user_policy`.*
5. *Aktualisieren Sie die **gesamten** Gruppenrichtlinien für den Knoten Benutzerkonfiguration mit dem Befehl `secedit /refreshpolicy user_policy /enforce`.*

Um bei dem Betriebssystem Windows 2003/XP eine manuelle Aktualisierung der Gruppenrichtlinien durchzuführen, ist der Befehl secedit durch den Befehl gpupdate abgelöst worden. Der Befehl gpupdate verwendet folgende Syntax:

gpupdate [/target:{computer | user}] [/force] [/wait:Wert] [/logoff] [/boot]

Parameter des Befehls gpupdate

/target:{computer|user}

Standardmäßig wird sowohl die Computer- als auch die Benutzerkonfiguration aktualisiert. Dieser Parameter kann die Aktualisierung entweder auf die Computer- oder auf die Benutzerkonfiguration begrenzen.

/force

Standardmäßig werden nur geänderte Gruppenrichtlinieneinstellungen aktualisiert. Mit diesem Parameter wird die gesamte Gruppenrichtlinie erneut verarbeitet, unabhängig davon, ob Einstellungen geändert wurden oder nicht.

/wait:Wert

Dieser Parameter steuert die Verfügbarkeit der Kommandozeile während der Verarbeitung der Gruppenrichtlinien. Der Standardwert beträgt 600 Sekunden. Wenn der Wert auf 0 geändert wird, ist die Kommandozeile sofort wieder verfügbar, während die Gruppenrichtlinien im Hintergrund weiterverarbeitet werden. Der Wert -1 bedeutet unbegrenzte Wartezeit, d. h. dass die Kommandozeile erst wieder zur Verfügung steht, wenn die Gruppenrichtlinien vollständig abgearbeitet sind.

/logoff

Manche Gruppenrichtlinien erfordern nach Änderung der Einstellungen ein erneutes Anmelden des Benutzers. Ist dieser Parameter gesetzt, wird bei der Verarbeitung der Gruppenrichtlinien überprüft, ob ein erneutes Anmelden für die korrekte Verarbeitung notwendig ist. Ist das der Fall, wird der Benutzer nach der Verarbeitung der Gruppenrichtlinie automatisch abgemeldet.

/boot

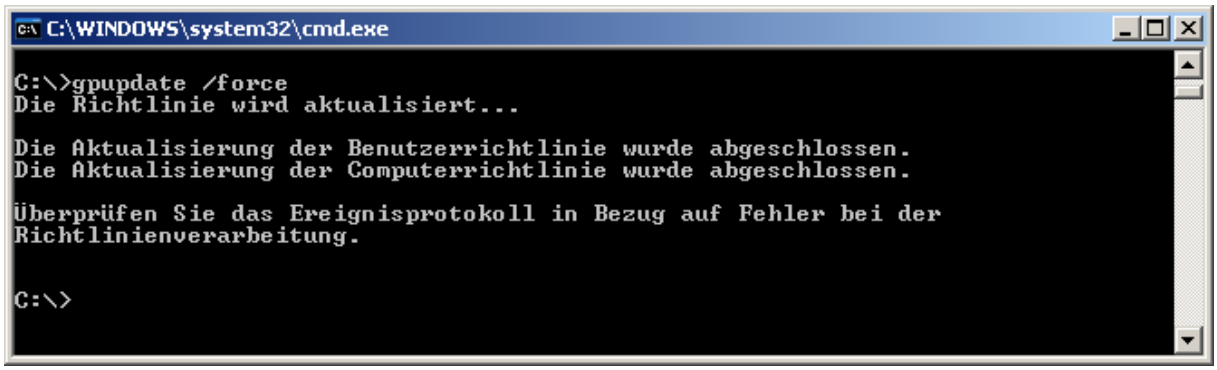
Analog zu dem Parameter /logoff benötigen einige Gruppenrichtlinien nach Änderung der Einstellungen einen Neustart des Computers. Ist dieser Parameter gesetzt, wird ein Computer automatisch neu gestartet, wenn bei der Verarbeitung die Notwendigkeit festgestellt wird.

/?

Mit diesem Schalter kann die Hilfe bzw. Parameterbeschreibung aufgerufen werden.

Gruppenrichtlinien mit `gpupdate` aktualisieren!

1. *Gehen Sie an den Computer, auf dem die Gruppenrichtlinien aktualisiert werden sollen.*
2. *Wählen Sie START-AUSFÜHREN und rufen Sie den Befehlsinterpreter `cmd` auf.*
3. *Aktualisieren Sie **geänderte** Gruppenrichtlinien mit dem Befehl `gpupdate`.*
4. *Aktualisieren Sie die **gesamten** Richtlinien einer Gruppenrichtlinie mit dem Befehl `gpupdate /force`.*
5. *Geben Sie ggf. `gpupdate /?` ein, um sich weitere Informationen über die Syntax des Befehls anzeigen zu lassen.*



Manuelle Aktualisierung der Gruppenrichtlinien mit gpupdate

Warum funktioniert es nicht? Ich habe doch alles richtig gemacht…

Manchmal steht man vor folgendem Problem: Man hat die Gruppenrichtlinien korrekt definiert, die Abarbeitungsreihenfolge genau nachvollzogen und offensichtlich alles richtig gemacht. Und dennoch erhält man nicht das gewünschte Ergebnis. Leider ist die Umsetzung der gewünschten Einstellungen alles andere als vorhersagbar. Hier kann man sich nur wie folgt helfen: den Benutzer mehrfach ab- und wieder anmelden, den Rechner neu starten und Geduld haben.

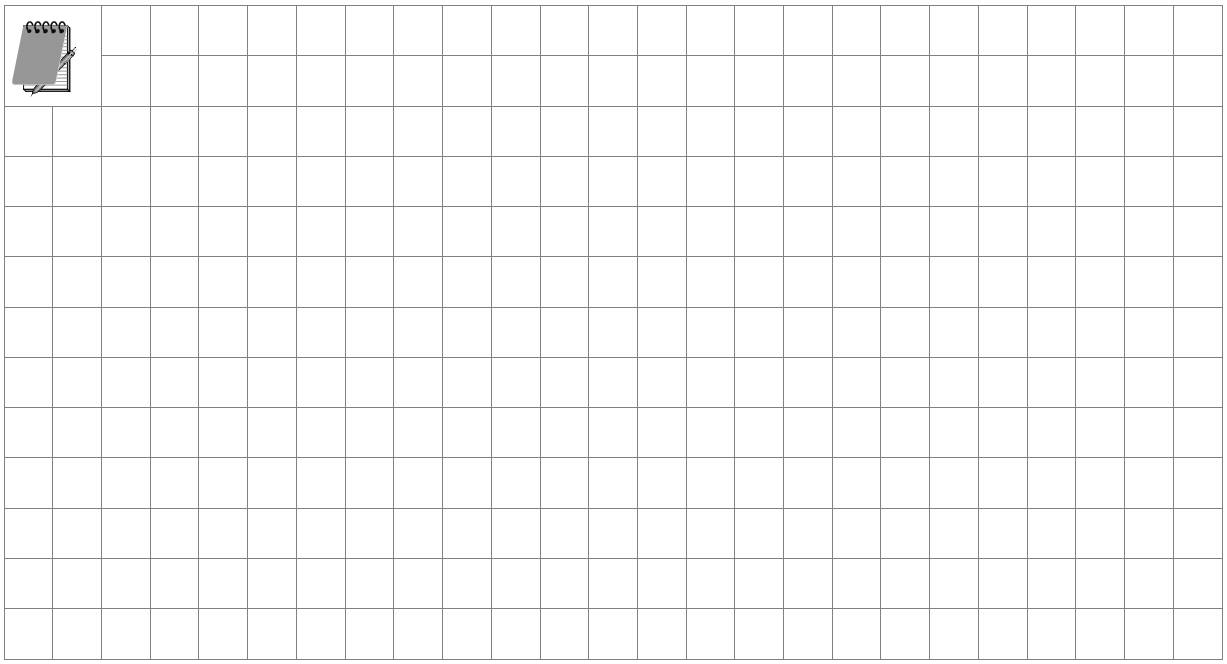
Die Abarbeitung der einzelnen Einstellungen wird nicht durch einen einzelnen Prozess des Betriebssystems durchgeführt. Vielmehr sind ein gutes Dutzend unterschiedlicher Prozesse mit der Umsetzung der Einstellungen beschäftigt, die in manchen Situationen unabhängig voneinander arbeiten. Dies erklärt, warum beispielsweise der Eindruck entstehen kann, dass Gruppenrichtlinien nur unvollständig abgearbeitet werden. Wahrscheinlicher ist, dass einer der notwendigen Prozesse noch arbeitet.

Gruppenrichtlinien für die Computerkonfiguration werden wie beschrieben grundsätzlich nur beim Start des Systems ausgelesen. Aber keine Regel ohne Ausnahme: Microsoft Windows XP bietet die Möglichkeit der „Schnellen Anmeldung“. Hier kann es zu unerwarteten Phänomenen kommen: Man kann sich bereits anmelden, obwohl die Abarbeitung der Gruppenrichtlinien noch nicht abgeschlossen wurde. Dieses in manchen Situationen irritierende Verhalten kann durch die Richtlinie COMPUTERKONFIGURATION/ADMINISTRATIVE VORLAGEN/SYSTEM/ANMELDUNG/BEIM NEUSTART DES COMPUTERS UND BEI DER ANMELDUNG IMMER AUF DAS NETZWERK WARTEN geändert werden.

Einige Einstellungen – gerade die Ordnerumleitungen und die Softwareinstallation – werden nur bei der Anmeldung oder beim Start des Betriebssystems ausgeführt. Eine manuelle Aktualisierung durch gpudate (Windows 2003/XP) oder secedit (Windows 2000) ist hier wirkungslos.

3.4 Sicherheitscheck

- *Beachten Sie, dass die Gruppenrichtlinien nicht auf Gruppenkonten, sondern auf **Benutzer- und Computerkonten** wirken. Einstellungen in dem Knoten Benutzerkonfiguration finden Anwendung auf Benutzerkonten und Einstellungen in dem Knoten Computerkonfiguration finden Anwendung auf Computerkonten.*
- *Es gibt eine **definierte Verarbeitungsreihenfolge** der Gruppenrichtlinien. Zuerst wird die LOKALE GRUPPENRICHTLINIE verarbeitet, danach folgen die Standort-Gruppenrichtlinie, die Domänen-Gruppenrichtlinie und zum Schluss die OE-Gruppenrichtlinien in den unterschiedlichen Hierarchieebenen.*
- *Die strukturelle Unterteilung der Gruppenrichtlinie in Computer- und Benutzerkonfiguration spiegelt sich in der **Verarbeitung der Gruppenrichtlinien** wider. Zuerst werden beim Starten des Computers die Einstellungen der Computerkonfiguration verarbeitet, danach unmittelbar nach dem Anmelden am System die Einstellungen der Benutzerkonfiguration.*
- *Gruppenrichtlinien werden in regelmäßigen Abständen **automatisiert** im Hintergrund **aktualisiert**. Das Aktualisierungsintervall beträgt für Domänencontroller 5 Minuten und für Mitgliedsserver und Clients 90 Minuten mit einem zufälligen Verzögerungsintervall von bis zu 30 Minuten.*
- *Die **Aktualisierungsintervalle** sind als Gruppenrichtlinien implementiert und können geändert werden.*
- *Sie können die Gruppenrichtlinien **manuell** mit den Befehlen secedit (Windows 2000) und gpupdate (Windows 2003/XP) aktualisieren.*



4 Vorbereitung des Active Directory

In diesem Kapitel erfahren Sie,

- welche Rolle die Organisationseinheiten bei dem Einsatz von Gruppenrichtlinien spielen,
- wie Sie die Organisationseinheiten nach unterschiedlichen Merkmalen strukturieren können und
- wie Sie die Struktur der Organisationseinheiten im Active Directory planen, testen und umsetzen können.

4.1 Planung des Active Directory

Das Active Directory stellt für eine Domänenstruktur das zentrale Verwaltungswerkzeug, den Verzeichnisdienst, dar. Alle Objekte einer Domäne werden im Active Directory gespeichert und können durch verschiedene Administrationswerkzeuge verwaltet werden. Das ***backUP***-Magazin Nr. 5 beschäftigt sich ausführlich mit den Verwaltungsaufgaben und –werkzeugen des Active Directory.

Die Basiseinheit für den logischen Aufbau des Active Directory bildet die Domäne. Sie grenzt den Administrations- und Sicherheitsbereich zu anderen Domänen ab. Die Organisationseinheit ist ein weiteres logisches Objekt im Active Directory. Sie stellt ein Containerobjekt dar, das andere Objekte, z. B. Benutzer, Gruppen, Computer oder auch andere Organisationseinheiten aufnehmen kann. Dabei ist die Organisationseinheit fest einer Domäne zugeordnet, d. h. sie kann nur Objekte aus der eigenen Domäne aufnehmen und die Domänengrenze nicht überschreiten.

Die Organisationseinheiten übernehmen wichtige Aufgaben im Active Directory:

- Sie sind ein Hilfsmittel zur internen Strukturierung des Active Directory. Mit ihrer Hilfe lassen sich Organisationen im Active Directory nach unterschiedlichen Modellen, die später in diesem Kapitel vorgestellt werden, hierarchisch strukturieren.
- Organisationseinheiten können eine Administrationsgrenze zu anderen Organisationseinheiten darstellen, indem administrative Aufgaben für eine bestimmte Organisationseinheit an einen bestimmten Benutzer oder Administrator delegiert werden. Die Delegierung administrativer Aufgaben wird im ***backUP***-Magazin Nr. 5 beschrieben.
- Gruppenrichtlinien lassen sich gezielt über Organisationseinheiten zuweisen, sodass sie nur auf ausgewählte Benutzer- und Computerkonten wirken. Diese Thematik soll in diesem Kapitel ausführlich erläutert werden.

Wenn Sie in Ihrer Organisation administrative Aufgaben oder Gruppenrichtlinien einsetzen möchten, dann müssen Sie sich vor der Strukturierung des Active Directory mit den Zielen, die Sie mit dem Einsatz der Gruppenrichtlinien erreichen möchten, auseinandersetzen und die Struktur des Active Directory daraufhin anpassen. Beachten Sie schon bei der Planung, dass die Struktur der Organisationseinheiten, und somit auch die Struktur der eingesetzten Gruppenrichtlinien, übersichtlich bleibt.

4.2 Modelle zur Strukturierung der Organisationseinheiten

Bei der Planung einer hierarchischen Struktur mit Hilfe von Organisationseinheiten (OE-Struktur) sollte darauf geachtet werden, dass sowohl die „funktionellen“ Anforderungen

- interne Strukturierung,
- Delegierung von administrativen Aufgaben und
- Einsatz von Gruppenrichtlinien

als auch die „ergonomischen“ Gesichtpunkte, z. B.

- Übersichtlichkeit,
- eine angemessene Verschachtelung der Organisationseinheiten sowie
- eine damit verbundene Arbeitserleichterung

für den Administrator berücksichtigt werden.

Wird eine OE-Struktur z. B. zu stark zergliedert oder verschachtelt, so kann es unter Umständen schwierig werden, den Organisationseinheiten in dieser Struktur Benutzer- und Computerkonten sinnvoll zuzuordnen bzw. Richtlinieneinstellungen der Gruppenrichtlinien nachzuvollziehen.

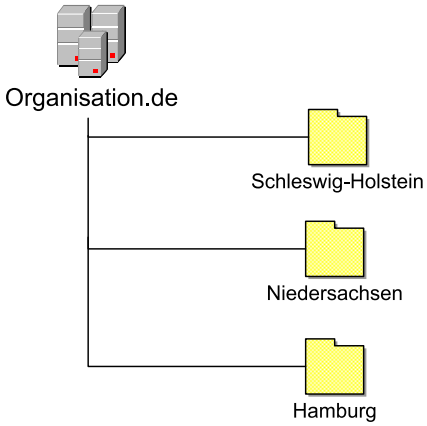
Das Active Directory kann auf Grundlage verschiedener Modelle strukturiert werden. Bei den hier vorgestellten Modellen handelt es sich um drei grundsätzliche Methoden zur Strukturierung:

- Geografisches Modell
- Organisatorisches Modell
- Administratives Modell

Die einzelnen Modelle können für sich alleine die Organisation häufig nicht ausreichend strukturiert darstellen. In diesen Fällen empfiehlt sich eine Mischstruktur.

Geografisches Modell

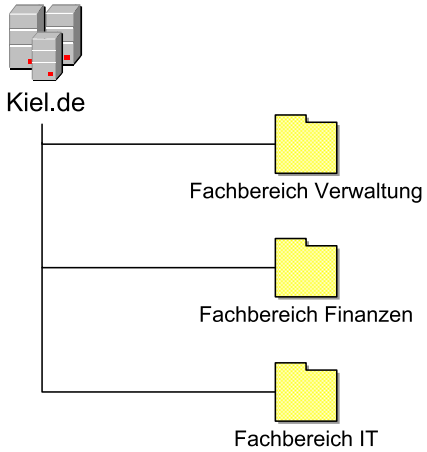
Die Organisationseinheiten können nach den geografischen Standorten der Organisation strukturiert werden.



Dieses Modell kann bei großen Organisationen mit mehreren Standorten oder bei Organisationen mit mehreren Außenstellen sinnvoll sein. Da dieses Modell keinen Überblick über die Organisationsstruktur oder die Arbeitsweise der Administratoren bietet, ist es insbesondere als Grundlage eines Mischmodells einsetzbar.

Organisatorisches Modell

Das organisatorische Modell bietet eine Möglichkeit, die aufbauorganisatorische Struktur und die Arbeitsweise einer Organisation im Active Directory abzubilden.

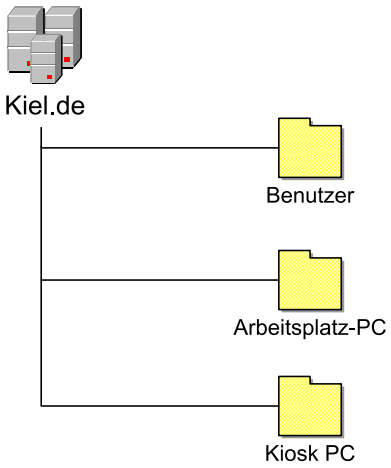


Da sich dieses Modell direkt an die Organisationsstruktur anlehnt und die Arbeitsweise der Organisation widerspiegelt, bietet es einen hohen Grad an Übersichtlichkeit. Gerade für kleinere Organisationen mit festen aufbauorganisatorischen Strukturen ist dieses Modell in seiner

reinen Form ein Mittel der Wahl. Soll zusätzlich die Arbeitsweise der Administratoren berücksichtigt werden, dann kann dieses Modell in Verbindung mit dem administrativen Modell als Mischmodell gewählt werden.

Administratives Modell

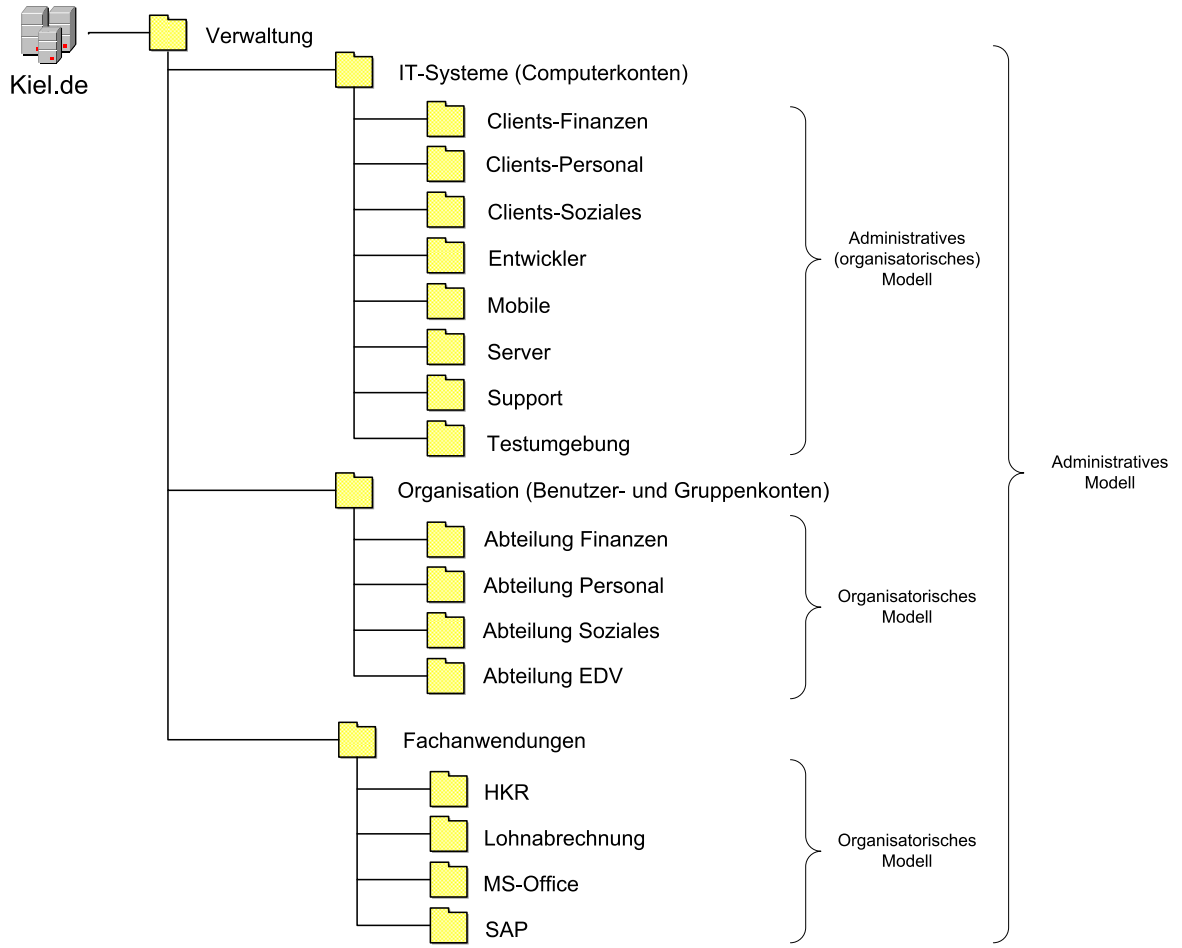
Das administrative Modell strukturiert das Active Directory nach den Active Directory-Objekten und der administrativen Arbeitsweise.



Der Grundgedanke dieses Modells ist es, die Struktur einer Organisation in die administrative Arbeitsweise mit Active Directory-Objekten zu übertragen. Kommt ausschließlich dieses Modell zum Einsatz, entsteht in der Regel eine relativ flache Hierarchie. Dabei wird es problematisch, gezielt Rechte zu vergeben bzw. Gruppenrichtlinien einzusetzen. Der Vorteil dieses Modells - die Berücksichtigung der administrativen Arbeitsweise - kann hingegen gut in Mischmodellen eingesetzt werden.

Mischmodell

In den Mischformen können die Vorteile der unterschiedlichen Modelle kombiniert und auf die Anforderungen einer Organisation angepasst werden. In der Active Directory-Struktur, die in der folgenden Abbildung dargestellt wird, werden beispielsweise das administrative und das organisatorische Modell kombiniert. Dieses Modell wird im Kapitel 10 noch einmal aufgegriffen.

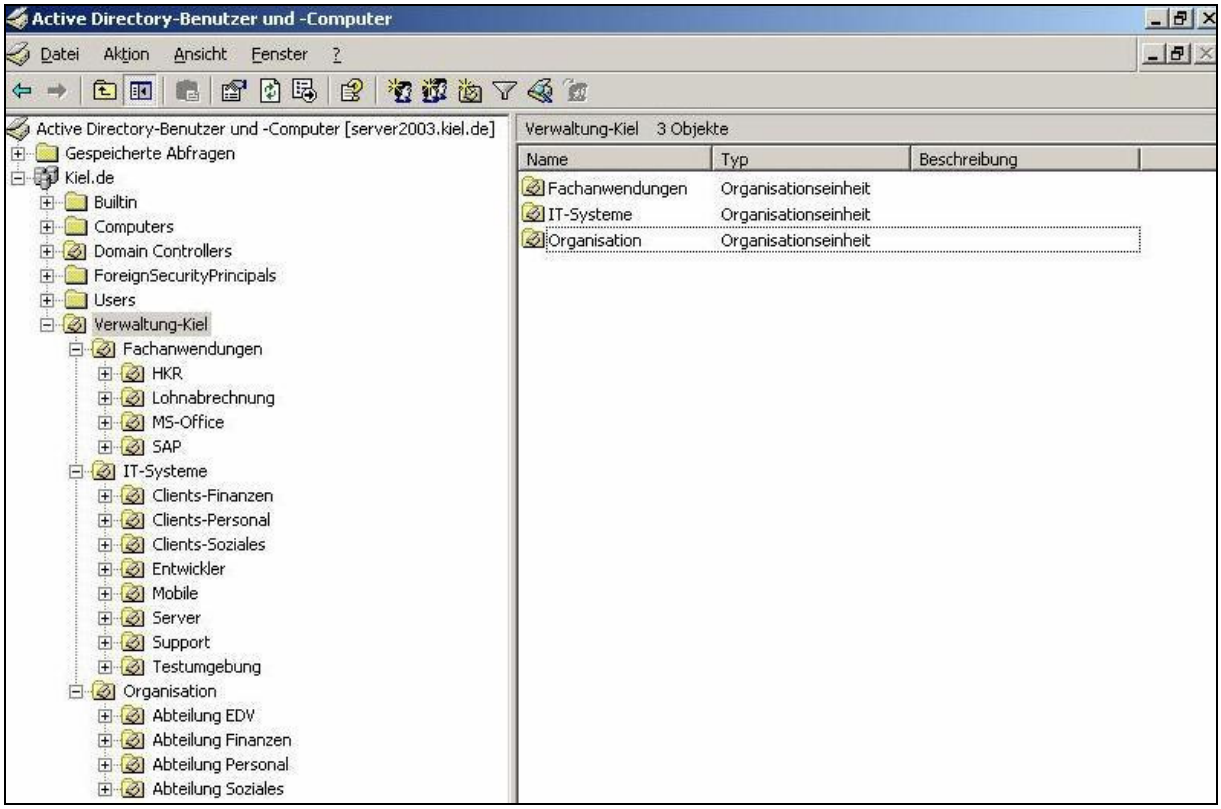


Aus folgenden Überlegungen wurde dieses Mischmodell gewählt:

- Die Organisationseinheit der ersten Ebene VERWALTUNG ist eingerichtet worden, um die Übersichtlichkeit im Active Directory zu gewährleisten (siehe auch Abbildung unten) und um diese Organisationseinheit von den standardmäßig eingerichteten Organisationseinheiten abzugrenzen. Darüber hinaus ist es möglich, schon auf dieser Ebene Gruppenrichtlinien einzusetzen, die dann auf alle Benutzer- und Computerkonten der untergeordneten Organisationseinheiten wirken.
- Die Organisationseinheiten der zweiten Ebene trennen die Computerkonten, die Benutzerkonten sowie die Fachanwendungen nach administrativen Gesichtspunkten. Auf dieser Ebene können nun Gruppenrichtlinien eingesetzt werden, die entsprechend entweder auf alle Computerkonten oder auf alle Benutzerkonten wirken.
- Die Organisationseinheiten der dritten Ebene teilen die Objekte der zweiten Ebene weiter auf und es besteht die Möglichkeit, Gruppenrichtlinien differenziert einzusetzen. So können z. B. auf Computerkonten der Organisationseinheit CLIENTS-FINANZEN andere Gruppenrichtlinien wirken als auf Computerkonten der Organisationseinheit TESTUMGEBUNG.

Die Computerkonten sind in dieser Ebene vorwiegend administrativ zusammengefasst worden, wenngleich die Organisationseinheiten CLIENTS-FINANZEN, CLIENTS-PERSONAL und CLIENTS-SOZIALES auch einen Bezug zur Organisationsstruktur haben.

- Die Organisationseinheiten unterhalb der Organisationseinheit FACHANWENDUNGEN spiegeln einen Teil der Arbeitsweise der Organisation wider und sind organisatorisch strukturiert worden. In diesem Beispiel ist diese Strukturierung nicht primär für die Zuweisung für Gruppenrichtlinien erstellt worden, sondern stellt ein vereinfachtes Konzept für die Zuweisung von NTFS-Berechtigungen[4]dar.



Active Directory-Design

Sie sollten darauf achten, dass Sie in Ihrer Active Directory-Struktur nicht zu viele Hierarchieebenen erstellen. Ansonsten droht die Gefahr, dass Ihnen genau die Übersichtlichkeit verloren geht, die Sie mit der Active Directory-Strukturierung eigentlich erreichen wollten. Sie sollten bei der Strukturierung Ihres Active Directory nicht mehr als 3 bis 4 Hierarchieebenen planen.

[4] NTFS-Berechtigungen werden im backUP-Magazin Nr.5 ausführlich beschrieben.

4.3 Planung und Umsetzung einer Active Directory-Struktur

Active Directory-Strukturen werden in jeder Organisation anders aussehen, je nachdem, welche Anforderungen diese Organisation an

- die Strukturierung,
- die Vergabe von administrativen Rechten und
- den Einsatz von Gruppenrichtlinien

stellt. Um diese Anforderungen bestmöglich umzusetzen, sollte vor allem der konzeptionelle Prozess der Planung nicht vernachlässigt werden. Es kostet weniger Energie, eine Active Directory-Struktur sorgfältig zu planen als eine schlecht konzipierte Struktur nachträglich zu ändern.

Zunächst sollte anhand der vorgestellten Modelle überprüft werden, welche Active Directory-Struktur die Anforderungen der Organisation in Bezug auf den Einsatz von Gruppenrichtlinien erfüllen kann. In dem oben dargestellten Beispiel (Mischmodell) sind z. B. folgende Anforderungen gestellt worden:

- Computerkonten und Benutzerkonten sollen administrativ getrennt werden. Das geschieht durch die Aufsplittung in die Organisationseinheiten IT-SYSTEME und ORGANISATION.
- Auf bestimmte Computer- und Benutzerkonten sollen je nach Einsatzbereich bzw. Aufgabengebiet unterschiedliche Gruppenrichtlinien wirken, daher wird eine weitere Ebene von Organisationseinheiten erstellt, die die Computer- und Benutzerkonten in weitere Verwaltungseinheiten aufteilt, z. B. Computerkonten der Abteilungen FINANZEN, PERSONAL und SOZIALES.

Mit der Festlegung auf eine Active Directory-Strukturierung ist ein wesentlicher Grundstein zur Vorbereitung auf den Einsatz der Gruppenrichtlinien gelegt worden.

Im zweiten Schritt geht es nun darum, dieses Modell mit systematisch geplanten Gruppenrichtlinien zu füllen. Dabei sollten zunächst folgende Überlegungen berücksichtigt werden:

- Welche Sicherheitsfunktionalitäten sollen mit Hilfe von Gruppenrichtlinien bereitgestellt bzw. welche Einschränkungen sollen umgesetzt werden?
- Auf welcher Ebene des erstellten Modells sollen die Sicherheitsfunktionalitäten umgesetzt werden?
- Sollen die Sicherheitsfunktionalitäten für Computer- oder Benutzerkonten gelten?
- Wie viele Einstellungen sollten in einer Gruppenrichtlinie vorgenommen werden, sodass die Übersichtlichkeit gewährleistet ist?

- Welche Namenskonvention sollte für die Bezeichnung der Gruppenrichtlinien gewählt werden?

Am Ende dieses Konzeptionsschrittes wird ein detailliertes Konzept zum Einsatz der Gruppenrichtlinien im Active Directory entstanden sein.

Abschließend sollten dann noch die Besonderheiten und Ausnahmen, die beim Arbeiten mit den Gruppenrichtlinien beachtet werden müssen, in das Konzept mit einfließen, z. B:

- Einige Richtlinien müssen zwingend in bestimmten Gruppenrichtlinien auf bestimmten Ebenen (z. B. Domäne, Standard-Organisationseinheiten) aktiviert werden, damit sie umgesetzt werden.
- Die Reihenfolge der Verarbeitung der Gruppenrichtlinien lässt sich beeinflussen. So können Gruppenrichtlinien deaktiviert, Vererbungen erzwungen bzw. unterbrochen oder die Anwendung der Gruppenrichtlinien gefiltert werden.
- Es können Berechtigungen auf Gruppenrichtlinien vergeben werden, die ebenfalls die Verarbeitung der Gruppenrichtlinien beeinflussen.

Diese Besonderheiten werden in den nächsten Kapiteln detaillierter dargestellt.

Konzeption der Active Directory-Struktur zum Einsatz von Gruppenrichtlinien!

1. *Schauen Sie sich die Gruppenrichtlinien an, Sie sind das Material, mit dem Sie arbeiten können.*
2. *Entwerfen Sie eine Active Directory-Struktur, die sowohl Ihren Organisationsaufbau und –ablauf als auch den Einsatz der Gruppenrichtlinien berücksichtigt (geografische, organisatorische und administrative Gesichtspunkte).*
3. *Legen Sie fest, welche Gruppenrichtlinien mit welchen Einstellungen auf welcher Ebene verarbeitet werden sollen.*
4. *Berücksichtigen Sie getrennte Gruppenrichtlinien für Computer und Benutzer.*
5. *Überlegen Sie, welche Richtlinien Sie in einer Gruppenrichtlinie aktivieren möchten. Berücksichtigen Sie, dass Sie pro Gruppenrichtlinie gezielt die Richtlinien aktivieren, die einen bestimmten Zweck erfüllen sollen.*
6. *Verwenden Sie für jede Gruppenrichtlinie einen aussagekräftigen Namen, sodass bereits über den Namen erkennbar ist, welches Sicherheitsziel die Gruppenrichtlinie erreichen soll, z. B. Softwareeinschränkung, Internetbeschränkung.*
7. *Berücksichtigen Sie, dass einige Richtlinien nur in bestimmten Gruppenrichtlinien auf bestimmten Ebenen umgesetzt werden.*
8. *Überlegen Sie, ob Sie Ausnahmen bei der Verarbeitungsreihenfolge der*

Gruppenrichtlinien realisieren oder die Anwendung von Gruppenrichtlinien filtern müssen.

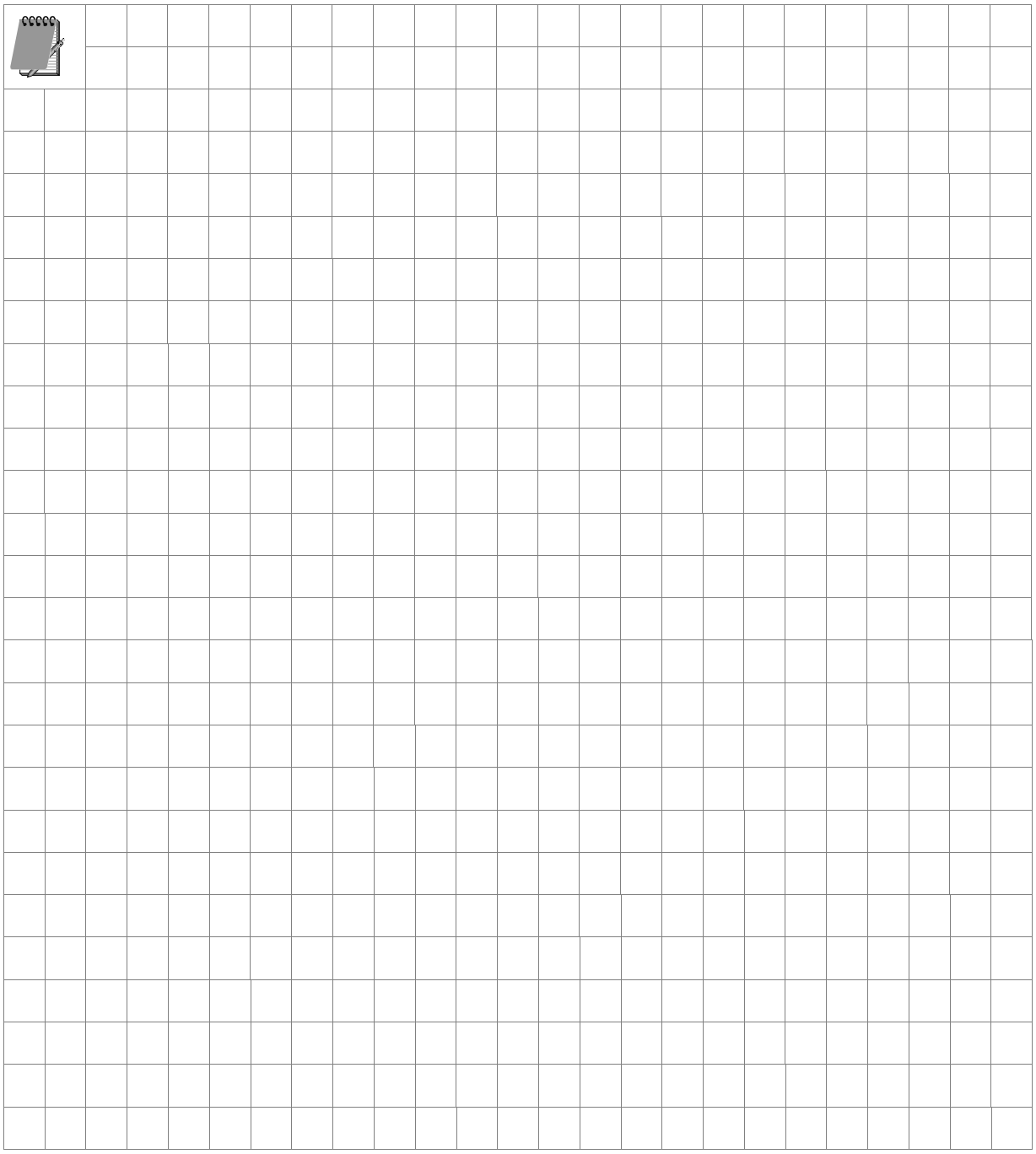
Umsetzung der geplanten Active Directory-Struktur!

1. *Am besten überprüfen Sie Ihr Konzept, indem Sie die nachfolgenden Schritte zunächst an einem Testsystem durchführen, bevor Sie es in den Echtbetrieb übernehmen.*
2. *Legen Sie entsprechend dem erarbeiteten Konzept die Organisationseinheiten im Active Directory an.*
3. *Erstellen Sie in den (bzw. verschieben Sie in die) Organisationseinheiten die geplanten Computer- oder Benutzerkonten.*
4. *Legen Sie die Gruppenrichtlinien entsprechend Ihrem Konzept an, aktivieren Sie die geplanten Richtlinien und verknüpfen diese mit den vorgesehenen Organisationseinheiten.*
5. *Setzen Sie eventuelle spezielle Anforderungen in Bezug auf die Verarbeitungsreihenfolge oder die Filterung von Gruppenrichtlinien um.*
6. *Prüfen Sie die Einstellungen der Richtlinien in ihrem Testsystem sorgfältig, indem Sie sich an einer oder mehreren Arbeitsstationen mit mehreren Benutzerkonten (auf die unterschiedliche Gruppenrichtlinien wirken) anmelden.*

4.4 Sicherheitscheck

- *Beachten Sie, dass Sie für einen **Einsatz der Gruppenrichtlinien** im Active Directory entsprechende Strukturen schaffen.*
- *Verwenden Sie Organisationseinheiten als Objekte **zum logischen Aufbau** des Active Directory.*
- *Sie können Organisationseinheiten verschachteln und so eine **hierarchische Struktur** im Active Directory aufbauen.*
- *Wählen Sie für die Strukturierung des Active Directory ein **geografisches, organisatorisches oder administratives** Modell. Wenn sich die Anforderungen Ihrer Organisation nicht in einem dieser Modelle darstellen lassen, dann kombinieren Sie sie zu einem Mischmodell, das Ihre Anforderungen am besten abbildet.*
- *Der Entwurf einer Active Directory-Struktur sollte eine **hohe Priorität** in Ihrer Konzeption zum Einsatz von Gruppenrichtlinien einnehmen.*
- *Legen Sie fest, welche **Sicherheitsanforderungen** in Ihrer Organisation mit Hilfe von Gruppenrichtlinien umgesetzt werden sollen.*
- *Planen Sie, welche **Gruppenrichtlinien** auf welchen Ebenen und mit welchen Einstellungen auf die Computer- und Benutzerkonten wirken sollen.*

- *Legen Sie für unterschiedliche Sicherheitsanforderungen jeweils gesonderte Gruppenrichtlinien an. Verwenden Sie für die Gruppenrichtlinien **aussagekräftige Namen**, die erkennen lassen, welches Sicherheitsziel die Gruppenrichtlinien erreichen sollen.*
- ***Überprüfen** Sie Ihr Konzept sorgfältig, bevor Sie es in den Echtbetrieb übernehmen. Benutzen Sie dazu am besten Testsysteme.*



5 Gruppenrichtlinien verwalten

In diesem Kapitel erfahren Sie,

- wie im Active Directory Gruppenrichtlinien erstellt, verknüpft und gelöscht werden können,
- wie sich mehrere Gruppenrichtlinien mit einer Organisationseinheit verknüpfen lassen und was eine Änderung der Verknüpfungsreihenfolge bewirkt,
- was bei der Vererbung von Gruppenrichtlinien zu beachten ist und wie die Vererbung beeinflusst werden kann,
- wie sich Gruppenrichtlinien filtern lassen und
- welche Möglichkeit besteht, auch ohne die Gruppenrichtlinien-Verwaltungskonsole eine gute Übersichtlichkeit im Active Directory zu erreichen.

5.1 Gruppenrichtlinien erstellen, verknüpfen und löschen

In den ersten Kapiteln dieses ***backUP***-Magazins ist allgemein der Begriff Gruppenrichtlinie verwendet worden. Es ist tatsächlich so, dass umgangssprachlich und z. T. auch in der Literatur ausschließlich von Gruppenrichtlinien gesprochen wird. Auch in diesem ***backUP***-Magazin wird weiterhin mit dem Begriff Gruppenrichtlinie gearbeitet. Systemtechnisch betrachtet ist eine Gruppenrichtlinie jedoch ein Active Directory-Objekt und wird als Gruppenrichtlinien-Objekt (Group Policy Objekt, GPO) bezeichnet. Nähere Informationen zu dem strukturellen Aufbau von Gruppenrichtlinien-Objekten und der Speicherung der unterschiedlichen Komponenten im System werden im Kapitel 9 beschrieben.

Sollen Gruppenrichtlinien zur zentralen Bereitstellung von Konfigurations- und/oder Sicherheitseinstellungen eingesetzt werden, sind folgende Voraussetzungen zu berücksichtigen:

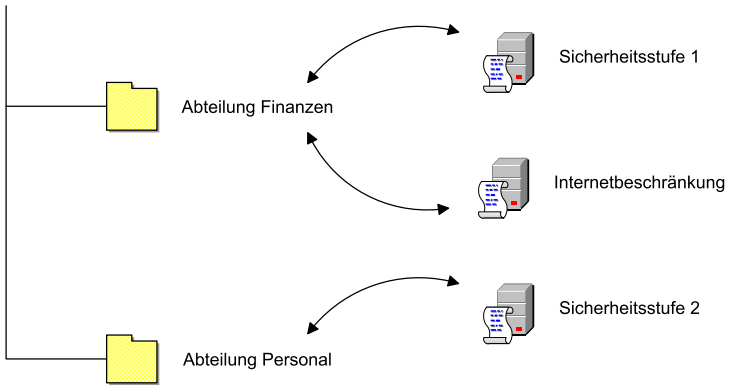
1. Es muss ein Gruppenrichtlinien-Objekt vorhanden sein, in dem die notwendigen Einstellungen in den entsprechenden Richtlinien vorgenommen werden können,
2. dieses Gruppenrichtlinien-Objekt muss mit einer Verwaltungseinheit (Standort, Domäne oder Organisationseinheit) verknüpft werden und
3. in dieser Verwaltungseinheit müssen sich auch die entsprechenden Computer- und Benutzerobjekte befinden, auf die diese Einstellungen wirken sollen.

Eine Gruppenrichtlinie wirkt also nicht direkt auf Computer- oder Benutzerkonten, sondern immer nur über eine Verknüpfung. Das hat den Vorteil, dass nicht nur eine Gruppenrichtlinie mit einer Verwaltungseinheit verknüpft werden kann, sondern auch mehrere, die in einer de-

finierten Reihenfolge nacheinander abgearbeitet werden. Diese Reihenfolge kann administrativ beeinflusst werden.

Im Beispiel unten sind drei Gruppenrichtlinien-Objekte erstellt worden, SICHERHEITSSTUFE 1, SICHERHEITSSTUFE 2 und INTERNETBESCHRÄNKUNG. Solange diese Objekte mit keiner Verwaltungseinheit verknüpft sind, haben die in ihr vorgenommenen Einstellungen keine Auswirkungen. In diesem Beispiel wurden die Gruppenrichtlinien folgendermaßen verknüpft:

- Die Gruppenrichtlinie SICHERHEITSSTUFE 1 ist mit der Organisationseinheit ABTEILUNG FINANZEN verknüpft worden. Die Einstellungen dieser Gruppenrichtlinie wirken auf die entsprechenden Objekte in dieser Organisationseinheit.
- Die Gruppenrichtlinie INTERNETBESCHRÄNKUNG ist ebenfalls mit der Organisationseinheit ABTEILUNG FINANZEN verknüpft worden. Die Einstellungen dieser Gruppenrichtlinie wirken somit auch auf die entsprechenden Objekte in dieser Organisationseinheit.
- Die Gruppenrichtlinie SICHERHEITSSTUFE 2 ist mit der Organisationseinheit ABTEILUNG PERSONAL verknüpft worden. Die Einstellungen dieser Gruppenrichtlinie wirken auf die entsprechenden Objekte in dieser Organisationseinheit. Die Einstellungen der Gruppenrichtlinien SICHERHEITSSTUFE 1 und INTERNETBESCHRÄNKUNG haben keinen Einfluss auf die Objekte in dieser Organisationseinheit.



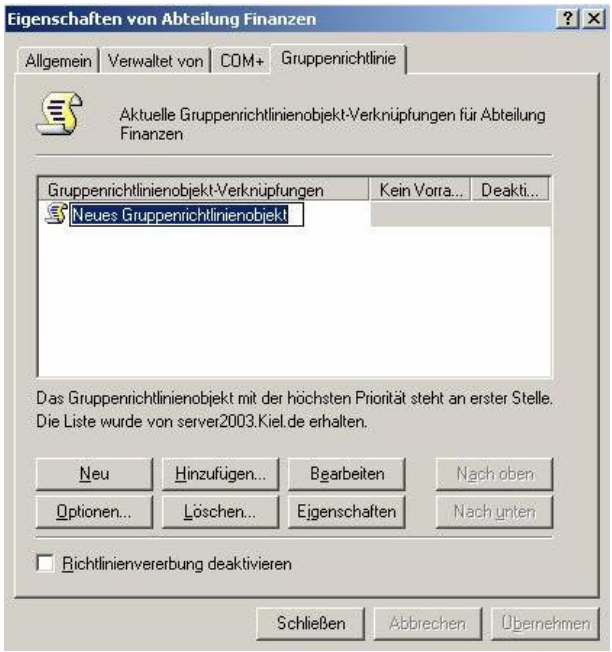
Sollen in diesem Beispiel die Einstellungen der Gruppenrichtlinie INTERNETBESCHRÄNKUNG auch auf die Objekte in der ABTEILUNG PERSONAL wirken, dann müsste die Gruppenrichtlinie INTERNETBESCHRÄNKUNG auch mit dieser Organisationseinheit verknüpft werden.

Die Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) ermöglicht eine übersichtlichere Verwaltung der Gruppenrichtlinien. In diesem Kapitel wird die Gruppenrichtlinien-Verwaltung ohne die Gruppenrichtlinien-Verwaltungskonsole erläutert. Das darauf folgende Kapitel beschäftigt sich dann ausführlich mit den Möglichkeiten, die die Gruppenrichtlinien-Verwaltungskonsole bietet.

Die Funktionalitäten zum Erstellen, Verknüpfen und Löschen von Gruppenrichtlinien werden über die Eigenschaften eines Standortes, einer Domäne oder einer Organisationseinheit aufgerufen (siehe auch Kapitel 2.5).

Gruppenrichtlinien erstellen (Schaltfläche NEU)

Standardmäßig werden beim Einrichten des Active Directory nur Gruppenrichtlinien für die Domäne *(Default Domain Policy)* und für den Domänencontroller *(Default Domain Controller Policy)* implementiert. Alle weiteren Gruppenrichtlinien müssen explizit erstellt werden.



Neue Gruppenrichtlinie erstellen

Eine neue Gruppenrichtlinie für eine Organisationseinheit erstellen!

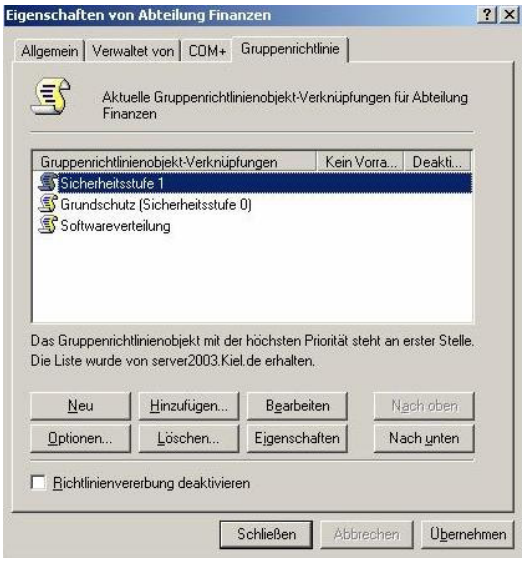
1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*

2. *Markieren Sie die Organisationseinheit, für die Sie eine neue Gruppenrichtlinie einrichten möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Klicken Sie auf die Schaltfläche NEU, um eine neue Gruppenrichtlinie zu erstellen und wählen Sie einen aussagekräftigen Namen.*
4. *In einer neu erstellten Gruppenrichtlinie sind standardmäßig keine Richtlinien aktiviert.*

Wenn Sie nach diesem Verfahren Gruppenrichtlinien erstellen, werden zwei Schritte im Hintergrund abgearbeitet. Es wird sowohl eine neue Gruppenrichtlinie als auch eine Verknüpfung mit der entsprechenden Organisationseinheit erstellt. Beide Komponenten sind notwendig, damit Einstellungen auf Benutzer und Computer angewendet werden können.

Die erstellte Gruppenrichtlinie ist aber nicht untrennbar mit der Organisationseinheit verbunden. Sie wird als Active Directory-Objekt sowohl im Active Directory als auch in dem Verzeichnis SYSVOL gespeichert und steht nur über die Verknüpfung mit der Organisationseinheit in Verbindung.

Es können auch mehrere Gruppenrichtlinien in einer Organisationseinheit erstellt werden. Dieses Verfahren bietet sich an, wenn, wie im Kapitel 3 und 4 beschrieben, die Gruppenrichtlinien modular geplant und eingesetzt werden sollen. Die erstellten Gruppenrichtlinien werden nacheinander (die zuletzt angelegte an unterster Stelle) in dem Feld Gruppenrichtlinienobjekt-Verknüpfungen aufgelistet und unterliegen einer definierten Vererbungsreihenfolge, die im Kapitel 5.2 näher erläutert wird.



Erstellung mehrerer Gruppenrichtlinien in einer Organisationseinheit

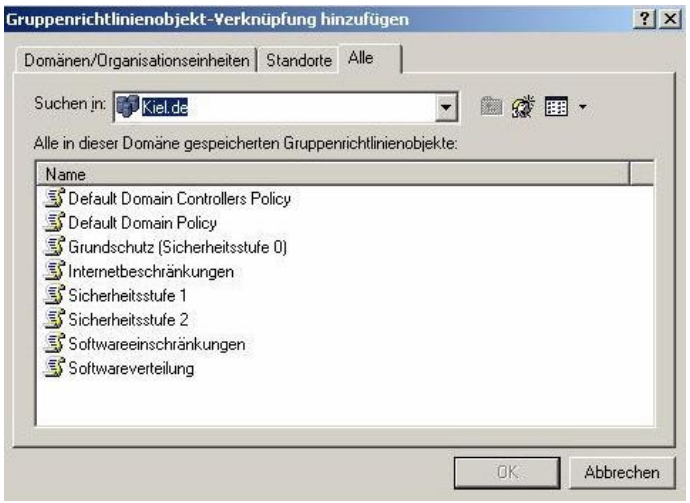
Gruppenrichtlinien verknüpfen (Schaltfläche HINZUFÜGEN)

Damit die Einstellungen der Gruppenrichtlinien auf Benutzer und Computer angewendet werden können, wird, wie oben schon erwähnt, sowohl die Gruppenrichtlinie als Active Directory-Objekt als auch die Verknüpfung zu einem Verwaltungsbereich im Active Directory (Standort, Domäne oder Organisationseinheit) benötigt.

Bei einer Verknüpfung wird auf eine schon bestehende Gruppenrichtlinie zurückgegriffen und nur die Verknüpfung an sich neu erstellt.

Eine Gruppenrichtlinie mit einer Organisationseinheit verknüpfen!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*
2. *Markieren Sie die Organisationseinheit, mit der Sie eine Gruppenrichtlinie verknüpfen möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Klicken Sie auf die Schaltfläche HINZUFÜGEN. Es öffnet sich ein Fenster, auf dem alle in der Domäne vorhandenen Gruppenrichtlinien aufgelistet sind.*
4. *Wählen Sie die entsprechende Gruppenrichtlinie und bestätigen Sie die Auswahl mit OK.*
5. *Die Gruppenrichtlinie ist nun mit allen Richtlinieneinstellungen der entsprechenden Organisationseinheit zugewiesen.*



Liste aller erstellten Gruppenrichtlinien

Es können auch mehrere Gruppenrichtlinien mit der Organisationseinheit verknüpft werden.

Die verknüpften Gruppenrichtlinien werden nacheinander (die zuletzt verknüpfte an unterster Stelle) in dem Feld Gruppenrichtlinienobjekt-Verknüpfungen aufgelistet und unterliegen einer definierten Vererbungsreihenfolge, die im Kapitel 5.2 näher erläutert wird.

Auch wenn eine Gruppenrichtlinie mit z. B. mehreren Organisationseinheiten verknüpft wird und sich in Bezug auf ihre Vererbung unterschiedlich verhalten kann, bleiben die Einstellungen in der Gruppenrichtlinie immer gleich. Das Verhalten der Gruppenrichtlinie wird als Status der Verknüpfung gespeichert (siehe grauer Kasten).

Status einer Verknüpfung

Die Verknüpfung stellt ein Active Directory-Attribut eines entsprechenden Verwaltungsbereichs (Standort, Domäne oder Organisationseinheit) dar. Dieses Active Directory-Attribut speichert sowohl den Pfad zu der entsprechenden Gruppenrichtlinie als auch den Status der Verknüpfung.

Status:	Bedeutung:
0	Kein besonderer Status aktiviert
1	Deaktiviert
2	Kein Vorrang
3	Deaktiviert und Kein Vorrang

Der Status der Verknüpfung ist wesentlich daran beteiligt, wie sich die Verknüpfung in Bezug auf die Vererbung verhält. Da nur der Status der Verknüpfung das Vererbungsverhalten definiert, kann eine Gruppenrichtlinie z. B. mit zwei unterschiedlichen Organisationseinheiten verknüpft werden und sich bei der einen Organisationseinheit in Bezug auf die Vererbung anders verhalten als bei der zweiten Organisationseinheit. Damit ist eine größtmögliche Flexibilität gegeben.

Die Bedeutung der unterschiedlichen Status wird im Kapitel 5.3 aufgegriffen.

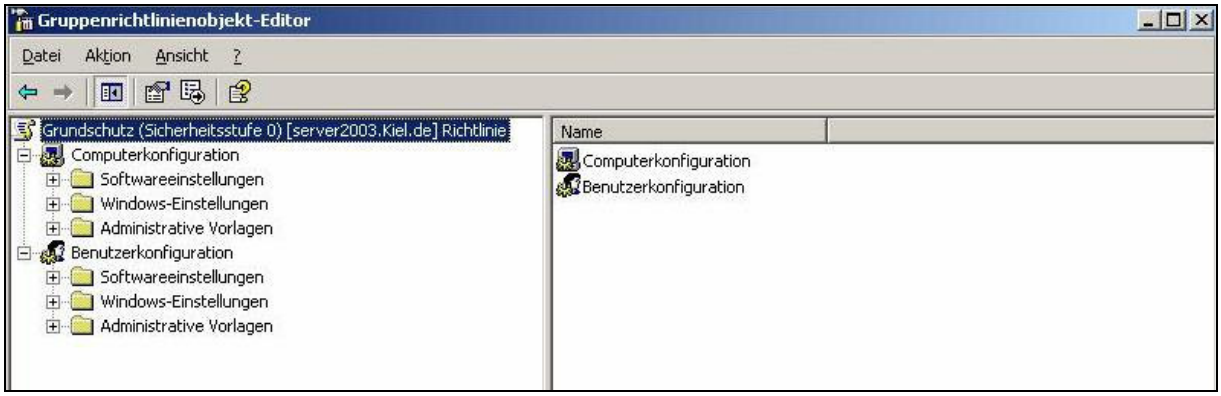
Gruppenrichtlinien bearbeiten (Schaltfläche BEARBEITEN)

Einstellungen in einer Gruppenrichtlinie können über den Gruppenrichtlinien-Editor vorgenommen oder verändert werden.

Eine Gruppenrichtlinie bearbeiten!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*

2. *Markieren Sie die Organisationseinheit, in der Sie eine Gruppenrichtlinie bearbeiten möchten, mit der rechten Maustaste und wählen Sie* EIGENSCHAFTEN *und danach die Registerkarte* GRUPPENRICHTLINIE.
3. *Klicken Sie auf die Schaltfläche* BEARBEITEN. *Es öffnet sich der Gruppenrichtlinien-Editor, in dem Sie Einstellungen oder Änderungen in den Richtlinien vornehmen können.*

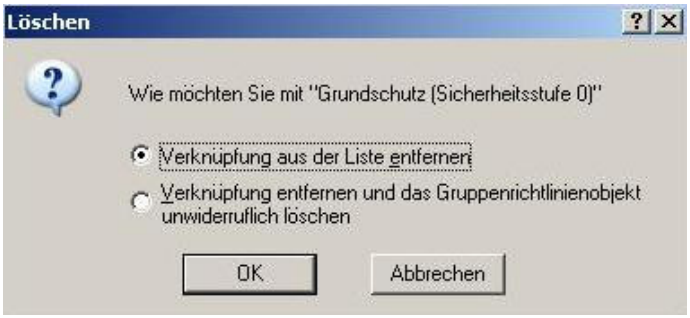


Gruppenrichtlinien-Editor

Nur die Titelzeile des Gruppenrichtlinien-Editors gibt einen Hinweis darauf, in welcher Gruppenrichtlinie Sie sich befinden, z. B. in der Gruppenrichtlinie GRUNDSCHUTZ *in der Abbildung oben. Sie sollten sich, bevor Sie Einstellungen in den Richtlinien vornehmen, immer vergewissern, dass Sie sich in der richtigen Gruppenrichtlinie befinden. Ansonsten besteht die Gefahr, dass Sie Einstellungen in einer „falschen" Gruppenrichtlinie vornehmen.*

Gruppenrichtlinien löschen (Schaltfläche LÖSCHEN)

Soll eine Gruppenrichtlinie z. B nicht mehr. auf eine bestimmte Organisationseinheit wirken, dann kann die Verknüpfung zwischen Gruppenrichtlinie und Organisationseinheit gelöscht werden. Die Gruppenrichtlinie an sich bleibt dabei mit allen Einstellungen erhalten. Weiterhin besteht die Möglichkeit, die Gruppenrichtlinie (als Active Directory-Objekt) inklusive aller Einstellungen und Verknüpfungen zu löschen.



Löschoptionen

Eine Gruppenrichtlinie oder eine Verknüpfung löschen!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*
2. *Markieren Sie die Organisationseinheit, in der Sie eine Gruppenrichtlinie oder eine Verknüpfung löschen möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Klicken Sie auf die Schaltfläche LÖSCHEN. Es öffnet sich ein Fenster, auf dem Sie zwischen zwei Löschungsoptionen wählen können.*
4. *Wählen Sie VERKNÜPFUNG AUS DER LISTE ENTFERNEN, um die Verknüpfung zwischen der Gruppenrichtlinie und der Organisationseinheit zu löschen.*
5. *Wählen SIE VERKNÜPFUNG ENTFERNEN UND DAS GRUPPENRICHTLINIENOBJEKT UNWIDERRUFLICH LÖSCHEN, wenn Sie sowohl die Gruppenrichtlinie als auch **alle** Verknüpfungen zu dieser Gruppenrichtlinie löschen möchten.*

Da Gruppenrichtlinien Registrierungseinträge auf dem Client verändern, kann es in Einzelfällen vorkommen, dass bei einer Löschung einer Gruppenrichtlinie nicht alle Registrierungseinstellungen wieder zurückgestellt werden. Das kann zur Folge haben, dass auch nach der Löschung der Gruppenrichtlinie noch Registrierungseinträge aktiv bleiben.

Deshalb sollten Sie vor dem Löschen einer Gruppenrichtlinie die vorgenommenen Einstellungen wieder rückgängig machen und die Gruppenrichtlinie danach auf die entsprechenden Benutzer- und Computerkonten erneut anwenden. Erst danach sollten Sie die Gruppenrichtlinie löschen.

Eine andere Möglichkeit besteht darin, alle Verknüpfungen zu der entsprechenden Gruppenrichtlinie zu löschen und die Gruppenrichtlinie zu deaktivieren (siehe Unterpunkt DEAKTIVIERT in diesem Kapitel).

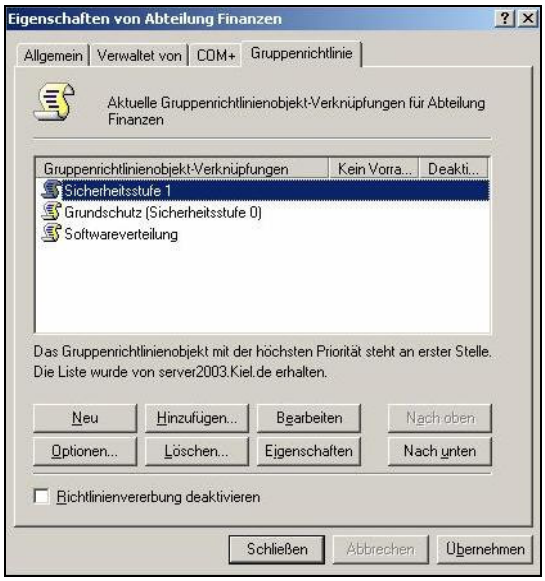
5.2 Vererbung von Gruppenrichtlinien

Wie in den vorangegangenen Kapiteln dargestellt, gibt es zahlreiche Möglichkeiten, im Active Directory mit Hilfe von Organisationseinheiten hierarchische Strukturen zu schaffen und auf diesen unterschiedlichen Hierarchieebenen mehrere Gruppenrichtlinien zu verknüpfen, die dann auf die Objekte der jeweiligen Organisationseinheiten einwirken. Damit diese Gruppenrichtlinien abweichend von der standardmäßigen Verarbeitungsreihenfolge (vgl. Kapitel 3.2) genau so wirken, wie sie gemäß der Planung wirken sollen, gibt es für den Administrator mehrere Möglichkeiten, die Verarbeitungs- und damit die Vererbungsreihenfolge zu beeinflussen und auf den eigenen Bedarf anzupassen.

Verarbeitungsreihenfolge ändern (Schaltflächen NACH OBEN/NACH UNTEN)

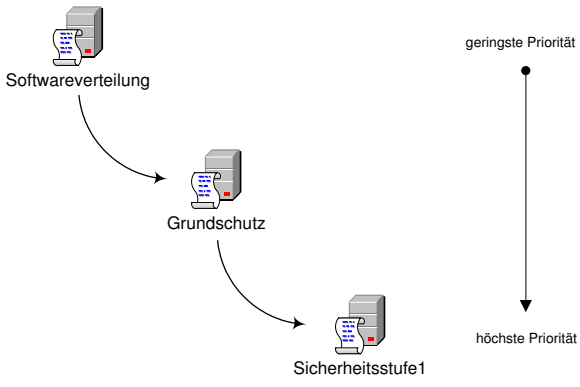
Bei der Verknüpfung von mehreren Gruppenrichtlinien mit einer Organisationseinheit werden die verknüpften Gruppenrichtlinien nacheinander (die zuletzt verknüpfte an unterster Stelle) in dem Feld Gruppenrichtlinienobjekt-Verknüpfungen aufgelistet (siehe Abbildung unten). Beachtet werden muss an dieser Stelle, dass die Gruppenrichtlinie mit der höchsten Priorität an oberster Stelle dieser Liste steht, in diesem Fall die Gruppenrichtlinie SICHERHEITSSTUFE 1.

Was bedeutet das für die Verarbeitung der Gruppenrichtlinien? In diesem Fall wird zunächst die Gruppenrichtlinie SOFTWAREVERTEILUNG verarbeitet, gefolgt von den Gruppenrichtlinien GRUNDSCHUTZ und SICHERHEITSSTUFE 1. Dabei ist zu beachten, dass eine Gruppenrichtlinie mit höherer Priorität (z. B. SICHERHEITSSTUFE 1) eine Gruppenrichtlinie mit geringerer Priorität (z. B. GRUNDSCHUTZ) überschreiben kann.



Verarbeitungsreihenfolge

Reihenfolge der Verarbeitung:

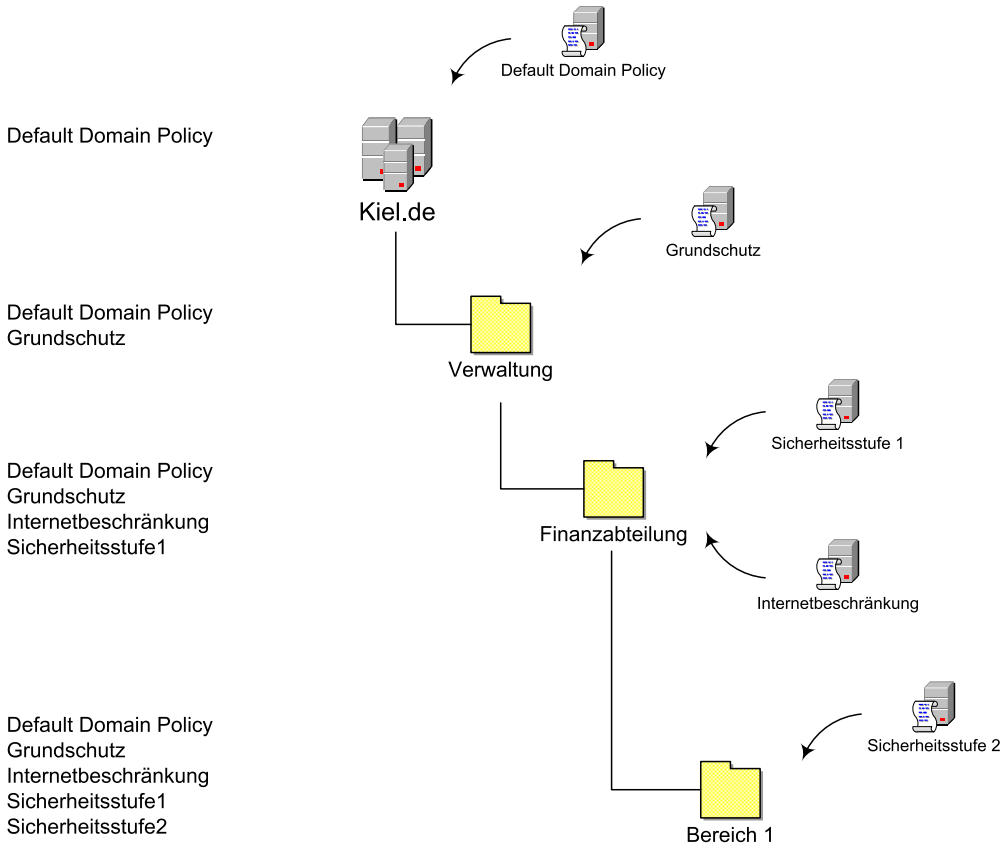


Die Verarbeitungsreihenfolge der Gruppenrichtlinien innerhalb einer Organisationseinheit ändern!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*
2. *Markieren Sie die Organisationseinheit, in der Sie die Verarbeitungsreihenfolge ändern möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Markieren Sie die Gruppenrichtlinie, deren Priorität Sie verändern möchten und wählen Sie die Schaltfläche NACH OBEN oder NACH UNTEN, um die Gruppenrichtlinie innerhalb der Liste nach oben oder unten zu verschieben.*

5.3 Vererbung - Optionen und Eigenschaften

Weitere Verfahren zur Beeinflussung der Abarbeitungs- und Vererbungsreihenfolge können über die Schaltflächen OPTIONEN und EIGENSCHAFTEN der jeweiligen Gruppenrichtlinien aufgerufen werden. Die Grundlage bei der Betrachtung der unterschiedlichen Möglichkeiten soll das unten stehende Beispiel darstellen.



Das Active Directory ist mit Hilfe von Organisationseinheiten in drei Hierarchieebenen strukturiert worden:

1. Ebene VERWALTUNG
2. Ebene FINANZABTEILUNG
3. Ebene BEREICH 1

Sowohl auf der Domänenebene als auch auf den unterschiedlichen Hierarchieebenen werden Gruppenrichtlinien eingesetzt, deren aktivierten Computer- und Benutzerrichtlinien Einfluss auf die Benutzer- und Computerkonten der einzelnen Organisationseinheiten nehmen.

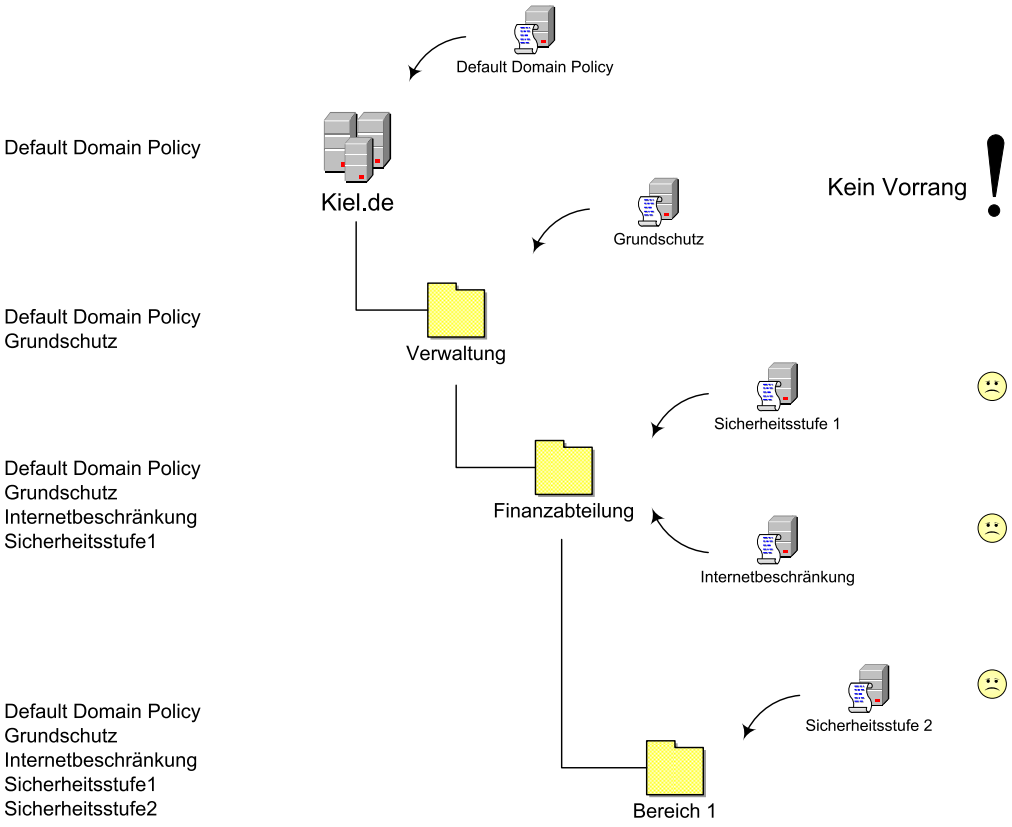
Für einen Benutzer (oder Computer) in der Organisationseinheit BEREICH 1 werden die Gruppenrichtlinien in folgender Reihenfolge verarbeitet:

- *Default Domain Policy*
- GRUNDSCHUTZ
- INTERNETBESCHRÄNKUNG (da diese Gruppenrichtlinie die niedrigste Priorität innerhalb der Organisationseinheit Finanzabteilung einnimmt)
- SICHERHEITSSTUFE 1 (da diese Gruppenrichtlinie die höchste Priorität innerhalb der Organisationseinheit Finanzabteilung einnimmt)
- SICHERHEITSSTUFE 2

Auf der linken Seite der Abbildung oben wird darstellt, welche Gruppenrichtlinien auf welcher Ebene verarbeitet werden. In den nachfolgenden Beispielen wird auf der rechten Seite der Abbildung symbolisch die administrative Maßnahme und zum Teil auch die mögliche Auswirkung auf die Verarbeitungsreihenfolge bzw. Vererbung abgebildet.

Kein Vorrang (Schaltfläche OPTIONEN)

Mit der Option KEIN VORRANG kann die Verarbeitung einer Gruppenrichtlinie erzwungen werden, d. h. diejenigen Richtlinien, die in einer mit KEIN VORRANG markierten Gruppenrichtlinie aktiviert wurden, können von den Richtlinien nachfolgender Gruppenrichtlinien nicht überschrieben bzw. geändert werden.



In diesem Beispiel können die aktivierten Richtlinien in der Gruppenrichtlinie GRUNDSCHUTZ nicht durch Richtlinien nachfolgender Gruppenrichtlinien z. B. in den Organisationseinheiten FINANZABTEILUNG oder BEREICH 1 geändert werden.

Die Option KEIN VORRANG kann (wie in diesem Beispiel) eingesetzt werden, wenn bestimmte aktivierte Richtlinien einer Gruppenrichtlinie als Grundsicherheitseinstellung für alle Computer- bzw. Benutzerkonten einer Organisation gelten sollen.

Ein pfiffiger Administrator könnte auf die Idee kommen, eine Gruppenrichtlinie, die von der höchsten Hierarchie mit der Option KEIN VORRANG erzwungen werden soll, mit einer weiteren Option RICHTLINIENVERERBUNG DEAKTIVIEREN (die nachfolgend beschrieben wird) zu blockieren.

Doch diese Rechnung geht nicht auf: Die Option KEIN VORRANG kann durch keine andere Option nachfolgender Gruppenrichtlinien beeinflusst werden.

Verknüpfungsoptionen

Die Option KEIN VORRANG auf eine Gruppenrichtlinie anwenden!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*
2. *Markieren Sie die Organisationseinheit, in der Sie die Verarbeitungsreihenfolge ändern möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Wählen Sie die Schaltfläche OPTIONEN und aktivieren Sie das Kontrollkästchen KEIN VORRANG.*
4. *Die Gruppenrichtlinie wird im Eigenschaftenfenster der Organisationseinheit mit der Option KEIN VORRANG gekennzeichnet (siehe Abbildung unten).*

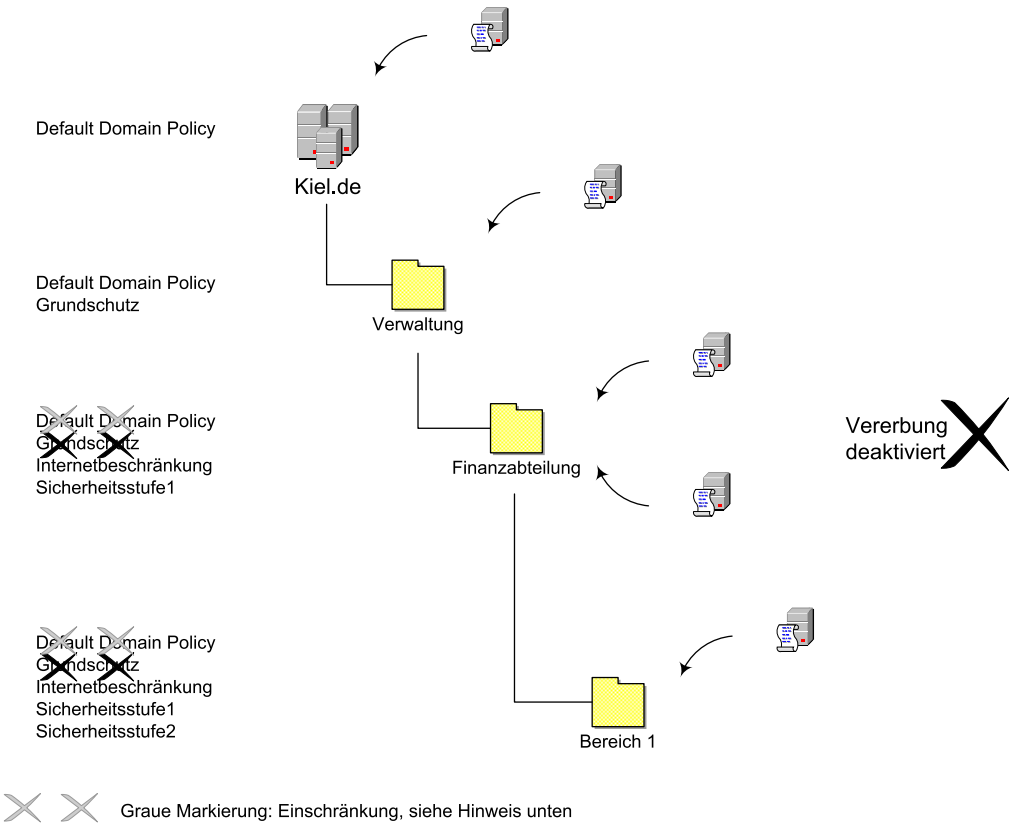
Aktivierte Option KEIN VORRANG

Bei der Option KEIN VORRANG handelt es sich um eine Verknüpfungsoption (vgl. auch grauer Kasten im Kapitel 5.1), d. h., die Option ist nicht mit der Gruppenrichtlinie sondern mit der Verknüpfung verbunden.

Eine Gruppenrichtlinie kann z. B. mit zwei unterschiedlichen Organisationseinheiten verknüpft werden, die in der Hierarchieebene einander nicht untergeordnet sind. Eine Verknüpfung kann mit der Option KEIN VORRANG versehen sein, die andere verhält sich standardmäßig. Beide Verknüpfungen zu der gleichen Gruppenrichtlinie verhalten sich demnach in Bezug auf die Vererbung anders.

Richtlinienvererbung deaktivieren

Die Deaktivierung bzw. Blockierung der Vererbung kann als Gegenstück zur Option KEIN VORRANG angesehen werden. Eine Gruppenrichtlinie mit der Option KEIN VORRANG erzwingt die Vererbung der aktivierten Richtlinien während eine Gruppenrichtlinie mit einer deaktivierten Vererbung verhindert, dass die Richtlinien von den übergeordneten Gruppenrichtlinien an die untergeordneten Gruppenrichtlinien weitergereicht werden.



Wird die Deaktivierung der Vererbung in diesem Fall für die Organisationseinheit FINANZABTEILUNG gewählt, so werden die Richtlinien der übergeordneten Gruppenrichtlinien DEFAULT DOMAIN POLICY (Ausnahme siehe Hinweis unten) und GRUNDSCHUTZ nicht auf die Organisationseinheit FINANZABTEILUNG (und allen ihr untergeordneten Organisationseinheiten) vererbt.

Die Verarbeitung der aktivierten Richtlinien der DEFAULT DOMAIN POLICY können von untergeordneten Gruppenrichtlinien mit der Option VERERBUNG DEAKTIVIEREN nicht vollständig verhindert werden. So wirken die Kontorichtlinien in dem Knoten Computerkonfiguration auch dann, wenn die Vererbung von untergeordneten Gruppenrichtlinien blockiert wird.

Werden in der DEFAULT DOMAIN POLICY allerdings Einstellungen in der Benutzerkonfiguration vorgenommen, die z. B. das Startmenü oder die Desktopoberfläche einschränken, dann können diese Einstellungen durch die Deaktivierung der Vererbung von untergeordneten Gruppenrichtlinien geblockt werden. Soll das verhindert werden, so muss die Option KEIN VORRANG der DEFAULT DOMAIN POLICY aktiviert werden.

Bei der Deaktivierung der Vererbung muss beachtet werden, dass sie alle übergeordneten Gruppenrichtlinien betrifft. Es besteht keine Möglichkeit, eine Auswahl vorzunehmen bzw. die Vererbung einzelner Gruppenrichtlinien zu deaktivieren.

Es mag Situationen geben, in denen es sinnvoll ist, die Richtlinienvererbung zu deaktivieren. Sie sollten die Werkzeuge zur Veränderung der Vererbung sparsam einsetzen und genau analysieren, welche erwünschten oder unerwünschten Wechselwirkungen in dieser Konstellation auftreten können (siehe Hinweis unten). Testen Sie Ihre Einstellungen in einem Testsystem, bevor Sie sie im Produktivsystem einsetzen!

Der Einsatz der Werkzeuge zur Veränderung der Vererbung können weiter reichende Wirkungen haben als gedacht. Das zeigt folgendes Beispiel:

Auch wenn in dem Beispiel oben die Organisationseinheit FINANZABTEILUNG eine aktivierte Verknüpfung zu der Gruppenrichtlinie GRUNDSCHUTZ hätte, würden die Einstellungen dieser Gruppenrichtlinie keinen Einfluss auf die Benutzer- und Computerkonten dieser Organisationseinheit nehmen. Erst wenn die Gruppenrichtlinie GRUNDSCHUTZ nicht mehr mit einer übergeordneten Organisationseinheit verknüpft ist oder wenn die Deaktivierung der Vererbung in der Organisationseinheit FINANZABTEILUNG aufgehoben wird, könnten die Einstellungen der Gruppenrichtlinie GRUNDSCHUTZ auf die Organisationseinheit FINANZABTEILUNG wieder Einfluss auf die Benutzer- und Computerkonten nehmen.

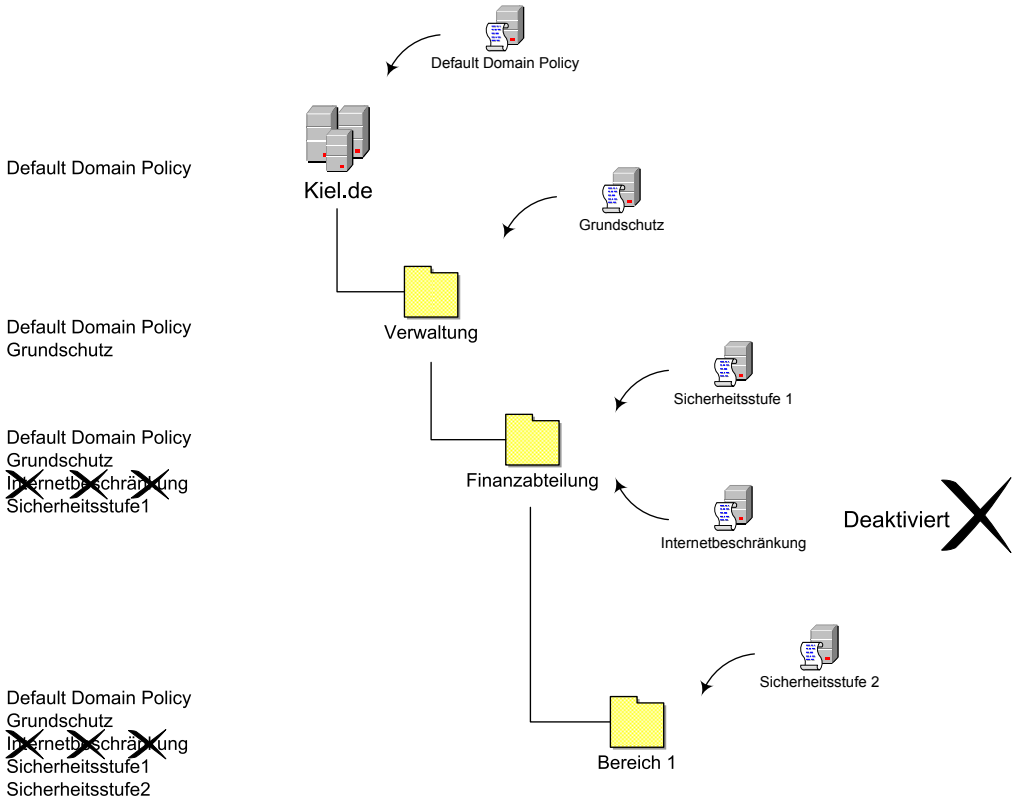
Richtlinienvererbung deaktivieren

RICHTLINIENVERERBUNG DEAKTIVIEREN auf eine Gruppenrichtlinie anwenden!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*
2. *Markieren Sie die Organisationseinheit, in der Sie die Verarbeitungsreihenfolge ändern möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Aktivieren Sie das Kontrollkästchen RICHTLINIENVERERBUNG DEAKTIVIEREN und bestätigen Sie mit ÜBERNEHMEN oder OK.*

Deaktiviert (Schaltfläche OPTIONEN)

Eine weitere administrative Einflussmaßnahme auf das Vererbungsverhalten von Gruppenrichtlinien stellt die Option DEAKTIVIERT dar. Sie bietet die Möglichkeit, eine Gruppenrichtlinie in einer bestimmten Organisationseinheit (und in den ihr untergeordneten Organisationseinheiten) zu deaktivieren und so die Verarbeitung der aktivierten Richtlinien auf die Benutzer- und Computerkonten zu unterbinden.



Wird im Beispiel oben die Gruppenrichtlinie INTERNETBESCHRÄNKUNG in der Organisationseinheit FINANZABTEILUNG deaktiviert, so wirken die aktivierten Richtlinien dieser Gruppenrichtlinie nicht auf die Benutzer- und Computerkonten dieser und ihr untergeordneten Organisationseinheiten.

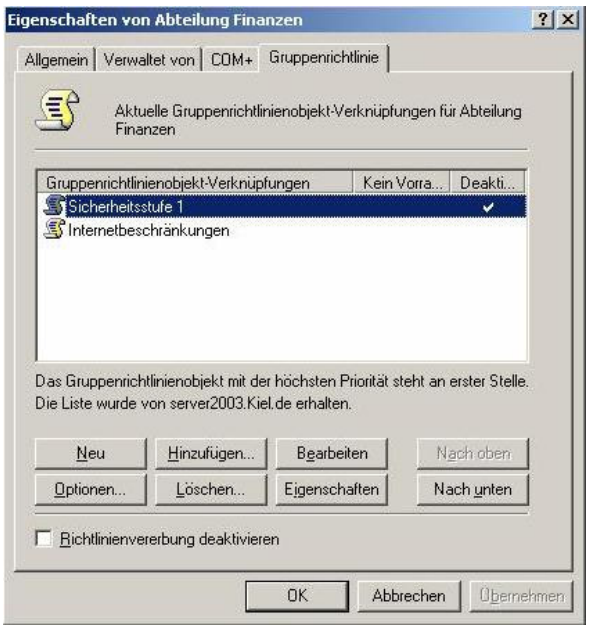
Denkbare Einsatzszenarien für die Option DEAKTIVIERT:

Sie können eine Gruppenrichtlinie deaktivieren, bevor Sie sie unwiderruflich löschen. So können Sie testen, ob durch den Wegfall der Gruppenrichtlinie unerwünschte Wechselwirkungen oder Nebeneffekte auftreten. Oder Sie deaktivieren eine Gruppenrichtlinie, um bestimmte Einstellungen temporär außer Kraft zu setzen.

Die Option DEAKTIVIERT auf eine Gruppenrichtlinie anwenden!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*

2. *Markieren Sie die Organisationseinheit, in der Sie die Verarbeitungsreihenfolge ändern möchten, mit der rechten Maustaste und wählen Sie* EIGENSCHAFTEN *und danach die Registerkarte* GRUPPENRICHTLINIE.
3. *Wählen Sie die Schaltfläche* OPTIONEN *und aktivieren Sie das Kontrollkästchen* DEAKTIVIERT.
4. *Die Deaktivierung wird im Eigenschaftenfenster der Organisationseinheit als deaktiviert gekennzeichnet (siehe Abbildung unten).*



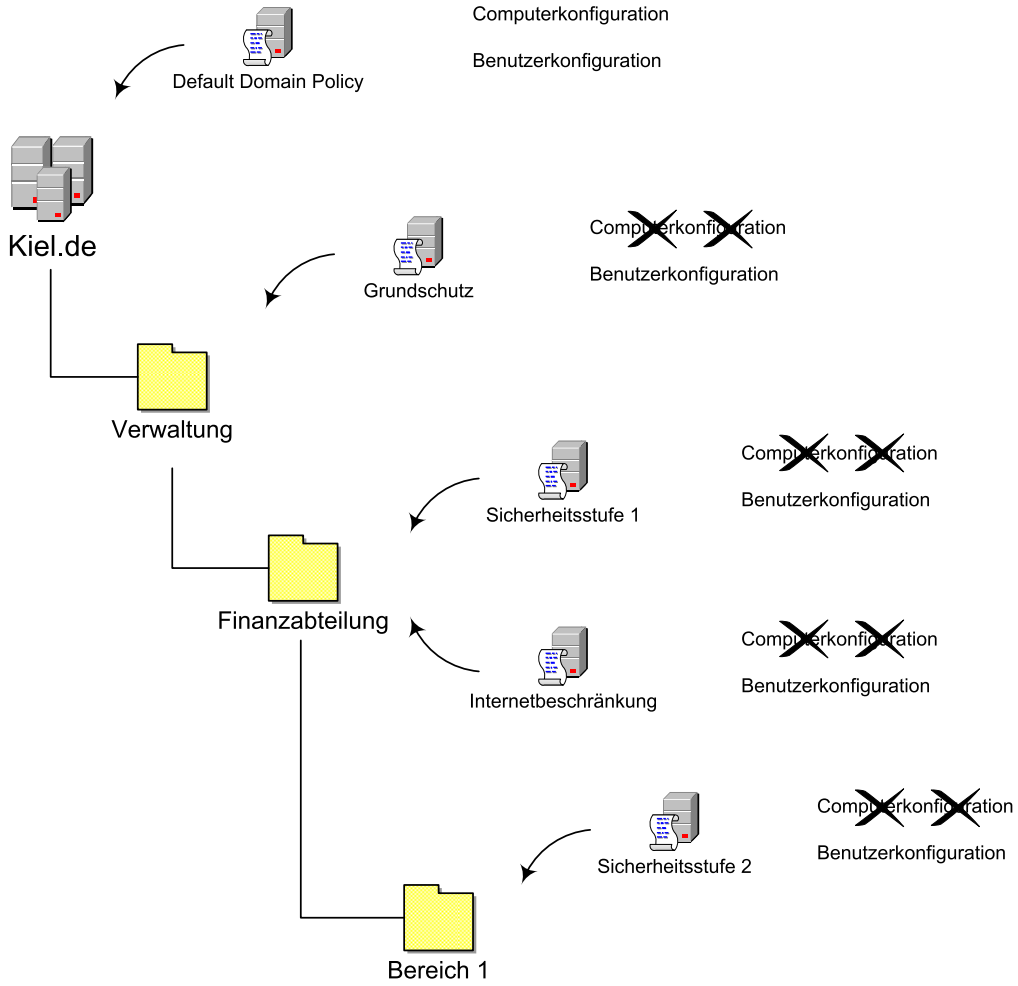
Deaktivierte Gruppenrichtlinie

Bei der Option DEAKTIVIERT *handelt es sich um eine Verknüpfungsoption (vgl. auch grauer Kasten im Kapitel 5.1), d. h., die Option ist nicht mit der Gruppenrichtlinie sondern mit der Verknüpfung verbunden.*

Eine Gruppenrichtlinie kann z. B. mit zwei unterschiedlichen Organisationseinheiten verknüpft werden, die in der Hierarchieebene einander nicht untergeordnet sind. Eine Verknüpfung kann mit der Option DEAKTIVIERT *versehen sein, die andere verhält sich standardmäßig. Beide Verknüpfungen zu der gleichen Gruppenrichtlinie verhalten sich demnach in Bezug auf die Vererbung anders.*

Deaktivierung von Gruppenrichtlinienkomponenten (Schaltfläche EIGENSCHAFTEN)

Das Kapitel 4 dieses ***backUP***-Magazins beschreibt die Strukturierung des Active Directory und den darauf abgestimmten Einsatz der Gruppenrichtlinien. Ein wichtiges Ergebnis dieses Kapitels ist u. a. die getrennte Erstellung von Gruppenrichtlinien für Benutzer- und Computerkonten.



Startet ein Benutzer seinen Computer und meldet sich danach an, werden alle Gruppenrichtlinien verarbeitet, die im Verwaltungsbereich des entsprechenden Computer- und Benutzerkontos liegen. Grundsätzlich werden dabei alle Richtlinien, unabhängig davon, ob Einstellungen in diesen Richtlinien vorgenommen wurden oder nicht, sowohl in der Computer- als auch in der Benutzerkonfiguration ausgelesen. Je nach Anzahl der eingesetzten Gruppenrichtlinien kann sich daher der Start- und Anmeldevorgang für den Benutzer zeitlich deutlich erhöhen. Zur Verminderung der Verarbeitungsgeschwindigkeit beim Start- und Anmeldevorgang sollte nur der jeweils genutzte Bereich (Computer- oder Benutzerkonfiguration) aktiviert bleiben und der jeweils ungenutzte Bereich deaktiviert werden.

In diesem Beispiel sind in den Gruppenrichtlinien GRUNDSCHUTZ, SICHERHEITSSTUFE 1, SICHERHEITSSTUFE 2 und INTERNETBESCHRÄNKUNGEN nur Einstellungen in den Richtlinien des Bereichs Benutzerkonfiguration vorgenommen worden. Daher wurde in diesen Gruppenrichtlinien der ungenutzte Bereich der Computerkonfiguration deaktiviert.

Deaktivierung von Gruppenrichtlinienkomponenten

Einzelne Gruppenrichtlinienkomponenten deaktivieren!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm Active Directory-Benutzer und -Computer auf.*
2. *Markieren Sie die Organisationseinheit, in der Sie die Verarbeitungsreihenfolge ändern möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Wählen Sie die Schaltfläche EIGENSCHAFTEN und aktivieren Sie auf der Registerkarte ALLGEMEIN das Kontrollkästchen KONFIGURATIONSEINSTELLUNGEN DES COMPUTERS DEAKTIVIEREN oder BENUTZERDEFINIERTE KONFIGURATIONSEINSTELLUNGEN DEAKTIVIEREN und bestätigen Sie mit OK.*
4. *Die Deaktivierung der Gruppenrichtlinienkomponente wird im Eigenschaftenfenster der Organisationseinheit mit einem Symbol als deaktiviert gekennzeichnet (siehe folgende Abbildung).*

Deaktivierte Gruppenrichtlinienkomponente

Bei der Deaktivierung von Gruppenrichtlinienkomponenten handelt es sich nicht um eine Verknüpfungsoption. Das bedeutet: Die Deaktivierung von Gruppenrichtlinienkomponenten bezieht sich immer auf die Gruppenrichtlinie an sich und wirkt sich auf alle Verknüpfungen aus.

Ist eine Gruppenrichtlinie mit z. B. zwei Organisationseinheiten verknüpft, dann kann nicht bei der einen Verknüpfung sowohl Benutzer- als auch Computerkonfiguration aktiviert sein und bei der anderen Verknüpfung die Computerkonfiguration deaktiviert werden.

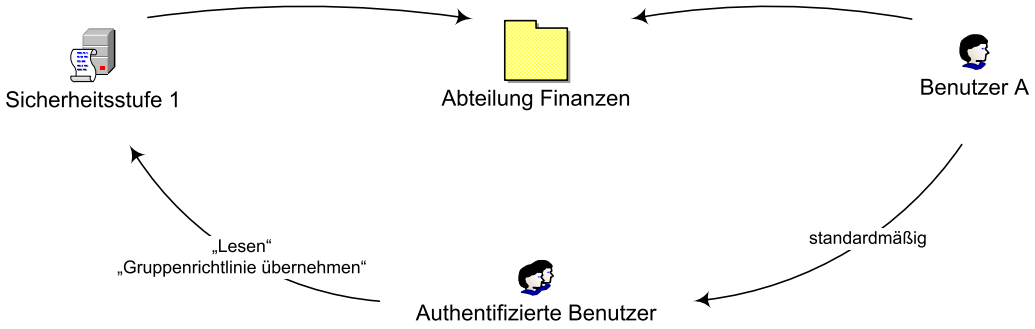
5.4 Filterung

Nachdem sich das Thema Vererbung mit der standardmäßigen Verarbeitungsreihenfolge der Gruppenrichtlinien befasst hat, werden in diesem Abschnitt die Werkzeuge vorgestellt, die dieses Standardverhalten verändern können.

Gruppenrichtlinien finden Anwendung auf die Benutzer- und Computerkonten, die innerhalb des Verwaltungsbereichs (Standort, Domäne, Organisationseinheit) liegen, mit der die Gruppenrichtlinie verknüpft ist. Diese Aussage besitzt auch weiterhin Gültigkeit. In diesem Abschnitt werden die Möglichkeiten beschrieben, wie einzelne Objekte (Benutzer, Computer) von der Verarbeitung der Gruppenrichtlinien ausgenommen werden können.

Sicherheitsfilterung

Mit der Sicherheitsfilterung ist es möglich, Benutzer- und Computerkonten von der Anwendung einer Gruppenrichtlinie auszuschließen. Jede Gruppenrichtlinie ist ein Active Directory-Objekt. Damit Benutzer- und Computerkonten auf Active Directory-Objekte und somit auch auf die Gruppenrichtlinien zugreifen können, benötigen sie grundsätzlich spezielle Berechtigungen auf diese Objekte. Mit den Active Directory-Berechtigungen LESEN und GRUPPENRICHTLINIE ÜBERNEHMEN können die Gruppenrichtlinien von Benutzer- und Computerkonten verarbeitet werden. Besitzt z. B. ein Benutzerkonto diese Berechtigungen nicht, dann wird die entsprechende Gruppenrichtlinie von der Verarbeitung für dieses Konto ausgenommen.

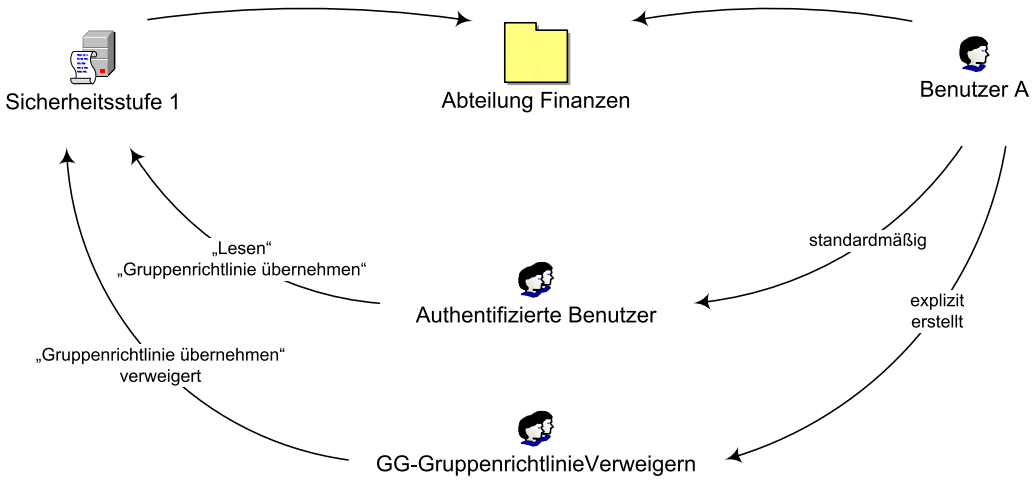


Im Beispiel oben ist das Benutzerkonto des Benutzers A der Verwaltungseinheit ABTEILUNG FINANZEN zugeordnet und die Gruppenrichtlinie SICHERHEITSSTUFE 1 ist mit dieser Verwaltungseinheit verknüpft. Betrachtet man die standardmäßigen Berechtigungen für den BENUTZER A auf diese Gruppenrichtlinie, dann stellt sich die Rechtevergabe wie folgt dar:

- Grundsätzlich wird jedes Benutzerkonto einer Domäne, einschließlich der administrativen Benutzerkonten, in die Gruppe AUTHENTIFIZIERTE BENUTZER aufgenommen. Dieser Gruppe sind die Berechtigungen LESEN und GRUPPENRICHTLINIE ÜBERNEHMEN zugewiesen. Somit kann die Gruppenrichtlinie verarbeitet werden und die aktivierten Richtlinien dieser Gruppenrichtlinie wirken auf das Benutzerkonto A.
- Wenn das Benutzerkonto A noch Mitglied in einer administrativen Gruppe wäre, z. B. in der Gruppe ADMINISTRATOREN, DOMÄNEN- oder ORGANISATIONSADMINISTRATOREN, dann würden dem Benutzerkonto über diese Gruppenmitgliedschaften noch zusätzliche Berechtigungen zugewiesen werden, um diese Gruppenrichtlinie verwalten zu können. Standardmäßig erhalten die Gruppen DOMÄNEN- und ORGANISATIONSADMINISTRATOREN die Berechtigungen LESEN, SCHREIBEN, ALLE UNTERGEORDNETEN OBJEKTE ERSTELLEN und ALLE UNTERGEORDNETEN OBJEKTE LÖSCHEN.

Soll nun für alle Benutzerkonten in der Organisationseinheit ABTEILUNG FINANZEN die Gruppenrichtlinie SICHERHEITSSTUFE 1 verarbeitet werden und nur für das Benutzerkonto A nicht, dann kann die Verarbeitung der Gruppenrichtlinie z. B. nach folgender Methode verweigert werden:

- Es wird eine zusätzliche Sicherheitsgruppe z. B. GG-GRUPPENRICHTLINIEVERWEIGERN eingerichtet und das Benutzerkonto A dieser Sicherheitsgruppe zugeordnet.
- Dieser Gruppe wird die Berechtigung GRUPPENRICHTLINIE ÜBERNEHMEN verweigert. Damit wird diese Berechtigung, die das Benutzerkonto A durch die Gruppe AUTHENTIFIZIERTE BENUTZER vorher erhalten hat, explizit verweigert. Die Berechtigung VERWEIGERN[5] überschreibt evtl. vorher vergebene positive Berechtigungen.
- Zur Verbesserung der Performance kann zusätzlich die Berechtigung LESEN verweigert werden. Grundsätzlich werden alle Gruppenrichtlinien ausgelesen, die mit der Verwaltungseinheit, in der das Benutzerkonto enthalten ist, verknüpft sind und die die Berechtigung LESEN auf diese Organisationseinheit besitzen. Besitzt ein Benutzerkonto diese Berechtigung auf diese Organisationseinheit nicht, wird die Gruppenrichtlinie nicht verarbeitet.



[5] backUP-Magazin Nr. 5, Kapitel 5.6

Gruppenrichtlinie verweigern

Eine Gruppenrichtlinie verweigern!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER und -COMPUTER auf.*
2. *Markieren Sie die Organisationseinheit, in der Sie eine Gruppenrichtlinie verweigern möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Wählen Sie die Schaltfläche EIGENSCHAFTEN und wechseln Sie auf die Registerkarte SICHERHEIT.*
4. *Fügen Sie die Sicherheitsgruppe hinzu, in der sich das Benutzerkonto befindet, dem Sie die Verarbeitung der Gruppenrichtlinie verweigern möchten (arbeiten Sie aufgrund der besseren Übersichtlichkeit und Administrierbarkeit immer mit Gruppen[6]).*
5. *Verweigern Sie der Sicherheitsgruppe die notwendigen Berechtigungen (mindestens GRUPPENRICHTLINIE ÜBERNEHMEN und evtl. zur Verbesserung der Performance LESEN, s. o.).*

[6] backUP-Magazin Nr. 5, Kapitel 6.4.5

Bei der Verweigerung der Option GRUPPENRICHTLINIE ÜBERNEHMEN handelt es sich nicht um eine Verknüpfungsoption. Das bedeutet, dass es nicht möglich ist, einzelne Gruppenrichtlinienverknüpfungen oder sogar einzelne Richtlinien der entsprechenden Gruppenrichtlinie in Bezug auf die Sicherheitsfilterung zu konfigurieren.

Wenn eine Einstellung im Bereich der Sicherheitskonfiguration z. B. in der Gruppenrichtlinie SICHERHEITSSTUFE 1 vorgenommen wurde, dann gilt diese Einstellung für alle Verknüpfungen, die mit dieser Gruppenrichtlinie erstellt wurden oder werden.

Beachten Sie, dass es keine Möglichkeit gibt, die Active Directory-Berechtigungen, die Sie im Rahmen der Gruppenrichtlinienverarbeitung vergeben, mit Systemmitteln übersichtlich aufzulisten. Sie müssen tatsächlich jede Gruppenrichtlinie anklicken und sich die entsprechenden Berechtigungen herausschreiben oder sie per Screenshot dokumentieren.

Überlegen Sie daher genau, ob und in welchem Maße Sie die Sicherheitsfilterung einsetzen möchten und ob es nicht Alternativen durch eine Anpassung der Active Directory-Struktur gibt. Wenn Sie mit der Sicherheitsfilterung arbeiten müssen, dokumentieren Sie die Rechtevergabe genau. Nur so haben Sie die Möglichkeit, bei evtl. Wechselwirkungen von positiven Berechtigungen und Verweigerungen den Überblick zu behalten.

WMI-Filter

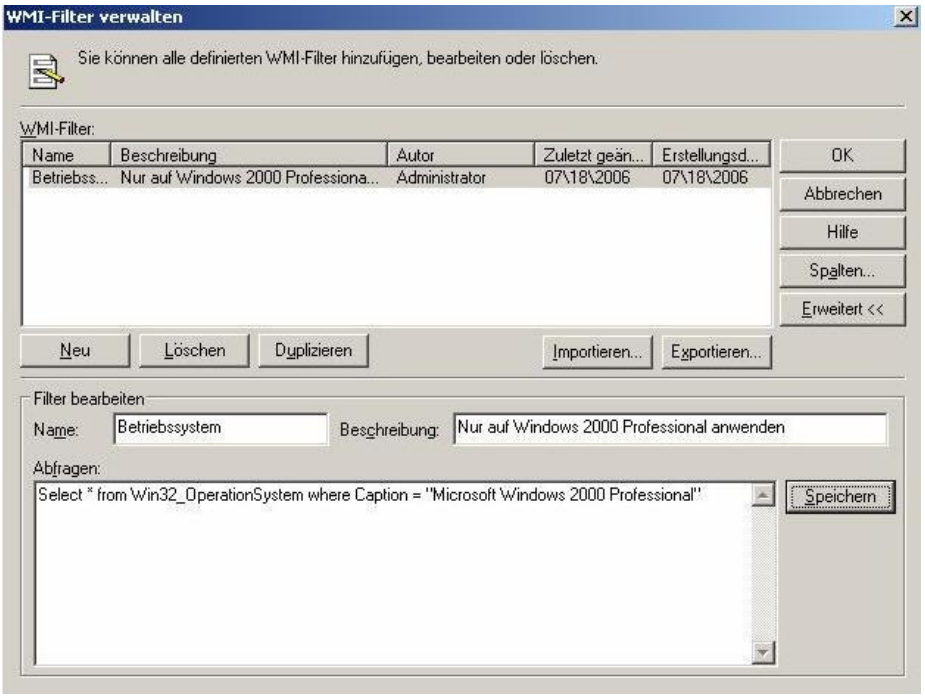
WMI-Filter (Windows Management Instrumentation) werden ab dem Betriebssystem Windows 2003/XP unterstützt.

WMI-Filter

Sie bieten die Möglichkeit, vor der Verarbeitung von Gruppenrichtlinien die technische Konfiguration auf den Client in Bezug z. B. auf Hardware, Software oder Systemeinstellungen abzufragen und die Ausführung der Gruppenrichtlinie davon abhängig zu machen. WMI-Filter können auf der Registerkarte EIGENSCHAFTEN-WMI-FILTER der jeweiligen Gruppenrichtlinie erstellt, bearbeitet und verwaltet werden.

Ist ein WMI-Filter mit einer Gruppenrichtlinie verknüpft, wird dieser vor der Anwendung der Gruppenrichtlinie auf dem Computer ausgewertet. Die WMI-Filter-Abfrage enthält eine Befehlszeile, die entweder das Ergebnis *false* oder *true* erhält. Nur bei dem Wert *true* wird die Gruppenrichtlinie umgesetzt, während sie bei *false* nicht zur Anwendung kommt.

WMI-Filter werden ab den Betriebssystemen Windows Server 2003/XP unterstützt.



WMI-Filter

WMI-Filter benutzen für die Erstellung von Abfragen die WMI-Query Language (WQL), die Syntax ist an die SQL-Abfragesprache angelehnt. Die Entwicklung von WMI-Abfragen setzt Kenntnisse im systemtechnischen Bereich voraus. Leider gibt es in der Fachliteratur und im Internet nur wenige Hilfestellungen zu diesem Themenkomplex. Die folgende Syntax ist Basis für die Erstellung einer WMI-Abfrage:

Namespace; Select * from `Klasse` where Name `Operator` Wert [AND/OR]

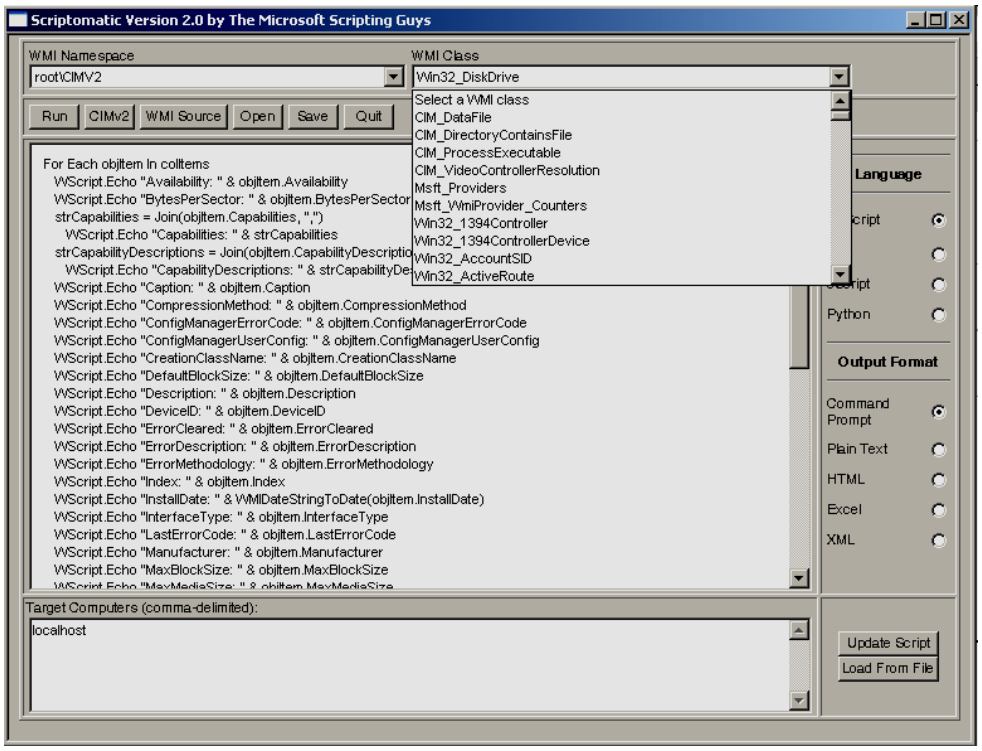
- **Namespace:** Gibt den Namensraum an, auf den sich die Abfrage bezieht. Standardmäßig wird root\CIMv2 verwendet.
- **Select * from Klasse where:** Die Klasse enthält Elemente, auf die die Abfrage bezogen wird.
- **Name:** Enthält das gewünschte Objekt der Klasse.
- **Operator:** Die Operatoren =,<,>, <> können für die Abfrage verwendet werden.
- **Wert:** Angabe des Werts, der für die Abfrage erfüllt werde muss.
- **AND/OR:** Erweiterung der Abfrage um weitere Kriterien.

In der nachfolgenden Tabelle sind einige Beispiele für WMI-Abfragen dargestellt:

Zeitzone	Die Gruppenrichtlinie soll angewendet werden, wenn die Zeitzone Berlin eingestellt ist.
`Root\CIMv2; Select * from win32_TimeZone where bias = 60`	
Hotfix	Die Gruppenrichtlinie wird angewendet, wenn der Hotfix mit der ID Q147222 installiert ist.
`Root\CIMv2; Select * from Win32_QuickFixEngineering where HotFixID = “Q147222”`	
Softwareinventar	Die Gruppenrichtlinie wird angewendet, wenn die Software MSIPackage1 oder MSIPackage2 installiert ist.
`Root\CIMv2; Select * from Win32_Product where Name = “MSIPackage1” OR Name = "MSIPackage2"`	
Betriebssystem	Die Gruppenrichtlinie wird angewendet, wenn das Betriebssystem Microsoft Windows XP installiert ist.
`Root\CIMv2; Select * from Win32_OperatingSystem where Caption = “Microsoft Windows XP Professional”`	

Ressourcen	Die Gruppenrichtlinie wird angewendet, wenn die Festplatte über mehr als 600 MB freien Speicherplatz verfügt.
`Root\CIMv2; Select * from Win32_LogicalDisk where FreeSpace > 629145600`	
Computersystem	Die Gruppenrichtlinie wird angewendet, wenn es sich um einen Toshiba Tecra Modell 800 und 810 handelt.
`Root\CIMv2; Select * from Win32_ComputerSystem where manufacturer = “Toshiba” and model = “Tecra 800” OR model = “Tecra 810”`	

Microsoft stellt auf seinen Web-Seiten für die Script-Programmierung eine Reihe von Hilfsmitteln zur Verfügung (URL im Anhang). Das Tool *Scriptomatic* gibt Einblick in die zahlreichen WMI-Klassen und die dazugehörigen Objekte. Über dieses Tool kann man sich einen ersten Überblick über den vielfältigen Einsatz von WMI-Abfragen verschaffen.



Tool Scriptomatic

Einen WMI-Filter erstellen!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER und -COMPUTER auf.*
2. *Markieren Sie die Organisationseinheit, in der sich die Gruppenrichtlinie befindet, die Sie mit dem WMI-Filter verknüpfen möchten, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte WMI-FILTER.*
3. *Wählen Sie die Option DIESER FILTER und danach die Schaltfläche DURCHSUCHEN/VERWALTEN.*
4. *Erweitern Sie das Ansichtsfenster durch die Betätigung der Schaltfläche ERWEITERT.*
5. *Wählen Sie NEU und vergeben Sie einen Namen und eine Beschreibung für den neuen WMI-Filter*
6. *Tragen Sie z. B. folgende Zeile in das Textfeld ein, um das Betriebssystem des Clients abzufragen: Root\CIMv2; Select * from Win32_OperatingSystem where Caption = "Microsoft Windows 2000 Professional".*
7. *Bestätigen sie Ihre Eingabe mit SPEICHERN und OK.*

In diesem Fall wird anhand des WMI-Filters vor der Verarbeitung der Gruppenrichtlinien überprüft, ob auf dem Client das Betriebssystem Windows 2000 Professional installiert ist. Nur wenn der Rückgabewert positiv (true) ist, wird die Gruppenrichtlinie verarbeitet, ansonsten wird sie nicht verwendet.

Der WMI-Filter wird als Attribut der Gruppenrichtlinie (als Active Directory-Objekt) gespeichert. Daher ist es nicht möglich, verschiedenen Verknüpfungen einer Gruppenrichtlinie verschiedene WMI-Filter zuzuweisen. Wird ein WMI-Filter einer Gruppenrichtlinie zugewiesen, gilt er für alle Verknüpfungen dieser Gruppenrichtlinie.

5.5 Übersichtlichkeit und Transparenz

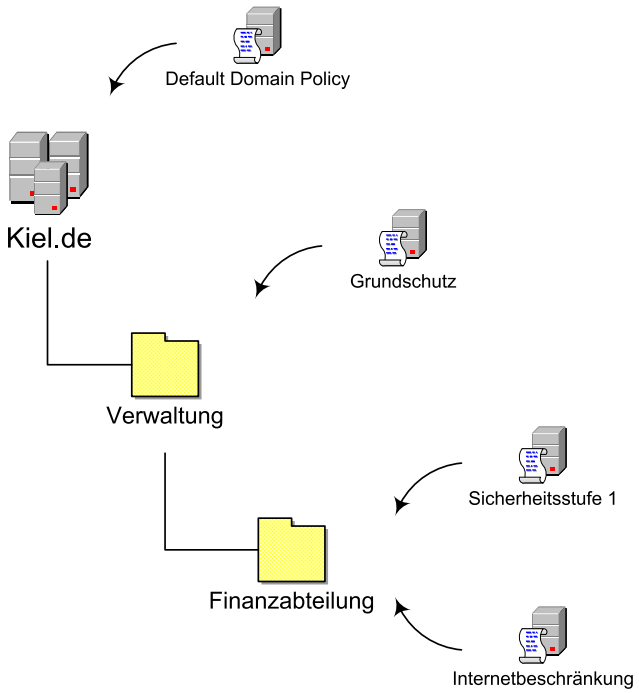
Wie in den einzelnen Unterkapiteln teilweise schon erwähnt, ist die Übersichtlichkeit und Transparenz im Bereich der Gruppenrichtlinienverwaltung nur unzureichend gegeben. Das gilt besonders dann, wenn die standardmäßigen Funktionalitäten durch die verschiedenen Werkzeuge erweitert, eingeschränkt oder beeinflusst werden. Die Dokumentation der verschiedenen Aktivitäten der Gruppenrichtlinienverwaltung gewinnt vor diesem Hintergrund einen hohen Stellenwert und sollte von den Systemverantwortlichen gewissenhaft durchge-

führt werden. Eine deutliche Verbesserung bietet die Gruppenrichtlinien-Verwaltungskonsole. Doch leider sind auch bei diesem neuen Werkzeug noch nicht alle Funktionalitäten berücksichtigt worden.

An dieser Stelle soll für alle Systemverantwortlichen, die noch ohne die Gruppenrichtlinien-Verwaltungskonsole auskommen müssen, eine Methode vorgestellt werden, wie der Einsatz der Gruppenrichtlinien strukturiert und übersichtlich gestaltet werden kann.

Die Abbildung unten zeigt einen Ausschnitt einer Organisationsstruktur mit den erstellten Organisationseinheiten und verknüpften Gruppenrichtlinien. Die Vorgehensweise bei der Erstellung der Gruppenrichtlinien war entsprechend der vorangegangenen Kapitel folgendermaßen:

- Die Gruppenrichtlinie GRUNDSCHUTZ wurde in der Organisationseinheit VERWALTUNG erstellt, verknüpft und bearbeitet.
- Die Gruppenrichtlinien SICHERHEITSSTUFE 1 und INTERNETBESCHRÄNKUNG wurden in der Organisationseinheit FINANZABTEILUNG erstellt, verknüpft und bearbeitet.
- usw.

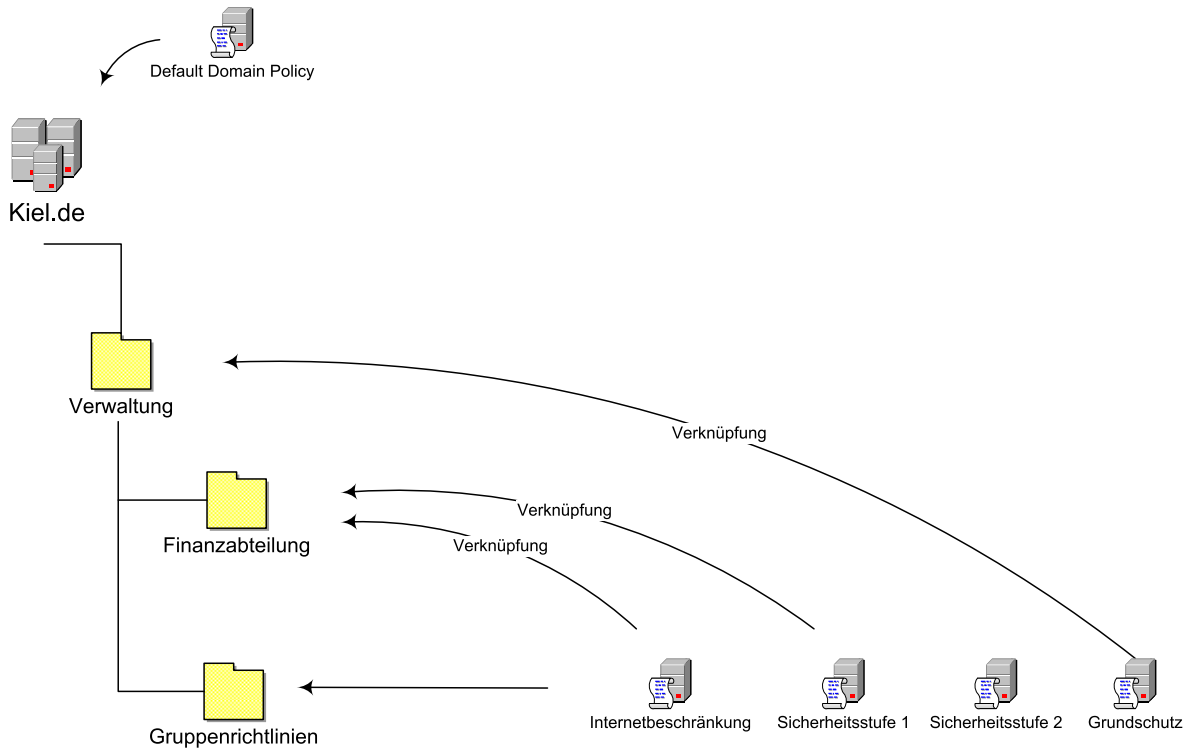


Für den Systemverantwortlichen bedeutet das, dass er, wenn er die unterschiedlichen Gruppenrichtlinien bearbeiten möchte, immer genau wissen muss, welche Gruppenrichtlinien er in welchen Organisationseinheiten erstellt und verknüpft hat. Dazu muss er dann über die Eigen-

schaften der entsprechenden Organisationseinheiten die Gruppenrichtlinien aufrufen und bearbeiten.

Ein bisschen mehr Übersichtlichkeit kann dadurch erreicht werden, wenn (wie im Beispiel unten) eine Organisationseinheit GRUPPENRICHTLINIEN eingerichtet wird, die nur dafür benutzt wird, um die Gruppenrichtlinien zu verwalten. Diese Organisationseinheit darf keine Benutzer- oder Computerkonten erhalten, da sonst alle Gruppenrichtlinien dieser Organisationseinheit auf diese Konten wirken würden. Die Organisationseinheit GRUPPENRICHTLINIEN stellt sozusagen den Sammelcontainer für alle Gruppenrichtlinien dar.

Der Systemverantwortliche hat in diesem Container alle Gruppenrichtlinien im Überblick und kann sie in diesem Container bearbeiten. Sollen eine oder mehrere Gruppenrichtlinien auf eine Organisationseinheit wirken, dann braucht nur noch die Verknüpfung zu dieser Organisationseinheit hergestellt werden. Soll eine Verknüpfung gelöscht werden, wird **nur** die Verknüpfung entfernt, die Gruppenrichtlinie an sich bleibt in dem Container GRUPPENRICHTLINIEN bestehen.

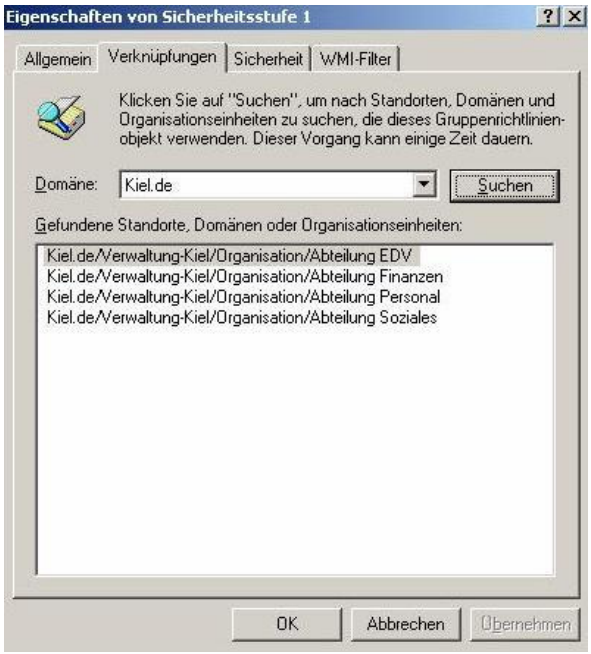


Strukturierungsvorschlag: Aufgelistete Gruppenrichtlinien

Auch die Verknüpfungen zu den unterschiedlichen Organisationseinheiten können in dieser Konstellation übersichtlich dargestellt werden:

Gruppenrichtlinien-Verknüpfungen auflisten!

1. *Wählen Sie START-AUSFÜHREN und rufen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER und -COMPUTER auf.*
2. *Markieren Sie die Organisationseinheit, die Sie als Sammelcontainer für Ihre Gruppenrichtlinien erstellt haben, mit der rechten Maustaste und wählen Sie EIGENSCHAFTEN und danach die Registerkarte GRUPPENRICHTLINIE.*
3. *Markieren Sie die Gruppenrichtlinie, deren Verknüpfungen Sie auflisten möchten, wählen Sie die Schaltfläche EIGENSCHAFTEN und wechseln Sie auf die Registerkarte VERKNÜPFUNGEN.*
4. *Wählen Sie die Domäne, in der Sie nach den Gruppenrichtlinien-Verknüpfungen suchen möchten, und starten Sie die Suche mit SUCHEN.*
5. *Die vorhandenen Gruppenrichtlinien-Verknüpfungen der ausgewählten Gruppenrichtlinien werden aufgelistet.*



Liste der Gruppenrichtlinien-Verknüpfungen

Mit dieser Strukturierung kann eine gewisse Übersichtlichkeit erreicht werden. Sie bietet aber keine Möglichkeit, Besonderheiten in der Vererbungsreihenfolge oder Vergabe von Active Directory-Berechtigungen darzustellen.

5.6 Sicherheitscheck

- *Machen Sie sich mit den **Funktionen** für die Verwaltung (Erstellen, Verknüpfen, Löschen) der Gruppenrichtlinien vertraut.*
- *Bevor Sie eine Gruppenrichtlinie endgültig löschen, sollten Sie sie zunächst **deaktivieren**, um zu überprüfen, ob es durch den Wegfall der Gruppenrichtlinie zu unerwünschten Nebeneffekten oder Wechselwirkungen kommt.*
- *Löschen Sie eine Gruppenrichtlinie erst dann, wenn alle Sicherheitseinstellungen wieder **rückgängig** gemacht wurden.*
- *Machen Sie sich mit der Verarbeitungs- bzw. die **Vererbungsreihenfolge** vertraut.*
- *Achten Sie bei einer Verknüpfung von mehreren Gruppenrichtlinien mit einer Organisationseinheit darauf, dass schon innerhalb der Organisationseinheit eine standardmäßige **Verarbeitungsreihenfolge** wirkt und passen Sie ggf. die Verarbeitungsreihenfolge an.*
- *Wählen Sie die Option **Kein Vorrang**, wenn bestimmte Einstellungen einer Gruppenrichtlinie als Grundsicherheitseinstellung für alle Computer- und Benutzerkonten gelten sollen.*

- *Setzen Sie die Werkzeuge zur **Veränderung** der Vererbung sparsam und überlegt ein und dokumentieren Sie die Änderungen sorgfältig.*
- *Wenn Sie Gruppenrichtlinien differenziert nach Computer- und Benutzerkonfiguration erstellen, achten Sie darauf, dass Sie nicht benötigte **Gruppenrichtlinienkomponenten** deaktivieren.*
- *Setzen Sie die **Sicherheitsfilterung** nur sehr sparsam und gezielt ein.*
- *Wählen Sie Ihre **Struktur** zur Verwaltung der Gruppenrichtlinien so, dass Sie einen maximalen Grad an Übersichtlichkeit erreichen.*

6 Gruppenrichtlinien-Verwaltungskonsole

In diesem Kapitel erfahren Sie,

- wie Sie die Gruppenrichtlinien-Verwaltungskonsole installieren,
- wie die Gruppenrichtlinien-Verwaltungskonsole strukturiert ist,
- wo sich die Funktionalitäten und administrativen Werkzeuge der Gruppenrichtlinien-Verwaltung befinden,
- welche neuen Funktionalitäten durch den Einsatz der Gruppenrichtlinien-Verwaltungskonsole bereitgestellt werden,
- welche Bedeutung die Gruppenrichtlinienmodellierung hat und
- was unter dem Gruppenrichtlinienergebnissatz zu verstehen ist.

Mit der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) wird die Verwaltung von Gruppenrichtlinien vereinfacht. Die Gruppenrichtlinien werden strukturiert und übersichtlich dargestellt und eine Reihe neuer Funktionalitäten stehen zur Erleichterung der Gruppenrichtlinienverwaltung zur Verfügung.

Dieses Kapitel ist so aufgebaut, dass zunächst im Unterkapitel 6.2 ausführlich auf den strukturellen Aufbau der Gruppenrichtlinien-Verwaltungskonsole eingegangen wird. Erst danach werden in den Unterkapiteln 6.3 bis 6.4 die einzelnen Funktionalitäten der Gruppenrichtlinien-Verwaltungskonsole aufgabenorientiert dargestellt. Als Hintergrundwissen sind die im Kapitel 5 behandelten Themenbereiche, vor allem die Themen Vererbung und Filterung von Gruppenrichtlinien, zwingend notwendig.

6.1 Gruppenrichtlinien-Verwaltungskonsole installieren

Auf einem Windows 2003 Domänencontroller ist die Gruppenrichtlinien-Verwaltungskonsole ab dem Service Pack 1 verfügbar. Sie steht aber auch gesondert auf den Microsoft Webseiten zum Download bereit (siehe URL-Adresse im Anhang). In einer Windows 2000 Domäne kann die Gruppenrichtlinien-Verwaltungskonsole nur auf einem Windows XP Client mit dem Service Pack 3 und Microsoft .NET Framework installiert werden. Weiterhin sollte auf dem Windows 2000-Domänencontroller das Service Pack 4 installiert sein.

Die Gruppenrichtlinien-Verwaltungskonsole auf einem Windows Server 2003-Domänencontroller installieren!

1. *Laden Sie sich die Gruppenrichtlinien-Verwaltungskonsole (gpmc.msi) von den Microsoft Webseiten herunter oder installieren Sie das aktuelle Servicepack auf Ihrem Domänencontroller.*
2. *Nach einem Doppelklick auf die Datei (oder über START-AUSFÜHREN und der Eingabe von* `gpmc.msi`*) wird die Installationsroutine gestartet.*
3. *Die Gruppenrichtlinien-Verwaltungskonsole fügt sich sowohl in die Verwaltungsprogramme ACTIVE DIRECTORY-BENUTZER und -COMPUTER und ACTIVE DIRECTORY-STANDORTE UND –DIENSTE als auch in das Startmenü ein.*

Nach der Installation der Gruppenrichtlinien-Verwaltungskonsole können die Gruppenrichtlinien nur noch über diese Konsole verwaltet werden. Die im Kapitel 5 beschriebenen Funktionen innerhalb des Active Directory sind deaktiviert und werden nur noch innerhalb der Verwaltungskonsole bereitgestellt.

Mit der Einführung der leistungsfähigeren 64-Bit-Proszessoren bietet Microsoft die Betriebssysteme Windows Server 2003 und XP als 64 Bit-Versionen an. Unter diesen Betriebssystemen ist die Gruppenrichtlinien-Verwaltungskonsole derzeit noch nicht lauffähig.

Die Gruppenrichtlinien-Verwaltungskonsole aufrufen!

- *Markieren Sie eine Organisationseinheit und rufen Sie über die rechte Maustaste die Eigenschaften auf. Wechseln Sie auf die Registerkarte GRUPPENRICHTLINIE und klicken Sie auf die Schaltfläche GRUPPENRICHTLINIENVERWALTUNG.*

Oder:

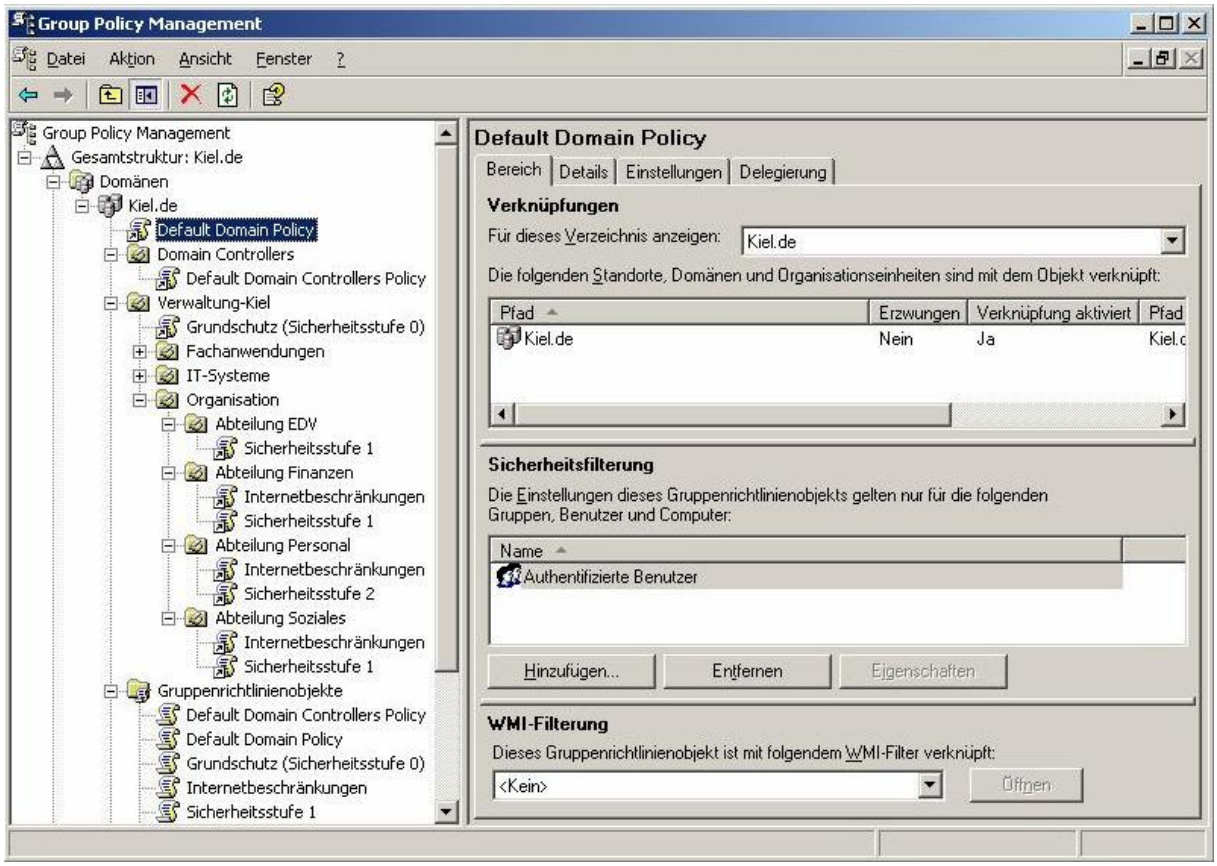
- *Wählen Sie START-VERWALTUNG-GRUPPENRICHTLINIENVERWALTUNG.*

Oder:

- *Rufen Sie die Gruppenrichtlinien-Verwaltungskonsole mit START-AUSFÜHREN und der Eingabe von* `gpmc.msc` *auf.*

6.2 Struktur der Gruppenrichtlinien-Verwaltungskonsole

Die Gruppenrichtlinien-Verwaltungskonsole liegt in Form einer Managementkonsole vor, die alle Verwaltungsbereiche der Gruppenrichtlinienverarbeitung strukturiert und übersichtlich darstellt.



Gruppenrichtlinien-Verwaltungskonsole

Die Managementkonsole ist unterteilt in zwei Bereiche. Auf der linken Seite wird die Gesamtstruktur mit verschiedenen Containern und Objekten abgebildet (Navigationsbereich). In dem Fensterbereich der rechten Seite werden, je nachdem, welches Objekt im Navigationsbereich ausgewählt wird, Informationen, Inhalte oder Verwaltungswerkzeuge zur Verfügung gestellt (Inhaltsbereich). Je nach Umfang der bereitgestellten Inhalte kann dieser Fensterbereich auch in verschiedene Registerkarten unterteilt sein.

Die Gruppenrichtlinien-Verwaltungskonsole kann eine oder mehrere Gesamtstrukturen abbilden, die jeweils in die Container DOMÄNEN, STANDORTE, GRUPPENRICHTLINIENMODELLIERUNG und GRUPPENRICHTLINIENERGEBNISSE untergliedert sind (siehe folgende Abbildung).

Struktur der Gruppenrichtlinien-Verwaltungskonsole

Eine Auswahl der anzuzeigenden Gesamtstrukturen (falls mehrere Gesamtstrukturen zu einem Verwaltungsbereich gehören) kann über das Kontextmenü des Hauptknotens GROUP POLICY MANAGEMENT vorgenommen werden

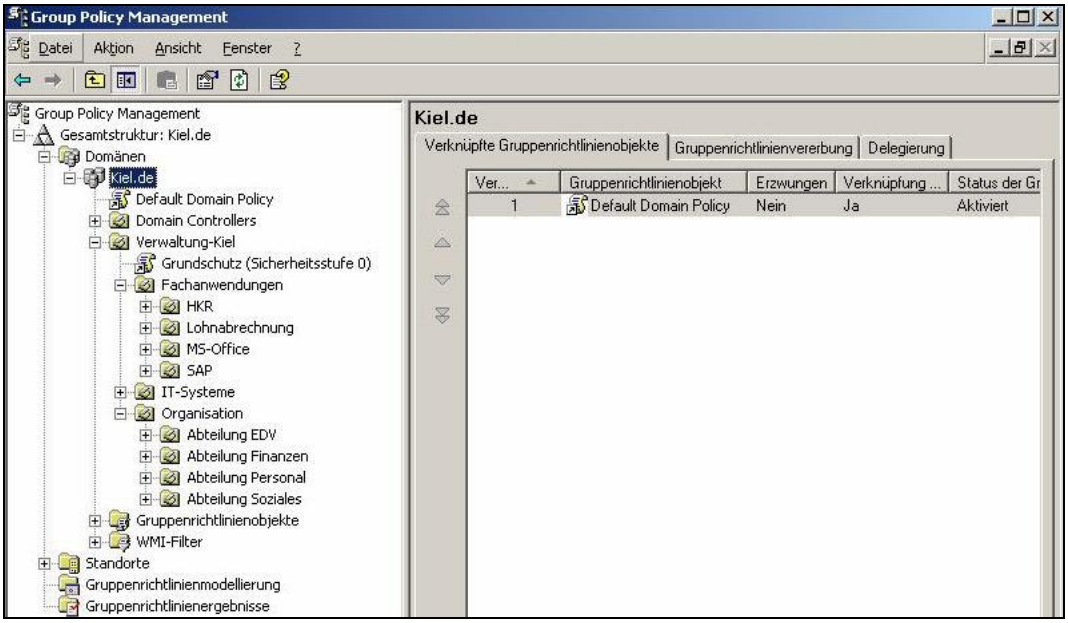
Container DOMÄNEN

Alle Domänen einer Gesamtstruktur werden standardmäßig in dem Container DOMÄNEN angezeigt. Sind in der Gesamtstruktur mehrere Domänen vorhanden, werden sie auf einer Hierarchieebene abgebildet. Die Ansicht des Containers DOMÄNEN lässt sich auf die individuellen Anforderungen und an die Organisationsgröße anpassen, indem die Domänen einer Gesamtstruktur in der Gruppenrichtlinien-Verwaltungskonsole ein- bzw. ausgeblendet werden können.

Domänen in der Gruppenrichtlinien-Verwaltungskonsole ein- bzw. ausblenden!

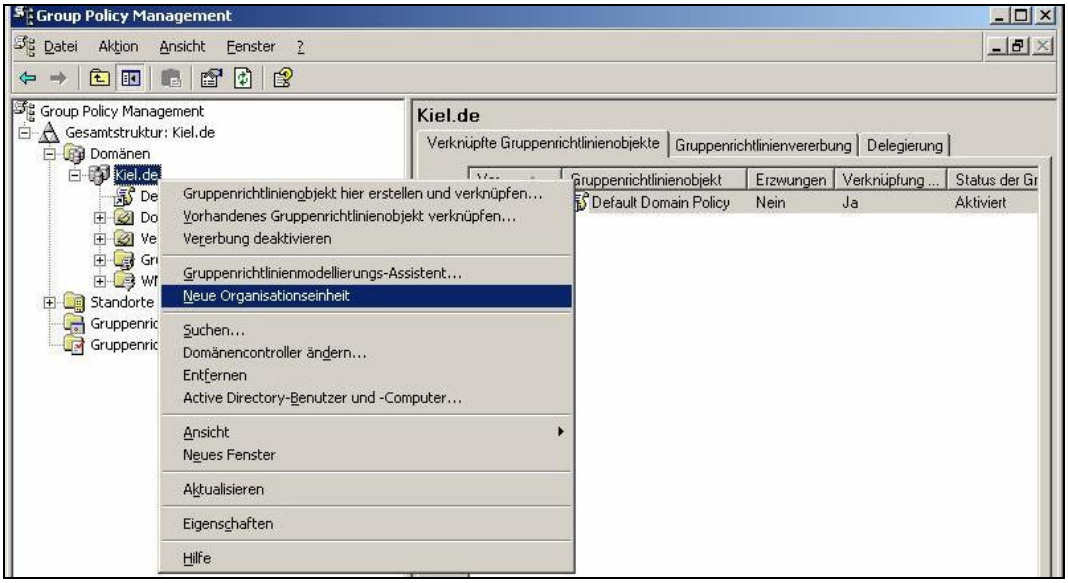
1. *Markieren Sie den Container DOMÄNEN und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
2. *Wählen Sie den Menüpunkt DOMÄNEN ANZEIGEN.*
3. *Es öffnet sich ein Fenster, in dem Sie alle in Ihrer Gesamtstruktur vorhandenen Domänen aufgelistet bekommen. Setzen Sie einen Haken in das Auswahlkästchen vor den Domänen, die Sie in Ihrer Gruppenrichtlinien-Verwaltungskonsole angezeigt bekommen möchten.*
4. *Bestätigen Sie Ihre Auswahl mit OK.*

Die Strukturierung unterhalb des Domänennamens erinnert an das Verwaltungswerkzeug *Active Directory-Benutzer und -Computer*. Tatsächlich werden alle für die Gruppenrichtlinienverwaltung notwendigen Container und Organisationseinheiten aus dem Active Directory übernommen und in der Gruppenrichtlinien-Verwaltungskonsole angezeigt.

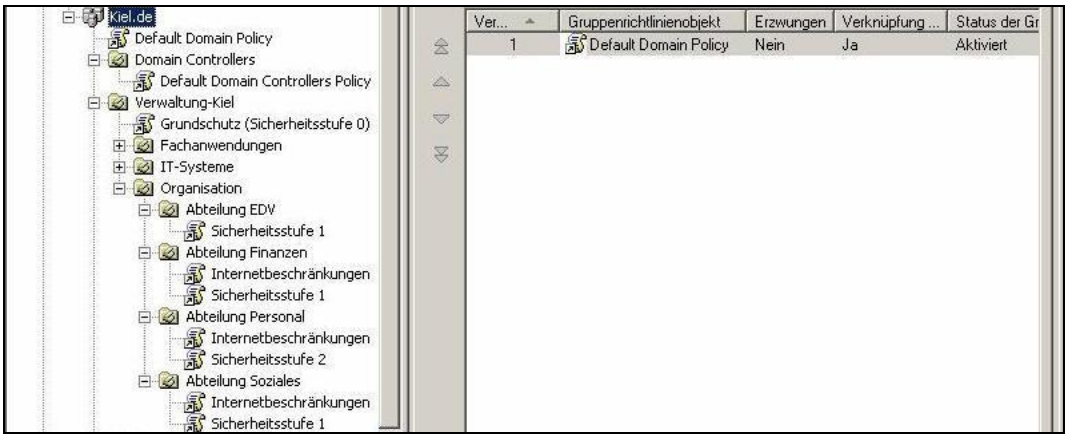


Container DOMÄNEN der Gruppenrichtlinien-Verwaltungskonsole

Auch wenn die angezeigten Container und Organisationseinheiten keine Active Directory-Objekte enthalten, so bleibt die Nähe zum Active Directory dennoch erhalten. So können z. B. über das Kontextmenü Organisationseinheiten erstellt und das Verwaltungswerkzeug *Active Directory-Benutzer und -Computer* aufgerufen werden (siehe Abbildung unten).



Kontextmenü der Domäne



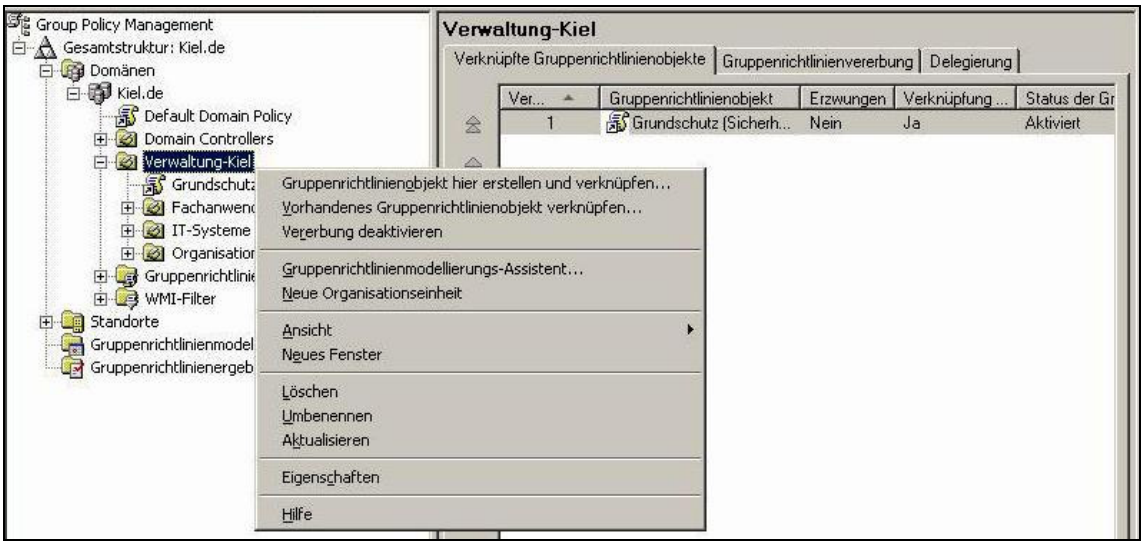
Strukturelle Gliederung einer Domäne in der Gruppenrichtlinien-Verwaltungskonsole

Die Gliederungsstruktur von Organisationseinheiten und Objekten unterhalb des Containers DOMÄNEN zeigt einen einheitlichen Aufbau (siehe Abbildung oben):

- Zuerst werden unterhalb einer Verwaltungseinheit alle verknüpften Gruppenrichtlinien angezeigt. Im Beispiel oben werden für die Domäne KIEL zunächst die Gruppenrichtlinie DEFAULT DOMAIN POLICY angezeigt, für die Organisationseinheit ABTEILUNG FINANZEN zuerst die Gruppenrichtlinien INTERNETBESCHRÄNKUNGEN und SICHERHEITSSTUFE 1 usw.
- Danach werden entsprechend der Active Directory-Strukurierung die einzelnen Container bzw. Organisationseinheiten abgebildet. Für die Organisationseinheit VERWALTUNG-KIEL werden demnach die untergeordneten Organisationseinheiten FACHANWENDUNGEN, IT-SYSTEME und ORGANISATION angezeigt, die jeweils eine eigene Unterstruktur aufweisen.

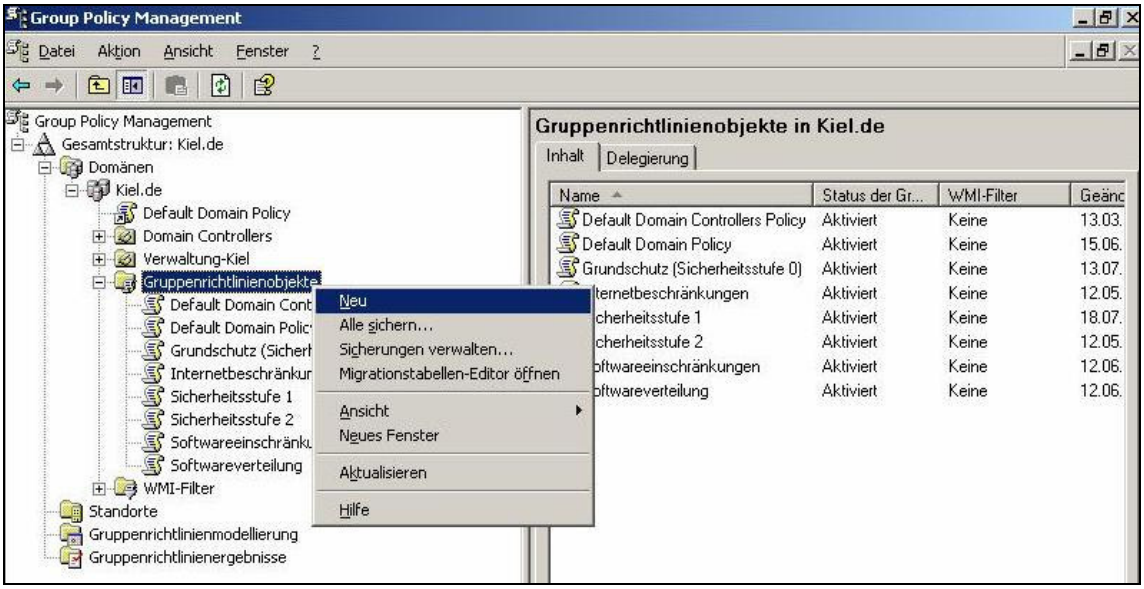
Alle Container aus dem Active Directory (Kennzeichnung mit einem geöffneten Buch) zeigen im Kontextmenü des Navigationsbereichs und im Inhaltsbereich der Gruppenrichtlinien-Verwaltungskonsole die gleichen Funktionalitäten (siehe folgende Abbildung).

- Der Inhaltsbereich ist in die drei Registerkarten VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE, GRUPPENRICHTLINIENVERERBUNG und DELEGIERUNG gegliedert. Sie geben Auskünfte zu den verknüpften Gruppenrichtlinien und bieten ergänzende Verwaltungsmöglichkeiten.
- Das Kontextmenü bietet zusätzliche administrative Funktionalitäten zur Verwaltung der Gruppenrichtlinienverknüpfungen.



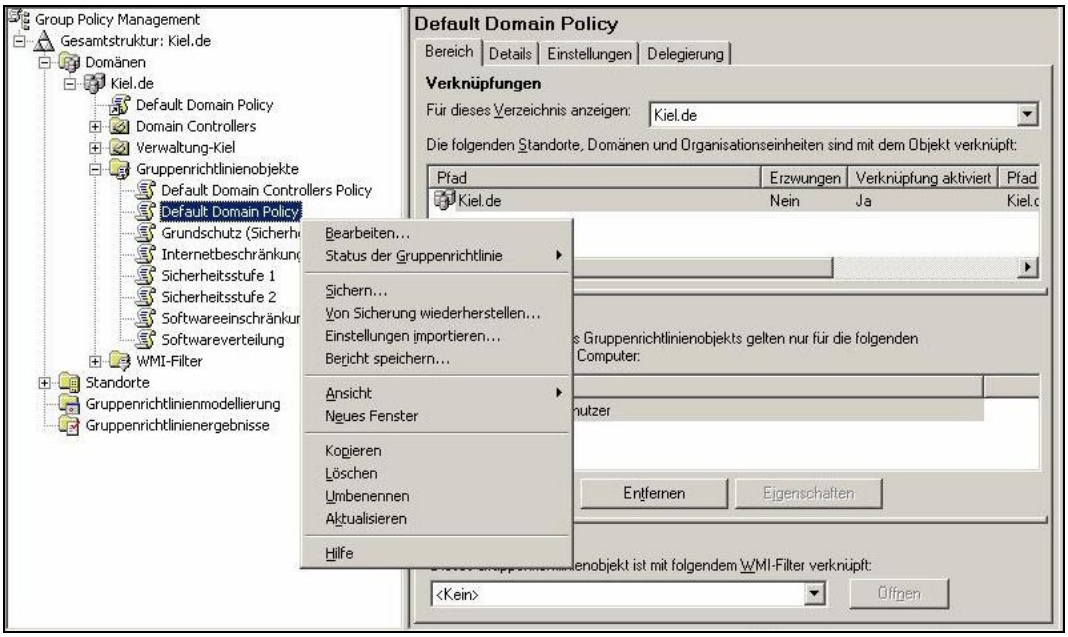
Funktionalitäten im Bereich einer Organisationseinheit

Eine Sonderstellung nimmt der Container GRUPPENRICHTLINIENOBJEKTE ein, der auch visuell speziell gekennzeichnet ist (siehe Abbildung unten). Er übernimmt die Funktion des zentralen Speicherorts aller Gruppenrichtlinien innerhalb einer Domäne. Der Container GRUPPENRICHTLINIENOBJEKTE stellt im Kontextmenü des Navigationsbereichs und im Inhaltsbereich der Gruppenrichtlinien-Verwaltungskonsole spezielle Funktionalitäten zur Verfügung.



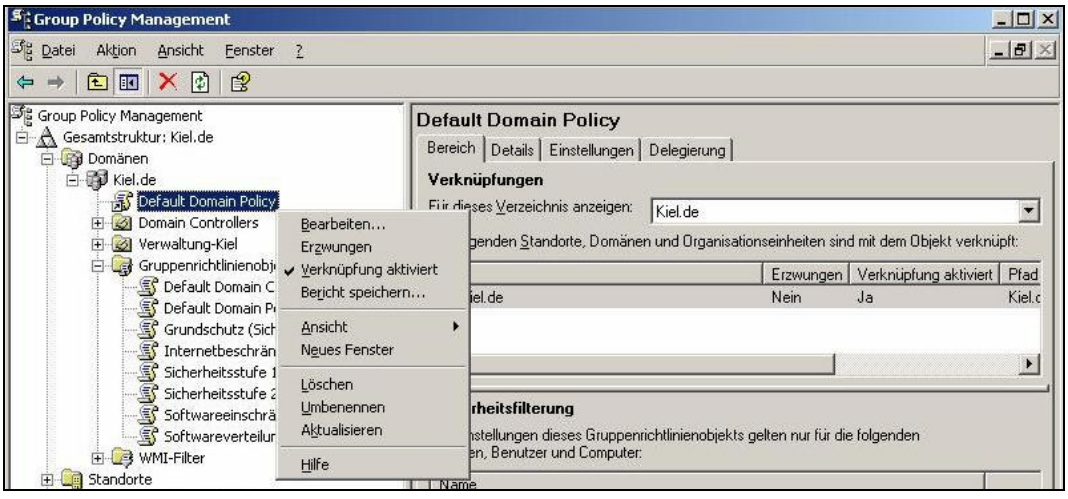
Container GRUPPENRICHTLINIENOBJEKTE der Gruppenrichtlinien-Verwaltungskonsole

Alle im Container GRUPPENRICHTLINIENOBJEKTE aufgeführten Gruppenrichtlinien stellen auf den vier Registerkarten BEREICH, DETAILS, EINSTELLUNGEN und DELEGIERUNG sowie im Kontextmenü alle Informationen und Verwaltungswerkzeuge zur Verfügung, die die entsprechende Gruppenrichtlinie als Objekt betreffen.



Gruppenrichtlinienobjekte

Im Vergleich zu den Gruppenrichtlinienobjekten unterscheidet sich das Kontextmenü der Gruppenrichtlinienverknüpfungen deutlich von dem der Gruppenrichtlinienobjekte.



Gruppenrichtlinienverknüpfungen

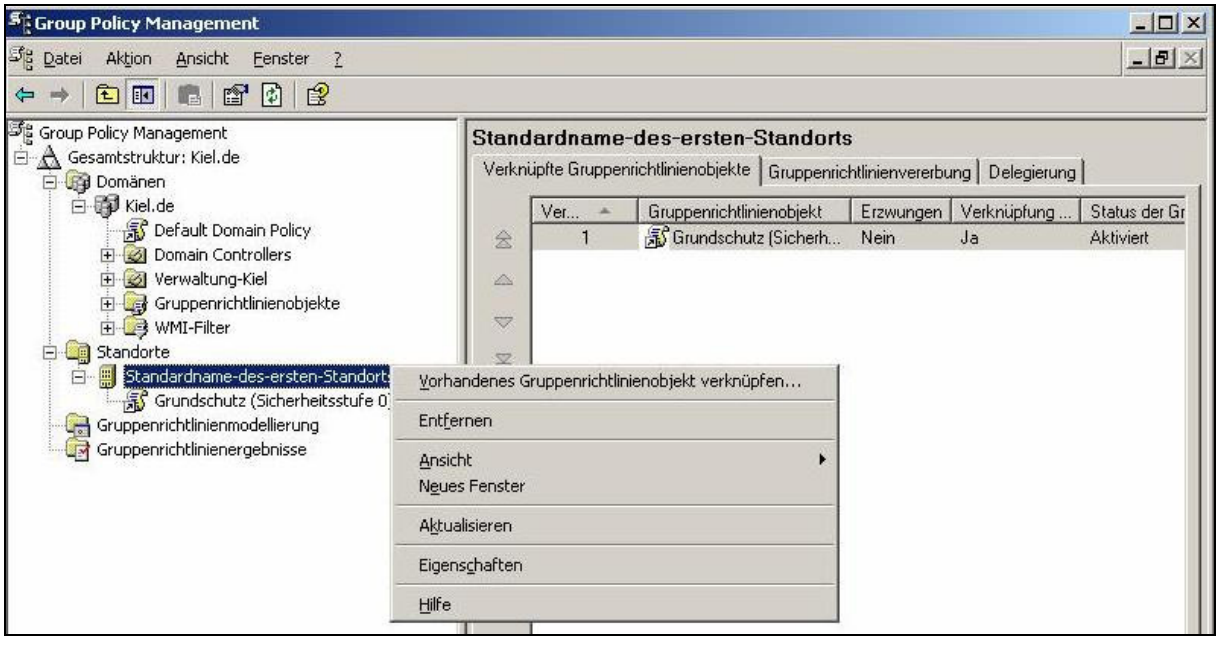
Es stellt die besonderen Funktionalitäten zur Verwaltung von Gruppenrichtlinienverknüpfungen zur Verfügung. Der Inhaltsbereich der Gruppenrichtlinien-Verwaltungskonsole unterscheidet sich hingegen nicht von dem des Gruppenrichtlinienobjekts.

Container STANDORTE

Im Container STANDORTE können die Standorte der Gesamtstruktur angezeigt werden. Standardmäßig zeigt die Verwaltungskonsole in diesem Container keine Standorte an. Wenn Gruppenrichtlinien auf Standortebene eingesetzt werden oder werden sollen, müssen diese Standorte explizit in die Ansicht der Gruppenrichtlinien-Verwaltungskonsole aufgenommen werden.

Standorte in die Gruppenrichtlinien-Verwaltungskonsole integrieren!

1. *Markieren Sie den Container STANDORTE und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
2. *Wählen Sie den Menüpunkt STANDORTE ANZEIGEN.*
3. *Es öffnet sich ein Fenster, in dem Sie die in Ihrer Gesamtstruktur vorhandenen Standorte aufgelistet bekommen. Setzen Sie einen Haken in das Auswahlkästchen vor den Standorten, die Sie in Ihrer Gruppenrichtlinien-Verwaltungskonsole angezeigt bekommen möchten.*
4. *Bestätigen Sie Ihre Auswahl mit OK.*

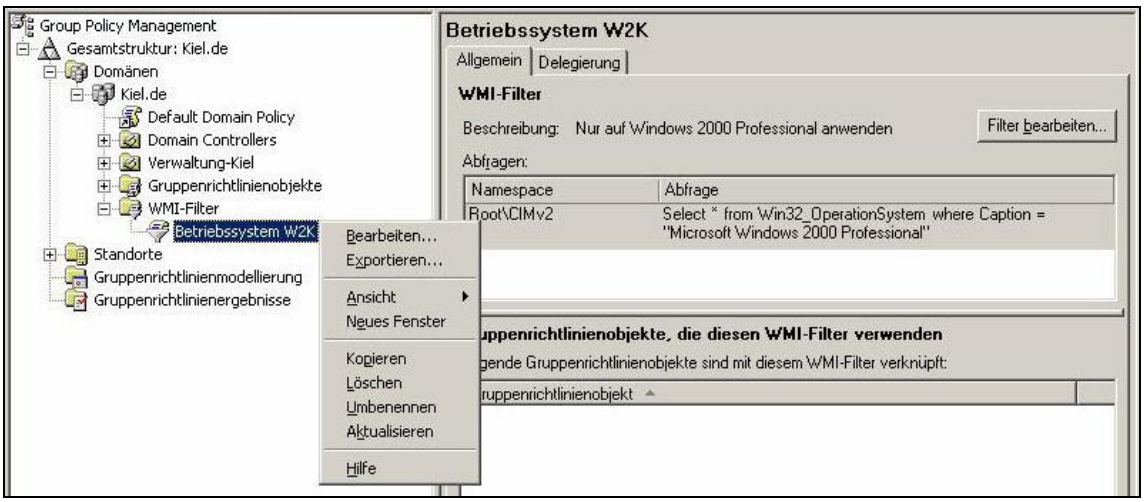


Container STANDORTE der Gruppenrichtlinien-Verwaltungskonsole

Die Standorte zeigen im Inhaltsbereich und Kontextmenü der Gruppenrichtlinien-Verwaltungskonsole vergleichbare Funktionalitäten wie die Domänen im Container DOMÄNEN.

Container WMI-FILTER

Der Container WMI-Filter bietet im Vergleich zur Administration der WMI-Filter ohne Gruppenrichtlinien-Verwaltungskonsole (siehe Kapitel 5.4) eine verbesserte Darstellung erstellter und verknüpfter WMI-Filter.



Container WMI-FILTER der Gruppenrichtlinien-Verwaltungskonsole

Container GRUPPENRICHTLINIENMODELLIERUNG

Der Container GRUPPENRICHTLINIENMODELLIERUNG stellt die neue Funktionalität der Gruppenrichtlinienmodellierung von Windows Server 2003 zur Verfügung. Mit Hilfe eines Assistenten kann die Anwendung einer Gruppenrichtlinie simuliert werden, ohne dass sie effektiv von Benutzern oder Computern übernommen wird. Die Funktionalität der Gruppenrichtlinienmodellierung wird im Kapitel 6.4 vorgestellt.

Container GRUPPENRICHTLINIENERGEBNISSE

Der Container GRUPPENRICHTLINIENERGEBNISSE stellt den Protokollierungsmodus des Richtlinienergebnissatzes zur Verfügung. Mit dieser Funktionalität können die tatsächlichen Richtliniendaten protokolliert werden, die für ein bestimmtes Benutzer- und Computerkonto angewendet werden. Die Funktionalität der Gruppenrichtlinienergebnisse wird im Kapitel 6.4 vorgestellt.

6.3 Funktionalitäten der Gruppenrichtlinien-Verwaltungskonsole

Dieses Kapitel befasst sich themenbezogen mit den Funktionen und administrativen Werkzeugen zur Verwaltung der Gruppenrichtlinien. Sofern die Themenbereiche im vorherigen Kapitel schon erläutert wurden, werden an dieser Stelle nur die Arbeitsschritte aufgezeigt und auf die entsprechenden Abschnitte des Kapitels 5 hingewiesen. Die neuen Funktionalitäten von Windows Server 2003 und der Gruppenrichtlinien-Verwaltungskonsole werden sowohl theoretisch als auch praktisch detailliert dargestellt.

Gruppenrichtlinien erstellen und verknüpfen

Die Gruppenrichtlinien-Verwaltungskonsole bietet verschiedene Wege, neue Gruppenrichtlinien zu erstellen und zu verknüpfen.

Neue Gruppenrichtlinien erstellen und verknüpfen!

1. *Markieren Sie den Container GRUPPENRICHTLINIENOBJEKTE und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
2. *Wählen Sie den Menüpunkt NEU. Vergeben Sie einen Namen für die neue Gruppenrichtlinie und bestätigen Sie mit OK.*
3. *Die neue Gruppenrichtlinie wird in die Liste der Gruppenrichtlinienobjekte aufgenommen, ist zu diesem Zeitpunkt aber noch mit keiner Verwaltungseinheit verknüpft.*
4. *Navigieren Sie zu der Verwaltungseinheit, mit der Sie die neue Gruppenrichtlinie verknüpfen möchten, und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
5. *Wählen Sie VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN, danach aus der Liste die entsprechende Gruppenrichtlinie und bestätigen Sie die Auswahl mit OK.*

Oder:

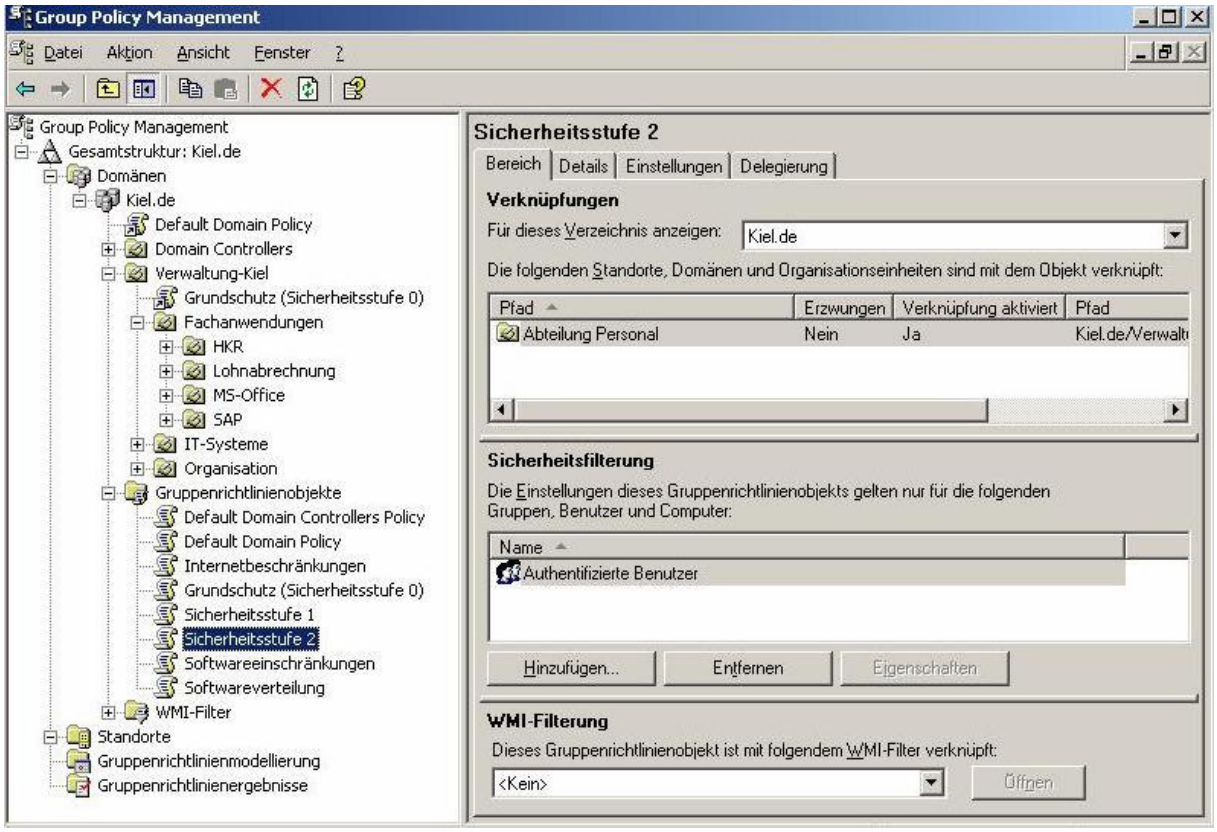
1. *Markieren Sie die Verwaltungseinheit, mit der Sie die neue Gruppenrichtlinie verknüpfen möchten, und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
2. *Wählen Sie GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN, vergeben Sie einen Namen für die neue Gruppenrichtlinie und bestätigen Sie mit OK.*
3. *Die Gruppenrichtlinie wird im Container GRUPPENRICHTLINIENOBJEKTE aufgenommen und gleichzeitig mit der entsprechenden Verwaltungseinheit verknüpft.*

Gruppenrichtlinien können mit mehreren Verwaltungseinheiten verknüpft werden (siehe Kapitel 5.1).

Gruppenrichtlinien verknüpfen!

1. *Wählen Sie die Verwaltungseinheit, mit der Sie eine Gruppenrichtlinie verknüpfen möchten, und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
2. *Wählen Sie VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN, danach aus der Liste die entsprechende Gruppenrichtlinie und bestätigen Sie die Auswahl mit OK.*

Nach der Erstellung einer Gruppenrichtlinie können den Registerkarten BEREICH und DETAILS des Inhaltsbereichs der Gruppenrichtlinien-Verwaltungskonsole detaillierte Informationen zu der Gruppenrichtlinie entnommen werden (Markierung eines Gruppenrichtlinienobjekts oder einer Gruppenrichtlinienverknüpfung).

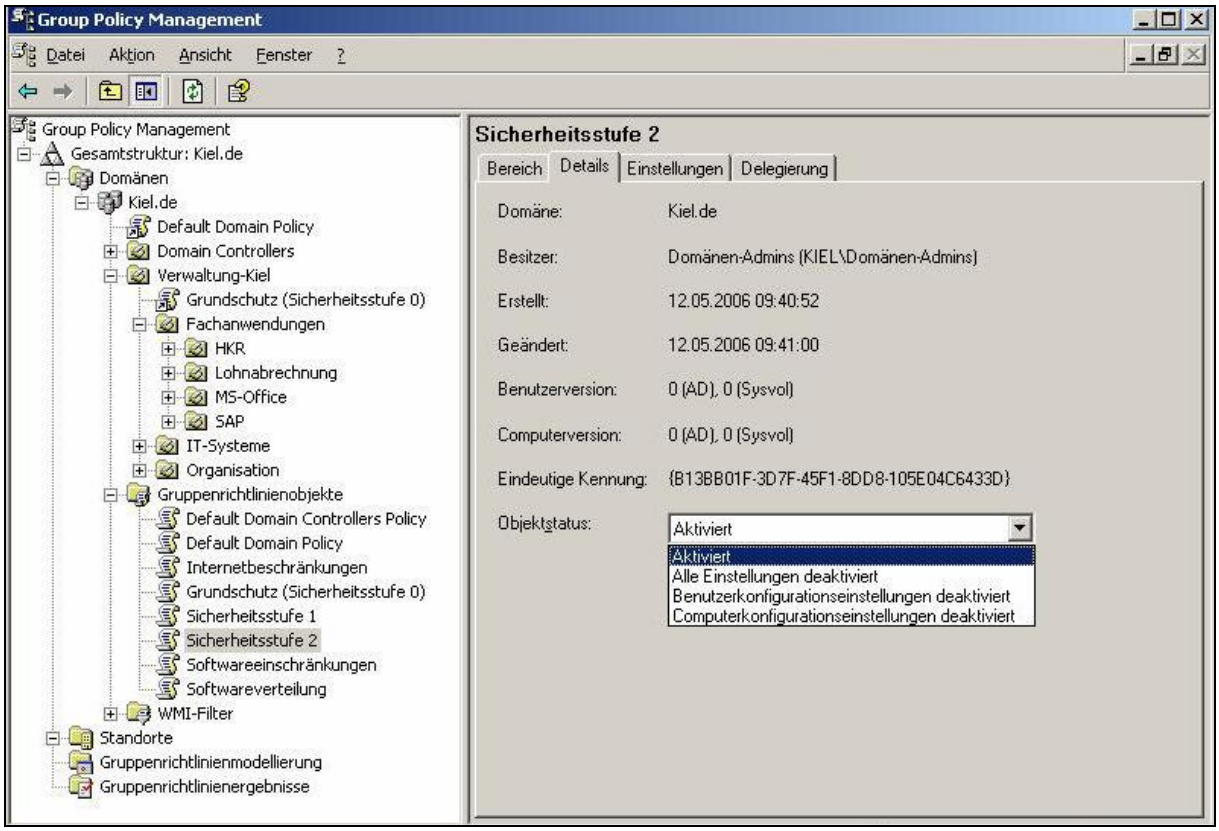


Registerkarte BEREICH der Gruppenrichtlinien-Verwaltungskonsole

Der Bereich VERKNÜPFUNGEN der Registerkarte BEREICH zeigt an, mit welchen Verwaltungseinheiten die entsprechende Gruppenrichtlinie verknüpft ist. In dem Beispiel oben wurde die Gruppenrichtlinie SICHERHEITSSTUFE 2 mit der Organisationseinheit ABTEILUNG PERSONAL verknüpft. Wird das Kontextmenü des entsprechenden Eintrags aufgerufen, können Einstellungen in Bezug auf den Status der Verknüpfung (Verknüpfung aktiviert oder deaktiviert) sowie den Vorrang (Erzwungen) vorgenommen werden.

Der Bereich SICHERHEITSFILTERUNG listet die Benutzer- und Gruppenkonten auf, für die die Einstellungen der Gruppenrichtlinien gelten sollen (siehe Kapitel 5.4). Standardmäßig ist die die Gruppe AUTHENTIFIZIERTE BENUTZER eingetragen.

Das Listenfeld des Bereichs WMI-FILTER gibt Auskunft darüber, ob ein WMI-Filter mit der Gruppenrichtlinie verknüpft ist. An dieser Stelle kann eine Verknüpfung mit einem WMI-Filter gelöst bzw. ein anderer WMI-Filter aus der Liste gewählt und mit der entsprechenden Gruppenrichtlinie verknüpft werden.

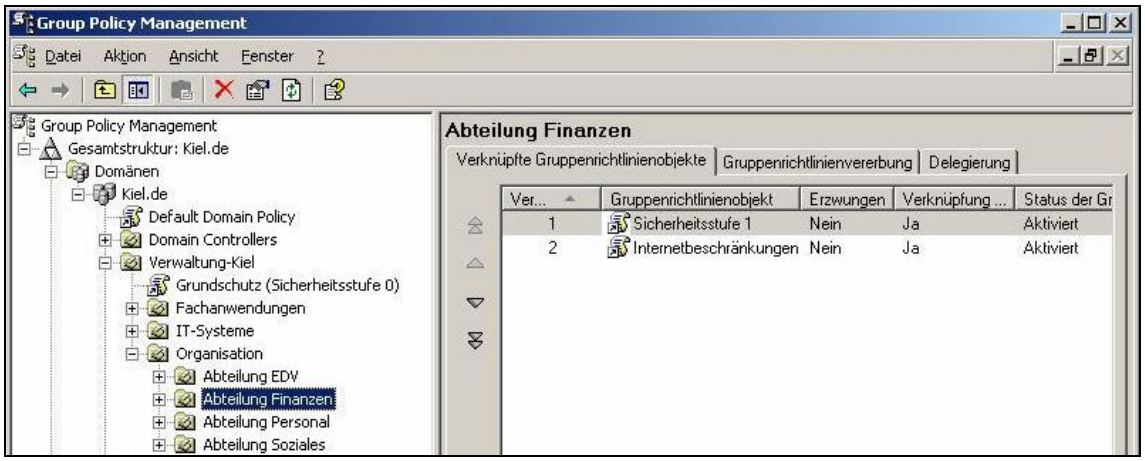


Registerkarte DETAILS der Gruppenrichtlinien-Verwaltungskonsole

Auf der Registerkarte DETAILS werden weitergehende Informationen zu der Gruppenrichtlinie angezeigt. Das Listenfeld OBJEKTSTATUS stellt Möglichkeiten zur vollständigen oder teilweisen Aktivierung und Deaktivierung zur Verfügung (siehe Abschnitt „Deaktivierung von Gruppenrichtlinien und Gruppenrichtlinienkomponenten“ in diesem Kapitel).

Gruppenrichtlinien löschen

Es können sowohl Gruppenrichtlinienverknüpfungen als auch ganze Gruppenrichtlinienobjekte gelöscht werden (siehe auch Kapitel 5.1). Zum Löschen von Gruppenrichtlinienverknüpfungen stehen mehrere Möglichkeiten zur Auswahl.



Registerkarte VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE einer Organisationseinheit

Gruppenrichtlinienverknüpfungen löschen!

1. *Wählen Sie die Gruppenrichtlinienverknüpfung, die Sie löschen möchten, und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
2. *Wählen Sie LÖSCHEN und bestätigen Sie die Sicherheitsabfrage mit OK.*

Oder:

1. *Markieren Sie die Verwaltungseinheit, in der die Gruppenrichtlinienverknüpfung aufgelistet ist, die Sie löschen möchten.*
2. *Wählen Sie im Inhaltsbereich der Gruppenrichtlinien-Verwaltungskonsole auf der Registerkarte VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE (siehe Abbildung oben) die entsprechende Gruppenrichtlinienverknüpfung und rufen Sie das Kontextmenü auf.*
3. *Wählen Sie LÖSCHEN und bestätigen Sie die Sicherheitsabfrage mit OK.*

Oder:

1. *Wählen Sie im Container GRUPPENRICHTLINIENOBJEKTE die Gruppenrichtlinie, deren Verknüpfung Sie löschen möchten. Markieren Sie die entsprechende Gruppenrichtlinie.*
2. *Markieren Sie auf der Registerkarte BEREICH die Verknüpfung, die Sie löschen möchten, und rufen Sie das Kontextmenü auf.*
3. *Wählen Sie VERKNÜPFUNG LÖSCHEN und bestätigen Sie die Sicherheitsabfrage mit OK.*

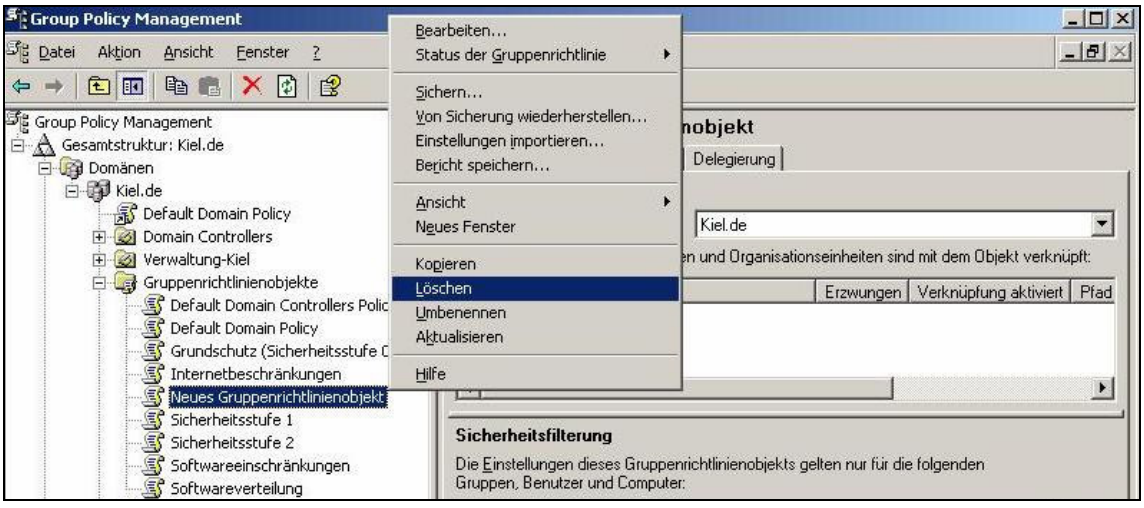
Sollen Gruppenrichtlinienobjekte gelöscht werden, so ist zu beachten, dass sowohl das Objekt an sich als auch alle seine Verknüpfungen gelöscht werden (siehe Kapitel 5.1).

Gruppenrichtlinienobjekte löschen!

1. *Wählen Sie den Container GRUPPENRICHTLINIENOBJEKTE.*
2. *Markieren Sie auf der Registerkarte INHALT die Gruppenrichtlinie, die Sie löschen möchten, und rufen Sie das Kontextmenü auf.*
3. *Wählen Sie LÖSCHEN und bestätigen Sie die Sicherheitsabfrage mit OK.*

Oder:

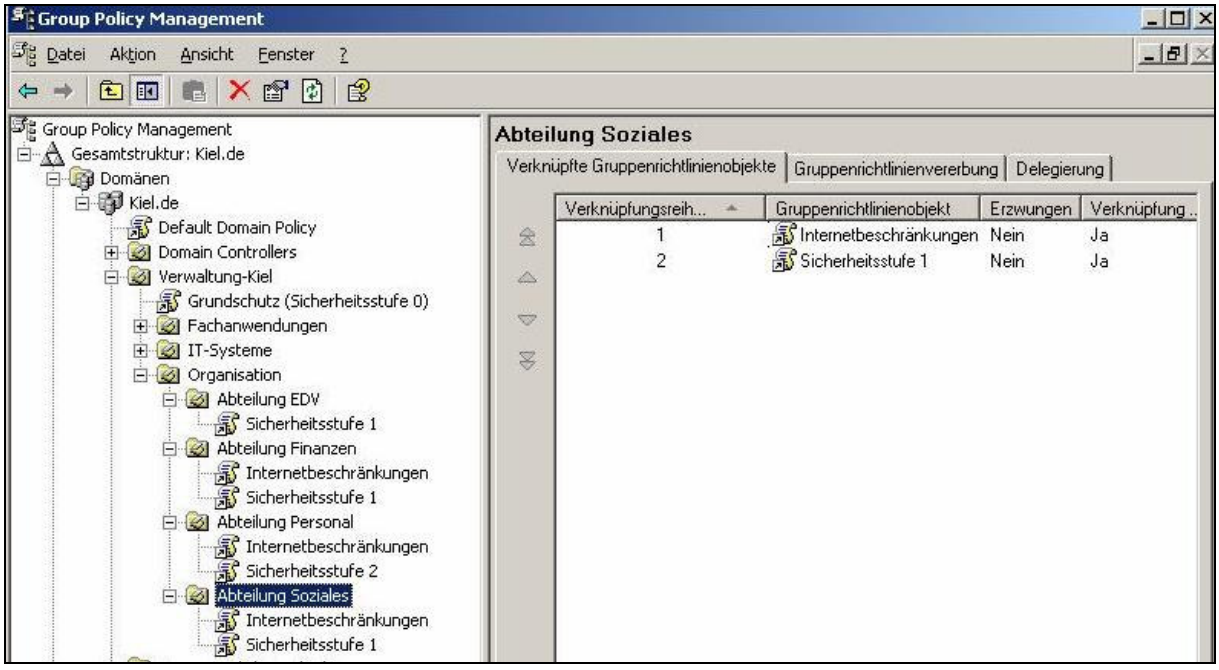
1. *Wählen Sie im Container GRUPPENRICHTLINIENOBJEKTE im Navigationsbereich der Gruppenrichtlinien-Verwaltungskonsole das Gruppenrichtlinienobjekt, das Sie löschen möchten (siehe Abbildung unten).*
2. *Rufen Sie das Kontextmenü auf, wählen Sie LÖSCHEN und bestätigen Sie die Sicherheitsabfrage mit OK.*



Gruppenrichtlinienobjekte löschen

Verknüpfungsreihenfolge ändern

Bei der Verknüpfung mehrerer Gruppenrichtlinien mit einer Verwaltungseinheit lässt sich die Verknüpfungs- bzw. Verarbeitungsreihenfolge (siehe auch Kapitel 5.2) auf der Registerkarte VERKNÜPFTE RICHTLINIENOBJEKTE anpassen. Dabei ist zu beachten, dass die Gruppenrichtlinie, die den Wert 1 der Verknüpfungsreihenfolge besitzt, die höchste Priorität hat und als Letztes verarbeitet wird (siehe Abbildung unten). Im Beispiel unten wird zunächst die Gruppenrichtlinie Sicherheitsstufe 1 verarbeitet, danach die Gruppenrichtlinie Internetbeschränkungen.



Verknüpfungsreihenfolge auf der Registerkarte VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE

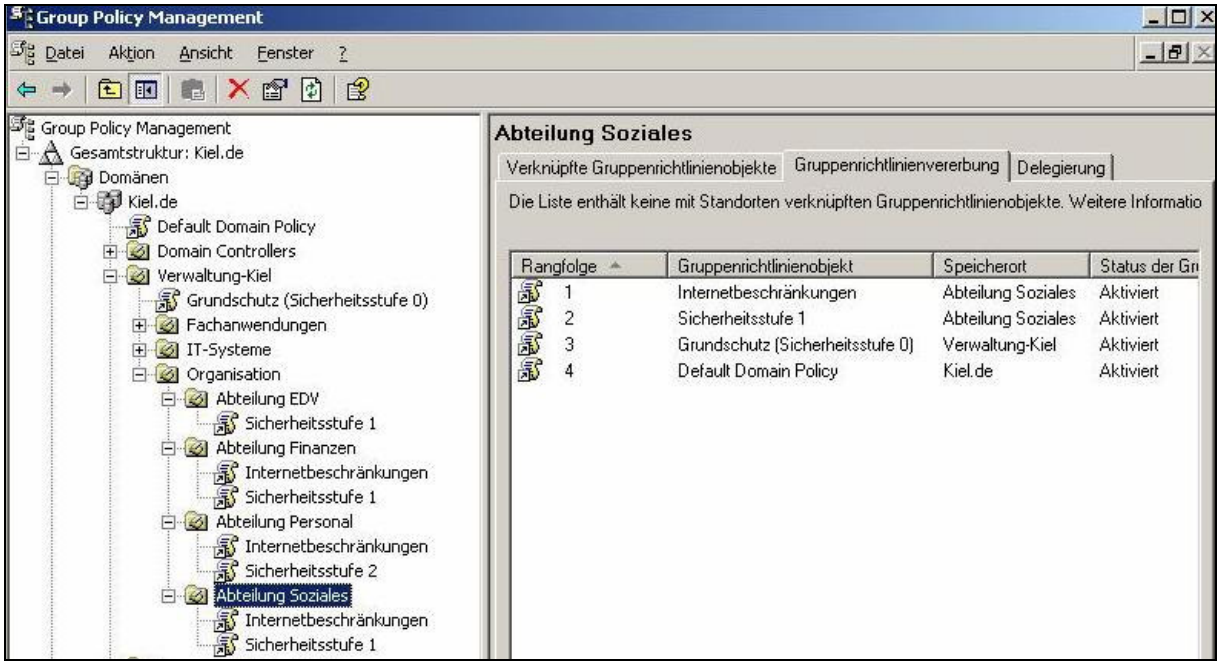
Verarbeitungsreihenfolge ändern!

1. *Wählen Sie die Verwaltungseinheit (z. B. Organisationseinheit), in der Sie die Verarbeitungsreihenfolge der verknüpften Gruppenrichtlinien ändern möchten.*
2. *Wählen Sie auf der Registerkarte VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE die entsprechende Gruppenrichtlinie und ändern Sie mit den Pfeiltasten den Wert der Verknüpfungsreihenfolge.*
3. *Die Gruppenrichtlinie mit dem höchsten Wert wird zuerst, die Gruppenrichtlinie mit dem Wert 1 wird als Letztes abgearbeitet.*

Vererbungsreihenfolge

Zusätzlich zu der Verarbeitungsreihenfolge innerhalb einer Verwaltungseinheit werden auf der Registerkarte GRUPPENRICHTLINIENVERERBUNG einer Verwaltungseinheit diejenigen Gruppenrichtlinien berücksichtigt, die ihre Einstellungen auf die Verwaltungseinheit vererben.

Im Beispiel (Abbildung unten) ist erkennbar, dass die Gruppenrichtlinien SICHERHEITSSTUFE 1 und INTERNETBESCHRÄNKUNGEN mit der Organisationseinheit ABTEILUNG SOZIALES verknüpft sind. Die Einstellungen der Gruppenrichtlinie GRUNDSCHUTZ wurden von der Organisationseinheit VERWALTUNG-KIEL und die Einstellungen der Gruppenrichtlinie DEFAULT DOMAIN POLICY von der Domäne KIEL vererbt. Effektiv werden die vererbten und verknüpften Gruppenrichtlinien in der angegebenen Rangfolge verarbeitet. In diesem Fall wird zunächst die DEFAULT DOMAIN POLICY verarbeitet, gefolgt von den Gruppenrichtlinien GRUNDSCHUTZ, SICHERHEITSSTUFE 1 und INTERNETBESCHRÄNKUNGEN.



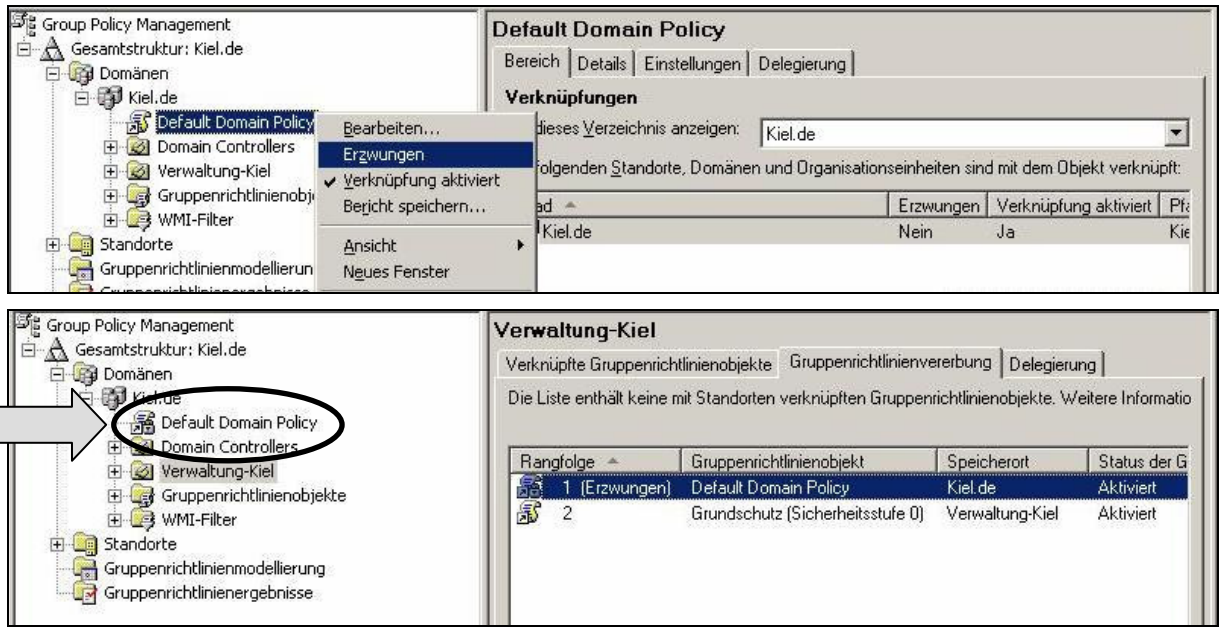
Vererbungsreihenfolge auf der Registerkarte GRUPPENRICHTLINIENVERERBUNG

Auf der Registerkarte GRUPPENRICHTLINIENVERERBUNG lassen sich keine Veränderungen in Bezug auf die Verarbeitungsreihenfolge vornehmen, angezeigt wird die effektive Abarbeitungsreihenfolge der Gruppenrichtlinien mit Berücksichtigung von Vererbungsoptionen (diese werden in den nächsten Absätzen behandelt).

Option ERZWUNGEN

Die Option KEIN VORRANG wurde von Microsoft begrifflich überarbeitet und ist gleichbedeutend mit der Option ERZWUNGEN. Wird sie auf eine Gruppenrichtlinie angewendet, kann keine nachfolgende Gruppenrichtlinie die Einstellungen der so markierten Gruppenrichtlinie überschreiben (siehe Kapitel 5.3).

Visuell wird die Option ERZWUNGEN in der Gruppenrichtlinien-Verwaltungskonsole mit einem (sehr) kleinen Pfeil in der rechten unteren Ecke der entsprechenden Gruppenrichtlinienverknüpfung gekennzeichnet. Diese Markierung ist auch auf der Registerkarte GRUPPENRICHTLINIENVERERBUNG der einzelnen Verwaltungseinheiten erkennbar, zusätzlich wird der Begriff ERZWUNGEN hinter der Rangfolge der Gruppenrichtlinie angehängt (siehe Abbildung unten). In dem Beispiel unten wurde die Option ERZWUNGEN auf die Gruppenrichtlinie DEFAULT DOMAIN POLICY angewendet.



Option ERZWUNGEN der Gruppenrichtlinien-Verwaltungskonsole

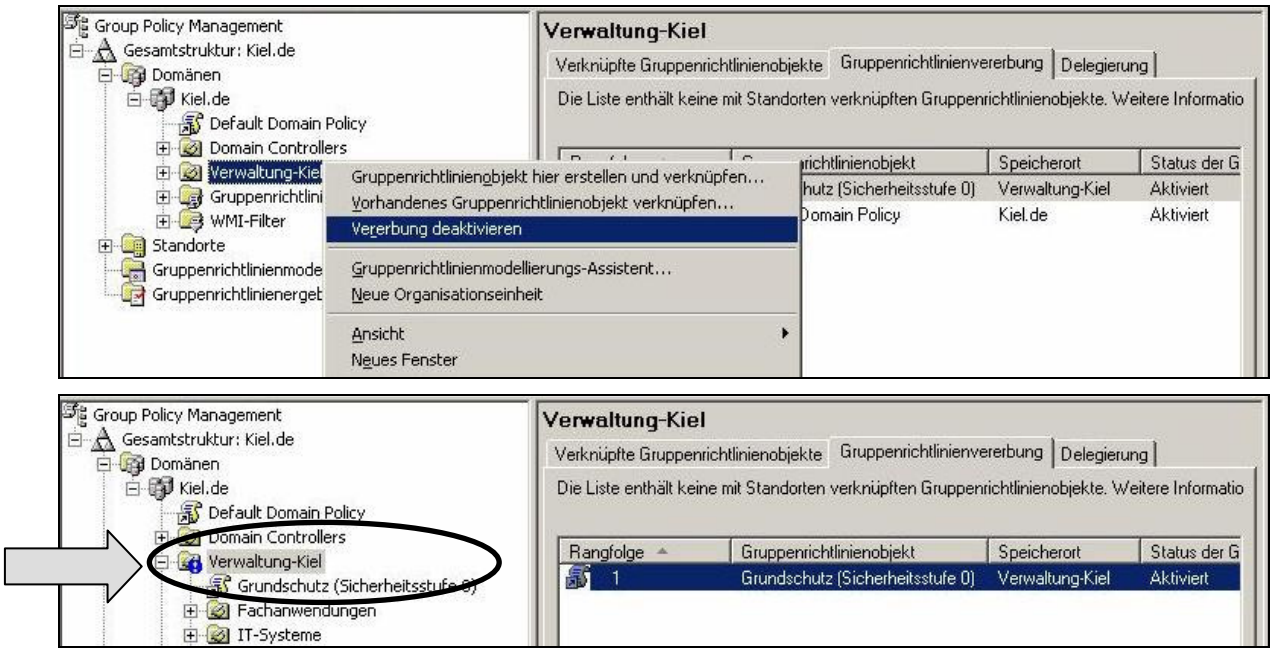
Option ERZWUNGEN auf eine Gruppenrichtlinienverknüpfung anwenden!

1. *Markieren Sie die Gruppenrichtlinienverknüpfung, auf die Sie die Option ERZWUNGEN anwenden möchten, und rufen Sie das Kontextmenü auf.*
2. *Wählen Sie den Eintrag ERZWUNGEN.*

Option VERERBUNG DEAKTIVIEREN

Die Option VERERBUNG DEAKTIVIEREN soll verhindern, dass Einstellungen von hierarchisch übergeordneten Gruppenrichtlinien auf die entsprechende Verwaltungseinheit angewendet werden (siehe Kapitel 5.3).

In der Gruppenrichtlinien-Verwaltungskonsole wird die Option VERERBUNG DEAKTIVIEREN mit einer blauen Markierung (Ausrufezeichen) gekennzeichnet.



Option VERERBUNG DEAKTIVIEREN der Gruppenrichtlinien-Verwaltungskonsole

Option VERERBUNG DEAKTIVIEREN auf eine Organisationseinheit anwenden!

1. *Markieren Sie die Organisationseinheit, auf die Sie die Option VERERBUNG DEAKTIVIEREN anwenden möchten, und rufen Sie das Kontextmenü auf.*
2. *Wählen Sie den Eintrag VERERBUNG DEAKTIVIEREN.*

Nachdem in einer Verwaltungseinheit die Option VERERBUNG DEAKTIVIEREN angewendet wurde, werden auf der Registerkarte GRUPPENRICHTLINIENVERERBUNG der entsprechenden Verwaltungseinheit die übergeordneten Gruppenrichtlinien ausgeblendet. In der Abbildung oben wurde die Option auf die Organisationseinheit VERWALTUNG-KIEL angewendet.

Deaktivierung von Gruppenrichtlinien und Gruppenrichtlinienkomponenten

Die Aktivierung bzw. Deaktivierung von Gruppenrichtlinien und Gruppenrichtlinienkomponenten werden in der Gruppenrichtlinien-Verwaltungskonsole unter dem Oberbegriff STATUS DER GRUPPENRICHTLINIE zusammengefasst. Dieser Status bietet die Möglichkeit, Gruppenrichtlinien ganz oder teilweise zu deaktivieren (siehe Kapitel 5.3).

STATUS DER GRUPPENRICHTLINIE in der Gruppenrichtlinien-Verwaltungskonsole

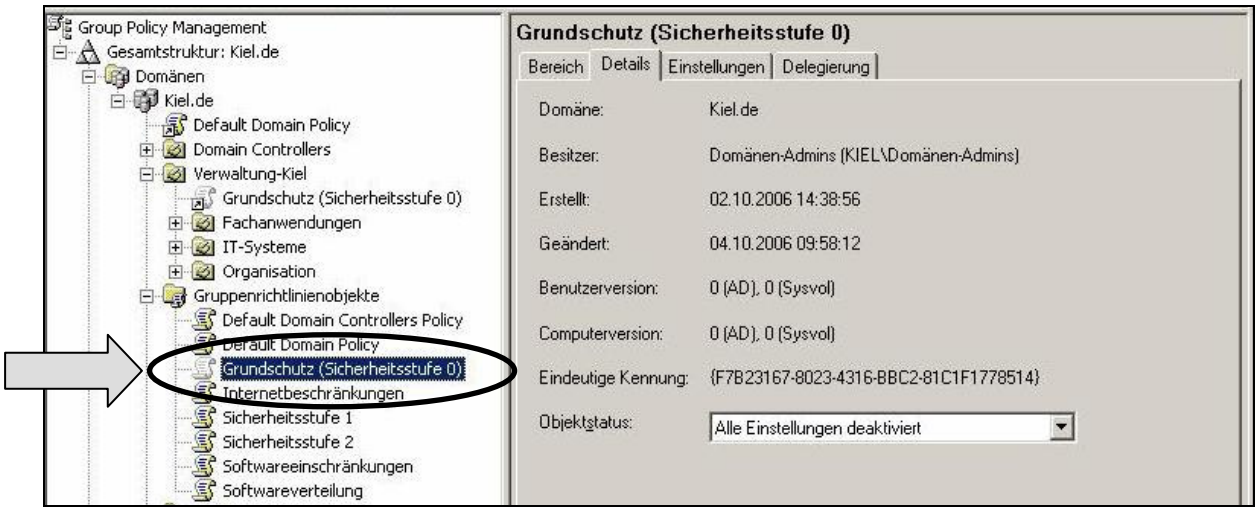
Gruppenrichtlinien oder Gruppenrichtlinienkomponenten deaktivieren!

1. *Navigieren Sie zu dem Container GRUPPENRICHTLINIENOBJEKTE und markieren Sie die Gruppenrichtlinie, die Sie ganz oder teilweise deaktivieren möchten.*
2. *Wählen Sie aus dem Kontextmenü den Eintrag STATUS DER GRUPPENRICHTLINIE und danach eine der Optionen AKIVIERT, BENUTZERKONFIGURATIONSEINSTELLUNGEN DEAKTIVIERT, COMPUTERKONFIGURATIONSEINSTELLUNGEN DEAKTIVIERT oder ALLE EINSTELLUNGEN DEAKTIVIERT.*

Oder:

1. *Navigieren Sie zu dem Container GRUPPENRICHTLINIENOBJEKTE und markieren Sie die Gruppenrichtlinie, die Sie ganz oder teilweise deaktivieren möchten.*
2. *Wechseln Sie im INHALTSBEREICH der Gruppenrichtlinien-Verwaltungskonsole auf die Registerkarte DETAILS und ändern Sie den Status der Gruppenrichtlinie durch Auswahl eines Eintrags im Listenfeld OBJEKTSTATUS.*

Die Deaktivierung einer Gruppenrichtlinie wird in der Gruppenrichtlinien-Verwaltungskonsole nur dann visuell angezeigt, wenn alle Einstellungen deaktiviert werden. Das Symbol der Gruppenrichtlinie und der Gruppenrichtlinienverknüpfung wird in diesem Fall durchscheinend (siehe folgende Abbildung) dargestellt.



Deaktivierte Richtlinie

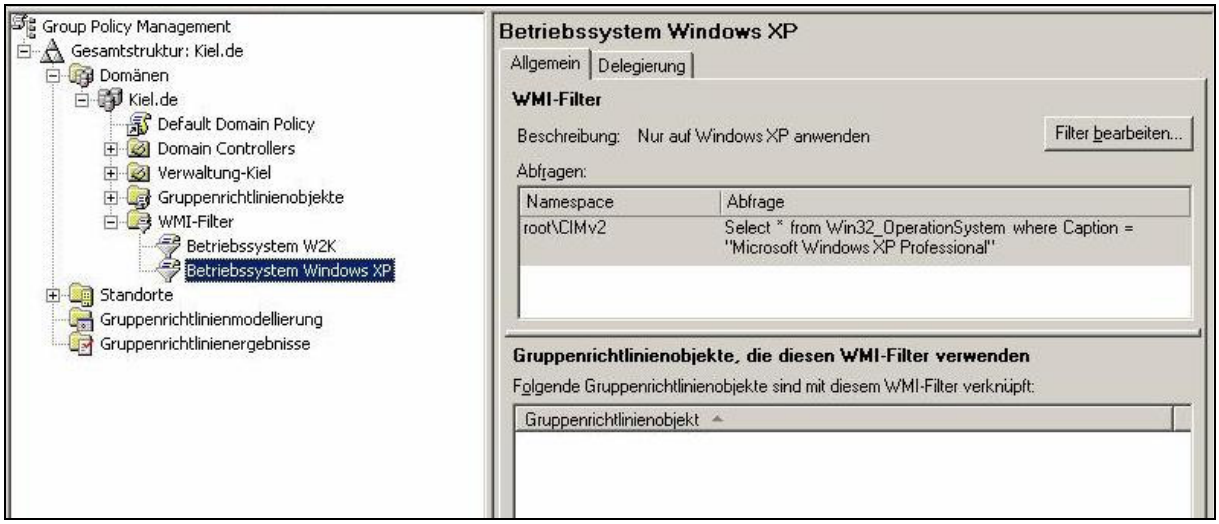
Eine teilweise Deaktivierung einer Gruppenrichtlinie im Bereich der Benutzer- bzw. der Computerkonfigurationseinstellungen ist in der Gruppenrichtlinien-Verwaltungskonsole auf den ersten Blick nicht erkennbar. Die Registerkarte GRUPPENRICHTLINIENVERERBUNG einer Verwaltungseinheit, im Beispiel unten der Organisationseinheit ABTEILUNG FINANZEN, gibt in diesem Fall Auskunft über die entsprechende Deaktivierung.

Teilweise deaktivierte Richtlinie

WMI-Filter einsetzen

WMI-Filter bieten die Möglichkeit, die technische Konfiguration auf dem Client abzufragen und die Ausführung einer Gruppenrichtlinie davon abhängig zu machen (siehe Kapitel 5.4). In der Gruppenrichtlinien-Verwaltungskonsole können WMI-Filter in zwei Bereichen bearbeitet bzw. verknüpft werden.

Der Container WMI-FILTER übernimmt die Sammelfunktion der in der Domäne erstellten WMI-Filter. Unterhalb des Containers WMI-FILTER werden alle Filter aufgelistet und die Registerkarten ALLGEMEIN und DELEGIERUNG im Inhaltsbereich der Gruppenrichtlinien-Verwaltungskonsole liefern weitere Informationen und Funktionalitäten zu dem markierten WMI-Filter. Über das Kontextmenü des Containers WMI-Filter können neue Filter erstellt oder vorhandene Filter importiert werden.



Container WMI-FILTER

Einen WMI-Filter erstellen!

1. *Markieren Sie den Container WMI-FILTER und rufen Sie das Kontextmenü auf.*
2. *Wählen Sie den Eintrag NEU. Vergeben Sie in dem Dialogfenster NEUER WMI-FILTER einen Namen und eine Beschreibung für den neuen Filter und öffnen Sie mit der Schaltfläche HINZUFÜGEN das WMI-Abfragefenster.*
3. *Tragen Sie Ihre WMI-Abfrage in das Textfeld ein und bestätigen Sie mit OK. Wählen Sie im Dialogfenster NEUER WMI-FILTER die Schaltfläche SPEICHERN.*
4. *Der neue WMI-Filter wird unterhalb des Containers WMI-FILTER aufgelistet.*

Ein WMI-Filter liegt nach dem Import oder der Erstellung zunächst als Objekt vor, standardmäßig wird noch keine Verknüpfung zu einer Gruppenrichtlinie erstellt. Eine Verknüpfung eines WMI-Filters mit einer Gruppenrichtlinie muss durch den Administrator explizit vorgenommen werden.

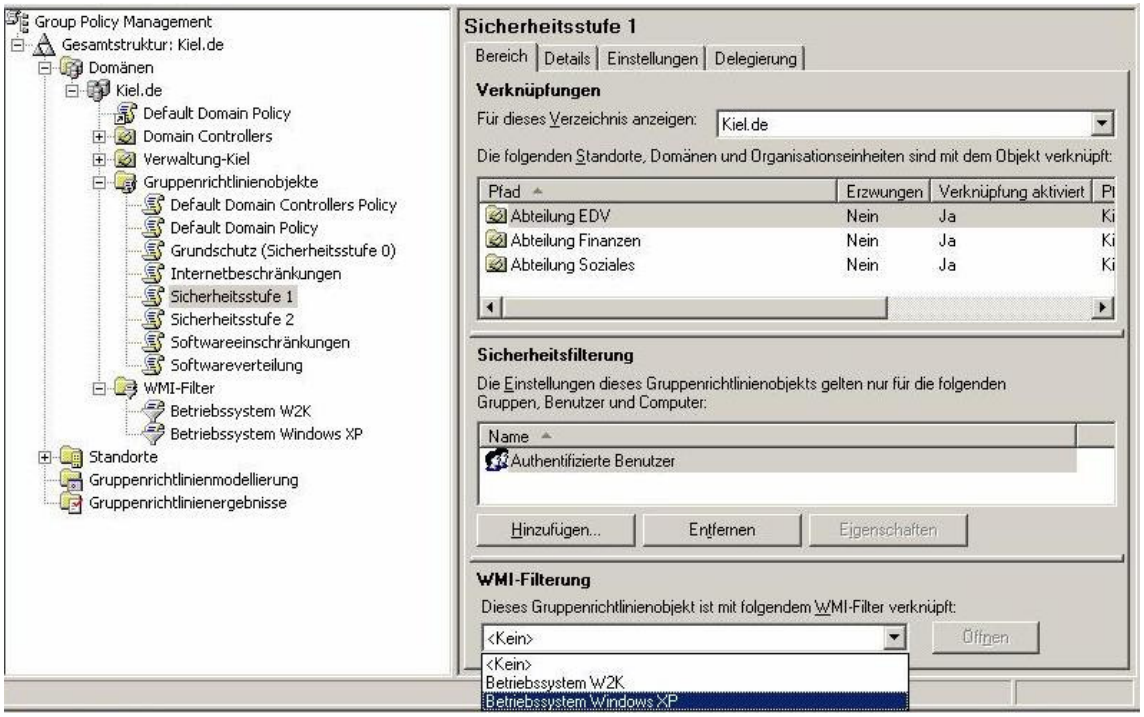
Einen WMI-Filter verknüpfen!

1. *Navigieren Sie zu dem Container WMI-FILTER und markieren Sie den Filter, den Sie mit einer Gruppenrichtlinie verknüpfen möchten.*
2. *Rufen Sie auf der Registerkarte ALLGEMEIN im unteren Textfeld GRUPPENRICHTLINIENOBJEKTE, DIE DIESEN WMI-FILTER VERWENDEN das Kontextmenü auf und wählen Sie HINZUFÜGEN.*
3. *Wählen Sie aus der Liste der Gruppenrichtlinien die entsprechende Gruppenrichtlinie aus und bestätigen Sie mit OK.*

Oder:

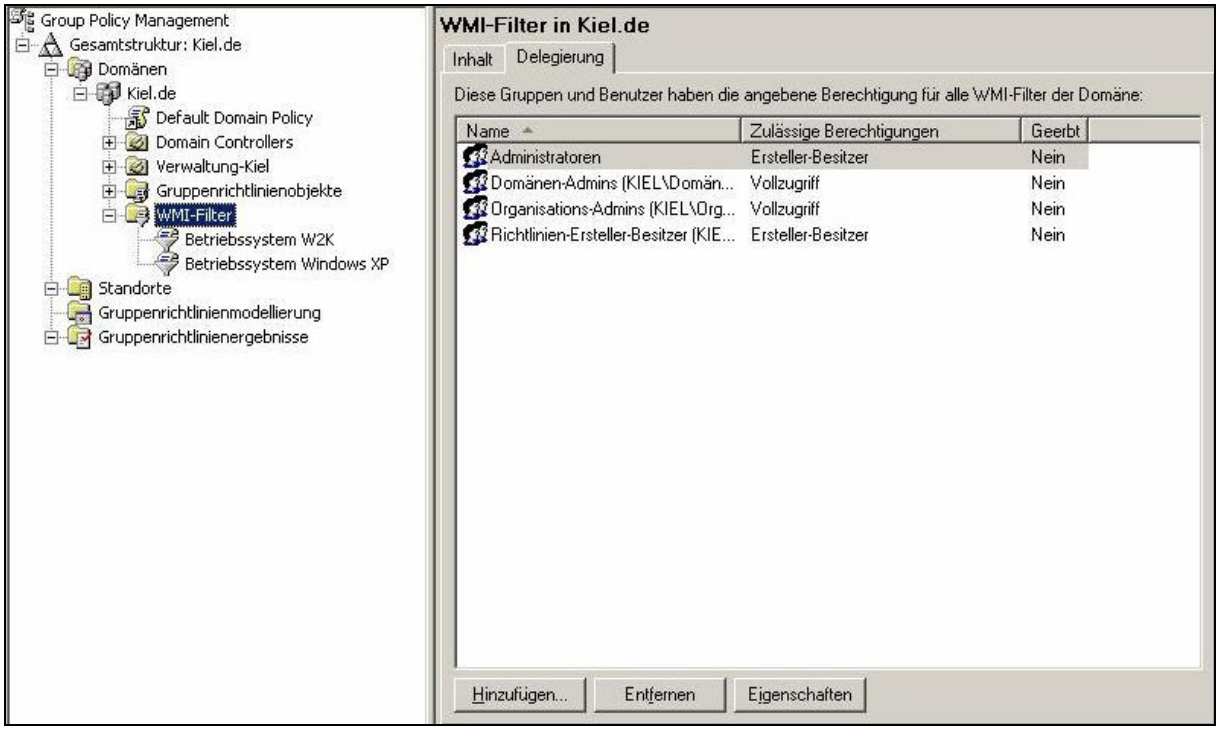
1. *Navigieren Sie zu der Gruppenrichtlinie oder der Gruppenrichtlinienverknüpfung, die Sie mit einem WMI-Filter verknüpfen möchten.*
2. *Öffnen Sie auf der Registerkarte BEREICH das Listenfeld WMI-FILTERUNG, markieren Sie den entsprechenden WMI-Filter (siehe folgende Abbildung) und bestätigen Sie mit JA.*

Ein WMI-Filter wird immer als Attribut der Gruppenrichtlinie gespeichert. Sie können zwar auf der Registerkarte BEREICH einer Gruppenrichtlinienverknüpfung einen WMI-Filter zuweisen, dieser wird im Hintergrund aber mit dem entsprechenden Gruppenrichtlinienobjekt verknüpft. Der WMI-Filter wirkt also nicht nur auf die einzelnen Gruppenrichtlinienverknüpfungen sondern auf alle Benutzer- und Computerkonten einer Verwaltungseinheit, die mit dem entsprechenden Gruppenrichtlinienobjekt verknüpft sind.



WMI-Filter verknüpfen

Auf der Registerkarte DELEGIERUNG eines WMI-Filters kann die Verwaltung von WMI-Filtern an andere Benutzer- und Gruppenkonten delegiert werden. Standardmäßig erhalten die administrativen Konten die Berechtigung, WMI-Filter zu erstellen und zu verwalten.



Registerkarte DELEGIERUNG des Containers WMI-FILTER

Berechtigungen auf Gruppenrichtlinien

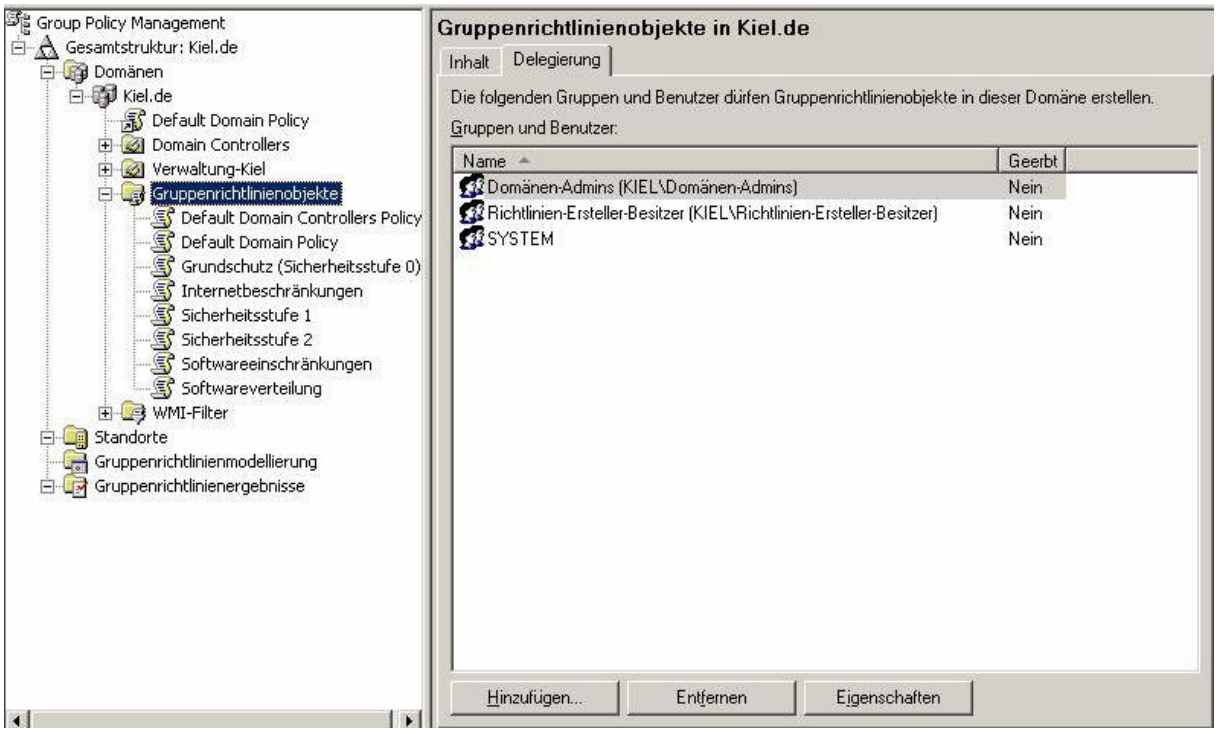
In der Gruppenrichtlinien-Verwaltungskonsole lassen sich auf unterschiedlichen Ebenen Berechtigungen zur Verwaltung von Gruppenrichtlinien vergeben (siehe auch Kapitel 5.4). Auf der Registerkarte DELEGIERUNG

- des Containers GRUPPENRICHTLINIENOBJEKTE,
- einer Verwaltungseinheit (Standort, Domäne und Organisationseinheit),
- einer Gruppenrichtlinie bzw. Gruppenrichtlinienverknüpfung

lassen sich differenzierte Rechte vergeben, die nachfolgend näher erläutert werden.

Die **Registerkarte DELEGIERUNG des Containers GRUPPENRICHTLINIENOBJEKTE** listet alle Benutzer- und Gruppenkonten auf, die in der entsprechenden Domäne Gruppenrichtlinien erstellen dürfen. Standardmäßig wird den administrativen Konten dieses Recht zugewiesen

(siehe Abbildung unten). Über die Schaltfläche HINZUFÜGEN kann das Recht zur Erstellung von Gruppenrichtlinien an weitere Benutzer- bzw. Gruppenkonten delegiert werden.

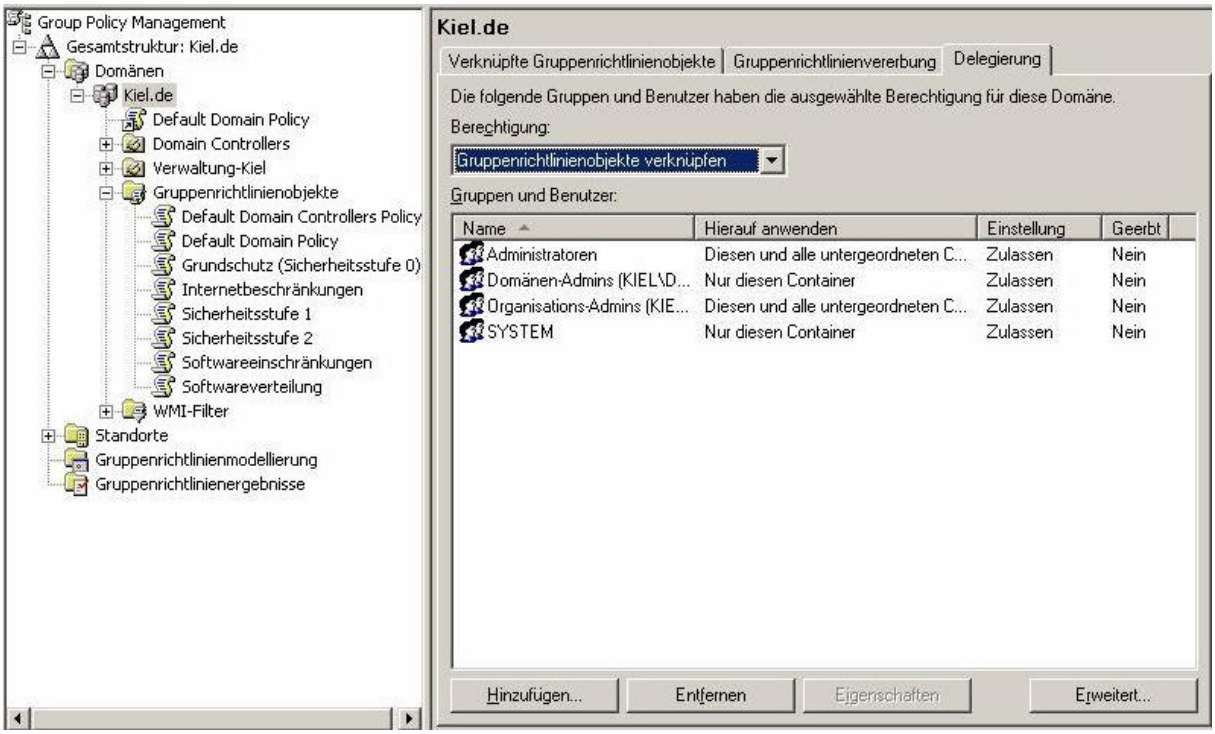


Registerkarte DELEGIERUNG des Containers GRUPPENRICHTLINIENOBJEKTE

Benutzern das Recht zur Erstellung von Gruppenrichtlinien delegieren!

1. *Wählen Sie auf der Registerkarte DELEGIERUNG die Schaltfläche HINZUFÜGEN.*
2. *Wählen Sie das entsprechende Gruppen- oder Benutzerkonto aus, das Gruppenrichtlinien erstellen soll, und bestätigen Sie mit OK.*
3. *Mit der Schaltfläche ENTFERNEN können Sie Gruppen- oder Benutzerkonten wieder aus der Liste entfernen, die Schaltfläche EIGENSCHAFTEN öffnet das Eigenschaftenfenster z. B. eines Gruppenkontos und Sie können an dieser Stelle die Gruppenmitgliedschaften verwalten.*

Die **Registerkarte DELEGIERUNG einer Verwaltungseinheit** listet alle Benutzer- und Gruppenkonten auf, die Gruppenrichtlinien mit dieser Verwaltungseinheit verknüpfen oder die Werkzeuge GRUPPENRICHTLINIENERGEBNISSE bzw. GRUPPENRICHTLINIENMODELLIERUNGEN ausführen dürfen. Standardmäßig werden den administrativen Konten diese Rechte zugewiesen (siehe folgende Abbildung).



Registerkarte DELEGIERUNG einer Verwaltungseinheit

Folgende Berechtigungen können auf der Ebene der Verwaltungseinheiten delegiert werden:

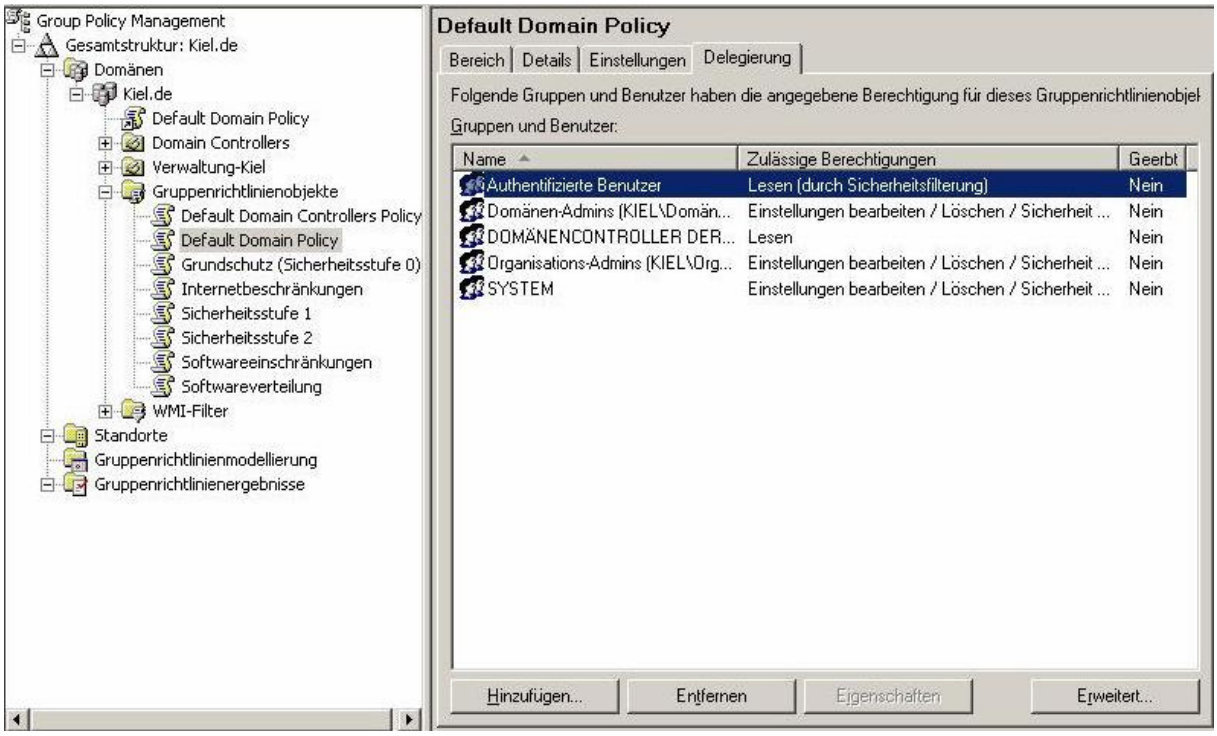
- Analysen zur Gruppenrichtlinienmodellierung durchführen,
- Gruppenrichtlinienergebnisse lesen und
- Gruppenrichtlinienobjekte verknüpfen.

Benutzern das Recht zur Verknüpfung von Gruppenrichtlinien delegieren!

1. *Wählen Sie auf der Registerkarte DELEGIERUNG im Listenfeld BERECHTIGUNG die Berechtigung GRUPPENRICHTLINIENOBJEKTE VERKNÜPFEN.*
2. *Wählen Sie über die Schaltfläche HINZUFÜGEN das entsprechende Gruppen- oder Benutzerkonto aus, dem Sie das entsprechende Recht delegieren möchten, und bestätigen Sie mit OK.*
3. *Mit der Schaltfläche ENTFERNEN können Sie Gruppen- oder Benutzerkonten wieder aus der Liste entfernen, die Schaltfläche EIGENSCHAFTEN öffnet das Eigenschaftenfenster z. B. eines Gruppenkontos und Sie können an dieser Stelle die Gruppenmitgliedschaften verwalten.*

Die Registerkarte DELEGIERUNG einer Gruppenrichtlinie oder Gruppenrichtlinienverknüpfung listet alle Benutzer- und Gruppenkonten auf, die Berechtigungen an dem Gruppenrichtlinien-

objekt besitzen. Standardmäßig erhalten die administrativen Konten Vollzugriff auf die Objektberechtigungen. Über die Schaltfläche HINZUFÜGEN können detaillierte und differenzierte Rechte am Gruppenrichtlinienobjekt an weitere Benutzer- bzw. Gruppenkonten delegiert werden.

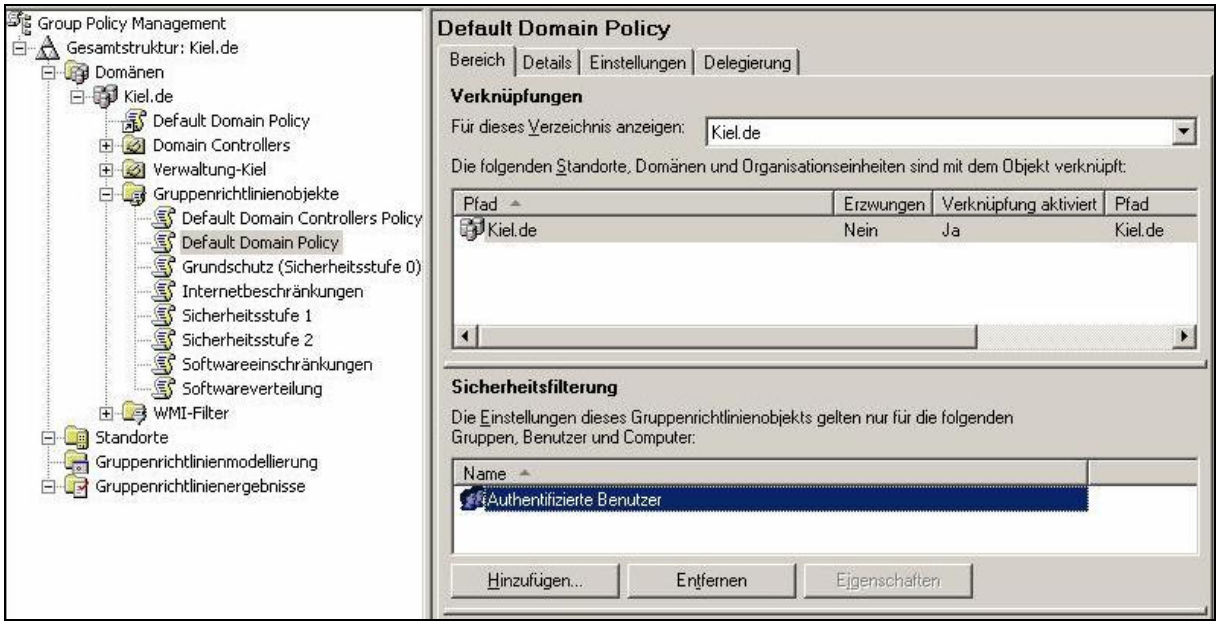


Registerkarte DELEGIERUNG eines Gruppenrichtlinienobjekts

Auf der Registerkarte DELEGIERUNG wird standardmäßig die Gruppe AUTHENTIFIZIERTE BENUTZER mit der Berechtigung LESEN (DURCH SICHERHEITSFILTERUNG) aufgelistet (siehe Abbildung oben). Diese Berechtigung beinhaltet die beiden Detailberechtigungen LESEN und GRUPPENRICHTLINIE ÜBERNEHMEN. Diese Berechtigungen sind für die Anwendung von Gruppenrichtlinien entscheidend (siehe Kapitel 5.4) und werden von der Registerkarte BEREICH im Abschnitt SICHERHEITSFILTERUNG übernommen (siehe folgende Abbildung).

In dem Abschnitt SICHERHEITSFILTERUNG werden alle für diese Gruppenrichtlinie aktivierten Sicherheitsfilterungen aufgelistet. Mit der Schaltfläche HINZUFÜGEN können gezielt Benutzer- und Gruppenkonten aufgenommen werden. Dabei werden im Hintergrund automatisch die beiden Berechtigungen LESEN und GRUPPENRICHTLINIE ÜBERNEHMEN konfiguriert und auf der Registerkarte DELEGIERUNG mit der Berechtigung LESEN (DURCH SICHERHEITSFILTERUNG) aufgeführt.

Mit der Schaltfläche ENTFERNEN können Benutzer- und Gruppenkonten entfernt werden, die Schaltfläche EIGENSCHAFTEN öffnet das Eigenschaftenfenster des entsprechenden Benutzer- oder Gruppenkontos im Active Directory.



Sicherheitsfilterung auf der Registerkarte BEREICH

Wenn Sie ein Benutzer- oder Gruppenkonto von der Anwendung einer Gruppenrichtlinie ausschließen wollen, so können Sie diese Einstellung nicht im Abschnitt SICHERHEITSFILTERUNG der Registerkarte BEREICH vornehmen, sondern müssen auf die Registerkarte DELEGIERUNG wechseln.

Die Anwendung einer Gruppenrichtlinie verweigern!

1. *Markieren Sie das Gruppenrichtlinienobjekt, dem Sie eine Verweigerung hinzufügen möchten, und wechseln Sie auf die Registerkarte DELEGIERUNG.*
2. *Wählen Sie ein vorhandenes Gruppen- oder Benutzerkonto oder fügen Sie über die Schaltfläche HINZUFÜGEN das entsprechende Benutzer- oder Gruppenkonto hinzu. Wählen Sie im Dialogfeld das vordefinierte Recht LESEN und bestätigen Sie mit OK.*
3. *Markieren Sie das erstellte Benutzer- oder Gruppenkonto und öffnen Sie über die Schaltfläche ERWEITERT die Detailberechtigungen.*
4. *Ändern Sie das Recht GRUPPENRICHTLINIE ÜBERNEHMEN von ZULASSEN in VERWEIGERN und bestätigen Sie mit OK.*

Die Übersichtlichkeit und Transparenz hat sich im Bereich der Gruppenrichtlinienverwaltung mit der Gruppenrichtlinien-Verwaltungskonsole deutlich verbessert. Auch die Dokumentation der delegierten Rechte, der Sicherheitsfilterung und Verweigerungen wurde in die Berichtserstellung der Gruppenrichtlinien-Verwaltungskonsole mit aufgenommen (siehe nächster Abschnitt). Allerdings ist eine strukturierte und detaillierte Auswertung mit den Werkzeugen der Gruppenrichtlinien-Verwaltungskonsole immer noch nicht möglich.

Dokumentation der Gruppenrichtlinien

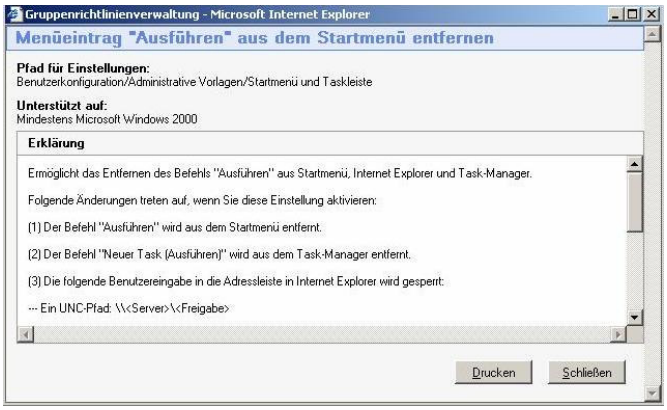
Bisher war es mit den Bordmitteln von Windows 2000/2003 nicht möglich, eine umfassende Dokumentation aller vorgenommenen Einstellungen der einzelnen Gruppenrichtlinien zu erstellen. Die Gruppenrichtlinien-Verwaltungskonsole bietet jetzt die Möglichkeit, die Einstellungen einer ausgewählten Gruppenrichtlinie

- auf der Registerkarte EINSTELLUNGEN in Form eines HTML-Berichts darzustellen,
- in Form einer HTML- oder XML-Datei abzuspeichern und
- als einen Bericht auszudrucken.

Die Registerkarte EINSTELLUNGEN zeigt in einer übersichtlichen Struktur die konfigurierten Richtlinien einer Gruppenrichtlinie. Damit ist für den Systemverantwortlichen auf einen Blick erkennbar, welche Einstellungen in der entsprechenden Gruppenrichtlinie vorgenommen wurden.

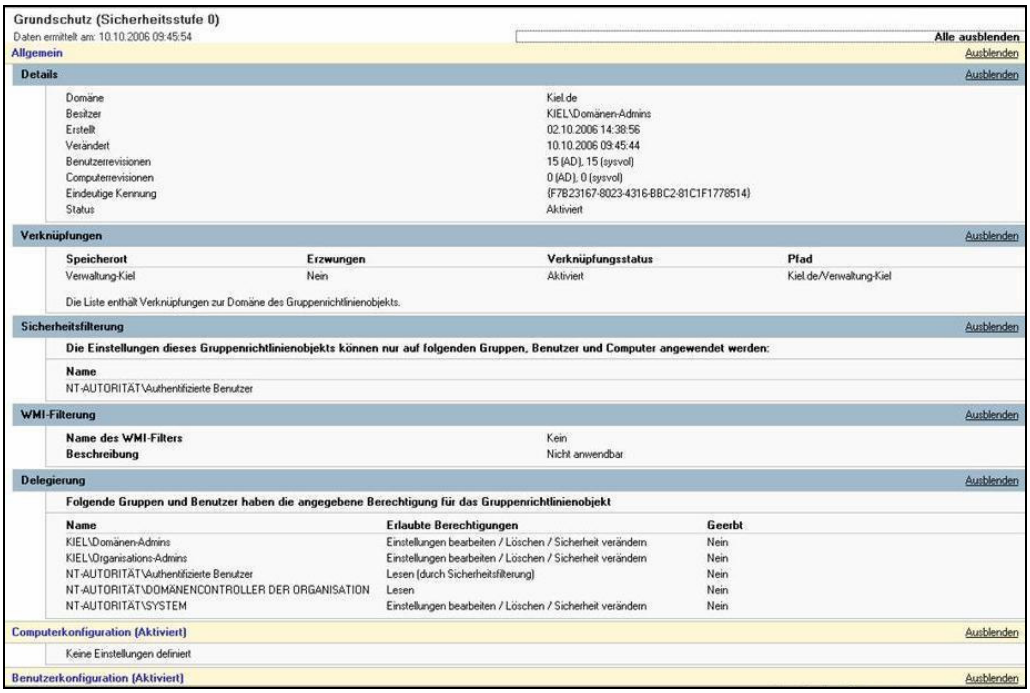
HTML-Bericht auf der Registerkarte EINSTELLUNGEN

Die einzelnen Einstellungen der ADMINISTRATIVEN VORLAGEN können als Link aktiviert werden, es öffnet sich dann ein Hilfetext zu der entsprechenden Einstellung (siehe Abbildung unten).



Hilfetext zu einer aktivierten Richtlinie

Der Bericht kann in Form einer HTML- oder XML-Datei abgespeichert werden. Er speichert nicht nur die aktivierten Richtlinien der Registerkarte Einstellungen, sondern auch alle wichtigen Konfigurationen, die auf den Registerkarten Bereich, Details und Delegierung vorgenommen wurden. Damit werden auch wichtige Informationen zur Sicherheitsfilterung, Delegierung und zum Status der Gruppenrichtlinie in den Bericht integriert (siehe Abbildung unten).



HTML-Bericht der Gruppenrichtlinie GRUNDSCHUTZ (SICHERHEITSSTUFE 0)

Die Berichtsfunktion der Gruppenrichtlinien-Verwaltungskonsole gibt einen guten Überblick über den Status der Gruppenrichtlinie, die Sicherheitsfilterung und Delegierung. Eine detaillierte und revisionsfeste Auswertung ist mit den Werkzeugen der Gruppenrichtlinien-Verwaltungskonsole aber noch nicht möglich.

Die Einstellungen einer Gruppenrichtlinie in einem Bericht speichern!

1. *Markieren Sie die Gruppenrichtlinie, deren Einstellungen Sie in einem Bericht speichern möchten.*
2. *Wechseln Sie auf die Registerkarte EINSTELLUNGEN und klicken Sie mit der rechten Maustaste in einen freien Bereich des erstellten Berichts. Wählen Sie aus dem Kontextmenü den Eintrag BERICHT SPEICHERN.*
3. *Wählen Sie einen Speicherort und vergeben Sie einen Dateinamen. Bestätigen Sie die Angaben mit der Schaltfläche SPEICHERN.*

Oder:

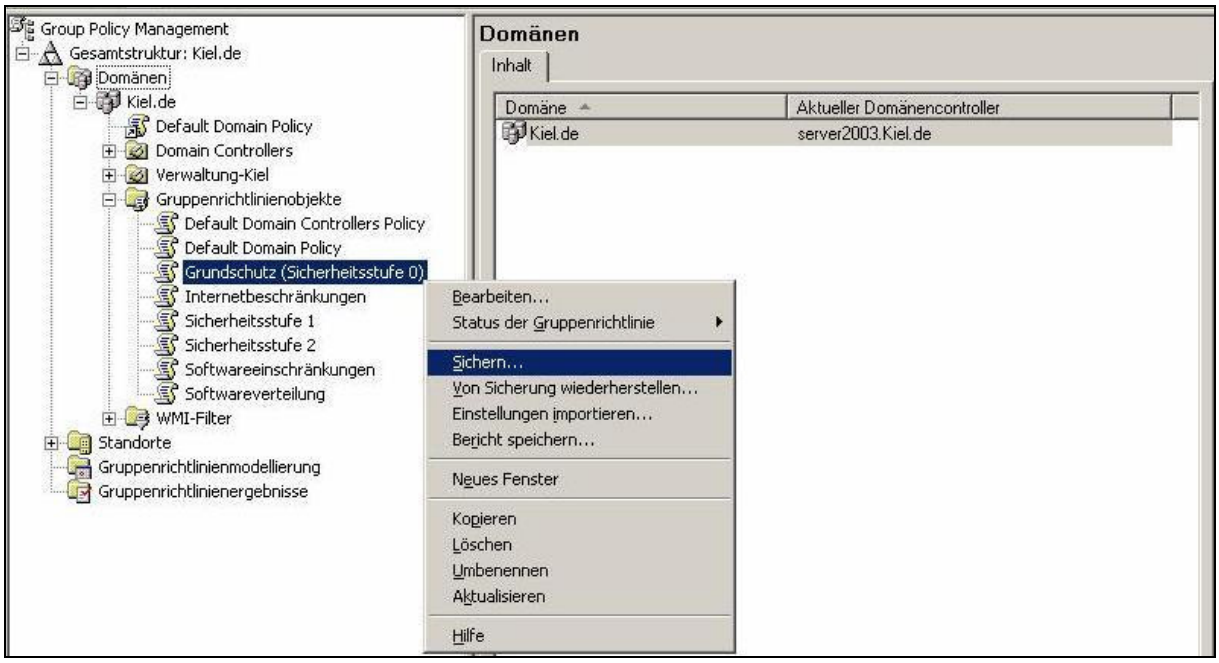
1. *Rufen Sie das Kontextmenü der Gruppenrichtlinie auf, deren Einstellungen Sie in einem Bericht speichern möchten, und wählen Sie den Eintrag BERICHT SPEICHERN.*
2. *Wählen Sie einen Speicherort und vergeben Sie einen Dateinamen. Bestätigen Sie die Angaben mit der Schaltfläche SPEICHERN.*

Sicherung und Wiederherstellung von Gruppenrichtlinien

Die Gruppenrichtlinien-Verwaltungskonsole bietet die Möglichkeit, Gruppenrichtlinien automatisiert zu sichern und wiederherzustellen. Es besteht die Möglichkeit,

- alle Gruppenrichtlinien zu sichern,
- einzelne Gruppenrichtlinien zu sichern,
- die Sicherungen der Gruppenrichtlinien zu verwalten und
- einzelne Gruppenrichtlinien wiederherzustellen.

Um Gruppenrichtlinien sichern zu können, wird ein Verzeichnis auf einer Festplatte benötigt, Bandlaufwerke werden nicht unterstützt.



Sicherung von einzelnen Gruppenrichtlinien

Eine einzelne Gruppenrichtlinie sichern!

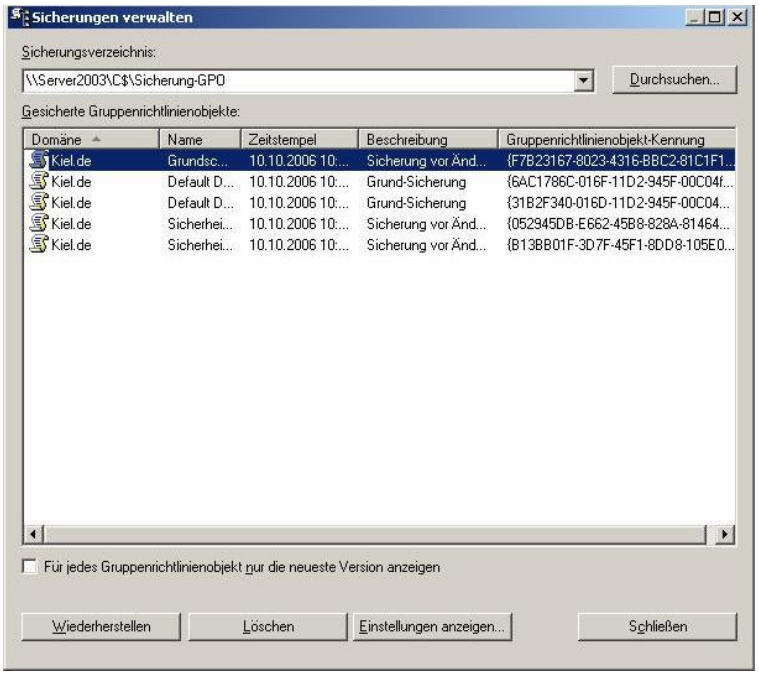
1. *Markieren Sie die Gruppenrichtlinie, die Sie sichern möchten, rufen Sie das Kontextmenü auf und wählen Sie* SICHERN.
2. *Geben Sie den Speicherort sowie eine geeignete Bemerkung an und bestätigen Sie die Eingaben mit der Schaltfläche* SICHERN.
3. *Der Sicherungsstatus wird Ihnen angezeigt, bestätigen Sie die Sicherung mit der Schaltfläche OK.*

Alle Gruppenrichtlinien einer Domäne sichern!

1. *Markieren Sie den Container Gruppenrichtlinienobjekte, rufen Sie das Kontextmenü auf und wählen Sie* ALLE SICHERN.
2. *Geben Sie den Speicherort sowie eine geeignete Bemerkung an und bestätigen Sie die Eingaben mit der Schaltfläche* SICHERN.
3. *Der Sicherungsstatus wird Ihnen angezeigt, bestätigen Sie die Sicherung mit der Schaltfläche OK.*

Damit der Überblick über die durchgeführten Sicherungen nicht verloren geht, kann über das Kontextmenü des Containers GRUPPENRICHTLINIENOBJEKTE eine Übersicht aller Sicherungen aufgerufen werden (siehe folgende Abbildung). Weiterhin können in diesem Fenster die

Sicherungen wiederhergestellt, gelöscht oder die Einstellungen der markierten Gruppenrichtlinie in Berichtsform angezeigt werden.



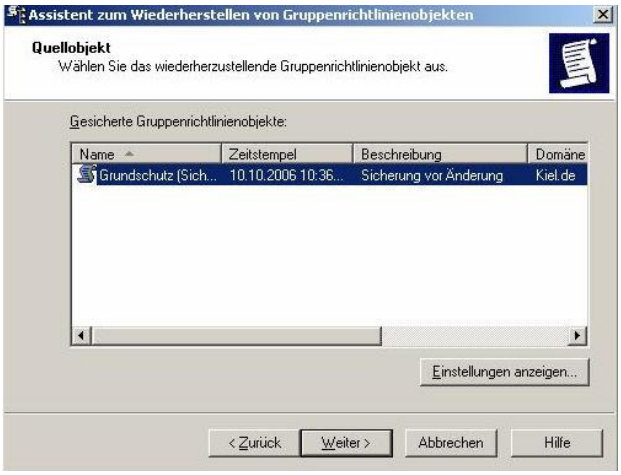
Funktion SICHERUNGEN VERWALTEN

Die Wiederherstellung von Gruppenrichtlinien, z. B. beim versehentlichen Löschen oder wenn neu konfigurierte Richtlinien nicht den gewünschten Effekt haben, ist ebenso einfach durchzuführen wie die Sicherung. Dabei müssen zwei unterschiedliche Szenarien betrachtet werden, bei der sich das Ergebnis der Wiederherstellung unterschiedlich darstellt:

1. Die gesicherte Gruppenrichtlinie soll eine bereits gelöschte Gruppenrichtlinie ersetzen. Dabei wird die Gruppenrichtlinie wiederhergestellt. Die Verknüpfungen der Gruppenrichtlinie mit den entsprechenden Verwaltungseinheiten werden allerdings nicht rekonstruiert, da die Verknüpfungen nicht an die Gruppenrichtlinie, sondern an die Verwaltungseinheiten gebunden sind.
2. Die gesicherte Gruppenrichtlinie soll eine bestehende Gruppenrichtlinie überschreiben. Dabei werden die Einstellungen der bestehenden Gruppenrichtlinie durch die der gesicherten Gruppenrichtlinie überschrieben. Die Verknüpfungen der Gruppenrichtlinie werden nicht aus der Sicherung übernommen, sondern die Verknüpfungen der bestehenden Gruppenrichtlinie bleiben unverändert.

Wiederherstellung einer gelöschten Gruppenrichtlinie!

1. *Markieren Sie den Container Gruppenrichtlinienobjekte, rufen Sie das Kontextmenü auf und wählen Sie SICHERUNGEN VERWALTEN.*
2. *Markieren Sie im Fenster GESICHERTE GRUPPENRICHTLINIENOBJEKTE die Gruppenrichtlinie, die Sie wiederherstellen möchten, wählen Sie die Schaltfläche WIEDERHERSTELLEN und bestätigen Sie mit OK.*
3. *Der Wiederherstellungsstatus wird Ihnen angezeigt, bestätigen Sie die Wiederherstellung mit OK.*



Wiederherstellen von gesicherten Gruppenrichtlinien

Wiederherstellung einer gelöschten Gruppenrichtlinie!

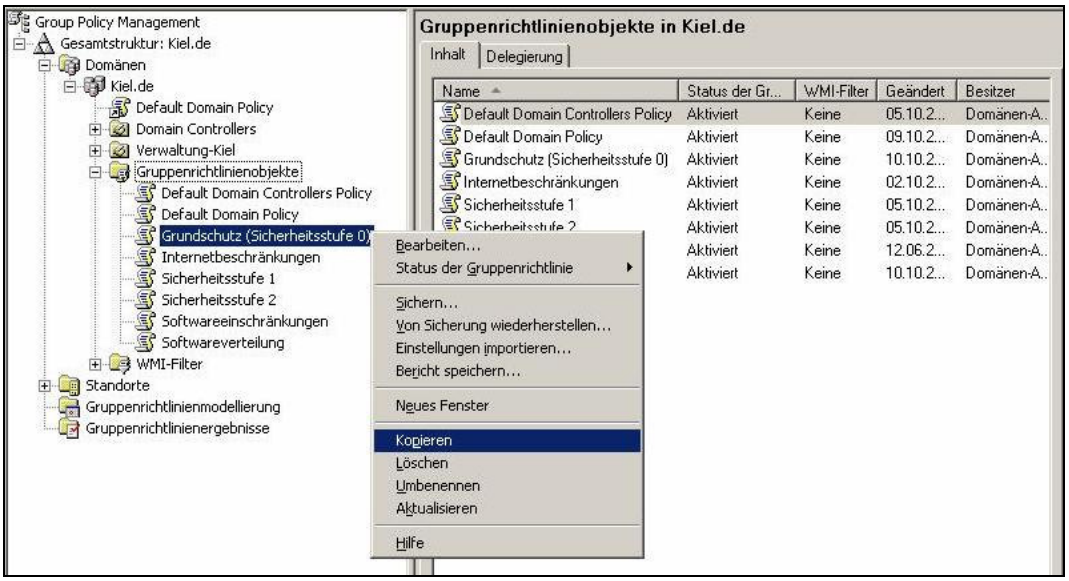
1. *Markieren Sie die Gruppenrichtlinie, die Sie mit der gesicherten Gruppenrichtlinie überschreiben möchten, rufen Sie das Kontextmenü auf und wählen Sie VON SICHERUNG WIEDERHERSTELLEN.*
2. *Folgen Sie den Anweisungen des Wiederherstellungsassistenten.*

Sind zwischen der Sicherung und Wiederherstellung einer Gruppenrichtlinie mehr als 60 Tage vergangen, wird das standardmäßige Zeitfenster zur Wiederherstellung von Active Directory-Objekten überschritten und die Wiederherstellung wird fehlschlagen

Achten Sie deshalb darauf, dass Sie Ihre Gruppenrichtlinien in regelmäßigen Abständen sowie vor jeder Änderung sichern!

Kopieren und Importieren von Gruppenrichtlinien

In der Praxis können sich Situationen ergeben, die Gruppenrichtlinien mit sehr ähnlichen Richtlinieneinstellungen erfordern. In diesem Fall kann es sich als nützlich erweisen, eine bestehende Gruppenrichtlinie mit samt ihren Einstellungen zu kopieren und die Kopie danach um die fehlenden Einstellungen zu ergänzen. Die Gruppenrichtlinien-Verwaltungskonsole unterstützt diesen Kopiervorgang.



Kopieren einer Gruppenrichtlinie

Kopieren einer Gruppenrichtlinie!

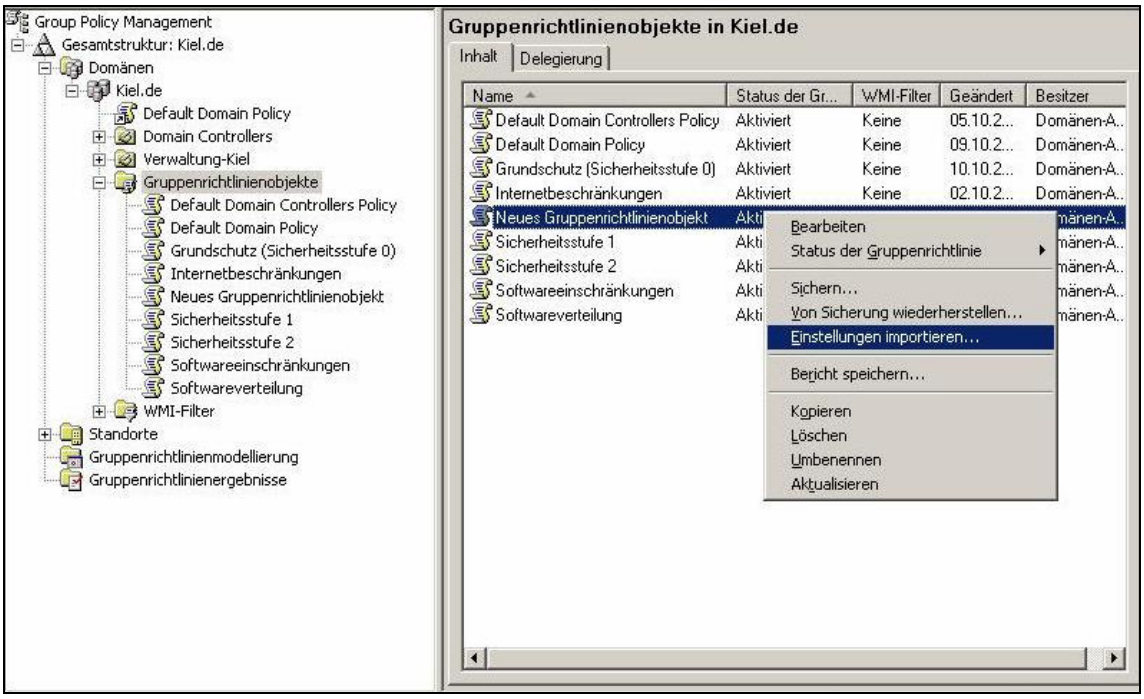
1. *Markieren Sie die Gruppenrichtlinie, die Sie kopieren möchten, rufen Sie das Kontextmenü auf und wählen Sie KOPIEREN.*
2. *Markieren Sie den Container GRUPPENRICHTLINIENOBJEKTE, rufen Sie das Kontextmenü auf und wählen Sie EINFÜGEN.*
3. *Wählen Sie die Berechtigungen für die neue Gruppenrichtlinie und bestätigen Sie mit OK.*
4. *Bestätigen Sie den Kopierstatus mit OK.*

Oder:

1. *Ziehen Sie die Gruppenrichtlinie, die Sie kopieren möchten, mit der linken Maustaste auf den Container GRUPPENRICHTLINIENOBJEKTE.*
2. *Wählen Sie die Berechtigungen für die neue Gruppenrichtlinie und bestätigen Sie mit OK.*
3. *Bestätigen Sie den Kopierstatus mit OK.*

Die Importfunktion der Gruppenrichtlinien-Verwaltungskonsole unterscheidet sich insoweit von der Kopierfunktion, dass die zu importierenden Einstellungen aus der Sicherung einer Gruppenrichtlinie in eine bereits bestehende Gruppenrichtlinie übernommen werden. Dabei muss beachtet werden, dass bei dem Importvorgang eventuell vorhandene Einstellungen in der Ziel-Gruppenrichtlinie verloren gehen.

Für den Import von Richtlinieneinstellungen ist ein direkter Kontakt zwischen der Quell- und Ziel-Gruppenrichtlinie nicht erforderlich, da die Einstellungen aus einer Sicherung importiert werden. Das hat die Vorteile, dass Richtlinieneinstellungen auch domänenübergreifend oder zwischen einem Test- und Produktivsystem übernommen werden können.



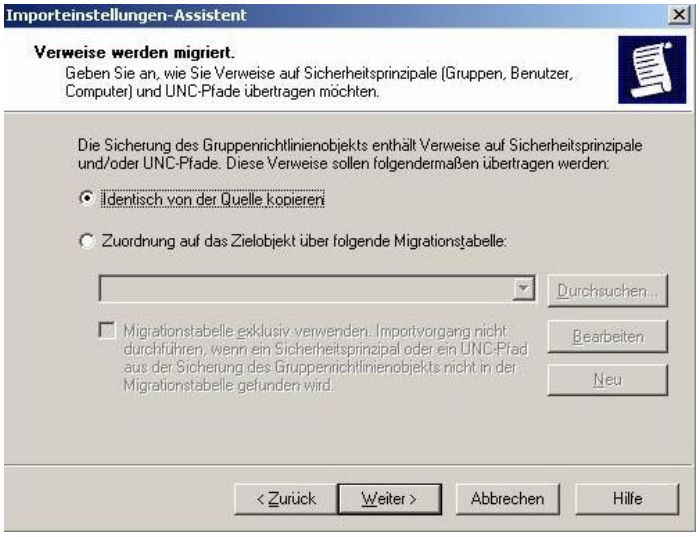
Importieren von Richtlinieneinstellungen

Importieren von Gruppenrichtlinieneinstellungen!

1. *Erstellen Sie eine neue Gruppenrichtlinie, indem Sie den Container GRUPPENRICHTLINIENOBJEKT markieren, das Kontextmenü aufrufen und NEU wählen.*
2. *Markieren Sie die neue Gruppenrichtlinie, rufen Sie das Kontextmenü auf und wählen Sie Einstellungen importieren.*
3. *Es öffnet sich ein Importassistent, der Sie durch den Importvorgang leitet. Bestätigen Sie Ihre Einstellungen.*
4. *Bestätigen Sie den Importstatus mit OK.*

Bei einem domänenübergreifenden Importvorgang kann es vorkommen, dass in einer Gruppenrichtlinie bestimmte UNC-Pfade und/oder Benutzer- und Gruppenkonten angegeben wurden, die domänenspezifisch sind und in der Ziel-Gruppenrichtlinie ggf. angepasst werden müssen. Der Importassistent überprüft die Quell- und Ziel-Gruppenrichtlinie und fragt in einem Dialogfenster, wie er die entsprechenden Einstellungen übernehmen soll (siehe Abbildung unten):

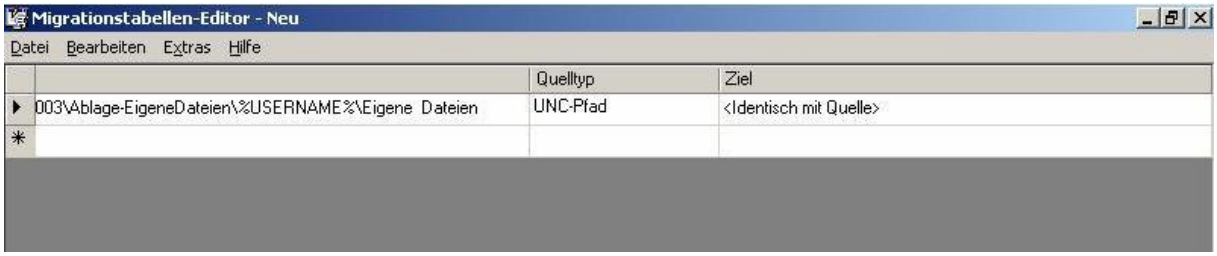
- Die Einstellungen der Quell-Gruppenrichtlinie ohne Änderung übernehmen oder
- die Einstellungen mit Hilfe einer Migrationstabelle (siehe nächster Abschnitt) ändern.



Importassistent

Erstellung von Migrationstabellen

Mit dem Menüpunkt MIGRATIONSTABELLEN-EDITOR ÖFFNEN können Migrationstabellen erzeugt werden.



Migrationstabelle

Migrationstabellen spielen eine Rolle bei domänenübergreifenden Import- und Kopiervorgängen von Gruppenrichtlinien. Sie übernehmen die Aufgabe, die Zuordnung von bestimmten domänenspezifischen Informationen in Gruppenrichtlinien (UNC-Pfade und Benutzer- und Gruppenkonten) beim Kopier- oder Importvorgang von der Quell- zur Zieldomäne entsprechend anzupassen. Diese Migrationstabellen

- können entweder vollständig manuell erstellt werden oder
- es werden die Hilfswerkzeuge des Migrationstabellen-Editors unter dem Menüpunkt EXTRAS eingesetzt. Sie übernehmen die Verweise auf Benutzer- und Gruppenkonten und UNC-Pfade der Quell-Gruppenrichtlinie in die Tabelle und der Systemadministrator muss anschließend die Zielangaben anpassen.

6.4 Richtlinienergebnissatz

Seit der Einführung von Windows XP ist es mit der Funktion Richtlinienergebnissatz (Resultant Set of Policy = RSoP) möglich, für bestimmte Benutzer- und Computerkonten einen Gruppenrichtlinienergebnissatz zu erzeugen. Mit diesem Hilfsmittel ist es möglich, die Gruppenrichtlinienimplementierung zu vereinfachen, differenzierte Problembehandlungen durchzuführen und Gruppenrichtlinien zu planen. Beim Richtlinienergebnissatz stehen

- der Planungsmodus (Gruppenrichtlinienmodellierung) und
- der Protokollierungsmodus (Gruppenrichtlinienergebnisse)

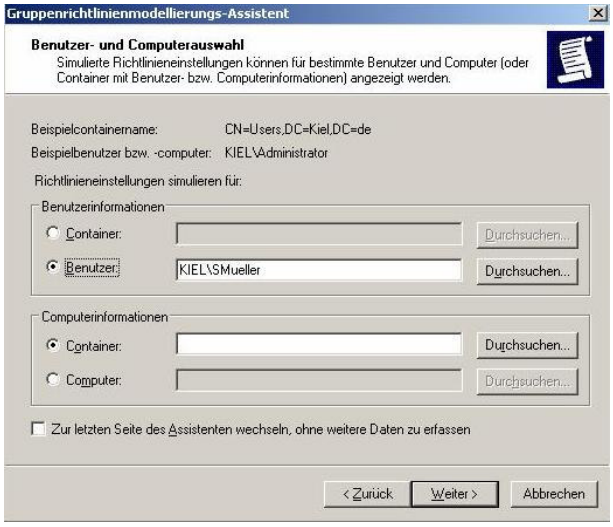
zur Verfügung.

Bei der Gruppenrichtlinienverwaltung ohne den Einsatz der Gruppenrichtlinien-Verwaltungskonsole konnte der Richtlinienergebnissatz als Snap-In über eine Managementkonsole (MMC) aufgerufen werden. Die Gruppenrichtlinien-Verwaltungskonsole hat die beiden Modi des Richtlinienergebnissatzes als eigenständige Werkzeuge in die grafische Oberfläche integriert.

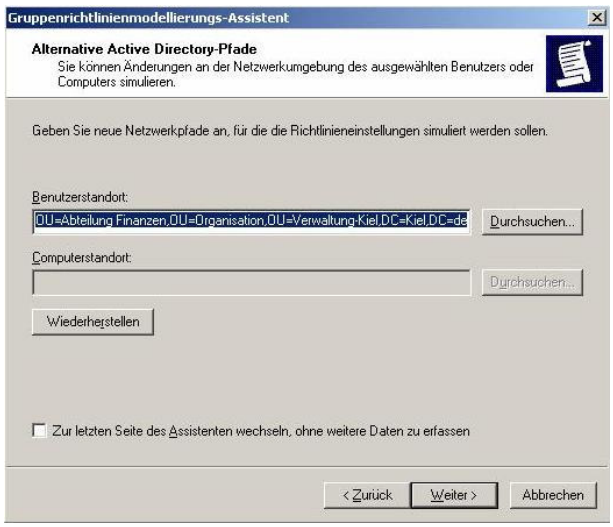
Der Richtlinienergebnissatz wird nur von Domänencontrollern mit dem Betriebssystem Windows Server 2003 und Clients mit dem Betriebssystem XP unterstützt.

Gruppenrichtlinienmodellierung

Sollen Änderungen im Active Directory vorgenommen werden, so können sich schon kleine Änderungen auf die Wirkungsweise der Gruppenrichtlinien auswirken. Mit der Gruppenrichtlinienmodellierung kann die Wirkungsweise einer Gruppenrichtlinie zu Test- und Planungszwecken simuliert werden. So kann z. B. überprüft werden, welche Richtlinien für ein Benutzer- oder Computerkonto verarbeitet werden, wenn man es z. B. in eine andere Organisationseinheit verschieben würde. Die vom Assistenten erfassten Parameter verändern dabei nicht die Einstellungen im System, sodass sich für das ausgewählte Benutzer- oder Computerkonto keine Auswirkungen ergeben. In den Abbildungen unten, wird z. B. ein Verschieben des Benutzerkontos SMUELLER in die Organisationseinheit ABTEILUNG FINANZEN simuliert.



Gruppenrichtlinienmodellierungs-Assistent

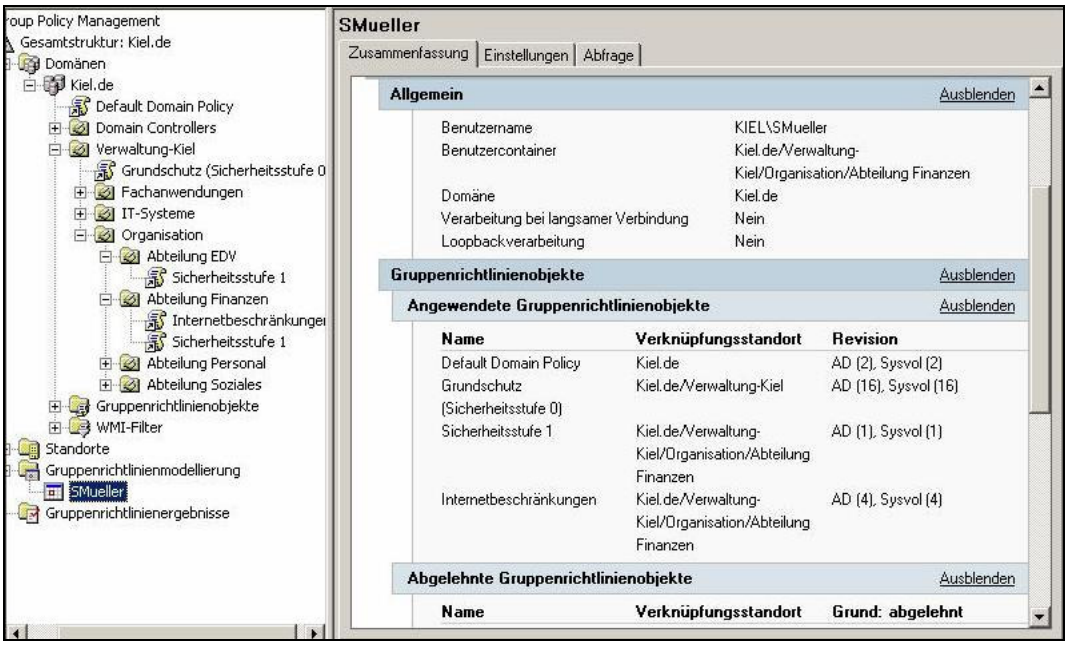


Zuweisen eines Benutzerkontos zu einer anderen Organisationseinheit

Im Gruppenrichtlinienmodellierungs-Assistenten können neben der Benutzer- bzw. Computerauswahl differenzierte Einstellungen im Zusammenhang mit der Gruppenrichtlinienverarbeitung simuliert werden, die die Wirkungsweise der Gruppenrichtlinien beeinflussen und die Abfrage entsprechend erweitern und spezifizieren:

- Veränderung der Zuweisung von Benutzer- und Computerkonten zu anderen Organisationseinheiten,
- Einsatz von WMI-Filtern,
- Loopbackverarbeitung sowie
- Mitgliedschaften in Sicherheitsgruppen.

Als Ergebnis listet der Gruppenrichtlinienmodellierungs-Assistent die durchgeführten Simulationen im Container GRUPPENRICHTLINIENMODELLIERUNG mit differenzierten Auskünften zur Durchführung der Modellierungen auf.



Registerkarte ZUSAMMENFASSUNG einer Gruppenrichtlinienmodellierung

Die Registerkarte ZUSAMMENFASSUNG einer ausgewählten Gruppenrichtlinienmodellierung, in der Abbildung oben die Simulation des Benutzerkontos SMUELLER, liefert Informationen,

- zur hypothetischen Zuordnung des Benutzerkontos im Active Directory (das Benutzerkonto SMUELLER ist eigentlich der Organisationseinheit ABTEILUNG EDV zugeordnet, in der Simulation wurde es der Organisationseinheit ABTEILUNG FINANZEN zugewiesen),

- zu den auf das Benutzerkonto angewendeten Gruppenrichtlinien,
- zur Mitgliedschaft in Sicherheitsgruppen sowie
- zum Einsatz von WMI-Filtern.

Die Registerkarte EINSTELLUNGEN fasst alle Einstellungen der Gruppenrichtlinien zusammen, die auf das entsprechende Benutzerkonto wirken. Im Unterschied zu dem Dokumentationsbericht einer einzelnen Gruppenrichtlinie oder einer Gruppenrichtlinienverknüpfung wird hier zu jeder Richtlinieneinstellung die ausschlaggebende Gruppenrichtlinie mit aufgeführt.

Registerkarte EINSTELLUNGEN einer Gruppenrichtlinienmodellierung

Die Registerkarte ABFRAGE fasst alle vorgenommenen Einstellungen der Simulation zu einer Übersicht zusammen.

Das Kontextmenü einer markierten Gruppenrichtlinienmodellierung bietet zusätzliche Verarbeitungs- und Ansichtsmöglichkeiten:

- Die Option ERWEITERTE ANSICHT öffnet die Managementkonsole GRUPPENRICHTLINIENERGEBNISSE. Diese Managementkonsole ist so aufgebaut wie der Gruppenrichtlinien-Editor, mit der Einschränkung, dass nur die angewendeten Richtlinieneinstellungen angezeigt werden.
- Die Option ABFRAGE ERNEUT AUSFÜHREN führt die Simulation mit den gleichen Einstellungen erneut durch.

- Die Option MIT HILFE DIESER ABFRAGE NEUE ABFRAGE ERSTELLEN kopiert die markierte Gruppenrichtlinienmodellierung. Diese Kopie kann dann als Grundlage für ähnliche Simulationen dienen und entsprechend angepasst werden.
- Mit der Option SPEICHERN kann die Gruppenrichtlinienmodellierung in einem HTML- oder XML-Bericht gespeichert werden.

Gruppenrichtlinienmodellierung für das Verschieben eines Benutzerkontos in eine andere Organisationseinheit erstellen!

1. *Markieren Sie den Container GRUPPENRICHTLINIENMODELLIERUNG, rufen Sie das Kontextmenü auf und wählen Sie GRUPPENRICHTLINIENMODELLIERUNGS-ASSISTENT.*
2. *Bestätigen Sie das Willkommensfenster mit WEITER. Wählen Sie im Fenster DOMÄNENCONTROLLERWAHL einen Domänencontroller, sofern die Abfrage sich nicht auf den voreingestellten Domänencontroller beziehen soll, und bestätigen Sie mit WEITER.*
3. *Wählen Sie im Fenster BENUTZER- UND COMPUTERAUSWAHL das Benutzerkonto aus, für das die Simulation durchgeführt werden soll. Bestätigen Sie mit WEITER.*
4. *Navigieren Sie zu dem Fenster ALTERNATIVE ACTIVE DIRECTORY-PFADE. Wählen Sie dort im Feld BENUTZERSTANDORT die Organisationseinheit, in die das Benutzerkonto zur Simulation verschoben werden soll. Wenn Sie keine weiteren Einstellungen vornehmen wollen, können Sie einen Haken im unteren Bereich des Fensters setzen, um auf die letzte Seite des Assistenten zu gelangen. Bestätigen Sie mit WEITER.*
5. *Bestätigen Sie Ihre Eingaben im Fenster ZUSAMMENFASSUNG mit WEITER und schließen Sie den Assistenten.*

Gruppenrichtlinienergebnisse

Mit den Gruppenrichtlinienergebnissen werden im Gegensatz zu der Gruppenrichtlinienmodellierung die tatsächlichen Richtlinieneinstellungen protokolliert. Mit ihrer Hilfe können entweder die Gruppenrichtlinieneinstellungen

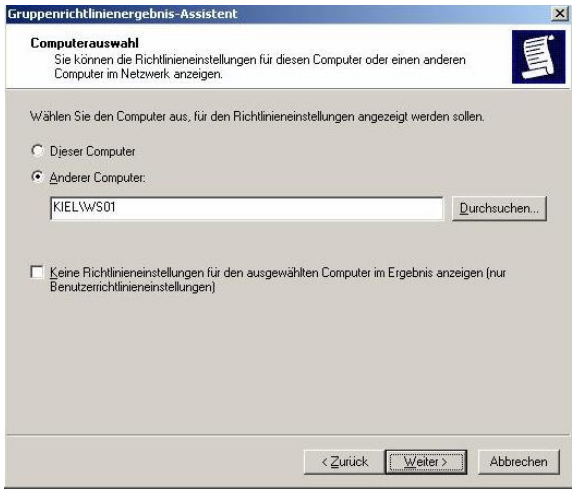
- für ein ausgewähltes Benutzer- oder Computerkonto oder
- für ein ausgewähltes Benutzerkonto an einem bestimmten Computer

ausgewertet werden. Diese Auswertungen können hilfreich sein, wenn Informationen darüber benötigt werden,

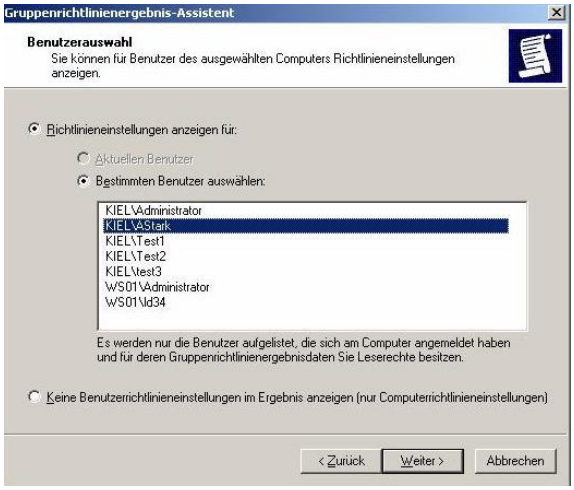
- welche Einstellungen z. B. auch über eine komplexe Vererbungshierarchie tatsächlich zugewiesen wurden,

- welche Einstellungen nicht oder fehlerhaft verarbeitet werden und
- welchen Einfluss die Änderung einer Gruppenmitgliedschaft auf die Verarbeitung der Richtlinien nimmt.

In den beiden Abbildungen unten wird z. B. mit Hilfe des Gruppenrichtlinienergebnis-Assistenten die Verarbeitung der Gruppenrichtlinien auf dem Computer WS01 bei Anmeldung mit dem Benutzerkonto ASTARK protokolliert. Sollen nur die Richtlinieneinstellungen für das Benutzerkonto oder nur für das Computerkonto angezeigt werden, müssten die entsprechenden Optionen im unteren Fensterbereich aktiviert werden.



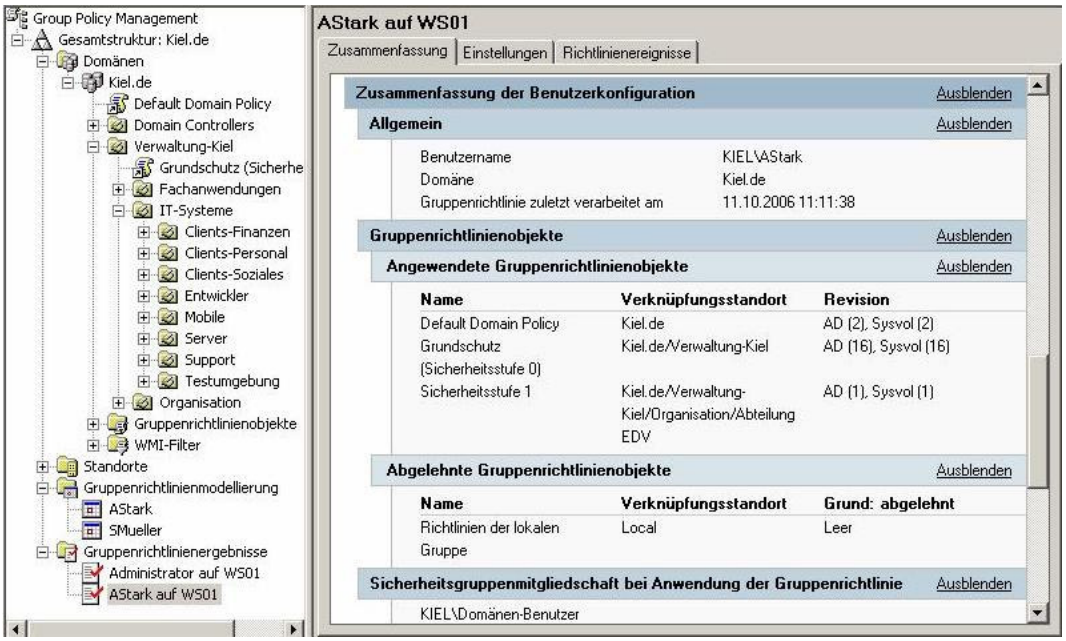
Computerauswahl des Gruppenrichtlinienergebnis-Assistenten



Benutzerauswahl des Gruppenrichtlinienergebnis-Assistenten

In dem Fenster Benutzerauswahl des Gruppenrichtlinienergebnis-Assistenten werden nur die Benutzerkonten angezeigt, die sich auf dem ausgewählten Computer schon einmal lokal oder an der Domäne angemeldet haben.

Der Gruppenrichtlinienergebnis-Assistent listet die durchgeführten Abfragen im Container GRUPPENRICHTLINIENERGEBNISSE auf.



Registerkarte ZUSAMMENFASSUNG der Gruppenrichtlinienergebnisse

Die Registerkarte ZUSAMMENFASSUNG eines ausgewählten Gruppenrichtlinienergebnisses, in der Abbildung oben die Abfrage der Richtlinienverarbeitung des Benutzerkontos ASTARK auf dem Computer WS01, liefert Informationen,

- zu den auf das Benutzerkonto angewendeten Gruppenrichtlinien,
- zur Mitgliedschaft in Sicherheitsgruppen sowie
- zum Einsatz von WMI-Filtern.

Die Registerkarte EINSTELLUNGEN fasst, analog zu der Gruppenrichtlinienmodellierung, alle Einstellungen der Gruppenrichtlinien zusammen, die auf das entsprechende Benutzer- und Computerkonto wirken. Auch hier wird zu jeder Richtlinieneinstellung die ausschlaggebende Gruppenrichtlinie mit aufgeführt.

Auf der Registerkarte RICHTLINIENEREIGNISSE können alle Ereignisse der Verarbeitung der bei der Gruppenrichtlinienergebnis-Abfrage beteiligten Gruppenrichtlinien eingesehen werden. Sie sind umfassend und geben Auskunft über die Verarbeitung der Richtlinien.

Protokolldaten auf der Registerkarte RICHTLINIENEREIGNISSE

Das Kontextmenü einer markierten Gruppenrichtlinienergebnis-Abfrage bietet zusätzliche Verarbeitungs- und Ansichtsmöglichkeiten:

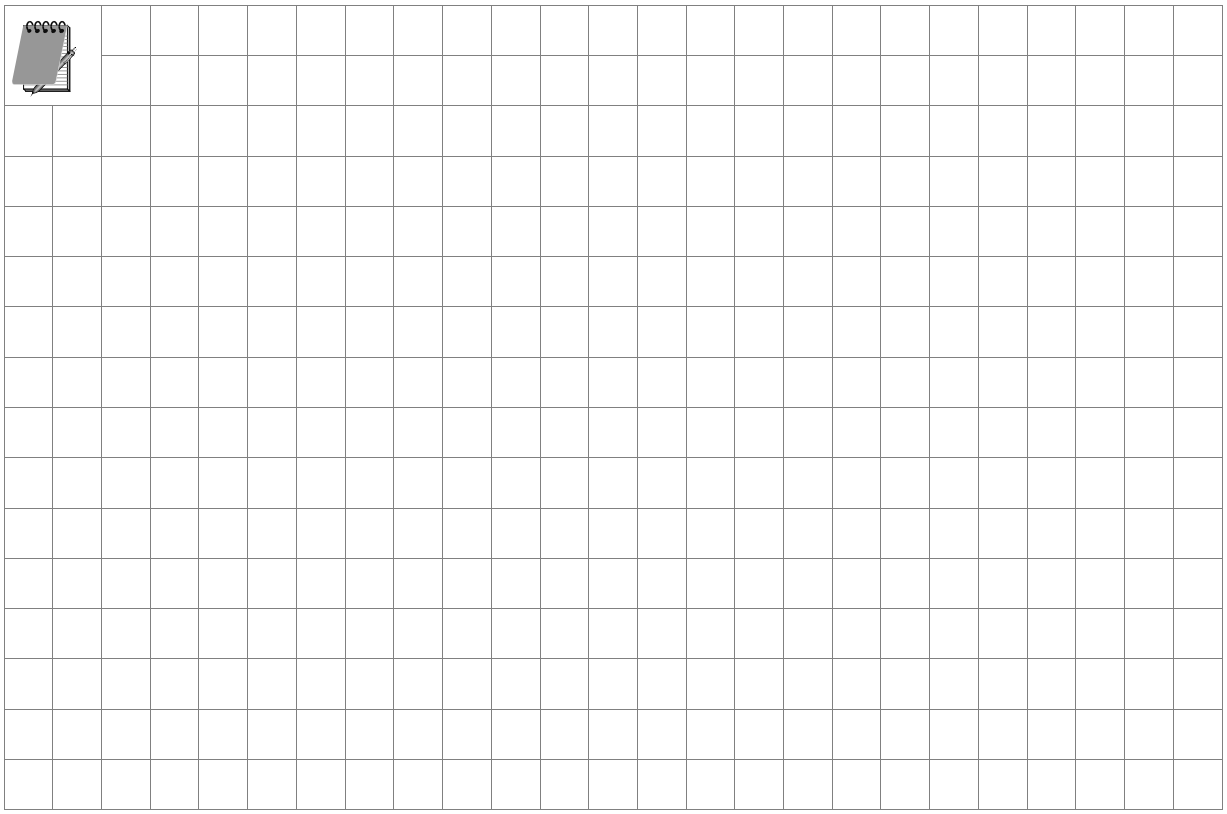
- Die Option ERWEITERTE ANSICHT öffnet die Managementkonsole GRUPPENRICHTLINIENERGEBNISSE. Diese Managementkonsole ist so aufgebaut wie der Gruppenrichtlinien-Editor, mit der Einschränkung, dass nur die angewendeten Richtlinieneinstellungen angezeigt werden.
- Die Option ABFRAGE ERNEUT AUSFÜHREN führt die Abfrage mit den gleichen Einstellungen erneut durch.
- Mit der Option SPEICHERN kann die Gruppenrichtlinienergebnis-Abfrage in einem HTML- oder XML-Bericht gespeichert werden.

Richtlinienergebnisse für ein Benutzerkonto auf einem definierten Computer abfragen!

1. *Markieren Sie den Container GRUPPENRICHTLINIENERGEBNISSE, rufen Sie das Kontextmenü auf und wählen Sie GRUPPENRICHTLINIENERGEBNIS-ASSISTENT.*
2. *Bestätigen Sie das Willkommensfenster mit WEITER. Aktivieren Sie im Fenster COMPUTERAUSWAHL die Option ANDERER COMPUTER, wählen Sie den Computer, für den die Abfrage erstellt werden soll, und bestätigen Sie mit WEITER.*
3. *Wählen Sie im Fenster BENUTZERAUSWAHL das Benutzerkonto, das in der Abfrage berücksichtigt werden soll. Bestätigen Sie mit WEITER.*
4. *Bestätigen Sie die Zusammenfassung mit WEITER, um die Abfrage zu erstellen.*
5. *Schließen Sie den Assistenten mit FERTIG STELLEN.*

6.5 Sicherheitscheck

- *Setzen Sie zur **Vereinfachung der Gruppenrichtlinienverwaltung** in einer Windows Server2003-Umgebung die Gruppenrichtlinien-Verwaltungskonsole ein.*
- ***Dokumentieren** Sie die Konfiguration und die Richtlinieneinstellungen der Gruppenrichtlinien mit der Berichtsfunktion der Gruppenrichtlinien-Verwaltungskonsole.*
- ***Sichern** Sie Ihre Gruppenrichtlinien in regelmäßigen Abständen sowie vor Änderungen der Richtlinieneinstellungen.*
- *Nutzen Sie die **Kopier- und Importfunktionalität** der Gruppenrichtlinien-Verwaltungskonsole, um Gruppenrichtlinien mit ähnlichen Richtlinieneinstellungen zu erstellen.*
- *Nutzen Sie die **Gruppenrichtlinienmodellierung**, um die Wirkungsweise einer Gruppenrichtlinie für ausgewählte Benutzer- und Computerkonten zu testen bzw. zu simulieren.*
- *Prüfen Sie mit der Funktion **Gruppenrichtlinienergebnisse**, welche Richtlinien auf einem Computer tatsächlich angewendet werden.*
- *Verwenden Sie das **Richtlinienereignisprotokoll** zur Fehleranalyse, wenn Gruppenrichtlinien nicht oder nur unvollständig verarbeitet werden.*



7 Gruppenrichtlinienobjekt-Editor

In diesem Kapitel erfahren Sie,

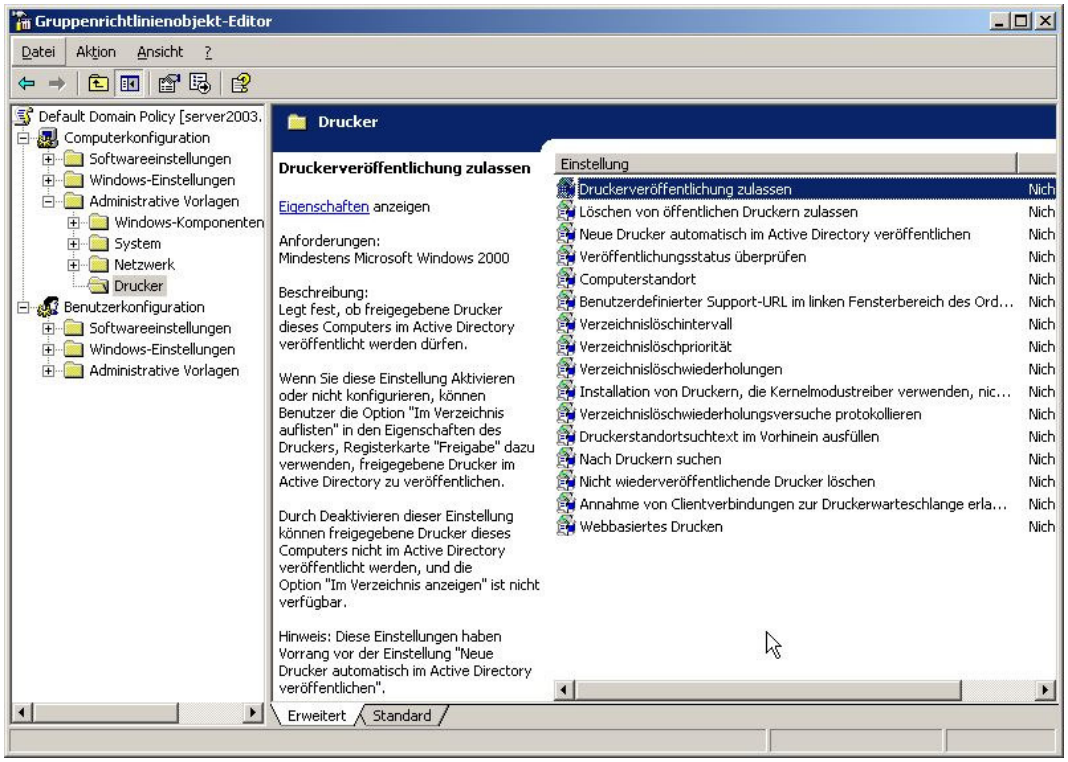
- wie der Gruppenrichtlinienobjekt-Editor aufgebaut ist,
- welche Möglichkeiten es gibt, den Gruppenrichtlinienobjekt-Editor aufzurufen,
- wie die Ansicht im Gruppenrichtlinienobjekt-Editor gefiltert werden kann,
- wie die Einstellungen der einzelnen Richtlinien einer Gruppenrichtlinie konfiguriert werden,
- wie adm-Dateien importiert werden können und
- inwieweit die Richtlinieneinstellungen dokumentiert werden können.

Dieses kurze Kapitel befasst sich ausschließlich mit dem Gruppenrichtlinienobjekt-Editor, der im Folgenden mit der gebräuchlichen Kurzform als Gruppenrichtlinien-Editor bezeichnet wird. Der Gruppenrichtlinien-Editor stellt das eigentliche Werkzeug zur Bearbeitung der Gruppenrichtlinien dar. In diesem Kapitel wird zunächst kurz der Aufbau beschrieben sowie die in den vorherigen Kapiteln teilweise erwähnten Wege, den Gruppenrichtlinien-Editor aufzurufen, zusammengefasst. Danach werden die Möglichkeiten zur Filterung der Ansicht, die Konfiguration der Einstellungen einzelner Richtlinien, die Importfunktion für adm-Dateien und die Dokumentationsmöglichkeit innerhalb des Gruppenrichtlinien-Editors angesprochen.

7.1 Aufbau und Aufruf des Gruppenrichtlinienobjekt-Editors

Der Gruppenrichtlinien-Editor wird in Form einer Managementkonsole zur Verfügung gestellt und hat folgenden Aufbau:

- Der linke Fensterbereich der Managementkonsole zeigt die im Kapitel 2.3 schon beschriebene Aufteilung der Gruppenrichtlinie in die Knoten COMPUTERKONFIGURATION und BENUTZERKONFIGURATION. Diese sind wiederum in die Unterknoten SOFTWAREEINSTELLUNGEN, WINDOWS-EINSTELLUNGEN und ADMINISTRATIVE VORLAGEN gegliedert. Die oberste Ebene zeigt an, um welche Gruppenrichtlinie es sich handelt.
- Der rechte Fensterbereich zeigt den Inhalt der links markierten Knoten. In diesem Fensterbereich kann zwischen zwei Ansichten gewechselt werden. Die Registerkarte STANDARD zeigt die Richtlinien bzw. die Einstellungen der Richtlinien über die ganze rechte Fensterbreite an. Die Registerkarte ERWEITERT zeigt ergänzende Informationen bzw. bei den ADMINISTRATIVEN VORLAGEN einen Hilfetext in einer zusätzlichen Spalte an (siehe folgende Abbildung).



Aufbau des Gruppenrichtlinien-Editors

Im Gruppenrichtlinien-Editor lässt sich auf der obersten Ebene (Bezeichnung der Gruppenrichtlinie) ein Eigenschaftenfenster aufrufen, das auf den Registerkarten ALLGEMEIN, VERKNÜPFUNGEN, SICHERHEIT und WMI-FILTER die Eigenschaften der entsprechenden Gruppenrichtlinie auflistet.

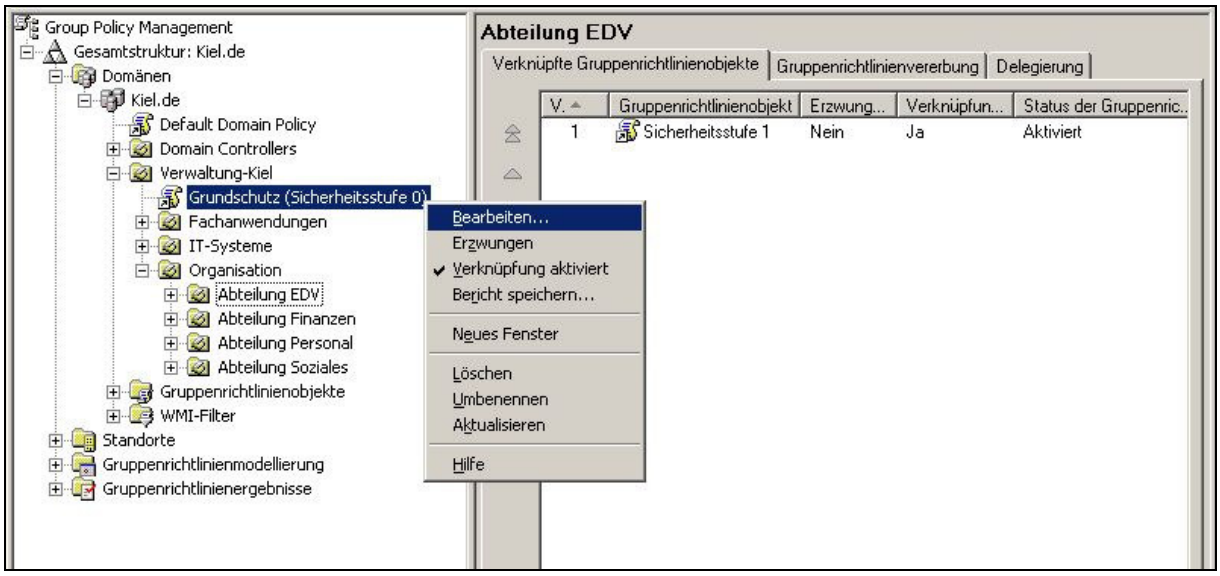
Eigenschaftenfenster der Gruppenrichtlinie

Aufrufen des Eigenschaftenfensters einer Gruppenrichtlinie im Gruppenrichtlinien-Editor!

1. *Markieren Sie im Gruppenrichtlinien-Editor die Gruppenrichtlinie im linken Fensterbereich.*
2. *Wählen Sie im Kontextmenü den Eintrag EIGENSCHAFTEN.*
3. *Es öffnet sich das Eigenschaftenfenster der entsprechenden Gruppenrichtlinie.*

Der Gruppenrichtlinien-Editor wird je nach Gültigkeit der Gruppenrichtlinie (*Lokale Gruppenrichtlinie* oder Active Directory-Gruppenrichtlinie) unterschiedlich aufgerufen:

- Die *Lokale Gruppenrichtlinie* wird über die Kommandozeile oder über eine benutzerdefinierte MMC (Managementkonsole) aufgerufen (siehe Kapitel 2.4).
- Die Active Directory-Gruppenrichtlinien werden wahlweise über das Verwaltungsprogramm *Active Directory-Benutzer und -Computer* (siehe Kapitel 2.5) oder über die Gruppenrichtlinien-Verwaltungskonsole aufgerufen.



Aufruf der Gruppenrichtlinie GRUNDSCHUTZ mit der Gruppenrichtlinien-Verwaltungskonsole

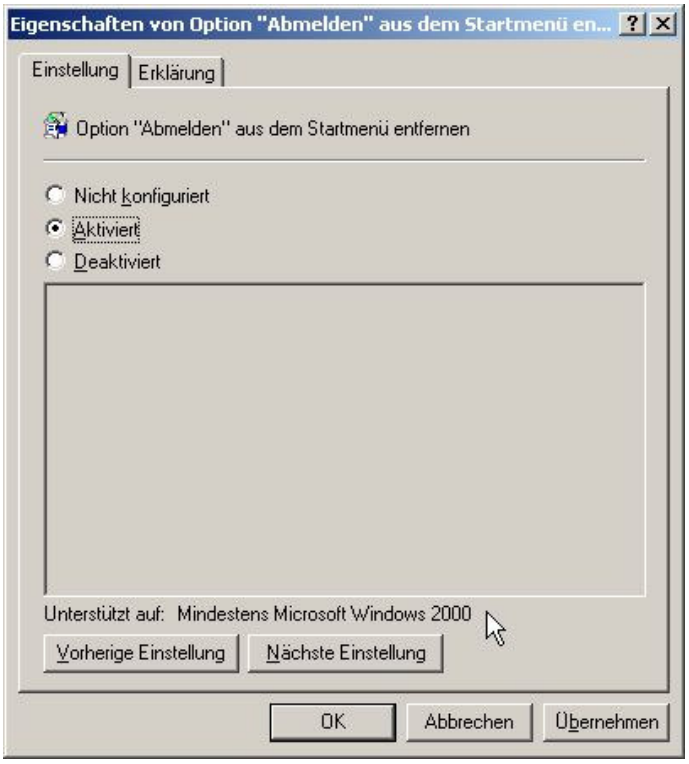
Aufrufen einer Gruppenrichtlinie in der Gruppenrichtlinien-Verwaltungskonsole!

1. *Markieren Sie im Gruppenrichtlinien-Editor die Gruppenrichtlinie, die Sie bearbeiten möchten.*
2. *Wählen Sie im Kontextmenü den Eintrag BEARBEITEN.*
3. *Es öffnet sich der Gruppenrichtlinien-Editor der entsprechenden Gruppenrichtlinie.*

7.2 Konfigurieren von Richtlinien

Die Art und Weise, wie Einstellungen in den Gruppenrichtlinien vorgenommen werden können, stellt sich in den unterschiedlichen Knoten der Gruppenrichtlinie unterschiedlich dar. In den Knoten SOFTWAREEINSTELLUNGEN und WINDOWS-EINSTELLUNGEN werden die Einstellungen der jeweiligen Richtlinien direkt durch Eingabe in Dialogfelder bzw. mit Hilfe von Assistenten konfiguriert. Diese Einstellungen sind für die unterschiedlichen Richtlinien spezifisch und zeigen daher kein einheitliches Schema zur Konfiguration. In dem Knoten ADMINISTRATIVE VORLAGEN ist die Oberfläche zur Konfiguration vereinheitlicht worden, sodass sich dem Systemadministrator bei jeder Richtlinie das gleiche Konfigurationsfenster zeigt.

Das Konfigurationsfenster der Richtlinien im Knoten ADMINISTRATIVE VORLAGEN (Computer- sowie Benutzerkonfiguration) ist in zwei Registerkarten eingeteilt. Die Registerkarte EINSTELLUNG zeigt den Status der Richtlinie und im unteren Bereich des Dialogfensters die Mindestanforderung an das Betriebssystem. Die Registerkarte ERKLÄRUNG enthält eine kurze Beschreibung der Richtlinie und Hinweise auf eventuelle weitere Konfigurationsmöglichkeiten.



Status einer Richtlinie

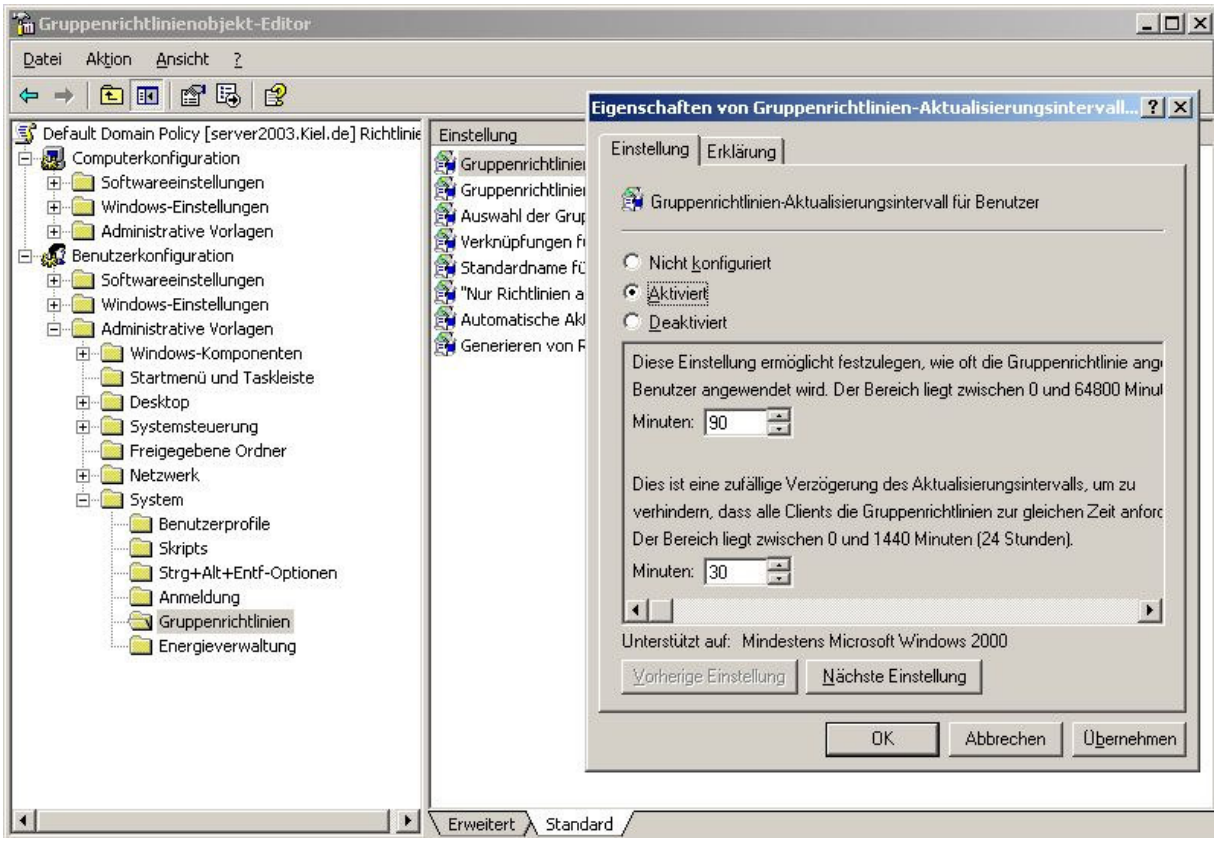
Der Status der Richtlinie kann entweder auf NICHT KONFIGURIERT, AKTIVIERT oder DEAKTIVIERT gesetzt werden:

- NICHT KONFIGURIERT
  Diese Option gibt an, dass die entsprechende Richtlinie nicht auf die Benutzer- bzw. Computerkonten der Verwaltungseinheit angewendet wird, mit der diese Gruppenrichtlinie verknüpft ist, d. h. die Richtlinie wird bei der Verarbeitung nicht berücksichtigt.
- AKTIVIERT
  Diese Option gibt an, dass die Einstellungen der entsprechenden Richtlinie auf die Benutzer- bzw. Computerkonten der Verwaltungseinheit wirken, mit der diese Gruppenrichtlinie verknüpft ist.
- DEAKTIVIERT
  Diese Option gibt an, dass die Einstellungen der entsprechenden Richtlinie nicht auf die Benutzer- bzw. Computerkonten der Verwaltungseinheit wirken, mit der diese Gruppenrichtlinie verknüpft ist, auch wenn sie auf einer höheren Hierarchieebene schon aktiviert und vererbt wurden.

  Diese Option kann z. B. im folgenden Szenario verwendet werden: In einer Gruppenrichtlinie auf einer hohen Hierarchieebene wurden mehrere Richtlinien konfiguriert und auf die darunter liegenden Organisationseinheiten vererbt. Auf die Benutzer- bzw. Computerkonten einer bestimmten untergeordneten Organisationseinheit soll eine dieser Richtlinien nicht wirken. In diesem Fall kann eine Gruppenrichtlinie eingerichtet, die entsprechende Richtlinie deaktiviert und die Gruppenrichtlinie mit der entsprechenden Organisationseinheit verknüpft werden.

Wenn Sie die Option DEAKTIVIERT einsetzen, müssen Sie die Vererbungsreihenfolge und die Auswirkungen der Optionen KEIN VORRANG bzw. ERZWUNGEN beachten. Eine erzwungene Richtlinie kann in einer untergeordneten Organisationseinheit nicht überschrieben werden (siehe auch Kapitel 5.3 und 6.3). Das bedeutet, dass Sie sie auch nicht deaktivieren können.

Einige Richtlinien der ADMINISTRATIVEN VORLAGEN einer Gruppenrichtlinie benötigen zusätzlich zum Status noch weitergehende Angaben. Diese Dialogfelder bzw. Schaltflächen sind standardmäßig beim Status NICHT KONFIGURIERT deaktiviert. Sie lassen sich konfigurieren, wenn der Status der Gruppenrichtlinie in AKTIVIERT geändert wird (siehe folgende Abbildung).



Erweiterte Konfigurationsmöglichkeit bei Richtlinien der ADMINISTRATIVEN VORLAGEN

7.3 Filterung der Ansicht

Die Ansicht des Gruppenrichtlinien-Editors im Bereich der ADMINISTRATIVEN VORLAGEN (Computer- sowie Benutzerkonfiguration) kann mit verschiedenen Filterfunktionen angepasst werden. Der Gruppenrichtlinien-Editor bietet mit dieser Möglichkeit eine effektive Hilfe zum Suchen nach Einstellungen der Richtlinien in den ADMINISTRATIVEN VORLAGEN.

Die Ansicht kann nach folgenden Kriterien gefiltert werden:

- NACH ANFORDERUNGSINFORMATIONEN FILTERN

  Mit dieser Filteroption können die Mindestanforderungen an eine Richtlinie definiert werden, sodass nur die Richtlinien angezeigt werden, die diese Kriterien erfüllen. Wird beispielsweise die Mindestanforderung FUNKTIONIERT NUR UNTER MICROSOFT WINDOWS 2000 gewählt, so werden lediglich die Richtlinien der ADMINISTRATIVEN VORLAGEN aufgelistet, die nur für das Betriebssystem Windows 2000 gelten.

- NUR KONFIGURIERTE RICHTLINIENEINSTELLUNGEN ANZEIGEN

  Die Auswahl dieser Option bewirkt, dass nur die Richtlinien der ADMINISTRATIVEN VORLAGEN angezeigt werden, die entweder den Status AKTIVIERT oder DEAKTIVIERT aufweisen. Alle Richtlinien, die den Status NICHT KONFIGURIERT besitzen, werden nicht angezeigt.

- NUR VOLLSTÄNDIG VERWALTBARE RICHTLINIENEINSTELLUNGEN ANZEIGEN

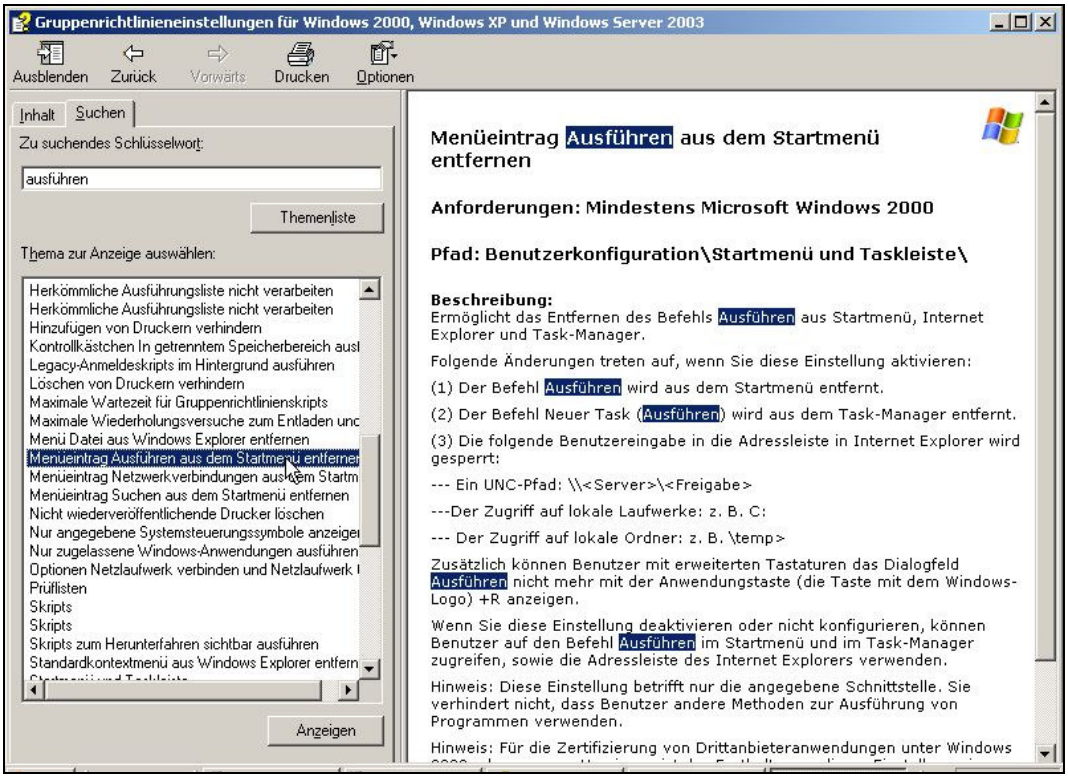
  Mit der Aktivierung dieser Option werden alle Richtlinien ausgeblendet, die feste Einstellungen in der Registrierung durchführen, das sind z. B. die Einstellungen der NT-Systemrichtlinien. Diese Option ist standardmäßig aktiviert.

Filterung der Ansicht der Administrativen Vorlagen

Eine weitere Möglichkeit, einzelne Richtlinien in den ADMINISTRATIVEN VORLAGEN zu finden, bietet die Suche nach Schlüsselwörtern (siehe folgende Abbildung) in den einzelnen Vorlagedateien, die im Kapitel 9.2 näher beschrieben werden. Diese Stichwortsuche bietet sich vor allem in den zahlreichen Richtlinien im Bereich System (Vorlagedatei *system.adm*) an. Leider versteckt sich die Stichwortsuche etwas in der normalen Hilfefunktion, der Aufruf der Suche ist in der Schrittanweisung beschrieben.

Stichwortsuche der ADMINISTRATIVEN VORLAGEN aufrufen!

1. *Markieren Sie im Gruppenrichtlinien-Editor den Knoten ADMINISTRATIVE VORLAGEN der Benutzer- bzw. der Computerkonfiguration und rufen Sie das Kontextmenü auf.*
2. *Wählen Sie den Menüpunkt HILFE und scrollen Sie im Hilfetext ADMINISTRATIVE VORLAGEN bis zu der Beschreibung STANDARDMÄßIGE ADM-DATEIEN IM LIEFERUMFANG VON WINDOWS.*
3. *Wählen Sie den Link SYSTEMEINSTELLUNGEN, um in der Vorlagendatei system.adm nach Schlüsselwörtern zu suchen (siehe Abbildung unten).*

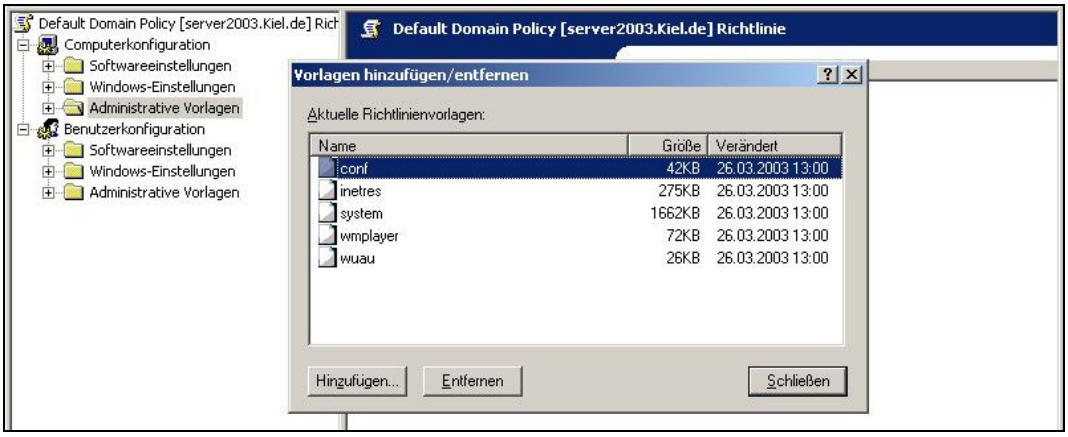


Stichwortsuche in den Vorlagedateien

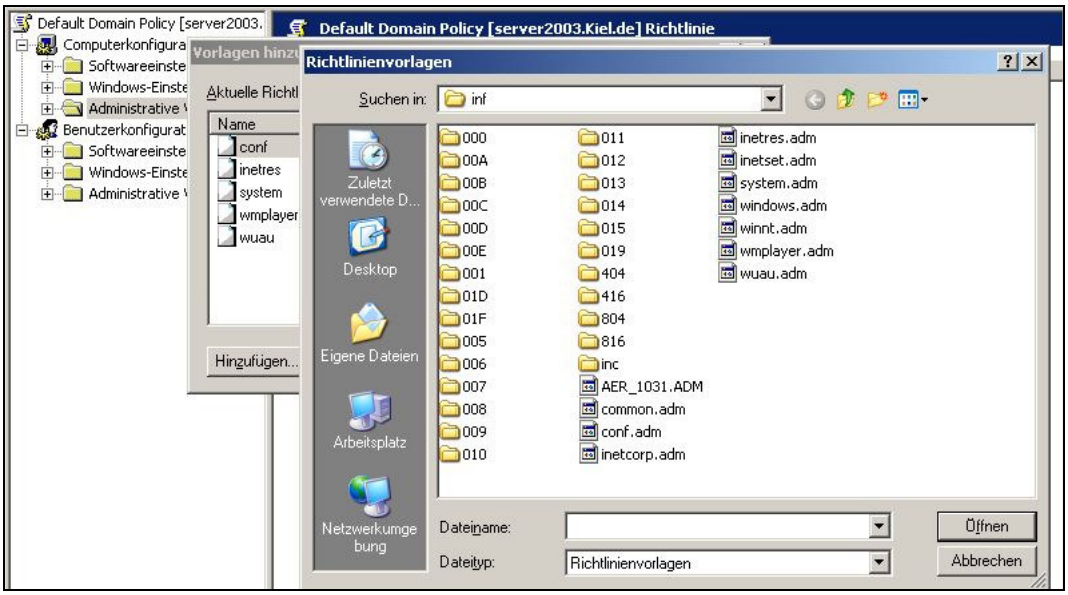
7.4 Importieren von adm-Dateien

Die Grundlage der Einstellungen, die in den Richtlinien der ADMINISTRATIVEN VORLAGEN der Computer- sowie Benutzerkonfiguration vorgenommen werden können, sind die adm-Dateien. Sie stellen die spezifischen Informationen zur Verarbeitung der Richtlinien zur Verfügung. Jedes Windows-Betriebssystem enthält einen spezifischen Satz an adm-Dateien (siehe auch Kapitel 9). Zusätzlich zu dem vordefinierten Satz können weitere adm-Dateien für

Windows-Komponenten oder Microsoft-Software, z. B. Microsoft Office, hinzugefügt werden. Diese können im Gruppenrichtlinien-Editor importiert werden.



Aktuelle Richtlinienvorlagen



Importieren von Richtlinienvorlagen

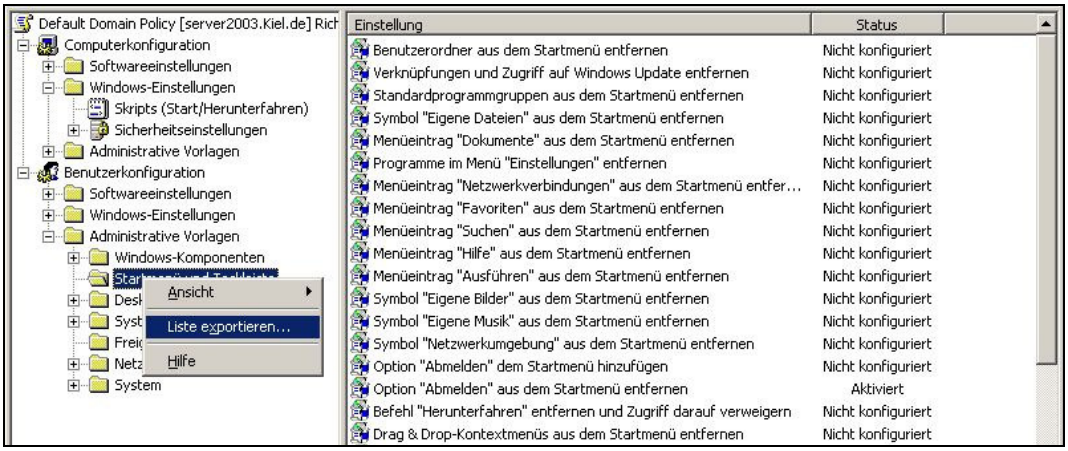
Adm-Dateien in die ADMINISTRATIVEN VORLAGEN einer Gruppenrichtlinie importieren!

1. *Speichern Sie Ihre adm-Dateien in dem Verzeichnis, in dem Sie Ihre adm-Dateien verwalten (Standard: Stammverzeichnis:\Windows\inf).*
2. *Öffnen Sie den Gruppenrichtlinien-Editor der Gruppenrichtlinie, in der Sie die adm-Dateien importieren möchten.*
3. *Markieren Sie den Knoten ADMINISTRATIVE VORLAGEN der Computer- oder*

Benutzerkonfiguration. Rufen Sie das Kontextmenü auf und wählen Sie VORLAGEN HINZUFÜGEN/ENTFERNEN.

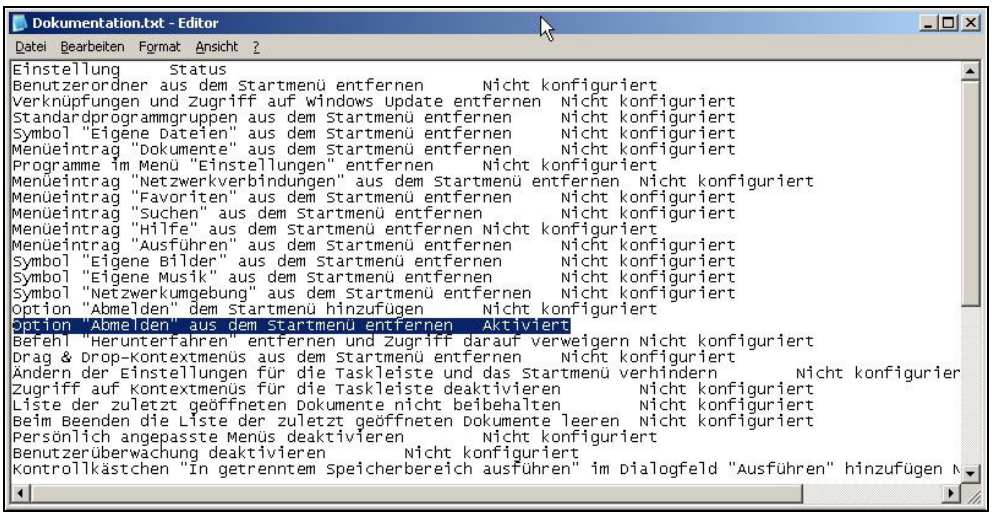
4. *Navigieren Sie zum Speicherort der entsprechenden adm-Datei und markieren Sie sie. Bestätigen Sie mit* ÖFFNEN *und danach mit* SCHLIEßEN.

7.5 Dokumentation von Richtlinieneinstellungen



Option LISTE EXPORTIEREN im Gruppenrichtlinien-Editor

Der Gruppenrichtlinien-Editor besitzt keine Möglichkeit zur strukturierten und übersichtlichen Dokumentation der Richtlinieneinstellungen. Die einzige Möglichkeit zur Dokumentation, für den Fall, dass die Gruppenrichtlinien-Verwaltungskonsole noch nicht eingesetzt wird oder eingesetzt werden kann, ist die Option Liste exportieren. Dabei wird eine Textdatei erzeugt, die allerdings nicht sehr übersichtlich ist (siehe Abbildung unten).

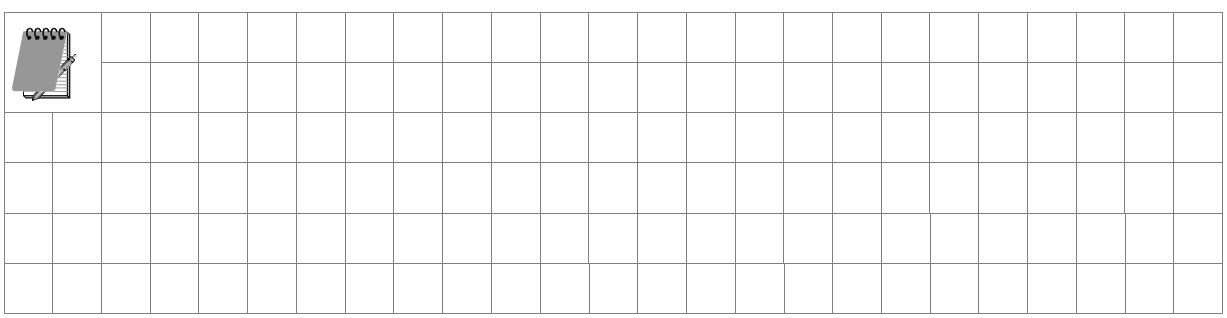


Dokumentation des Gruppenrichtlinien-Editors

Wenn Sie die Option LISTE EXPORTIEREN einsetzen, müssen Sie darauf achten, dass Sie die Option auf einem Knoten einsetzen, der die entsprechenden Richtlinien enthält. Wenn Sie die Option z. B. auf den Knoten ADMINISTRATIVE VORLAGEN anwenden, dann wird Ihnen nur die Unterstruktur der ADMINISTRATIVEN VORLAGEN angezeigt, nicht aber die Unterstrukturen und Richtlinien der untergeordneten Knoten.

7.6 Sicherheitscheck

- *Sie haben **verschiedene Möglichkeiten**, den Gruppenrichtlinien-Editor aufzurufen, je nachdem mit welcher Gruppenrichtlinie Sie arbeiten. Überprüfen Sie beim Arbeiten mit dem Gruppenrichtlinien-Editor immer die oberste Ebene. Sie gibt den Hinweis darauf, um welche Richtlinie es sich handelt.*
- *Benutzen Sie bei den ADMINISTRATIVEN VORLAGEN zur Konfiguration der Richtlinien die Option **NICHT KONFIGURIERT**, wenn die Richtlinie für die Benutzer- oder Computerkonten der entsprechenden Verwaltungseinheit nicht verarbeitet werden soll.*
- *Benutzen Sie bei den ADMINISTRATIVEN VORLAGEN zur Konfiguration der Richtlinien die Option **AKTIVIERT**, wenn die Richtlinie auf die Benutzer- oder Computerkonten der entsprechenden Verwaltungseinheit angewendet werden soll.*
- *Benutzen Sie bei den ADMINISTRATIVEN VORLAGEN zur Konfiguration der Richtlinien die Option **DEAKTIVIERT**, wenn die Richtlinie **nicht** auf die Benutzer- oder Computerkonten der entsprechenden Verwaltungseinheit angewendet werden soll, auch wenn sie auf einer höheren Hierarchieebene schon aktiviert und vererbt wurde.*
- *Benutzen Sie die **Filterung** des Gruppenrichtlinien-Editors, um die Übersichtlichkeit im Bereich der ADMINISTRATIVEN VORLAGEN der Computer- und Benutzerkonfiguration zu erhöhen.*
- *Benutzen Sie die **Stichwortsuche** der Hilfefunktion, um in den Vorlagedateien nach Richtlinien zu suchen.*
- *Nutzen Sie die **Importfunktion**, um adm-Dateien in die Gruppenrichtlinien zu integrieren.*



8 Software- und Windows-Einstellungen

In diesem Kapitel erfahren Sie,

- welche Richtlinien in den Containern SOFTWARE- UND WINDOWSEINSTELLUNGEN enthalten sind,
- wie Software von einem Server auf Clients verteilt werden kann,
- wie Systemeinstellungen über Skripts zugewiesen werden können,
- welche Bedeutung die Richtlinien unter den Sicherheitseinstellungen haben,
- mit welcher Richtlinie die Ausführung von Software eingeschränkt wird,
- wann der Einsatz der Remoteinstallationsdienste sinnvoll ist,
- wie die Daten der lokalen Profile durch eine Ordnerumleitung auf den Server verschoben werden können und
- welche Möglichkeiten bestehen, den Internet Explorer zentral zu konfigurieren.

In diesem Kapitel werden die Container SOFTWARE- und WINDOWS-EINSTELLUNGEN der Computer- und Benutzerkonfiguration einer Gruppenrichtlinie beschrieben. Die ADMINISTRATIVEN VORLAGEN werden aufgrund ihrer besonderen Bedeutung in dem Kapitel 9 dargestellt.

8.1 Softwareverteilung

Mit Hilfe der Active Directory-Gruppenrichtlinien wird eine zentrale Softwareverteilung auf Basis der Windows-Installer-Technologie unterstützt. Über sogenannte msi-Pakete lassen sich die Software-Installationsvorgänge auf dem Client automatisieren. Mit dem Einsatz dieser Installationsmethode können die meisten Anwendungen entsprechend den Bedürfnissen der Anwender bestimmt und freigegeben werden, sodass sich der Anteil nicht erforderlicher Software auf dem Client erheblich reduzieren lässt.

Folgendes ist bei der Softwareverteilung zu beachten:

1. *Erstellen Sie eine Liste der Software, die mit Hilfe der Gruppenrichtlinien zentral auf den Clients installiert werden soll.*
2. *Prüfen Sie, ob sich mit der entsprechenden Software msi-Pakete erstellen lassen.*
3. *Für die Softwareverteilung benötigen Sie einen bestimmten Festplattenbereich oder einen dedizierten Computer, auf dem die Software zur Installation bereitgestellt wird.*

4. *Erzeugen Sie im Active Directory eine Organisationseinheiten-Struktur, die eine differenzierte Softwareverteilung ermöglicht (siehe Arbeitsanweisung weiter unten).*

Softwareinstallationen können sowohl in der COMPUTER- als auch in der BENUTZERKONFIGURATION eingerichtet werden:

- Anwendungen, die in dem Knoten Computerkonfiguration bereitgestellt werden, stehen allen Benutzern, die sich an dem entsprechenden Computer anmelden, zur Verfügung. In der Computerkonfiguration kann die Software nur zugewiesen werden, d. h. sie wird während des Startvorganges des Computers installiert.
- In dem Knoten Benutzerkonfiguration können die Anwendungen einem einzelnen Benutzerkonto bereitgestellt werden. Sie werden dem Benutzer an jedem Computer, an dem er sich anmeldet, zur Verfügung gestellt. In der Benutzerkonfiguration kann Software entweder zugewiesen oder veröffentlicht werden. Zugewiesene Software wird bei der Anmeldung des Benutzers installiert. Veröffentlichte Software wird entweder beim ersten Aufruf der Anwendung installiert oder dem Benutzer in der Rubrik Software der Systemsteuerung angezeigt, sodass er sich die Anwendung bei Bedarf eigenverantwortlich installieren kann.

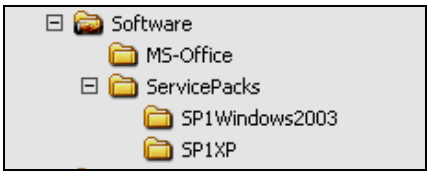
Es gibt zwei Methoden zur Erstellung von Windows-Installer msi-Paketen:

- Die Software unterstützt die Windows-Installer-Technologie und es kann über das Setup ein msi-Paket generiert werden.
- Die Software stellt keine Funktion zur Erstellung eines msi-Paketes bereit. Mit Hilfe des Tools WinINSTALL LE wird ein msi-Paket erstellt.

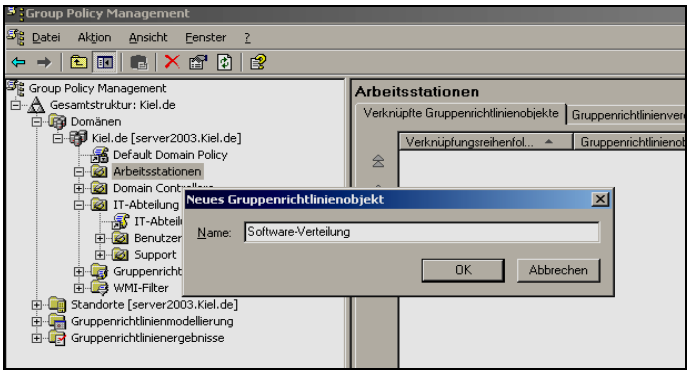
Für eine professionelle Softwareverteilung in größeren Netzwerken sollte eine professionelle Softwareverteilungs-Software eingesetzt werden. Diese verfügt in der Regel über viele weitere Funktionen, wie z. B. der System- und Sicherheitsaktualisierung (Patches), die beim Einsatz der Softwareverteilung mit Hilfe der Gruppenrichtlinien nicht unterstützt werden.

MS-Office XP über die Softwareverteilung bereitstellen!

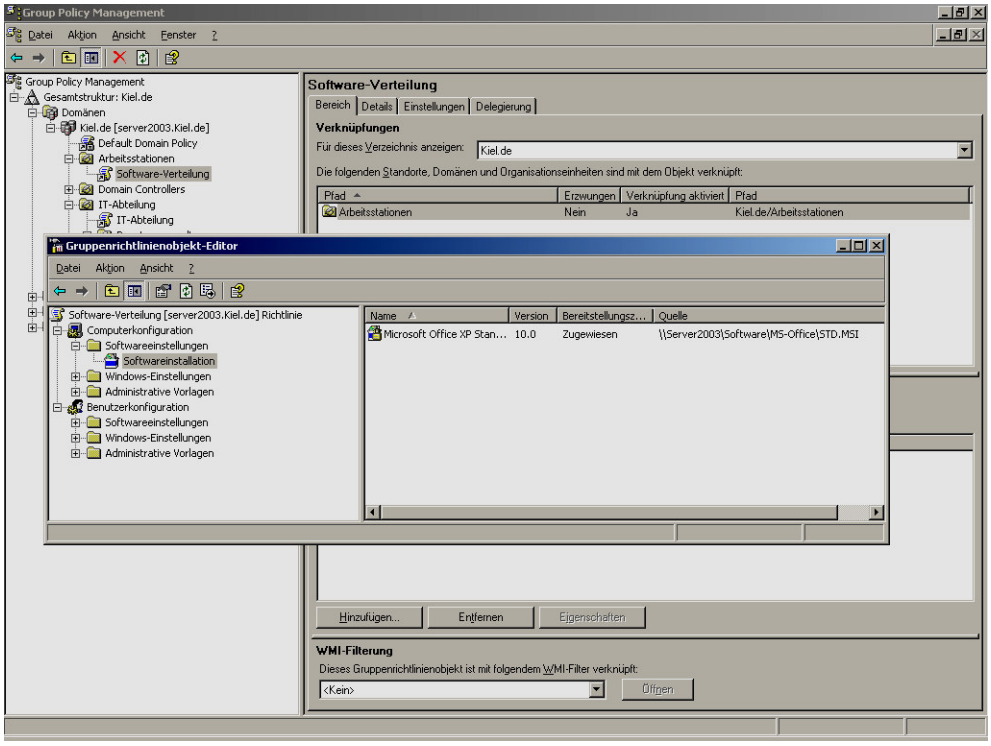
1. *Legen Sie auf einem Fileserver eine Ordnerstruktur für die Softwareverteilung an, die untenstehende Abbildung zeigt ein Beispiel.*



2. *Vergeben Sie dem ersten Ordner eine Freigabe für die Gruppe JEDER mit der Berechtigung LESEN.*
3. *Weisen Sie der Gruppe JEDER in den nachfolgenden Ordnern die NTFS-Berechtigung LESEN, AUSFÜHREN zu.*
4. *Starten Sie MS-Office XP von der Installations-CD mit dem Befehl* `setup /a`*. Es öffnet sich das Installationsfenster zur Eingabe des Installationsordners und des Produkt-Keys. Im Folgenden wird dann MS-Office XP als msi-Paket im angegebenen Ordner generiert.*
5. *Legen Sie fest, ob Sie MS-Office XP computer- oder benutzerbezogen zur Verfügung stellen möchten. Entsprechend müssen Sie im Active Directory eine Struktur anlegen, die den Anforderungen einer zentralen Softwareverteilung mit Hilfe von Gruppenrichtlinien gerecht wird. Für eine computerbezogene Softwareverteilung sollten Sie die Computerkonten in eine eigenständige Organisationseinheit (z. B. in der Abbildung auf der nächsten Seite die Organisationseinheit ARBEITSSTATIONEN) verschieben und diese mit der entsprechenden Gruppenrichtlinie verknüpfen (in der Abbildung auf der nächsten Seite die Gruppenrichtlinie SOFTWARE-VERTEILUNG).*
6. *Markieren Sie den Container COMPUTERKONFIGURATION-SOFTWAREEINSTELLUNGEN in der Gruppenrichtlinie und rufen Sie das Kontextmenü auf. Über die Option NEU können Sie das msi-Paket zuweisen.*
7. *Beachten Sie, dass Sie das msi-Paket über den Netzwerkpfad öffnen (siehe Abbildung auf der nächsten Seite).*
8. *Für eine benutzerbezogenen Softwareverteilung sollten Sie die Gruppenrichtlinie einer Organisationseinheit zuordnen, in der sich die entsprechenden Benutzerkonten befinden. Wählen Sie für die Zuweisung oder Veröffentlichung der Software dann den Container BENUTZERKONFIGURATION-SOFTWAREEINSTELLUNGEN.*



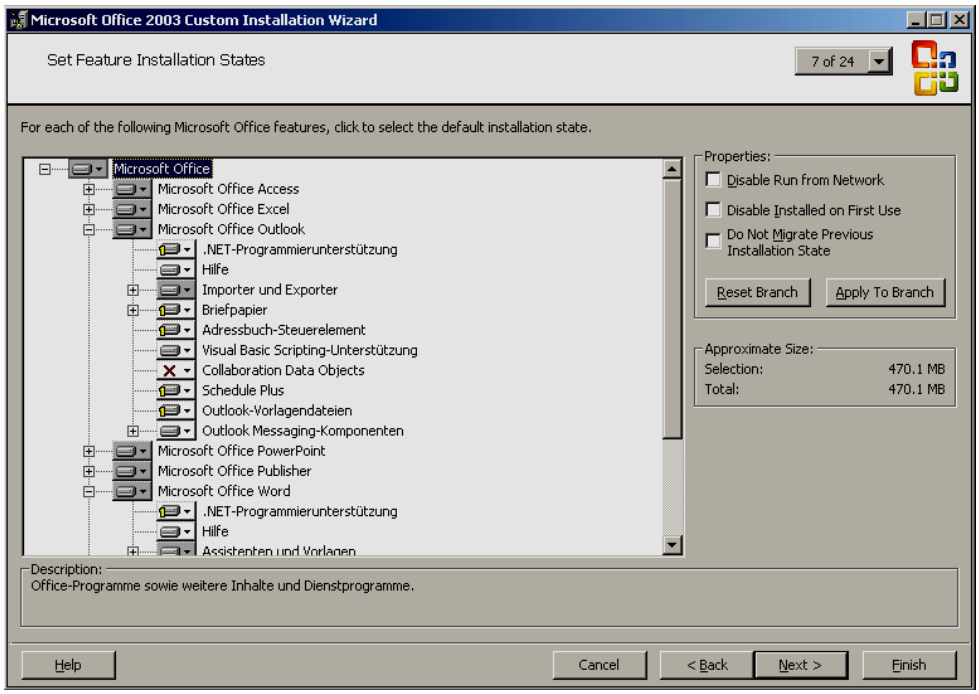
Gruppenrichtlinie für die computerbezogene Softwareverteilung



Computerbezogene Richtlinie im Knoten COMPUTERKONFIGURATION

In größeren Organisationen besteht häufig die Anforderung, die Software an die Bedürfnisse der Benutzer anzupassen. Es besteht die Möglichkeit, über eine sogenannte mst-Datei Anpassungen an eine benutzerbezogene Softwareverteilung durchzuführen. Für die Erzeugung einer mst-Datei stellt Microsoft für MS-Office das Tool *Custom Installation Wizard* zur Verfügung. Es ist Bestandteil des *Office Resource Kit*.

Für MS-Office 2000, 2003 und XP gibt es jeweils ein gesondertes Resource Kit. Die Erstellung einer mst-Datei ist nur mit dem passenden Resource Kit möglich.



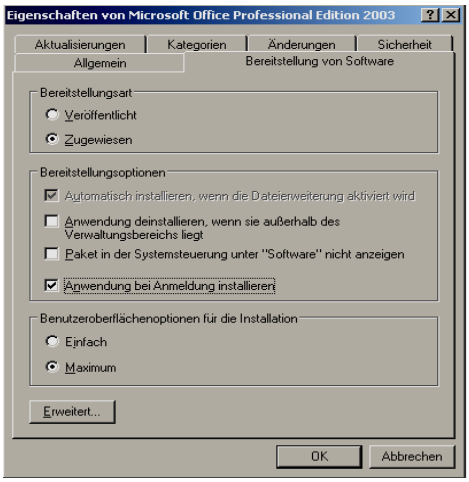
Funktionsanpassung für Office-Komponenten

Die mst-Datei wird auf dem Fileserver in dem angegebenen Ordner für die Softwareverteilung gespeichert. Bei der Zuweisung des benutzerbezogenen msi-Paketes ist dann noch die mst-Datei einbezogen. Bei der nächsten Installation werden dann die in der mst-Datei aufgeführten Konfigurationseinstellungen berücksichtigt.

Erstellen einer mst-Datei für MS-Office 2003!

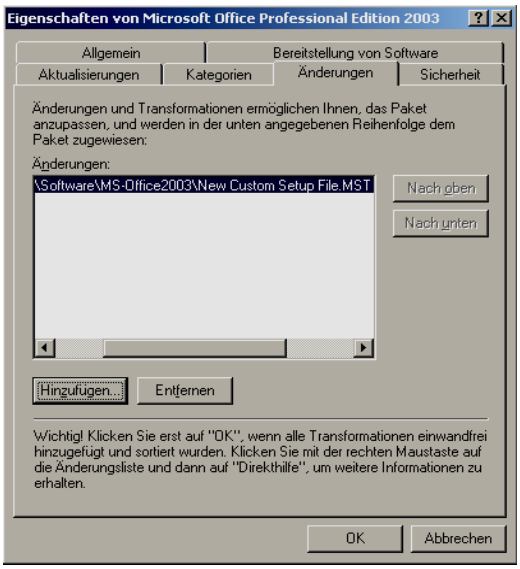
1. *Installieren Sie das Office Resource Kit 2003 und rufen Sie anschließend den Custom Installations Wizard auf. Folgen Sie den Eingabeaufforderungen.*
2. *Führen Sie die gewünschten Funktionsanpassungen durch und erstellen Sie die mst-Datei.*
3. *Rufen Sie nun die Gruppenrichtlinie für die Softwareverteilung auf. Weisen Sie im Container* BENUTZERKONFIGURATION-SOFTWAREEINSTELLUNG *ein neues msi-Paket für MS-Office 2003 zu.*
4. *Im Fenster* BEREITSTELLUNGSMODUS *wählen sie die Option* ERWEITERT.

5. *Auf der Registerkarte BEREITSTELLUNG VON SOFTWARE wählen Sie ZUGEWIESEN und ANWENDUNG BEI ANMELDUNG INSTALLIEREN.*



Registerkarte Bereitstellung von Software

6. *Die mst-Datei können Sie anschließend auf der Registerkarte ÄNDERUNGEN mit der Schaltfläche HINZUFÜGEN integrieren.*

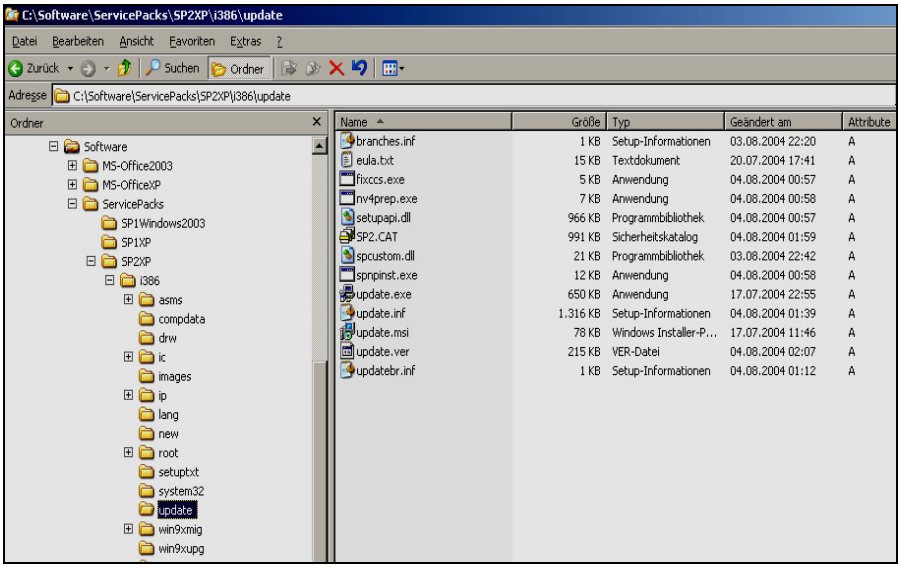


Registerkarte Änderungen

Ein weiteres Anwendungsbeispiel für die computerbezogene Softwareverteilung stellt die Verteilung von Service-Packs auf die Clients dar.

Windows XP Service Pack über die Softwareverteilung bereitstellen!

1. *Öffnen Sie das Windows XP Service Pack, indem Sie es unmittelbar über die Eingabeaufforderung mit dem Befehl windowsxp-kb835935-sp2-deu.exe /x starten.*
2. *Durch die Angabe des Parameters /x werden Sie aufgefordert, den Pfad für den Speicherort der Dateien anzugeben (als Beispiel in der Abbildung unten das Verzeichnis SP2XP als Unterverzeichnis von SERVICE PACKS). Dieser sollte sich auf dem Softwareverteilungsserver befinden.*



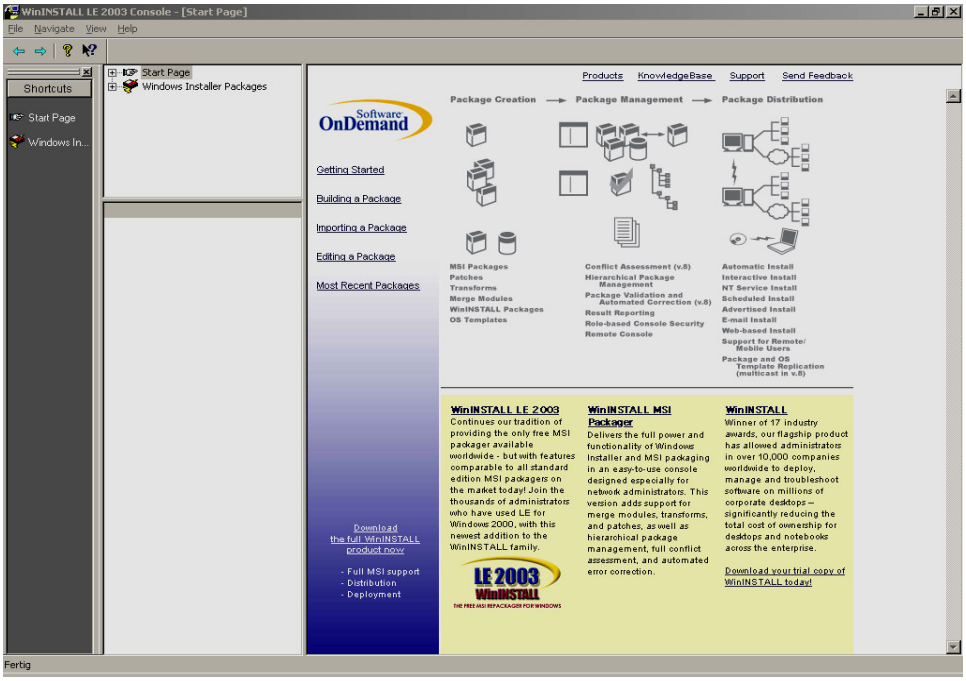
Windows XP Servicepack

3. *Nach dem Entpacken finden Sie das MSI-Paket update.msi im Ordner \i386\update (siehe Abbildung oben).*
4. *Rufen Sie nun die Gruppenrichtlinie für die computerbezogene Softwareverteilung auf und weisen Sie im Container COMPUTERKONFIGURATION-SOFTWAREVERTEILUNG das msi-Paket zu. Achten Sie darauf, dass Sie diese Gruppenrichtlinie der Organisationseinheit zuweisen, in der sich die Computerkonten befinden, denen Sie das Paket zuweisen möchten.*
5. *Führen Sie die weiteren Schritte analog zur Arbeitsanweisung „Softwareverteilung für MS-Office XP“ aus.*

Beachten Sie, dass bei der Softwareverteilung der Fileserver und das Netzwerk nicht überlastet werden. Bei einer computerbezogenen Softwareverteilung werden die zugewiesenen Anwendungen unmittelbar nach dem Start des Clients installiert. Die Veröffentlichung einer Anwendung, die eine Installation erst bei dem ersten Gebrauch der Anwendung aktiviert, ist nur bei der benutzerbezogenen Softwareverteilung möglich.

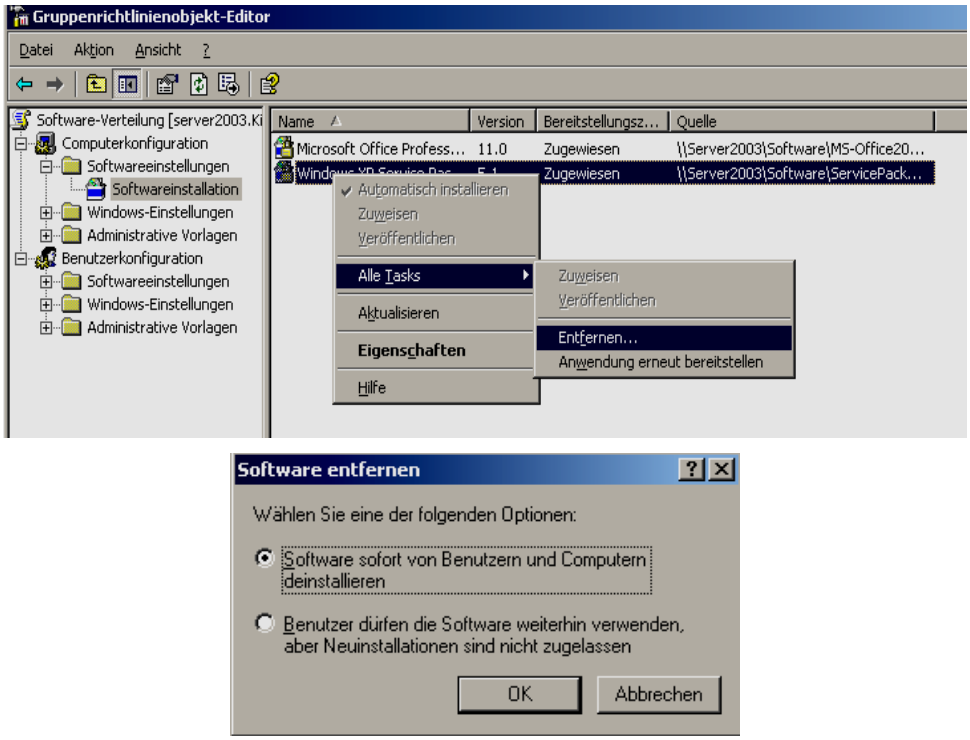
Stellt eine Software keine Methode zur Erstellung einer msi-Datei zur Verfügung, kann ein Snapshotverfahren zum Einsatz kommen. Dabei wird mit Hilfe eines Tools das System in Bezug auf seine Konfiguration analysiert und die Systemdaten in einer Datenbank festgehalten. Anschließend wird auf dem System die Software installiert, die für die Softwareverteilung vorgesehen ist. Nach Abschluss der Installation wird das System erneut in Bezug auf die durchgeführten Veränderungen untersucht und eine msi-Datei generiert.

Der Einsatz des Snapshotverfahren bietet sich immer dann an, wenn sich mit der Anwendung keine msi-Pakete erstellen lassen oder wenn mit Hilfe einer mst-Datei nicht die gewünschte Konfigurationseinstellung erzielt werden kann. Sie sollten aber beachten, dass immer die gleichen Systemvoraussetzungen sowohl auf dem Referenzsystem als auch auf dem Zielsystem vorhanden sein müssen. Ansonsten gibt die Anwendung bei der Installation eine Fehlermeldung heraus.



Snapshot-Tool WinINSTALL LE

Das Löschen von zugewiesener Software kann ebenfalls über die Richtlinie SOFTWAREVERTEILUNG zentral verwaltet werden. Hierfür stehen zwei Optionen zur Auswahl. Entweder wird die Software vom Client entfernt, sobald das entsprechende msi-Paket entfernt wird (siehe Abbildung), oder weitere Installationen werden verhindert.

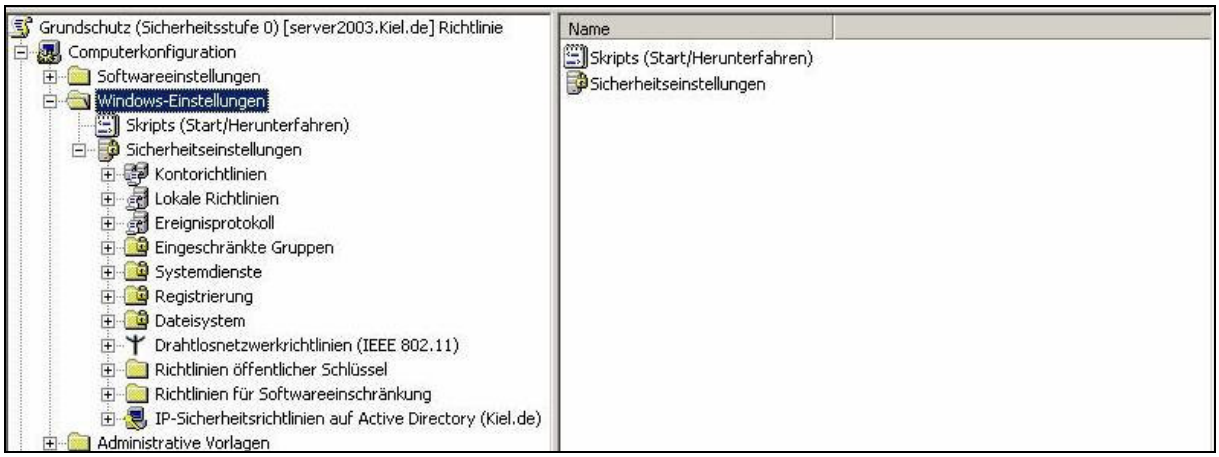


msi-Paket entfernen

8.2 Windows-Einstellungen

In dem Knoten Windows-Einstellungen sind eine Vielzahl von systemnahen Konfigurationseinstellungen zusammengefasst worden. So können beispielsweise neben einer zentralen Skriptzuweisung auch Benutzerrechte, Sicherheitsoptionen, Zugriffsrechte auf Dienste, Richtlinien für Kennwörter, das Dateisystem und Registrierungsschlüssel verwaltet werden.

Dieser Bereich stellt sich so komplex dar, dass eine ausführliche Beschreibung aller Einstellungsparameter den Umfang dieses ***backUP***-Magazins sprengen würde.



Windows-Einstellungen der Computerkonfiguration

Aus diesem Grund werden nachfolgend die für das Grundverständnis bedeutsamen Strukturen beschrieben und der Schwerpunkt auf die für die Sicherheit wichtigen Gruppenrichtlinien gelegt.

8.2.1 Skripts

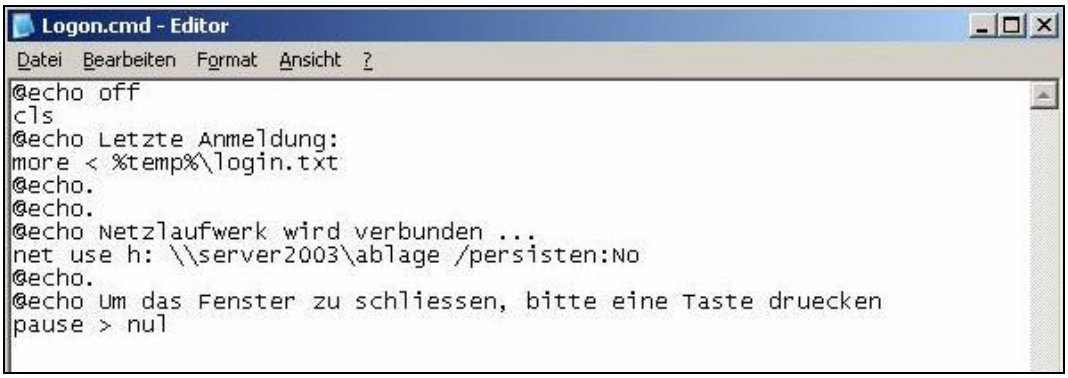
Ein Skript ist ein Programm, das in einer interpretierbaren Sprache geschrieben wird, aus einer Reihe von Befehlen besteht und bestimmte Anwendungsaufgaben automatisiert. Skripte können dazu verwendet werden, um definierte Konfigurationen an der Arbeitsumgebung von Benutzern vorzunehmen.

Bei den Microsoft Serverbetriebssystemen vor Windows 2000 konnte der Systemadministrator dem Benutzer über die Benutzereigenschaften ein einzelnes Skript zuweisen, dass bei der Anmeldung des Benutzers am Client abgearbeitet wurde. Das ist aufgrund der Abwärtskompatibilität weiterhin möglich. Mit der Zuweisung von Skripten über die Gruppenrichtlinien können

- ein oder mehrere Skripte für die Verarbeitung während des Startens oder Herunterfahrens eines Systems angegeben werden. Die Skripte werden zentral in der Gruppenrichtlinie Skripts (Start/Herunterfahren) im Knoten Computerkonfiguration verwaltet.
- ein oder mehrere Skripte für die Verarbeitung während der An- oder Abmeldung von Benutzern angegeben werden. Die Skripte werden zentral in der Gruppenrichtlinie Skripts (Anmelden/Abmelden) im Knoten Benutzerkonfiguration verwaltet.

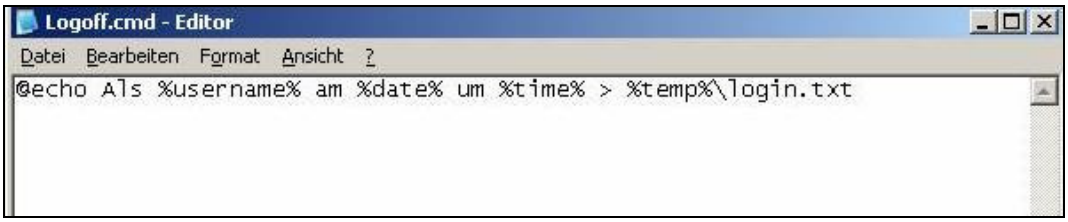
Unterstützt werden alle gängigen Skriptformate wie z. B. Batch, Perl, Visual Basic oder Java.

Anhand eines Beispiels wird nachfolgend eine benutzerbezogene Zuweisung eines An- und Abmeldeskripts dargestellt. Das Anmeldeskript soll beim Anmelden am System die gespeicherten Daten aus der Datei login.txt auslesen und den Inhalt der Datei am Bildschirm ausgeben (siehe Abbildung unten). Zusätzlich wird dem Benutzer die Ablagestruktur auf dem Server als Laufwerk h: zur Verfügung gestellt. Die entsprechende Ablagestruktur, in diesem Beispiel das Verzeichnis ABLAGE, muss auf dem Server eingerichtet worden sein.



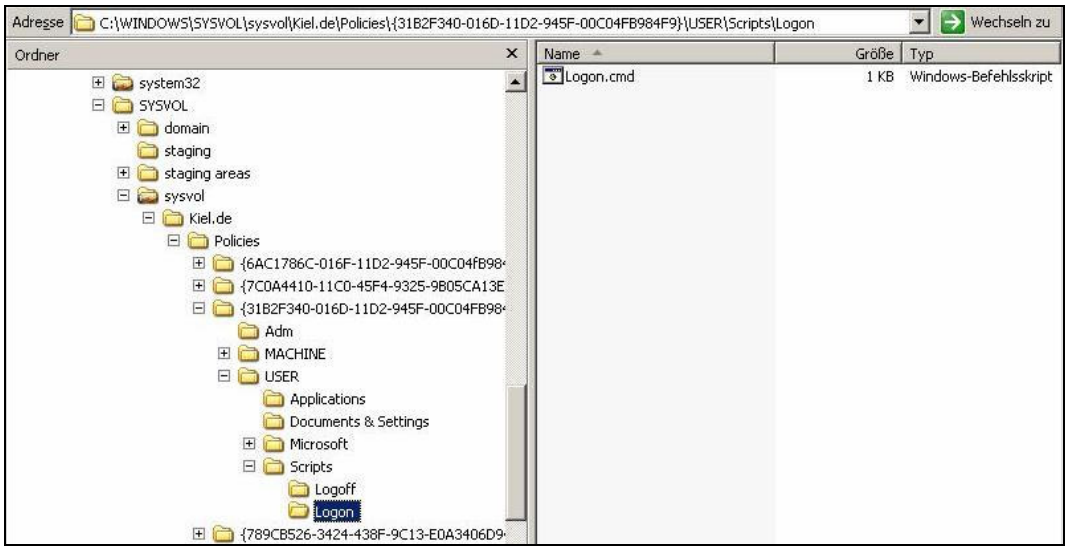
Anmelde-Skript

Die Datei login.txt wird beim ersten Abmelden des Benutzers vom System im temporären Verzeichnis TEMP seines Benutzerprofils gespeichert (<Stammverzeichnis>\Dokumente und Einstellungen\<User>\Lokale Einstellungen\Temp) und dann bei jedem erneuten Abmelden vom System aktualisiert. Es werden die Werte der Variablen USERNAME, DATE und TIME gespeichert (siehe Abbildung unten).



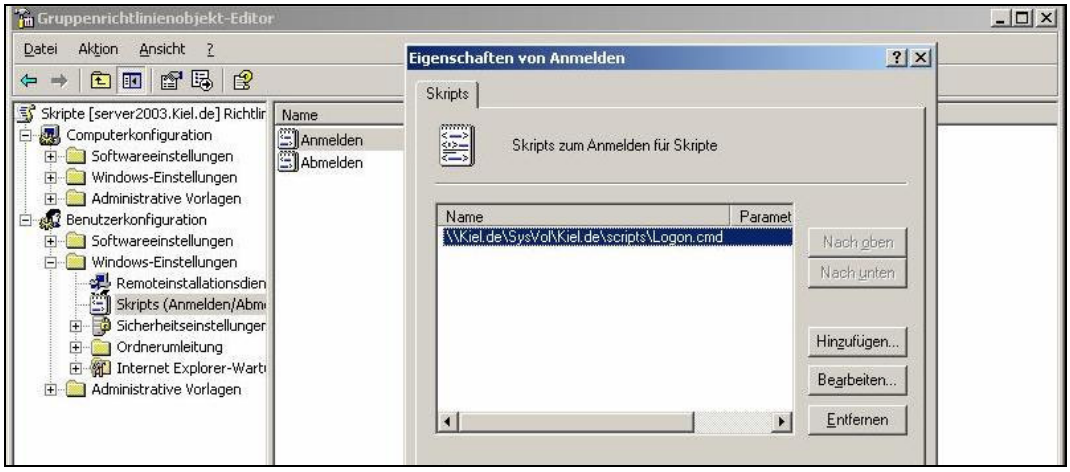
Abmelde-Skript

Die erstellten An- und Abmeldeskripts müssen in dem Verzeichnis SKRIPTS derjenigen Gruppenrichtlinie, die das An- und Abmeldeskript zur Verfügung stellen soll, gespeichert werden (siehe folgende Abbildung). Dazu wird entweder eine neue Gruppenrichtlinie eingerichtet oder eine schon vorhandene Gruppenrichtlinie genutzt. Wichtig ist, dass sie mit der Verwaltungseinheit verknüpft ist, in der die Benutzerkonten gespeichert sind, denen die Skripte zugewiesen werden sollen. Die genaue Vorgehensweise der Speicherung wird in der Schrittanweisung näher beschrieben.



Speicherort des Anmeldeskripts

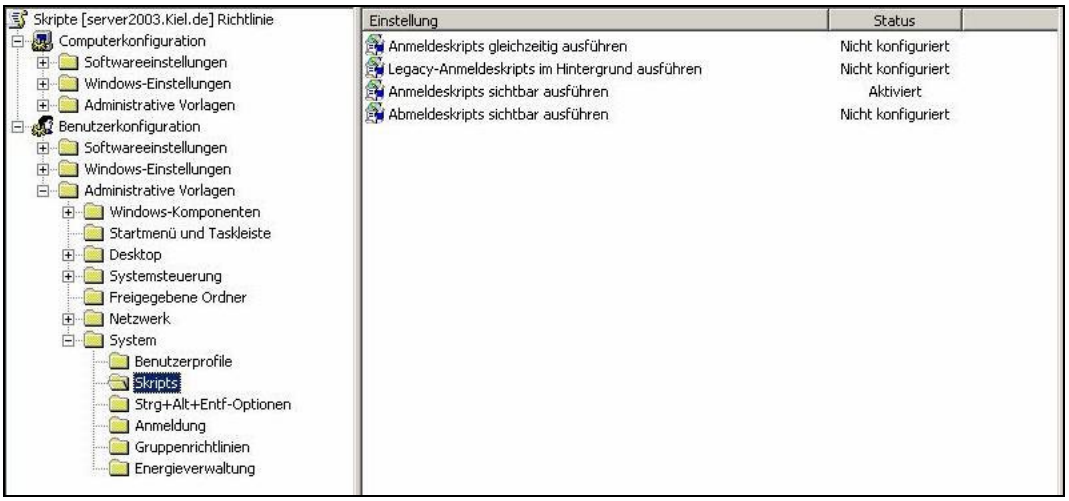
Im nächsten Schritt müssen das An- und Abmeldeskript mit dem Knoten WINDOWS-EINSTELLUNGEN-SKRIPTS der Benutzerkonfiguration der entsprechenden Gruppenrichtlinie (in der Abbildung unten die Gruppenrichtlinie SKRIPTE) geknüpft werden.



Zuweisung des Anmeldeskripts

In diesem Beispiel sollen dem Benutzer beim Anmelden Informationen am Bildschirm angezeigt werden, die in der Datei login.txt gespeichert sind. Standardmäßig werden die Gruppenrichtlinien-Skripte im Hintergrund verarbeitet. Damit die Skripte für den Benutzer sichtbar werden, muss die Verarbeitungssteuerung der Skripte in der entsprechenden Gruppenrichtlinie angepasst werden.

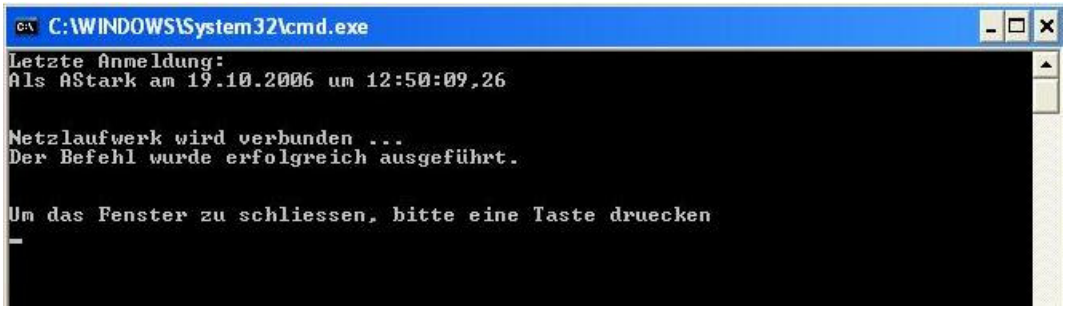
In dem Container ADMINISTRATIVE VORLAGEN-SYSTEM-SKRIPTS des Knotens BENUTZERKONFIGURATION kann die Verarbeitung der Skripte mit entsprechenden Richtlinien angepasst werden. Soll die Skriptverarbeitung für den Benutzer sichtbar ausgeführt werden, so muss die Richtlinie ANMELDESKRIPTS SICHTBAR AUSFÜHREN aktiviert werden.



Richtlinien für die Skriptverarbeitung

Anmeldeskripte, die über die Benutzereigenschaften des jeweiligen Benutzerkontos zugewiesen werden, werden auch Legacy-Anmeldeskripte genannt. Ein Benutzer kann sowohl über ein Legacy-Anmeldeskript als auch über ein Gruppenrichtlinien-Anmeldeskript verfügen. Dann wird zunächst (standardmäßig) das Gruppenrichtlinien-Anmeldeskript im Hintergrund verarbeitet und danach das Legacy-Anmeldeskript in einem Fenster der Eingabeaufforderung ausgeführt.

Nachdem alle beschriebenen Schritte durchgeführt wurden, zeigt der Bildschirm bei der Anmeldung eines Benutzers am System folgendes Eingabeaufforderungs-Fenster:



Sichtbar ausgeführtes Anmeldeskript

An- und Abmeldeskript benutzerbezogen zuweisen!

1. *Erstellen Sie die An- und Abmeldeskripte und speichern Sie die Dateien entweder in einem für die Skriptverwaltung erstellten Verzeichnis oder in dem Verzeichnis <Stammverzeichnis>\Windows\Sysvol\sysvol\<Domäne>\scripts.*
2. *Öffnen Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND –COMPUTER oder die Gruppenrichtlinien-Verwaltungskonsole.*
3. *Wählen Sie die Gruppenrichtlinie, die die Skriptzuweisung durchführen soll, und rufen Sie den Gruppenrichtlinien-Editor auf.*
4. *Markieren Sie den Container WINDOWS-EINSTELLUNGEN-SKRIPTS (ANMELDEN/ABMELDEN) im Knoten BENUTZERKONFIGURATION. Rufen Sie das Kontextmenü der Richtlinie ANMELDEN auf und wählen Sie die Schaltfläche EIGENSCHAFTEN.*
5. *Es öffnet sich ein Fenster für die Skriptzuweisung. Mit der Schaltfläche HINZUFÜGEN können Sie das Skript, z. B. logon.cmd, auswählen bzw. den Dateinamen und eventuelle Startparameter angeben.*
6. *Wiederholen Sie die Schritte 4 und 5 für die Richtlinie ABMELDEN und das Skript logoff.cmd.*
7. *Beachten Sie, dass die Skriptdateien mit dem von der Gruppenrichtlinie verwendeten Ordner verknüpft werden. Der Pfad zum tatsächlichen Speicherort wird auf der Eigenschaftenseite der Richtlinien ANMELDEN bzw. ABMELDEN des Containers WINDOWS-EINSTELLUNGEN-SKRIPTS (ANMELDEN/ABMELDEN) angezeigt.*
8. *Führen Sie für die Aktualisierung des Gruppenrichtlinienobjekts auf dem Server den Befehl* `gpupdate` *aus.*
9. *Prüfen Sie auf dem Client, ob beide Skripte fehlerfrei ausgeführt werden.*

8.2.2 Sicherheitseinstellungen

Die Sicherheitseinstellungen spielen eine wichtige Rolle für den sicheren Betrieb eines Computers. Aus diesem Grunde werden standardmäßig bereits bei der Installation des Betriebssystems in der Gruppenrichtlinie DEFAULT DOMAIN POLICY Sicherheitskonfigurationseinstellungen im Bereich der KONTORICHTLINIEN und in der Gruppenrichtlinie DEFAULT DOMAIN CONTROLLERS POLICY im Bereich der LOKALEN RICHTLINIEN vorgenommen.

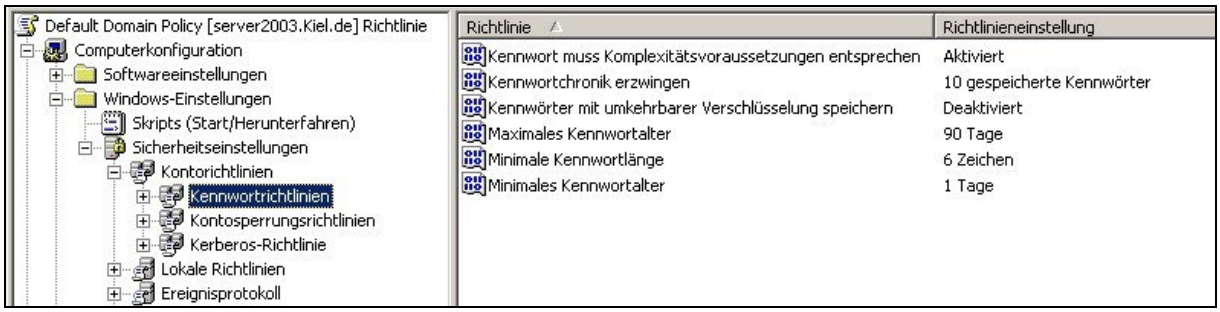
Kontorichtlinien

Die KONTORICHTLINIEN umfassen alle Richtlinien, die die Anmeldung in der Domäne betreffen. Sie sind in die Bereiche KENNWORTRICHTLINIEN, KONTOSPERRUNGSRICHTLINIEN und KERBEROSRICHTLINIEN gegliedert, die in den nachfolgenden drei Abschnitten näher erläutert werden.

Auf einem Domänencontroller müssen die KONTORICHTLINIEN (KENNWORT-, KONTOSPERRUNGS- und KERBEROSRICHTLINIEN) zwingend in der Gruppenrichtlinie DEFAULT DOMAIN POLICY oder einer Gruppenrichtlinie auf Domänenebene aktiviert werden. Kontorichtlinien, die in einer Gruppenrichtlinie auf Ebene der Organisationseinheiten aktiviert werden, werden für Active Directory-Benutzerkonten nicht angewendet (siehe auch Kapitel 2.5).

Kennwortrichtlinien

Die KENNWORTRICHTLINIEN definieren, wie ein gültiges Kennwort für ein Benutzerkonto in einer Domäne aussehen muss.



KENNWORTRICHTLINIEN

KENNWORT MUSS KOMPLEXITÄTSANFORDERUNGEN ENTSPRECHEN

Die Auswahl dieser Richtlinie legt folgende Bedingungen für das gewählte Kennwort fest:

- Drei der folgenden vier Elemente müssen im Kennwort enthalten sein: kleine Buchstaben, große Buchstaben, Zahlen und Sonderzeichen.
- Weder Benutzer- noch Vor- bzw. Nachname dürfen Teil des Kennwortes sein.

Um ein schnelles Erraten oder "Knacken" von Kennwörtern, auch durch den Einsatz von Hacker-Tools, zu verhindern, sollten Sie die Komplexitätsanforderungen an die Kennwörter aktivieren.

KENNWORTCHRONIK ERZWINGEN

Diese Richtlinie speichert die verwendeten Kennwörter eines Benutzers, sodass er bei einem Kennwortwechsel keines seiner gespeicherten Kennwörter wieder verwenden kann. Es können Werte zwischen 0 und 24 vergeben werden.

Um zu verhindern, dass die Benutzer beim Kennwortwechsel wieder ihr altes Kennwort verwenden, sollten Sie die Richtlinie KENNWORTCHRONIK ERZWINGEN aktivieren und einen Wert für die Anzahl der gespeicherten Kennwörter wählen, der Ihrem Sicherheitsniveau entspricht.

KENNWÖRTER MIT UMKEHRBARER VERSCHLÜSSELUNG SPEICHERN

Standardmäßig werden die Kennwörter in der Active Directory Datenbank verschlüsselt gespeichert. Der Schlüssel für den dafür verwendeten Hash-Algorithmus wird nur für die Verschlüsselung benutzt, kann aber nicht für die Entschlüsselung verwendet werden. Das hat den Vorteil, dass ein Kennwort nicht durch die Kenntnis des Algorithmus entschlüsselt werden kann.

Die umkehrbare Verschlüsselung wird auf Systemen benötigt, die einen Zugriff auf „Klartextkennwörter“ benötigen. Dazu wird ein Algorithmus verwendet, der sowohl zum Ver- als auch zum Entschlüsseln den gleichen Schlüssel (Hash-Algorithmus) anwendet. Anwendungen, die z. B. das Protokoll CHAP (Challenge-Handshake Authentication Protocol) benötigen, erfordern die Aktivierung dieser Richtlinie.

Die Aktivierung der Richtlinie KENNWÖRTER MIT UMKEHRBARER VERSCHLÜSSELUNG SPEICHERN stellt eine deutliche Reduzierung der Kennwortsicherheit dar. Wägen Sie den Sicherheitsverlust gegen den erzielbaren Nutzen ab und setzen Sie diese Richtlinie nur sehr überlegt ein.

MAXIMALES KENNWORTALTER

Diese Richtlinie stellt sicher, dass Benutzer ihr Kennwort in regelmäßigen Abständen ändern müssen. Vor Ablauf der eingestellten Frist (Werte zwischen 0 und 999 Tagen) wird der Benutzer vom System aufgefordert, sein Kennwort zu wechseln. Der Wert 0 bedeutet, dass das Kennwort des Benutzers nie abläuft.

Die Wahl des maximalen Kennwortalters hängt von dem Sicherheitsniveau Ihrer Organisation ab. Achten Sie bei der Planung der Kennwortrichtlinien auch auf die Akzeptanz der Mitarbeiter. Wenn die Benutzer ihr Kennwort zu häufig ändern müssen, besteht die Gefahr, dass Trivial-Kennwörter gewählt werden oder sie aufgeschrieben bzw. in einer Datei gespeichert werden.

MINIMALE KENNWORTLÄNGE

Zur Gewährleistung einer ausreichenden Kennwortsicherheit ist die Wahl eines ausreichend langen Kennwortes unerlässlich. Es können Werte zwischen 0 (ein leeres Kennwort ist möglich) und 14 vergeben werden. Dabei muss beachtet werden, dass Windows 2000/2003 seine Kennwörter in 7er-Blöcken abspeichert (siehe Informationsbox unten).

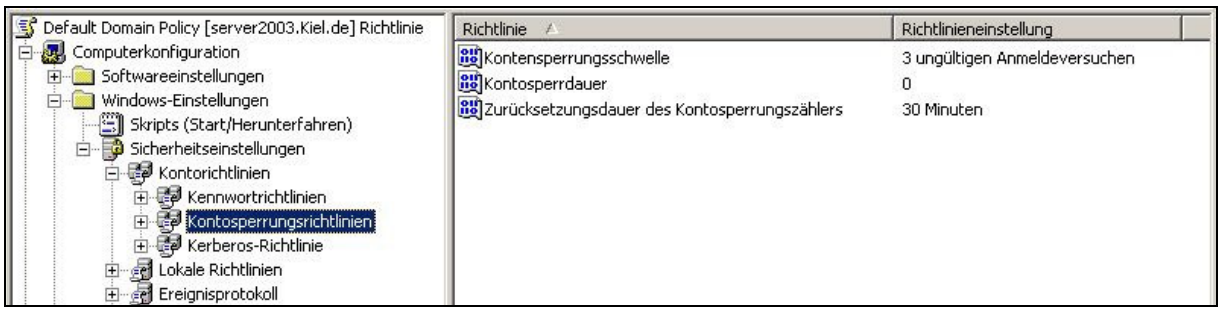
Wenn Sie ein Kennwort mit 10 Zeichen wählen, wird es in zwei Blöcken gespeichert (ein Block mit 7 Zeichen und ein Block mit 3 Zeichen). Jeder Block wird von Crackprogrammen als einzelnes Kennwort betrachtet und der Block mit den geringeren Zeichen ist dementsprechend schnell zu „knacken". Häufig kann von dem „geknackten" Teil des Kennworts auch auf das gesamte Kennwort geschlossen werden. Ein längeres Kennwort muss nicht unbedingt sicherer sein. Wählen Sie unter Berücksichtigung der anderen Kennwortrichtlinien (z. B. Komplexität etc.), Ihrem Sicherheitsniveau und der Akzeptanz der Mitarbeiter ein Kennwort mit 6-7 Zeichen.

MINIMALES KENNWORTALTER

Die Richtlinie gibt an, nach wie vielen Tagen der Benutzer sein Kennwort ändern darf. Sie korrespondiert mit der Richtlinie KENNWORTCHRONIK. Dürfen beispielsweise die letzten 5 Kennwörter entsprechend der Kennwortchronik nicht gewählt werden und das minimale Kennwortalter ist auf 0 Tage eingestellt, dann können die Benutzer bei der Aufforderung zur Kennwortänderung sofort ihr Kennwort fünfmal ändern und dürfen dann ihr „altes" Kennwort wieder wählen. Ist das minimale Kennwortalter aber beispielsweise auf 3 Tage eingestellt, dann können die Benutzer erst nach 3 Tagen ihr Kennwort erneut ändern, danach wieder erst nach 3 Tagen usw. Es können Werte von 0 – 998 Tage eingestellt werden.

Vergeben Sie ein minimales Kennwortalter (z. B. 3 Tage). Sie verhindern damit, dass die Benutzer bei der Aufforderung zur Kennwortänderung ihr Kennwort in einem kurzen Zeitraum so oft ändern, bis sie ihr „altes" Kennwort wieder wählen dürfen (d. h. die Kennwortchronik umgehen).

Kontosperrungsrichtlinien



KONTOSPERRUNGSRICHTLINIEN

KONTOSPERRUNGSSCHWELLE

Diese Richtlinie gibt die Anzahl der Versuche an, die ein Benutzer hat, um sich mit seinem Benutzernamen und Kennwort am System zu authentifizieren. Wird die angegebene Anzahl überschritten, wird das Benutzerkonto gesperrt. Es können Werte von 0 (Konto wird nicht gesperrt, d. h. unbegrenzte Anzahl an Anmeldeversuchen) bis 999 (Konto wird nach 999 ungültigen Anmeldeversuchen gesperrt) eingegeben werden.

Aktivieren Sie die Kontosperrungsschwelle, um zu verhindern, dass ein Kennwort durch „Ausprobieren" an der Konsole geknackt wird, und um zu gewährleisten, dass Sie (in Verbindung mit der Kontosperrdauer und den Protokollierungsrichtlinien) versuchte Angriffe erkennen können.

KONTOSPERRDAUER

Die Kontosperrdauer gibt an, wie lange das Konto im Falle einer Sperrung gesperrt bleibt. Es können Werte zwischen 0 (nur der Administrator kann die Sperrung des Kontos wieder aufheben) und 99 999 Minuten gewählt werden.

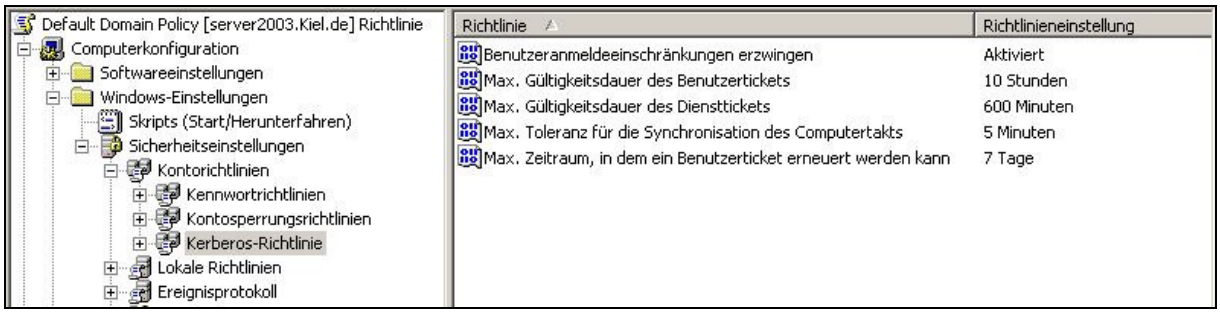
Definieren Sie die Kontosperrungsdauer entsprechend dem Sicherheitsniveau Ihrer Organisation. Wenn Sie die Kontosperrdauer auf 0 einstellen, haben Sie den Vorteil der direkten Kommunikation mit dem Benutzer auf Ihrer Seite und können die Sperrung gleich kategorisieren: entweder nur Passwort vergessen bzw. Eingabefehler oder vielleicht doch ein „Einbruchversuch".

ZURÜCKSETZUNGSDAUER DER KONTOSPERRUNGSZÄHLERS

Dieser Wert legt die Zeit fest, in dem die Zahl der ungültigen Anmeldeversuche wieder auf 0 gesetzt wird (vorausgesetzt das Konto wurde noch nicht gesperrt). Wird der Kontosperrungszähler beispielsweise auf 30 Minuten eingestellt, so werden alle Fehlversuche einer Anmeldung innerhalb dieser Zeitspanne aufaddiert. Wird die definierte Kontosperrschwelle innerhalb der 30 Minuten nicht erreicht, fällt der nächste Fehlversuch (z. B. nach 33 Minuten) in den nächsten 30-Minuten-Zyklus und wird wieder als 1. Ereignis gewertet. Es können Werte zwischen 1 und 99 999 Minuten verwendet werden.

Definieren Sie die Zurücksetzungsdauer Ihres Kontosperrungszählers entsprechend dem Sicherheitsniveau Ihrer Organisation. Wählen Sie die Zeitspanne so groß, dass für einen potentiellen Angreifer kein Anreiz besteht, durch Ausprobieren von Zugangsdaten Zugriff auf das System zu erlangen (z. B. 30 Minuten).

Kerberosrichtlinien



KERBEROSRICHTLINIEN

BENUTZERANMELDEEINSCHRÄNKUNGEN ERZWINGEN

Mit dieser Einstellung wird festgelegt, ob das Kerberos V5-Schlüsselverteilungscenter die Gültigkeit jeder Anfrage für ein Sitzungsticket überprüft und mit den für das Benutzerkonto vergebenen Richtlinien ZUWEISEN VON BENUTZERRECHTEN vergleicht.

MAXIMALE GÜLTIGKEITSDAUER DES BENUTZERTICKETS

Mit dieser Richtlinie kann der maximale Zeitraum (in Minuten) festgelegt werden, in dem ein erteiltes Sitzungsticket zum Zugreifen auf bestimmte Dienste verwendet werden kann.

MAXIMALE GÜLTIGKEITSDAUER DES DIENSTTICKETS

Mit der Richtlinie wird der maximale Gültigkeitszeitraum (in Stunden) eines Tickets festgelegt, das den Benutzern erteilt wird (TGT, Ticket-Granting Ticket). Wenn die Gültigkeit des TGT eines Benutzers abläuft, muss entweder ein neues Ticket angefragt werden oder das bestehende TGT „erneuert“ werden.

MAXIMALE TOLERANZ FÜR DIE SYNCHRONISATION DES COMPUTERTAKTES

In dieser Richtlinie wird der maximale von Kerberos V5 tolerierte Zeitunterschied (in Minuten) zwischen der Uhrzeit auf dem Client und der Zeit des Domänencontrollers, auf dem die Kerberos-Authentifizierung unter Windows Server 2003 ausgeführt wird, bestimmt.

MAXIMALER ZEITRAUM, IN DEM EIN BENUTZERTICKET ERNEUERT WERDEN KANN

Die Richtlinie legt den maximalen Zeitraum (in Tagen) fest, in dem ein TGT erneuert werden kann.

Kerberos-Protokoll

Microsoft verwendet Kerberos als Standard-Protokoll für die Authentifizierung bei Windows 2000/2003 basierten Netzwerken sowie für den Windows XP-Client.

Kerberos bietet eine sichere und einheitliche Authentisierung in einem ungesicherten TCP/IP-Netzwerk. Die Authentifizierung übernimmt eine *vertrauenswürdige dritte Partei*. Diese dritte Partei ist ein besonders geschützter Kerberos 5-Netzwerkdienst bzw. das Kerberos V5-Schlüsselverteilungscenter (*Key Distribution Center, KDC*). Kerberos unterstützt *Single Sign On*, d. h., ein Benutzer muss sich nur noch einmal anmelden. Anschließend kann er alle Netzwerkdienste nutzen, ohne ein weiteres Mal ein Passwort eingeben zu müssen. Damit ein Netzwerkdienst Kerberos nutzen kann, ist es nötig, dass der Dienst in der Lage ist, mit Kerberos-Tickets umzugehen.

Bei Kerberos sind drei Parteien beteiligt: Der Client, der Server, den der Client nutzen will, und der Kerberos-Server. Der Kerberos-Dienst authentifiziert sowohl den Server gegenüber dem Client, als auch den Client gegenüber dem Server. Auch der Kerberos-Server selbst authentifiziert sich gegenüber dem Client und dem Server und verifiziert selbst deren Identität.

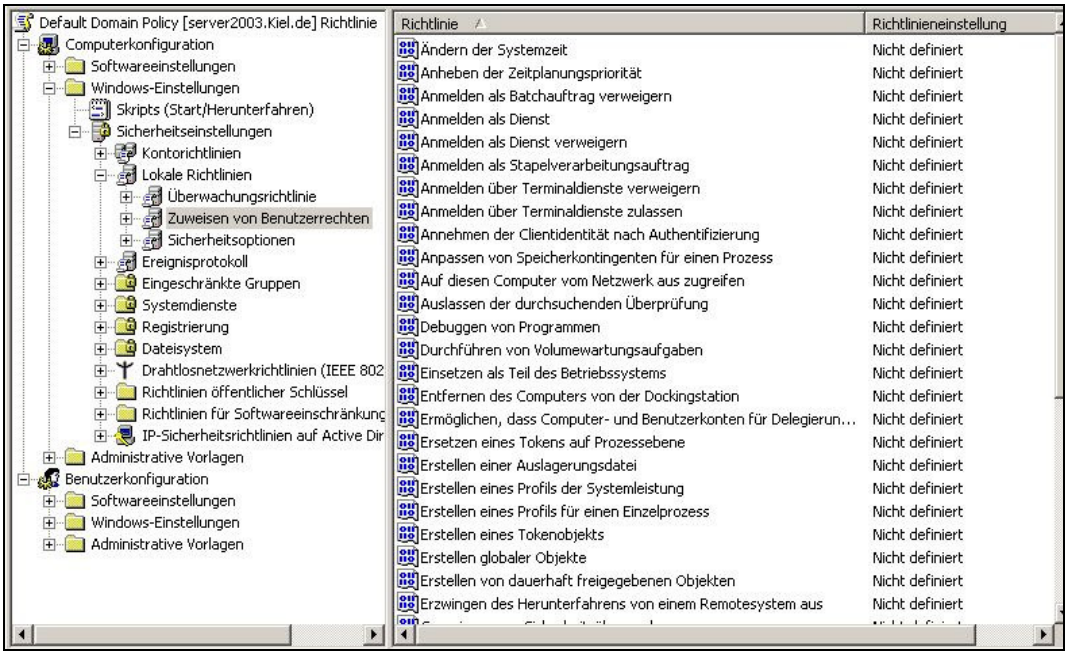
Kerberos verwendet sog. Tickets zur Authentifizierung. Um den Kerberos-Dienst nutzen zu können, muss sich ein Client zuerst beim Kerberos-Server anmelden. Er fordert vom Kerberos-Server ein sog. *Ticket Granting Ticket* (TGT) an. Hierzu muss der Benutzer entweder ein Passwort eingeben oder das TGT wird direkt bei der Benutzeranmeldung angefordert. Mit dem TGT ist der Client in der Lage, weitere Tickets für Dienste anzufordern, ohne noch mal ein Passwort eingeben zu müssen. Es wird ein Sitzungsschlüssel für die Kommunikation zwischen Client und Kerberos-Server ausgehandelt. Er wird benutzt, um den Datenverkehr zu verschlüsseln.

Um einen Dienst, der Kerberos unterstützt, benutzen zu können, fordert der Nutzer ein weiteres Ticket an. Dieses Ticket sendet der Client dann an den Dienst, der überprüft, ob er dem Client den Zugriff gestatten soll. Auch hierbei wird ein Sitzungsschlüssel vereinbart und die Identität von Client, Server und Kerberos-Server überprüft. Durch Kerberos werden insbesondere Angriffe durch Sniffing unterbunden.

Veränderungen der Standard-Einstellungen in den Kerberos-Richtlinien können dazu führen, dass die Authentifizierung zu einer Verzögerung führt oder sogar ganz fehlschlägt.

Lokale Richtlinien

Die LOKALEN RICHTLINIEN in dem Knoten COMPUTERKONFIGURATION\WINDOWS-EINSTELLUNGEN\SICHERHEITSEINSTELLUNGEN\LOKALE RICHTLINIEN sind untergliedert in ÜBERWACHUNGSRICHTLINIEN, ZUWEISEN VON BENUTZERRECHTEN und SICHERHEITSOPTIONEN. Die LOKALEN RICHTLINIEN sind nicht mit den Richtlinien für den lokalen Computer (*Lokale Gruppenrichtlinie*) zu verwechseln, die sich mit dem Programm *gpedit.msc* aufrufen lassen.



Container ZUWEISEN VON BENUTZERRECHTEN der Richtlinie LOKALE RICHTLINIE

In den LOKALEN RICHTLINIEN einer Gruppenrichtlinie können die Sicherheitseinstellungen für lokale Systeme und Systeme im Active Directory verwaltet werden. Standardmäßig werden beim Einrichten des Active Directory viele Richtlinien in den Lokalen Richtlinien voreingestellt, die ein gewisses Sicherheitsniveau gewährleisten sollen. Dabei sollte folgende Systematik beachtet werden:

- Auf einem Computer mit dem Betriebssystem Windows 2000 Professional / XP (Client) sind die Lokalen Richtlinien in der Lokalen Gruppenrichtlinie aktiviert.
- Auf einem Computer mit einem Serverbetriebssystem Windows Server 2000/2003 (Alleinstehender Server oder Mitgliedserver), der also nicht die Funktion eines Domänencontrollers übernimmt, sind die Lokalen Richtlinien ebenfalls in der Lokalen Gruppenrichtlinie aktiviert.
- Auf einem Domänencontroller korrespondieren die Lokalen Richtlinien in der Lokalen Gruppenrichtlinie mit der Default Domain Controllers Policy Gruppenrichtlinie. Für den Domänencontroller können daher die Lokalen Richtlinien in der Default Domain Controllers Policy administriert werden.

In der Lokalen Gruppenrichtlinie des Domänencontrollers finden Sie zwei unterschiedlich markierte Richtlinien:

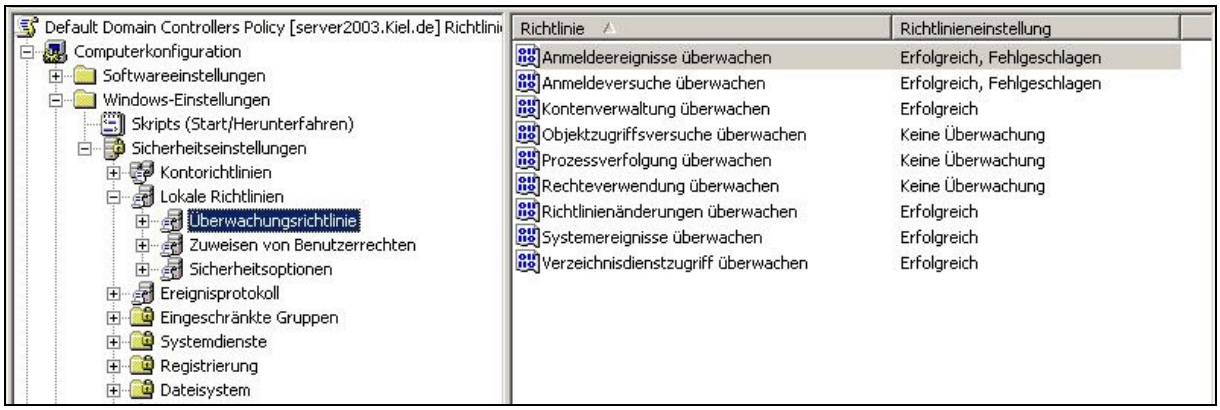
In den blau markierten Richtlinien können Sie Einstellungen vornehmen.

Die grau markierten Richtlinien können Sie in der Lokalen Gruppenrichtlinie nicht bearbeiten (die Dialogfelder und Schaltflächen sind deaktiviert). Sie geben den Hinweis darauf, dass Sie zur Bearbeitung der Richtlinien in die Default Domain Controllers Policy wechseln müssen.

Überwachungsrichtlinien

Mit den Überwachungsrichtlinien kann festgelegt werden, welche Systemereignisse überwacht werden sollen. Die überwachten Ereignisse werden dann in dem Verwaltungsprogramm *Ereignisanzeige* aufgelistet. Es lassen sich folgende Einstellungen vornehmen:

- Erfolgreich: Das Ereignis wird bei erfolgreicher Aktion protokolliert.
- Fehlgeschlagen: Das Ereignis wird nur protokolliert, wenn die Aktion fehlerhaft ist.
- Keine Überwachung: Es werden keine Protokolleinträge erzeugt.



ÜBERWACHUNGSRICHTLINIEN in der *Default Domain Controllers Policy*

Je nach aktivierter Überwachungsrichtlinie entstehen unterschiedliche Protokolleinträge in der Ereignisanzeige. Die Kategorie eines Protokolleintrags gibt den Hinweis darauf, welche Richtlinie welchen Protokolleintrag erstellt hat. Einen Überblick gibt die unten abgebildete Tabelle.

Überwachungsrichtlinie	**Kategorie in der Ereignisanzeige**
Anmeldeereignisse überwachen	Anmeldung/Abmeldung
Anmeldeversuche überwachen	Kontoanmeldung
Kontenverwaltung überwachen	Kontenverwaltung
Objektzugriffsversuche überwachen	Objektzugriff
Prozessverfolgung überwachen	Detaillierte Überwachung
Rechteverwendung überwachen	Berechtigungen
Richtlinienänderungen überwachen	Richtlinienänderungen
Systemereignisse überwachen	Systemereignis
Verzeichnisdienstzugriff überwachen	Verzeichnisdienstzugriff

Eine Übersicht und Beschreibung der Protokolleinträge mit den entsprechenden Ereigniskennungen finden Sie im Anhang. Vor der Aktivierung einer Überwachungsrichtlinie sollten Sie sich über den Umfang der Protokolleinträge anhand der im Anhang aufgeführten Übersicht informieren.

Folgendes ist bei der Überwachung von Systemaktivitäten zu beachten:

1. *Die Überwachungsrichtlinien bieten nur begrenzte Möglichkeiten, die Systemaktivitäten zu protokollieren. Berücksichtigen Sie deshalb, welche Sicherheitsaspekte Sie mit der Überwachung verfolgen möchten.*
2. *Achten Sie auf die Systemressourcen. Durch eine umfangreiche Überwachung, z. B. des gesamten Dateisystems, kann leicht eine Überlastung des Servers herbeigeführt werden.*
3. *Vor Aktivierung der Protokollierung von Systemaktivitäten sollten Sie festgelegen, welchem Zweck die Protokollierung dient und welche Zielgruppe (Anwender und/oder Administratoren) erfasst werden soll.*
4. *Eine Protokollierung von Systemaktivitäten macht nur dann Sinn, wenn organisatorisch festgelegt ist, wer die Protokolle auswertet.*

ANMELDEEREIGNISSE UND ANMELDEVERSUCHE ÜBERWACHEN

Beide Richtlinien protokollieren die erfolgreiche und/oder fehlerhafte Authentifizierung eines System- oder Benutzerkontos. Die Protokolleinträge unterscheiden sich dabei bezüglich der im Hintergrund ablaufenden Systemaktivitäten. Standardmäßig werden erfolgreiche und fehlgeschlagene Anmeldeereignisse und -versuche protokolliert (Windows 2003).

KONTENVERWALTUNG ÜBERWACHEN

Die Richtlinie überwacht die Administration der Benutzer- und Gruppenkonten. Im Protokoll ist erkennbar, mit welchem Benutzerkonto Veränderungen an Benutzer- und Gruppenkonten durchgeführt wurden. Standardmäßig wird die erfolgreiche Kontenverwaltung protokolliert (Windows 2003).

OBJEKTZUGRIFFSVERSUCHE ÜBERWACHEN

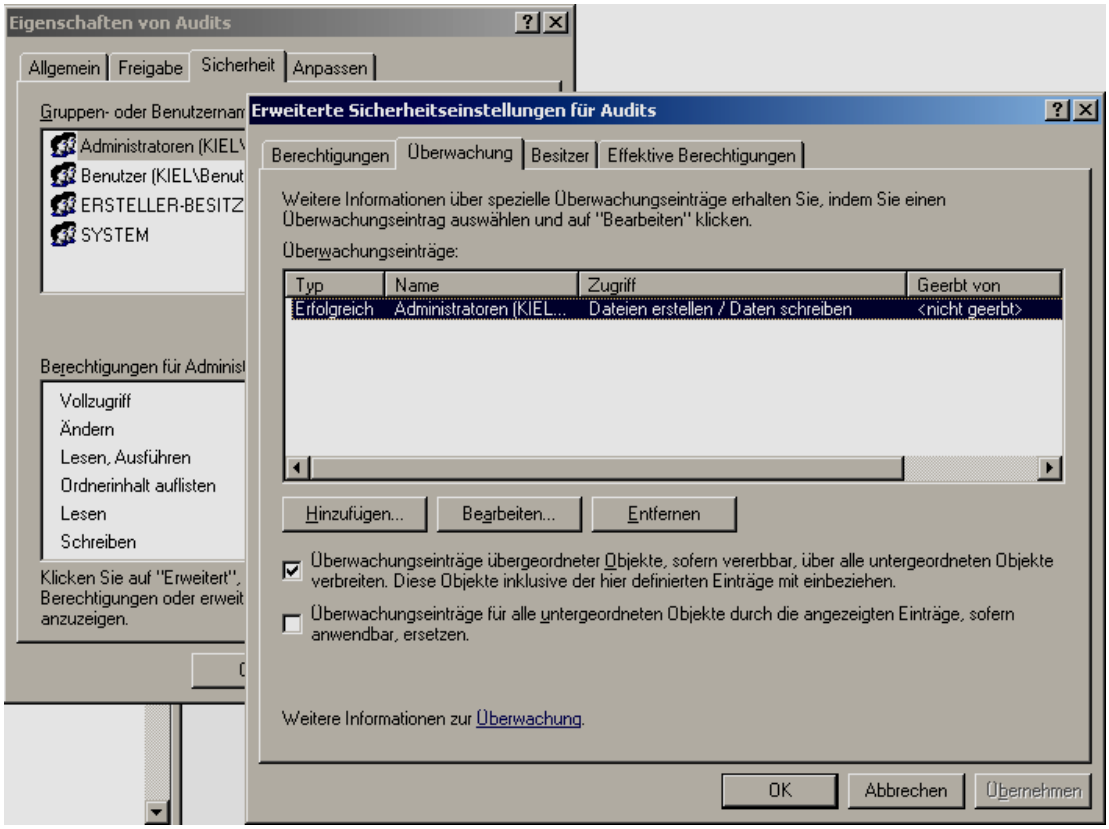
Mit dieser Richtlinie können Zugriffe von Benutzerkonten auf Drucker, Ordner und Dateien protokolliert werden. Bei Aktivierung dieser Richtlinie muss zusätzlich die Überwachung des entsprechenden Objektes aktiviert werden.

Die Protokollierung der Objektzugriffsversuche orientiert sich an den NTFS-Berechtigungen des zu überwachenden Objektes. So kann beispielsweise ein ändernder Zugriff der Gruppe ADMINISTRATOREN auf das Verzeichnis AUDITS protokolliert werden (siehe folgende Abbildung). Dazu muss sowohl die Überwachung (Erfolgreich) der entsprechenden Berechtigungen (z. B. Dateien erstellen/Daten schreiben) in den erweiterten Eigenschaften des Verzeichnisses als auch die Richtlinie OBJEKTZUGRIFFSVERSUCHE ÜBERWACHEN

(Erfolgreich) aktiviert werden. Danach werden alle erfolgreichen Zugriffe der überwachten NTFS-Berechtigungen des entsprechenden Objektes in dem Sicherheitsprotokoll der Ereignisanzeige protokolliert.

Fehlerhafte Zugriffe werden dann protokolliert, wenn die fehlgeschlagene Protokollierung in den erweiterten Eigenschaften des Objektes und der entsprechenden Gruppenrichtlinie aktiviert wurde und ein entsprechendes Benutzerkonto in dem Objekt (z. B. einem Verzeichnis) Aktionen durchführen möchte, für die er nicht die entsprechenden NTFS-Berechtigungen besitzt.

Standardmäßig werden keine Objektzugriffsversuche protokolliert (Windows 2003).



Erweiterte Sicherheitseinstellungen des Ordners AUDITS

PROZESSVERFOLGUNG ÜBERWACHEN

Bei Aktivierung dieser Richtlinie werden Systemprozesse ausführlich protokolliert. Bei der Aktivierung dieser Richtlinie entsteht eine Vielzahl von Protokolleinträgen, sodass sich das Sicherheitsprotokoll sehr schnell füllt. Daher sollte diese Richtlinie nur bei einer Systemfehlersuche angewendet und danach wieder deaktiviert werden. Standardmäßig wird keine Prozessverfolgung protokolliert (Windows 2003).

RECHTEVERWENDUNG ÜBERWACHEN

Wird diese Richtlinie aktiviert, protokolliert sie jede Aktivität, bei dem ein privilegiertes Benutzerrecht benötigt und eingesetzt wurde. In den Protokolleinträgen lässt sich allerdings nicht nachvollziehen, um welche Benutzerrechte es sich handelt. Standardmäßig wird keine Rechteverwendung protokolliert (Windows 2003).

RICHTLINIENÄNDERUNGEN ÜBERWACHEN

Mit Hilfe dieser Richtlinie können Änderungen an einigen Sicherheitsrichtlinien protokolliert werden. Dazu zählen u.a. Änderungen an den Überwachungsrichtlinien und Benutzerrechten. Standardmäßig werden die erfolgreichen Richtlinienänderungen protokolliert (Windows 2003).

SYSTEMEREIGNISSE ÜBERWACHEN

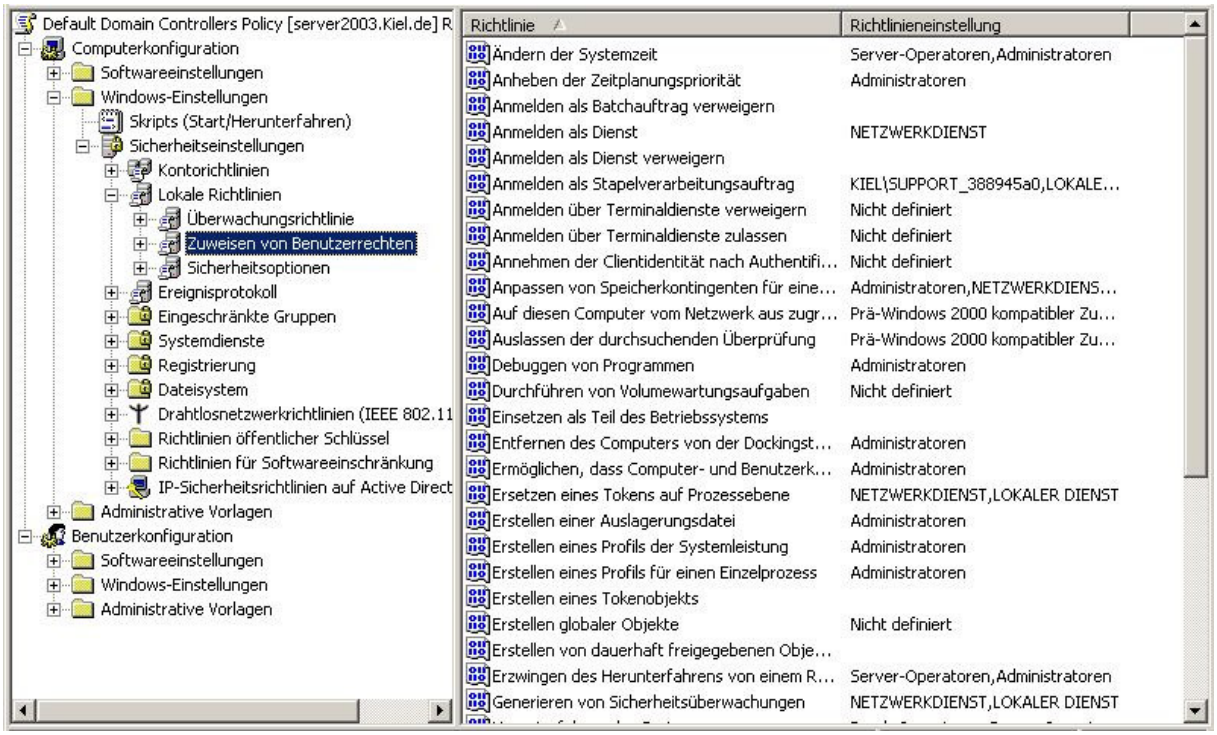
Mit der Aktivierung dieser Richtlinie können Systemereignisse, wie z. B. das Starten oder Herunterfahren des Computers oder das Auftreten eines Ereignisses, das sich entweder auf die Systemsicherheit oder auf das Sicherheitsprotokoll auswirkt, überwacht werden. Standardmäßig werden die erfolgreichen Systemereignisse protokolliert (Windows 2003).

VERZEICHNISDIENSTZUGRIFF ÜBERWACHEN

Bei Aktivierung dieser Richtlinie werden administrative Aktivitäten im Active Directory protokolliert. Ähnlich wie bei der Richtlinie OBJEKTZUGRIFFSVERSUCHE ÜBERWACHEN, muss im Active Directory für das entsprechende Objekt in den erweiterten Objekteigenschaften und auf der Registerkarte ÜBERWACHUNG zusätzlich festgelegt werden, welche Ereignisse überwacht werden sollen. Standardmäßig sind hier bereits bei der Installation des Domänencontrollers einige Überwachungseinstellungen eingerichtet worden, die jedoch erst dann Protokolleinträge erzeugen, wenn die Richtlinie VERZEICHNISDIENSTZUGRIFF ÜBERWACHEN aktiviert wird. Standardmäßig wird der erfolgreiche Verzeichnisdienstzugriff protokolliert (Windows 2003).

Die Überwachungsrichtlinien sind unter Windows 2003 noch unzureichend. Es lassen sich nur einige wenige Systemaktivitäten protokollieren. Hinzu kommt, dass die erzeugten Protokolle nicht immer hinreichend aussagekräftig sind.

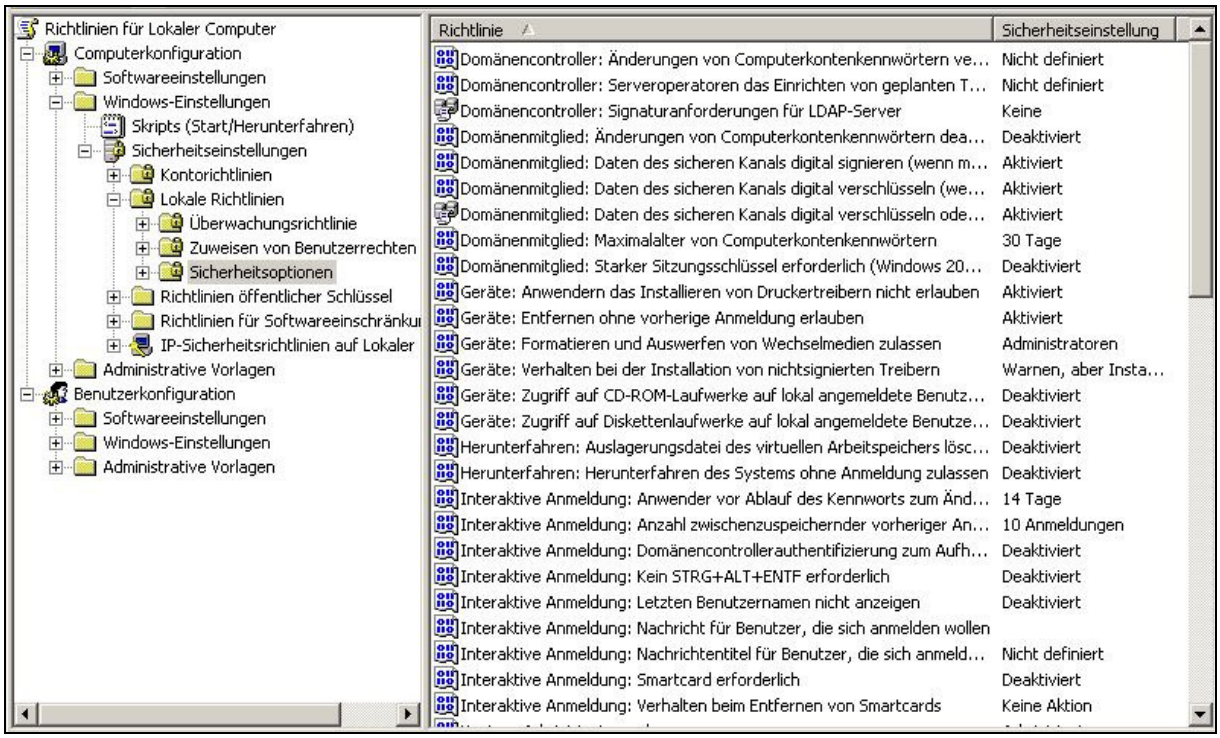
Zuweisen von Benutzerrechten



ZUWEISEN VON BENUTZERRECHTEN in der *Default Domain Controllers Policy*

In dem Knoten ZUWEISEN VON BENUTZERRECHTEN befinden sich Richtlinien, die Benutzer- und Gruppenkonten bestimmte Systemaufgaben zuweisen. So kann beispielsweise festgelegt werden, ob ein Benutzer- oder Gruppenkonto Gerätetreiber installieren oder die Systemzeit ändern darf. Für die Administration des Betriebssystems ist es notwendig, dass die Gruppe Administratoren über umfassende Systemrechte verfügt, um alle Systemaufgaben durchführen zu können. Mit der Installation des Betriebssystems werden bereits die meisten Richtlinien in der *Default Domain Controllers Policy* aktiviert, sodass die Gruppe ADMINISTRATOREN über umfangreiche Systemrechte verfügt. Änderungen dieser Richtlinien sind nur dann erforderlich, wenn administrative Aufgaben delegiert werden sollen.

Sicherheitsoptionen



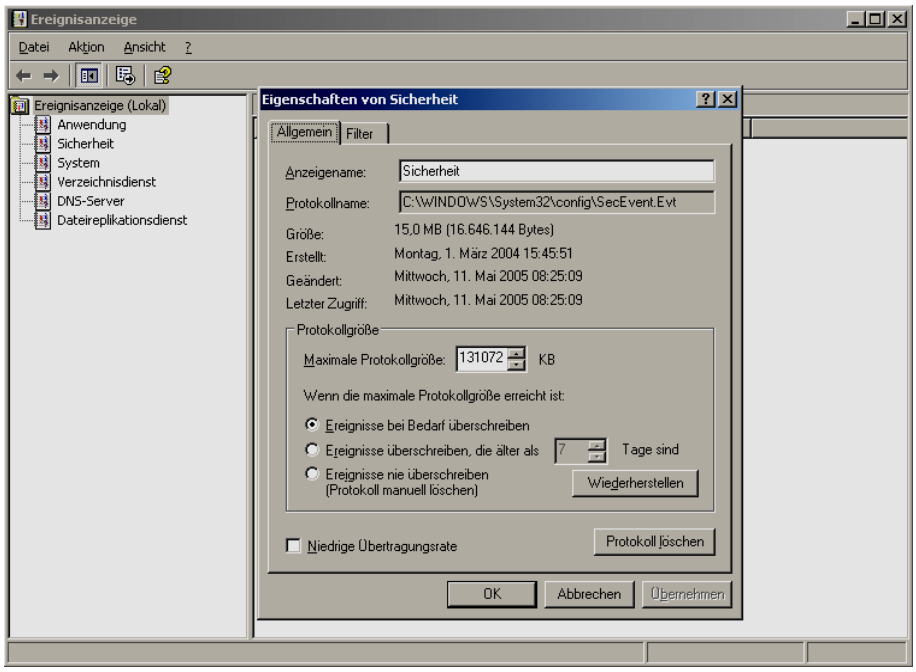
SICHERHEITSOPTIONEN in der *Lokalen Gruppenrichtlinie* (Richtlinie für lokaler Computer)

Die SICHERHEITSOPTIONEN enthalten Einstellungen, die benutzerkontenunabhängig die Netzwerkkommunikation des Computers reglementieren. Es handelt sich hier um Sicherheitsgrundeinstellungen, die unmittelbar mit der Installation des Betriebssystems durchgeführt werden. Die meisten Richtlinien sind deshalb in der *Lokalen Gruppenrichtlinie* aktiviert. Mit der Einrichtung eines Domänencontrollers werden in der Gruppenrichtlinie *Default Domain Controllers Policy* ergänzende Sicherheitseinstellungen durchgeführt. Die Richtlinien wirken kumulativ.

Ereignisprotokoll

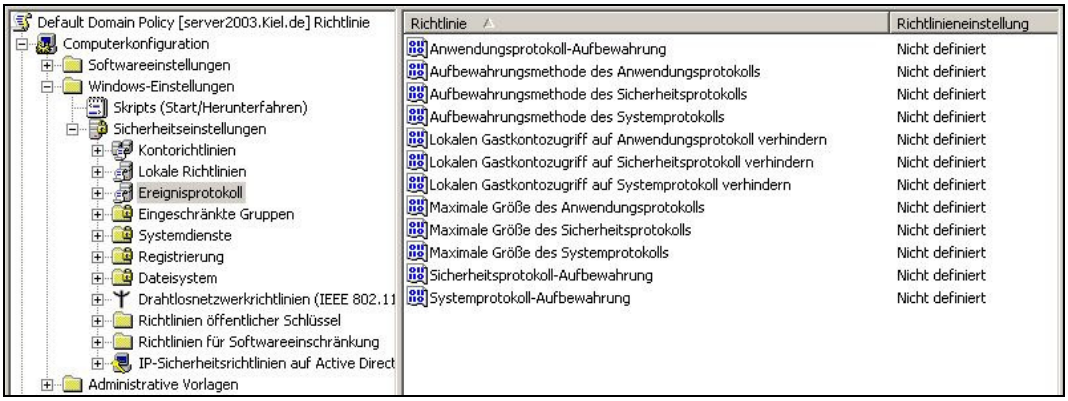
Mit dem Verwaltungsprogramm *Ereignisanzeige* lassen sich für den jeweiligen Computer Grundeinstellungen für die Behandlung der einzelnen Protokolle durchführen. Auf dem Client werden standardmäßig die Protokolle ANWENDUNG, SICHERHEIT und SYSTEM verwaltet, während auf einem Domänencontroller zusätzlich die Protokolle VERZEICHNISDIENST, DNS-SERVER und DATEIREPLIKATIONSDIENST hinzukommen.

In den Eigenschaften jedes einzelnen Protokolls lassen sich Einstellungen zur maximalen Protokollgröße sowie zur Aufbewahrungsmethode vornehmen (siehe folgende Abbildung).



Verwaltungsprogramm *Ereignisanzeige*, Eigenschaften des Sicherheitsprotokolls

Der Knoten EREIGNISPROTOKOLL enthält einige Richtlinien zur zentralen Konfiguration der Protokolle für die in der Domäne integrierten Computer. Diese Richtlinien ermöglichen es, die Kapazität und die Aufbewahrungsmethode der Protokolle ANWENDUNG, SICHERHEIT und SYSTEM festzulegen. Die Richtlinien sollten in der Gruppenrichtlinie *Default Domain Policy* aktiviert werden, wenn die Einstellungen für alle in der Domäne integrierten Computer gelten sollen. Sollen die Einstellungen nur für bestimmte Computer gelten, z. B. für alle Fileserver, kann für diese Computer eine eigene Gruppenrichtlinie mit den entsprechenden Einstellungen erstellt werden und sie mit der Verwaltungseinheit verknüpft werden, in der die Fileserver im Active Directory gespeichert sind. Die Einstellungen gelten dann für alle Computerkonten in der entsprechenden Verwaltungseinheit.



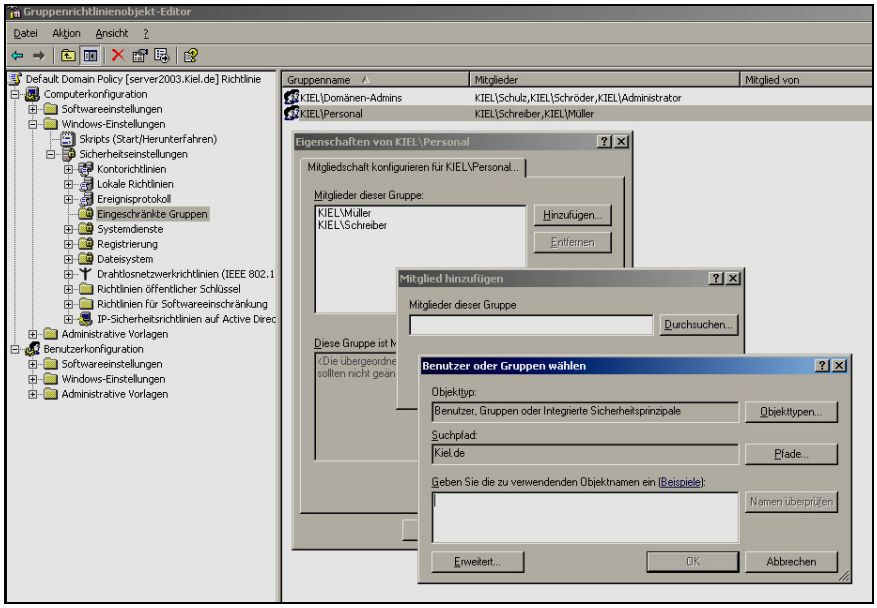
Richtlinien Container Ereignisprotokoll

Eingeschränkte Gruppen

Die Richtlinie EINGESCHRÄNKTE GRUPPEN ermöglicht es, die einem Gruppenkonto zugewiesenen Benutzer- und Gruppenkonten und die Mitgliedschaft in anderen Gruppen zu erzwingen.

Mit dieser Richtlinie kann beispielsweise ein Gruppenkonto aus dem Active Directory ausgewählt und die Mitglieder für diese Gruppe sowie die Mitgliedschaft in anderen Gruppen verbindlich festgelegt werden. Damit wird gewährleistet, dass keine Veränderungen der Mitgliedschaften in diesem Gruppenkonto über das Verwaltungsprogramm *Active Directory-Benutzer und -Computer* vorgenommen werden können.

Wird eine eingeschränkte Gruppe definiert, so werden alle Benutzer- und Gruppenkonten, die nicht im Feld *Mitglieder dieser Gruppe* aufgeführt sind, aus dem Gruppenkonto entfernt und alle aufgeführten Benutzer- und Gruppenkonten, die momentan kein Mitglied des Gruppenkontos sind, hinzugefügt.



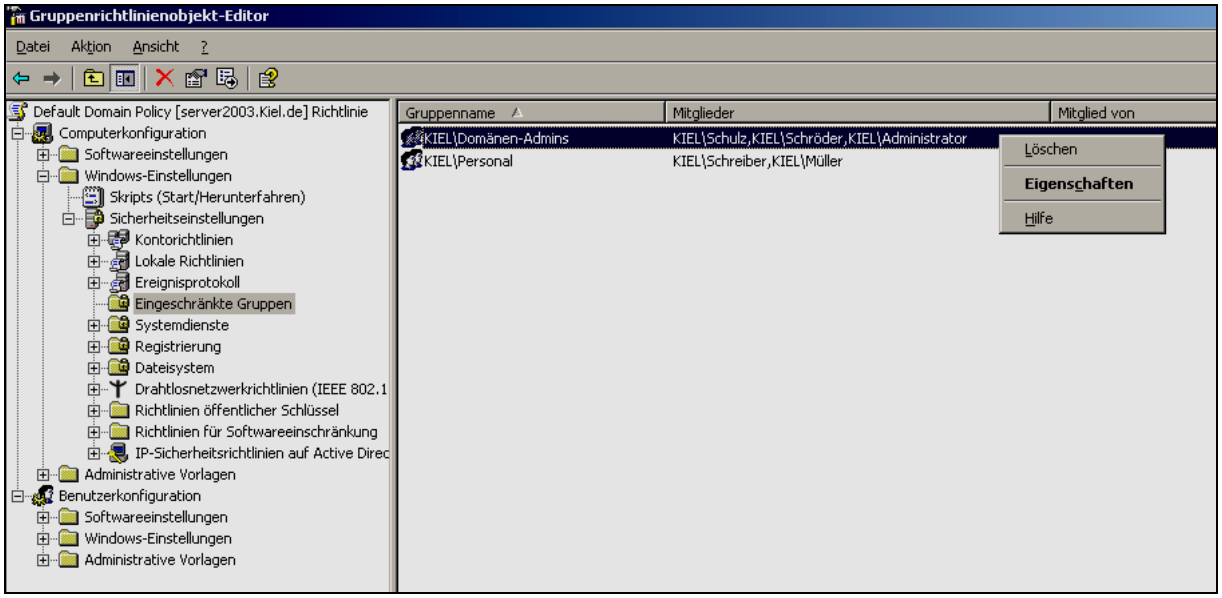
Mitglieder eines Gruppenkontos über die Richtlinie Eingeschränkte Gruppen erzwingen

Der Einsatz dieser Richtlinie ist sinnvoll für die standardmäßig eingerichteten administrativen Gruppenkonten (*Administratoren, Domänen-Admins, Organisations-Admins*) oder für erstellte Gruppenkonten in Organisationseinheiten, die besonders schützenswert sind.

Zur Steuerung der Mitgliedschaften von Active Directory-Gruppenkonten muss die Richtlinie in einem Gruppenrichtlinienobjekt auf Domänenebene, wie z.B. der Default Domain Policy, durchgeführt werden.

Mitgliedschaft für das Gruppenkonto DOMÄNEN-ADMINS erzwingen!

1. *Rufen Sie die Gruppenrichtlinie Default Domain Policy auf.*
2. *Navigieren Sie zu dem Knoten COMPUTERKONFIGURATION\WINDOWS-EINSTELLUNGEN\SICHERHEITSEINSTELLUNGEN\EINGESCHRÄNKTE GRUPPE und rufen Sie mit der rechten Maustaste das Kontextmenü auf.*
3. *Wählen Sie den Menüpunkt GRUPPE HINZUFÜGEN.*
4. *Mit der Schaltfläche DURCHSUCHEN können Sie sich die im Active Directory verwalteten Gruppen anzeigen lassen und das Gruppenkonto DOMÄNEN-ADMINS auswählen.*
5. *Es öffnet sich ein Dialogfenster. Weisen Sie der Gruppe DOMÄNEN-ADMINS mit der Schaltfläche HINZUFÜGEN administrative Benutzerkonten zu.*
6. *Sobald Sie den Vorgang über die Schaltfläche OK abschließen, wird die Gruppe DOMÄNEN-ADMINS mit den entsprechenden Mitgliedern im Gruppenrichtlinienobjekt-Editor im Inhaltsfenster der Gruppenrichtlinien-Verwaltungskonsole angezeigt. Sie können sie dann mit der Option EIGENSCHAFTEN (Kontextmenü) verwalten.*
7. *Aktualisieren Sie die Gruppenrichtlinie mit dem Befehl gpupdate.*



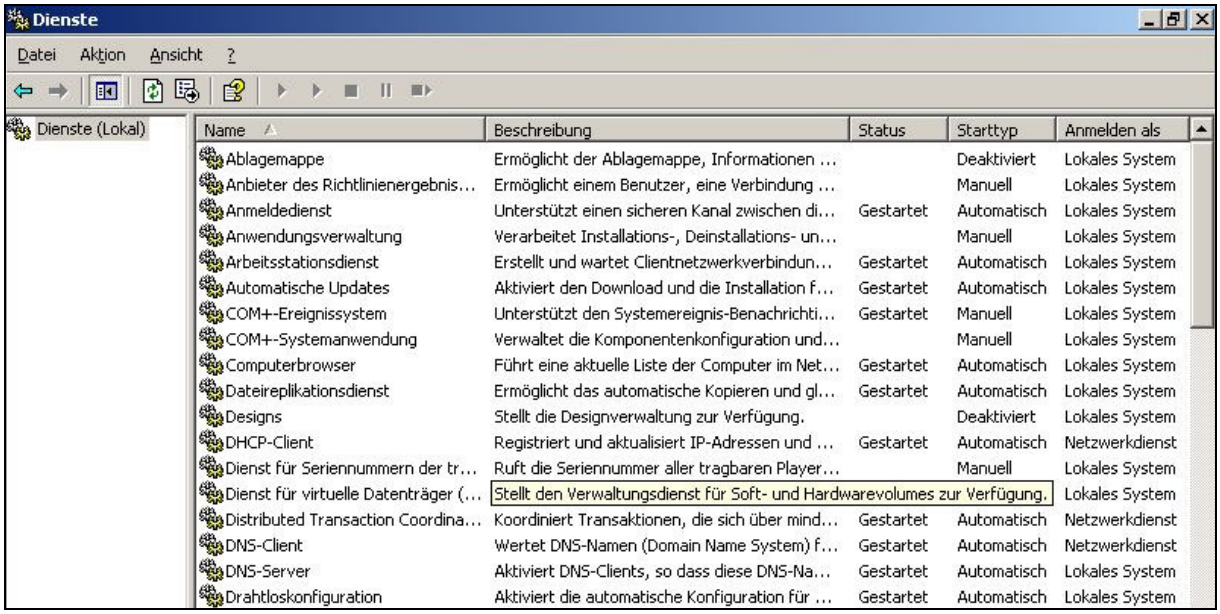
Richtlinie EINGESCHRÄNKTE GRUPPEN

Eine fehlerhafte Zuordnung von Benutzerkonten kann dazu führen, dass Benutzer aufgrund falscher Gruppenzuweisung falsche Berechtigungen erhalten.

Eine Einschränkung der standardmäßig eingerichteten Gruppenkonten, wie z. B. die Gruppen DOMÄNEN-BENUTZER, DOMÄNEN-ADMINS und ORGANISATIONS-ADMINS, sollte mit Vorsicht durchgeführt werden. Wird das Feld MITGLIEDER DIESER GRUPPE oder das Feld DIESE GRUPPE IST MITGLIED VON nicht ausgefüllt, werden alle Benutzerkonten und die Mitgliedschaft des entsprechenden Gruppenkontos entfernt. Hierunter fallen auch die administrativen Benutzer- und Gruppenkonten.

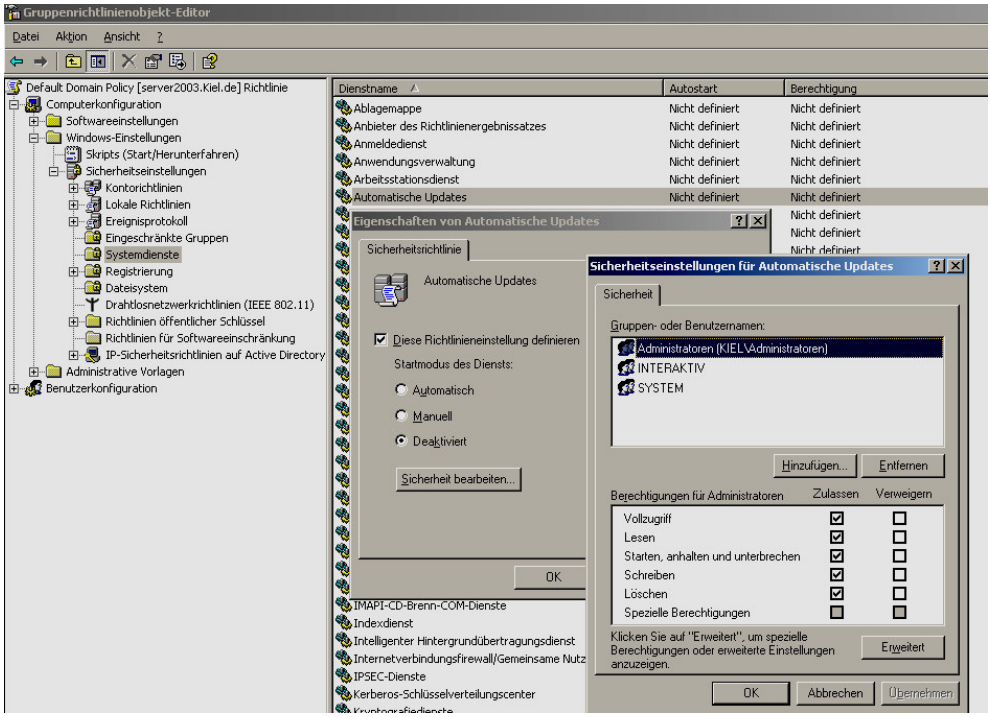
Systemdienste

Die vom Betriebssystem unterstützten Dienste können mit dem Verwaltungsprogramm *Dienste* verwaltet werden.



Verwaltungsprogramm *Dienste*

Die Richtlinie SYSTEMDIENSTE der SICHERHEITSEINSTELLUNGEN einer Active Directory-Gruppenrichtlinie bietet die Möglichkeit, die Dienste für die in der Domäne integrierten Computer zentral zu steuern. Es werden analog zum Verwaltungsprogramm *Dienste* die einzelnen Systemdienste mit dem Status *Nicht definiert* aufgeführt. Über die Gruppenrichtlinie lassen sich sowohl die Zugriffsberechtigungen als auch der Startmodus eines Dienstes zentral verwalten.



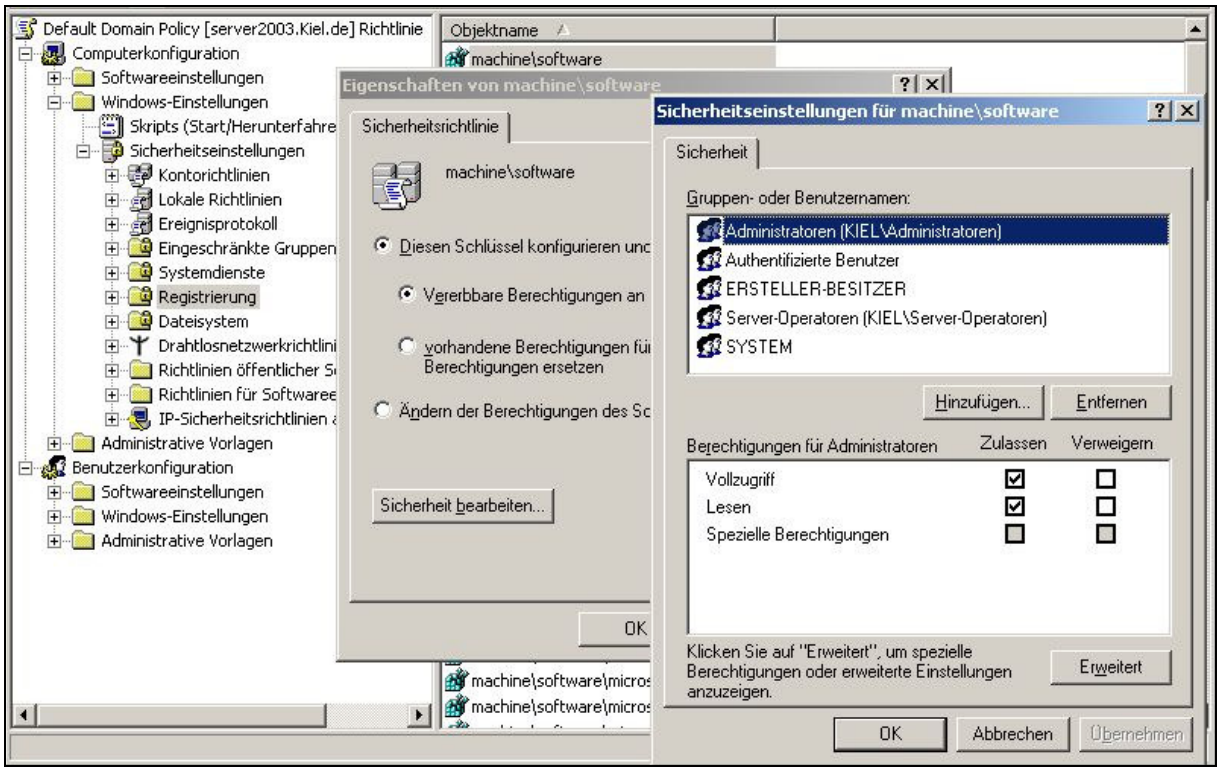
SYSTEMDIENSTE in der Gruppenrichtlinie *Default Domain Policy*

Registrierung

Die Richtlinie REGISTRIERUNG der SICHERHEITSEINSTELLUNGEN einer Active Directory-Gruppenrichtlinie erlaubt die zentrale Verwaltung der Registrierungseinträge in Bezug auf die Zugriffsberechtigungen und den Überwachungseinstellungen für die in der Domäne integrierten Computer. Es können jedoch keine Einträge hinzugefügt, verändert oder gelöscht werden.

Werden Zugriffsberechtigungen für einen Registrierungseintrag festgelegt, wird er als Objekt im Inhaltsfenster der Gruppenrichtlinien-Verwaltungskonsole aufgeführt. Anschließend können über das Kontextmenü die Eigenschaften des Objektes aufgerufen werden, um Veränderungen an den Einstellungen durchzuführen.

Sie sollten unter dem Container Registrierung nur dann Richtlinien erstellen, wenn Sie über ausreichende Kenntnisse über die Zusammenhänge der Registry verfügen. Eine fehlerhafte Administration kann zu erheblichen Betriebssystemstörungen auf den der Richtlinie zugewiesenen Computern führen.



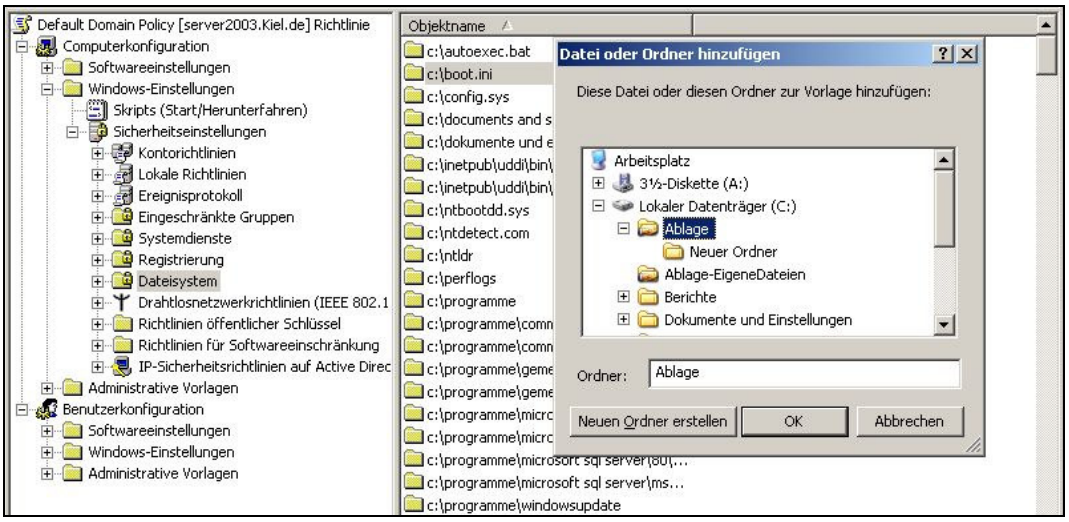
Zugriffsberechtigungen für einen Registrierungseintrag festlegen

Dateisystem

Die Richtlinie DATEISYSTEM der SICHERHEITSEINSTELLUNGEN einer Active Directory-Gruppenrichtlinie bietet analog zu der Konfiguration der Berechtigung auf die Registrierungsschlüssel die Möglichkeit, zentral für Dateien, Verzeichnisse und Laufwerke Zugriffsberechtigungen und Überwachungseinstellungen für alle in der Domäne integrierten Computer festzulegen.

So können z. B. einer Benutzergruppe für ein Verzeichnis, das auf mehreren Computern innerhalb der Domäne vorhanden ist (mit dem gleichen Namen und Pfad), zentral Zugriffsberechtigungen zugewiesen werden. Dazu wird eine neue Gruppenrichtlinie eingerichtet, in der Richtlinie DATEISYSTEM der SICHERHEITSEINSTELLUNGEN das entsprechende Verzeichnis hinzugefügt, die Berechtigungen vergeben und die Gruppenrichtlinie der entsprechenden Verwaltungseinheit mit den dazugehörigen Computerkonten zugewiesen.

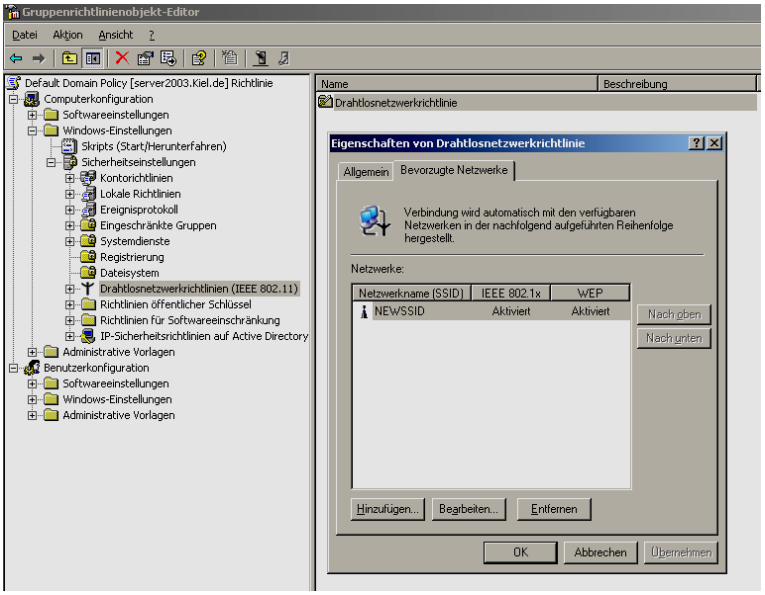
Eine weitere Einsatzmöglichkeit dieser Richtlinie liegt beispielsweise darin, verbindlich Zugriffsberechtigungen für eine auf einem Server genutzte Datenablage vorzugeben (siehe auch Abbildung unten).



Zugriffsberechtigungen für einen Ordner festlegen

Drahtlosnetzwerkrichtlinien (IEEE 802.11)

Mit den DRAHTLOSNETZWERKRICHTLINIEN der SICHERHEITSEINSTELLUNGEN können zentral Konfigurationseinstellungen für die Verwendung von Wireless LAN-Netzwerkkarten auf Windows XP- und Windows Server 2003-Computer zugewiesen werden. Dadurch wird eine einheitliche Konfiguration, insbesondere in Bezug auf die Sicherheitseinstellungen, gewährleistet.



Zentrale Konfiguration eines drahtlosen Netzwerkes

In dem Container kann nur eine Richtlinie für eine zentrale Konfiguration des drahtlosen Netzwerkes für Netzwerkkarten erstellt werden, die den IEEE 802.11-Standard erfüllt. Sie hat Vorrang vor lokalen Einstellungen. Auf Computern, die nicht über derartige Netzwerkkarten verfügen, findet die Richtlinie keine Anwendung.

Sicherheitsinformationen zu drahtlosen Netzwerken

Drahtlose Netzwerktechnologien bieten Benutzerfreundlichkeit und Mobilität. Sie stellen jedoch auch ein Sicherheitsrisiko im Netzwerk dar. Wenn keine Mechanismen für die Authentifizierung und Autorisierung implementiert sind, kann jeder Benutzer, der über einen kompatiblen drahtlosen Netzwerkadapter verfügt, auf das Netzwerk zugreifen. Ohne Verschlüsselung werden die drahtlosen Daten als Text gesendet, sodass jeder Benutzer, der sich in entsprechender Entfernung zum drahtlosen Zugriffspunkt befindet, sämtliche Daten ermitteln und empfangen kann, die zu und von einem drahtlosen Zugriffspunkt gesendet werden.

Mit Hilfe der folgenden Sicherheitsmechanismen wird die Sicherheit in drahtlosen Netzwerken erhöht:

802.11-Identitätsüberprüfung und -Authentifizierung

802.11 WEP-Verschlüsselung (Wired Equivalent Privacy)

802.1X-Authentifizierung

IAS-Unterstützung für 802.1X-Authentifizierung

802.11-Identitätsüberprüfung und -Authentifizierung

IEEE 802.11 (Institute of Electrical and Electronics Engineers) definiert für die Identitätsüberprüfung und Authentifizierung die Untertypen Open System- und Shared Key-Authentifizierung:

Die Open System-Authentifizierung stellt keine eigentliche Authentifizierung bereit, sie führt lediglich eine Identitätsüberprüfung durch den Austausch von Meldungen zwischen dem Initiator (einem drahtlosen Client) und dem Empfänger (einem drahtlosen Zugriffspunkt) aus.

Die Shared Key-Authentifizierung stellt eine Authentifizierung bereit, da überprüft wird, ob der Initiator einen gemeinsamen geheimen Schlüssel kennt. Beim 802.11-Standard wird vorausgesetzt, dass der gemeinsame geheime Schlüssel über einen sicheren, von 802.11 unabhängigen Kanal an den drahtlosen Zugriffspunkt gesendet wird.

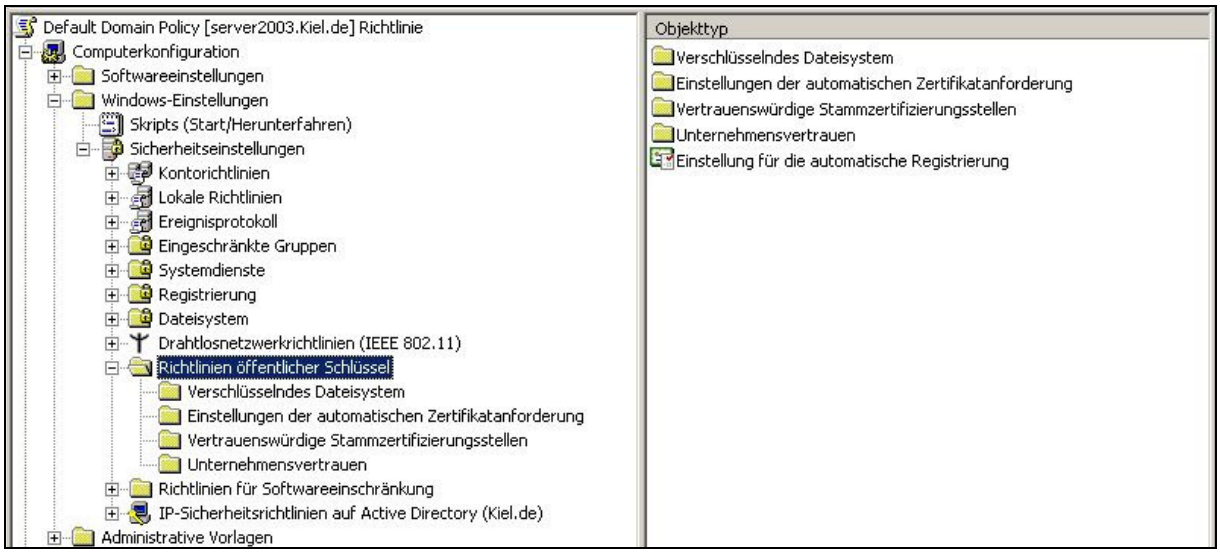
Zur Erhöhung der Sicherheit steht im Windows XP Service Pack 1 und in der Windows Server 2003-Produktfamilie die 802.1X-Authentifizierung nur für das interne Netzwerk zur Verfügung, die die Verwendung eines Netzwerkschlüssels erfordern.

Es wird dringend empfohlen, die 802.1X-Authentifizierung bei jeder Verbindung zu einem drahtlosen 802.11-Netzwerk zu verwenden.

Weitere Informationen zur Einrichtung eines drahtlosen 802.11-Netzwerks stehen in der Microsofthilfe zur Verfügung.

Richtlinien öffentlicher Schlüssel

In dem Knoten RICHTLINIEN ÖFFENTLICHER SCHLÜSSEL der SICHERHEITSEINSTELLUNGEN können Zertifikate auf Computer verteilt, Zertifikatsvertrauenslisten und allgemein vertrauenswürdige Zertifizierungsstellen eingerichtet und außerdem Wiederherstellungsrichtlinien für EFS (Encrypting File System) verwaltet werden. Der Einsatz einiger dieser Richtlinien erfordert eine Public Key Infrastructure (PKI) bzw. eine Zertifizierungsstelle (CA) für die Verwaltung der Zertifikate.



Richtlinien öffentlicher Schlüssel

VERSCHLÜSSELTES DATEISYSTEM

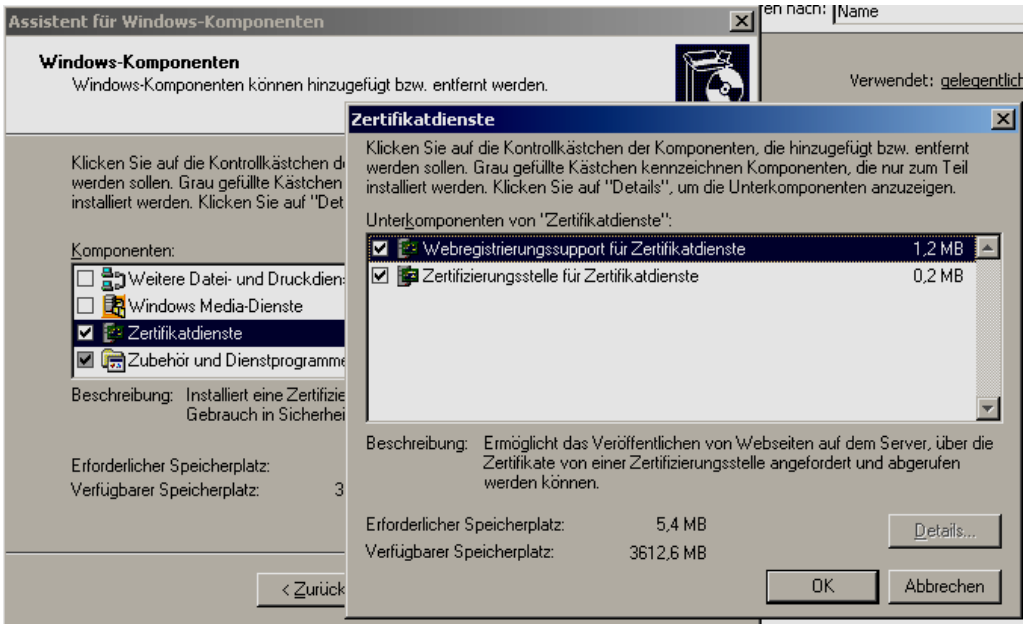
In diesem Container kann ein Zertifikat für einen Wiederherstellungsagenten zur Wiederherstellung verschlüsselter Daten und zum Ändern der Richtlinieneinstellungen für die Wiederherstellung verschlüsselter Daten eingerichtet werden. Ein Wiederherstellungsagent hat die Möglichkeit, die von einem Benutzer mittels EFS verschlüsselten Ordner und Dateien zu entschlüsseln. Das Benutzerkonto ADMINISTRATOR verfügt bei einer Standardinstallation über das entsprechende Zertifikat[7].

EINSTELLUNGEN DER AUTOMATISCHEN ZERTIFIKATANFORDERUNG

Computer können automatisch eine Zertifikatsanforderung an eine Zertifizierungsstelle über-

[7] backUP-Magazin Nr. 5, Tz. 8.6 Verschlüsselung von Ordnern und Dateien

mitteln und das ausgestellte Zertifikat installieren. Das gewährleistet, dass Computer über die Zertifikate verfügen, die in der Organisation zum Verschlüsseln mit öffentlichen Schlüsseln benötigt werden. Einsatzgebiete für diese Option sind z. B. IP-Sicherheit oder Clientauthentifizierung.



Windows-Komponenten Zertifizierungsdienste

Die Installation einer Zertifizierungsstelle zum Ausstellen und Verwalten digitaler Zertifikate kann über die Systemsteuerung und dem Verwaltungsprogramm SOFTWARE *mit der Funktion* WINDOWSKOMPONENTEN HINZUFÜGEN *durchgeführt werden.*

VERTRAUENSWÜRDIGE STAMMZERTIFIZIERUNGSSTELLEN

Diese Richtlinieneinstellung wird eingesetzt, wenn zusätzlich zu den Stellen, denen einzelne Computer bzw. Benutzer bereits vertrauen, gemeinsame Stammzertifizierungsstellen für Computer und/oder Benutzer eingerichtet werden sollen. Für Zertifizierungsstellen in einer Windowsdomäne wird diese Einstellung nicht benötigt, da alle Computer und Benutzer in der Domäne dieser vertrauen. Diese Richtlinie ist notwendig, um Vertrauensstellungen zu Stammzertifizierungsstellen außerhalb der Organisation einzurichten.

UNTERNEHMENSVERTRAUEN

In diesem Container kann eine Zertifikatsvertrauensliste erstellt werden. Dabei handelt es sich

um eine signierte Liste mit Zertifikaten einer Stammzertifizierungsstelle, die die Organisation für bestimmte Zwecke, z. B. für die Clientauthentifizierung oder für sichere E-Mail, als glaubwürdig ansieht.

Public Key Infrastruktur (PKI)

Public Key Infrastrukturen (PKI) bestehen aus Protokollen, Diensten und Standards, die verschiedene Applikationen für die Public Key Verschlüsselung unterstützen. In einer PKI wird jedem Benutzer ein kryptographisches Schlüsselpaar zugewiesen, das sich aus einem Public Key (Öffentlicher Schlüssel) und einem Private Key (Privater Schlüssel) zusammensetzt. Die beiden Schlüssel stehen in einem mathematischen Verhältnis zueinander. Der Public Key wird veröffentlicht, der Private Key wird geheim gehalten.

Digitale Signaturen

Eine Digitale Signatur wird mit dem Private Key einer Person erstellt, um die Gültigkeit seiner Anfrage sicherzustellen. Diese Technologie kann verwendet werden, um Nachweisbarkeit bei verschiedenen Transaktionen zu garantieren.

Digitale Zertifikate

Digitale Zertifikate bestehen aus Inhalten, die eine Zusammengehörigkeit eines Public Key mit einer Benutzerkennung beglaubigen und verhindern, dass jemand einen falschen Public Key zur Personenidentifizierung nutzen kann.

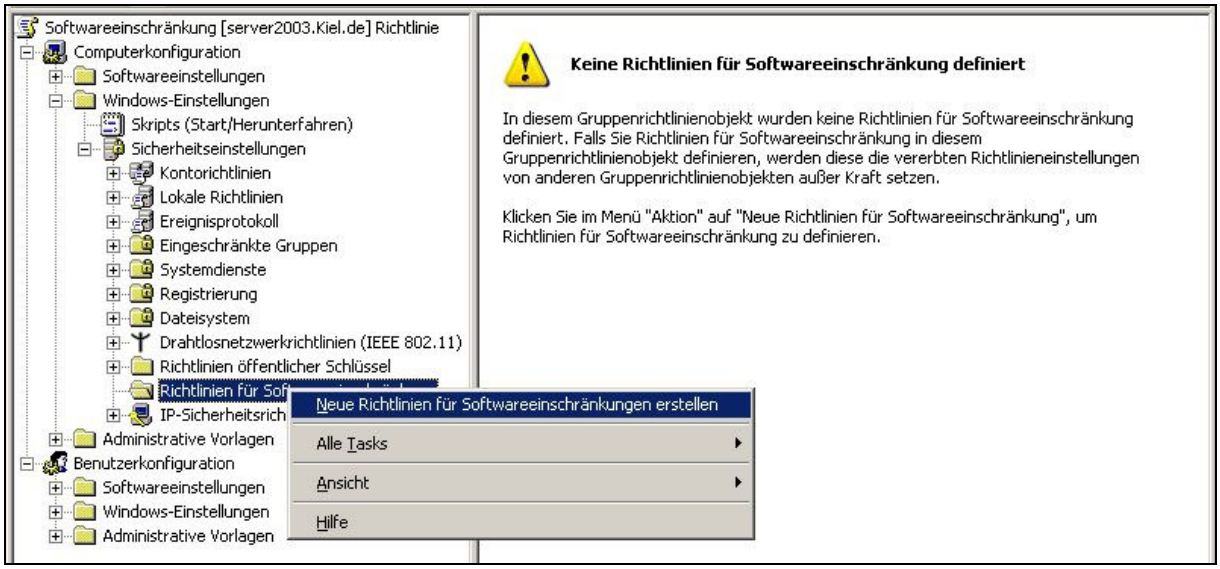
Ein Zertifikat verbindet einen Public Key mit einer Einzelperson. Zertifikate beinhalten ein Ablaufdatum, den Namen der Zertifizierungsstelle (CA), die das Zertifikat ausstellt, und eine eindeutige Seriennummer.

Die sicherste Anwendung der Authentifizierung erfolgt, indem ein Zertifikat an eine signierte Nachricht angehängt wird. Der Empfänger überprüft das Zertifikat mit dem Public Key der CA. Wenn der Public Key des Absenders gültig ist, wird dem Empfänger die Gültigkeit der Digitalen Signatur dieser Nachricht bestätigt. Die Digitale Signatur, die mit einem Private Key erstellt wurde, wird mit dem Digitalen Zertifikat überprüft, das den Public Key enthält.

Richtlinien für Softwareeinschränkungen

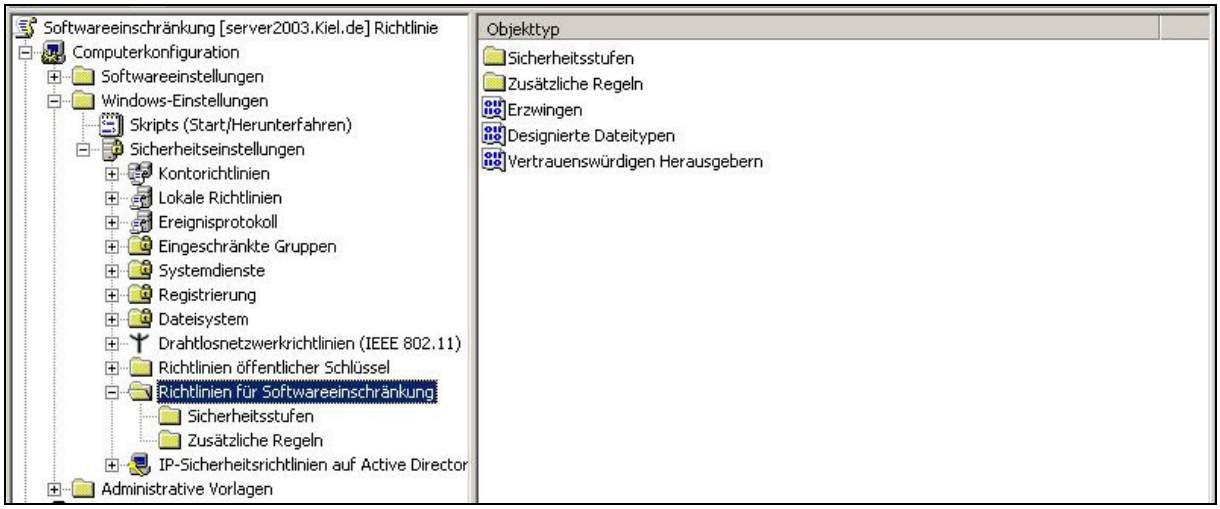
Die RICHTLINIEN FÜR SOFTWAREEINSCHRÄNKUNGEN der SICHERHEITSEINSTELLUNGEN ermöglichen es dem Administrator computer- und benutzerbezogen festzulegen, welche Programme und Dateien ein Benutzer auf dem Computer ausführen darf.

Die Richtlinien werden nur in einer Windows Server 2003- und Windows XP-Umgebung unterstützt.



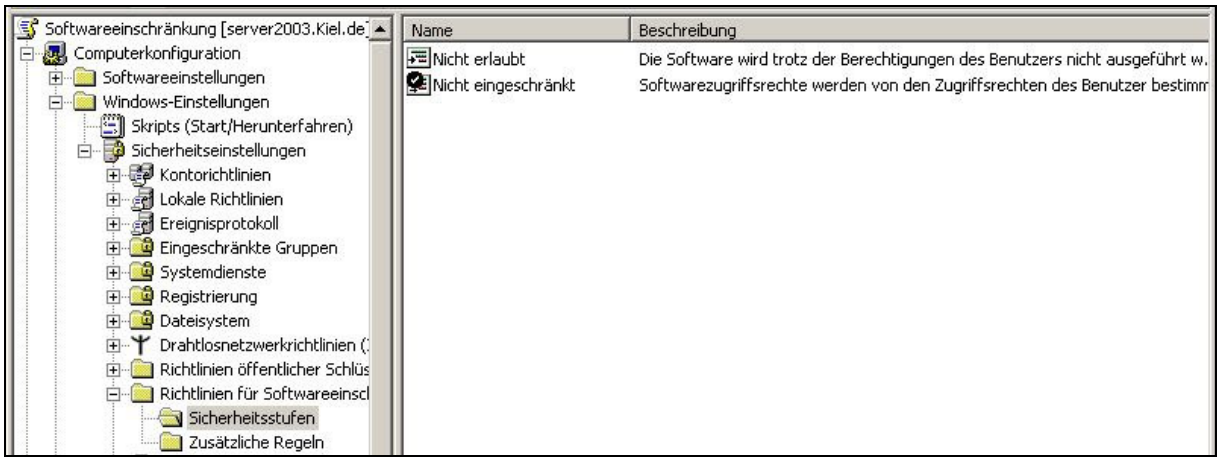
Richtlinien für Softwareeinschränkungen erstellen

Zunächst müssen in einer Gruppenrichtlinie (in diesem Beispiel die Gruppenrichtlinie SOFTWAREEINSCHRÄNKUNG) die RICHTLINIEN FÜR SOFTWAREEINSCHRÄNKUNGEN computer- oder benutzerbezogen eingerichtet werden. Sie bestehen aus den Containern SICHERHEITSSTUFEN und ZUSÄTZLICHE REGELN sowie aus drei dazugehörigen Richtlinien.

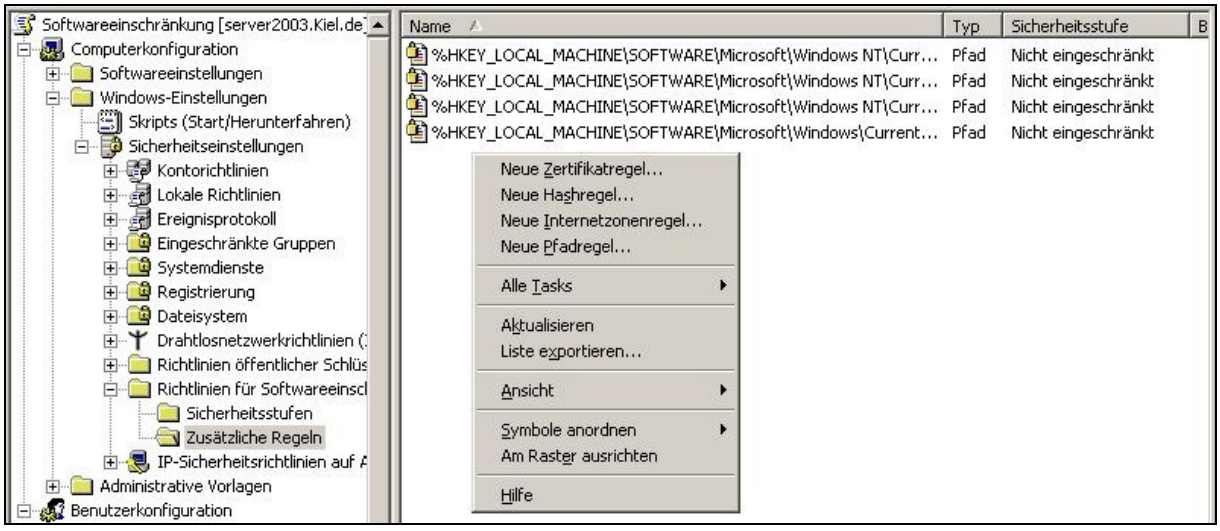


Richtlinien für Softwareeinschränkungen

In dem Container SICHERHEITSSTUFEN können die Standardsicherheitsstufen NICHT EINGESCHRÄNKT oder NICHT ERLAUBT definiert werden, sodass die auf dem Computer installierten Softwareprodukte bzw. Anwendungen entweder standardmäßig ausgeführt oder nicht ausgeführt werden. Anschließend können mit Hilfe der ZUSÄTZLICHEN REGELN für bestimmte Softwareprodukte bzw. Anwendungen Ausnahmen von der Standardsicherheitsstufe festgelegt werden.



Definition der Sicherheitsstufen



Definition der zusätzlichen Regeln

Folgende Regeltypen stehen zur Verfügung:

HASHREGEL

Mit einer Hashregel wird eine ausführbare Datei über einen Hashwert bzw. einer Bytefolge eindeutig identifiziert. Der Hashwert wird von einem internen Hash-Algorithmus ermittelt und der Richtlinie zugeordnet. Versucht ein Benutzer die ausführbare Datei zu starten, wird

der Hashwert der Datei mit dem Hashwert der Richtlinie verglichen. Ist die Sicherheitsstufe NICHT ERLAUBT aktiviert, so kann die Anwendung nicht ausgeführt werden.

Ausführung der Cmd.exe über Hashregel nicht erlauben

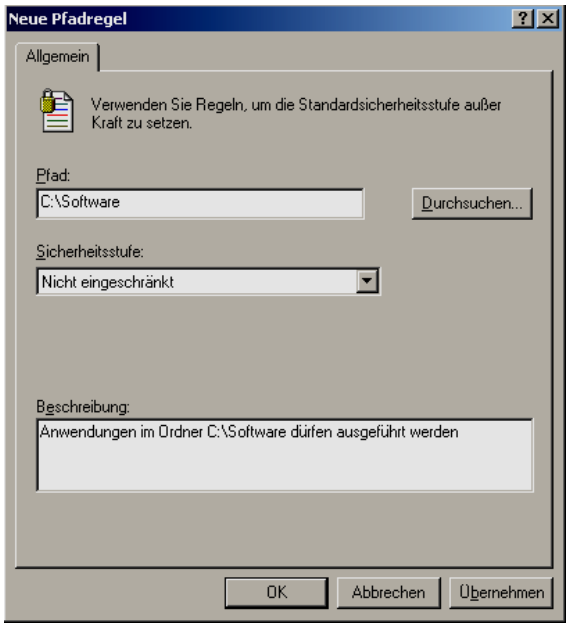
ZERTIFIKATREGEL

Mit Hilfe einer Zertifikatregel können Dateien, die über ein Zertifikat verfügen, zur Ausführung zugelassen werden. Damit kann z. B. sichergestellt werden, dass nur vertrauenswürdige Dateien aufgerufen werden können.

PFADREGEL

Eine Pfadregel identifiziert ausführbare Dateien über ihren Dateipfad. So kann beispielsweise festgelegt werden, dass alle Dateien im Pfad <C:\Software> ausgeführt werden dürfen. Nur Dateitypen, die unter Designierte Dateitypen aufgelistet werden, sind von den Pfadregeln betroffen.

Sollen Anwendungen auf dem Client ausgeführt werden, so ist bei der Pfadangabe zu beachten, dass der Pfad auf der Festplatte des Clients mit der Richtlinieneinstellung übereinstimmt.



Pfadregel

INTERNETZONENREGEL

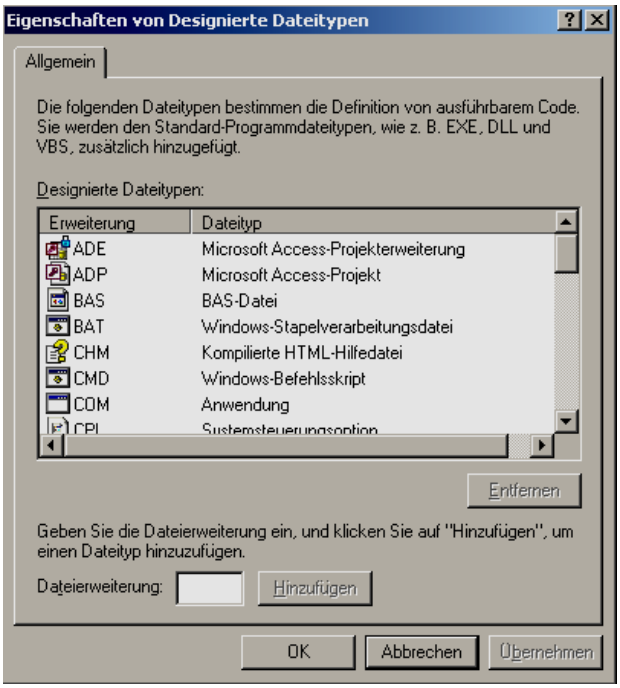
Zonenregeln gelten nur für Windows Installer-Pakete. Eine Zonenregel kann ein über den Internet Explorer aufgerufenes Windows-Installer-Paket bezüglich der Zone (INTERNET, LOKALES INTRANET, EINGESCHRÄNKTE SITES, VERTRAUENSWÜRDIGE SITES und ARBEITSPLATZ) identifizieren.

Softwareausführung auf dem Client nur im Ordner C:\Software erlauben!

1. *Erstellen Sie eine neue Gruppenrichtlinie und vergeben Sie einen aussagekräftigen Namen, z. B. Softwareeinschränkung.*
2. *Ordnen Sie die Gruppenrichtlinie einer Organisationseinheit zu, für die Sie Softwareeinschränkungen zuweisen möchten.*
3. *Navigieren Sie unter dem Knoten Benutzerkonfiguration zu dem Container WINDOWS-EINSTELLUNGEN\SICHERHEITSEINSTELLUNGEN\RICHTLINIEN FÜR SOFTWAREEINSCHRÄNKUNGEN.*
4. *Markieren Sie die Richtlinie mit der rechten Maustaste und wählen Sie im Kontextmenü NEUE RICHTLINIEN FÜR DIE SOFTWAREEINSCHRÄNKUNG ERSTELLEN.*
5. *Aktivieren Sie im Container SICHERHEITSSTUFEN die Sicherheitsstufe NICHT ERLAUBT als Standard.*
6. *Für die Erstellung einer Pfadregel markieren Sie die Richtlinie ZUSÄTZLICHE REGELN mit der rechten Maustaste und wählen die Option NEUE PFADREGEL.*
7. *Es öffnet sich ein Fenster, in dem Sie den Pfad <C:\Software> mit der Sicherheitsstufe NICHT EINGESCHRÄNKT eintragen.*

Löschen Sie die vier standardmäßig eingerichteten Registrierungspfadrichtlinien nicht! Diese sind notwendig, damit sich der Benutzer am Client anmelden kann. Sie erlauben den Zugriff auf ausführbare Betriebssystemdateien im Windows-Betriebssystemverzeichnis und den Zugriff auf alle Anwendungen im Verzeichnis PROGRAMME.

Die Richtlinie DESIGNIERTE DATEITYPEN enthält die Dateitypen, die als ausführbare Dateien definiert werden. Es besteht die Möglichkeit, entweder aufgelistete Dateitypen zu entfernen oder weitere aufzunehmen.



Richtlinie DESIGNIERTE DATEITYPEN

Die Aktivierung der Richtlinien für Softwareeinschränkungen kann bei falscher Anwendung zu erheblichen Problemen beim Betrieb der Computer führen. Beachten Sie deshalb folgende Punkte:

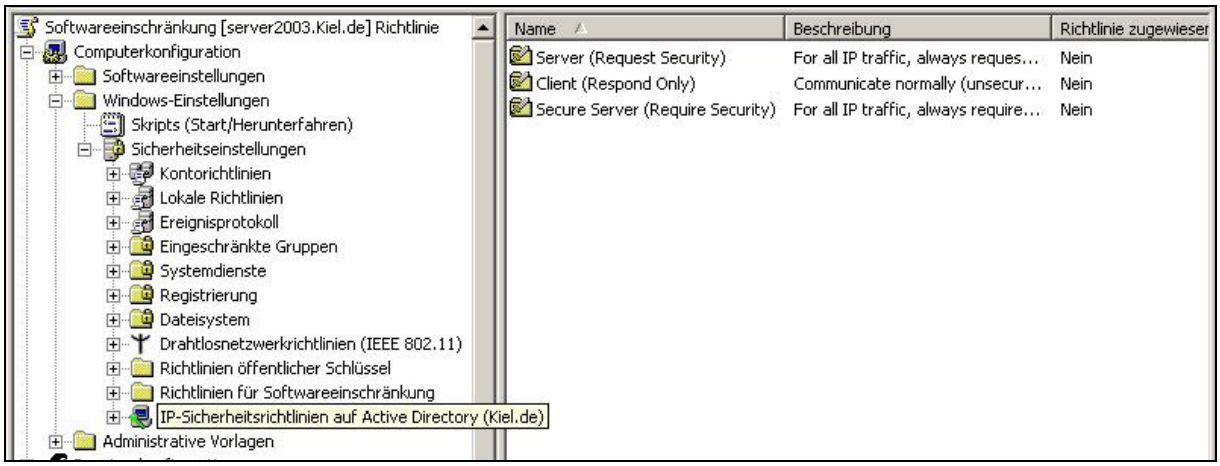
- *Aktivieren Sie die Richtlinien nicht in einem Gruppenrichtlinienobjekt auf Domänenebene, wie z. B. der Default Domain Policy. Das führt dazu, dass auch Domänencontroller und Mitgliedserver diesen Richtlinien unterliegen, sodass Anwendungen auf diesen Systemen bei einer restriktiven Einstellung nicht mehr aufrufbar sind. Im schlimmsten Fall kann der Administrator nicht mehr auf den Domänencontroller zugreifen. Starten Sie dann den Computer im abgesicherten Modus mit Netzwerktreibern und machen Sie Ihre Einstellungen rückgängig.*
- *Erstellen Sie eine separate Gruppenrichtlinie. Sie können sie dann notfalls unabhängig von den restlichen Domänenrichtlinien deaktivieren.*

- *Gehen Sie bei der Einstellung der Standardeinstellung Nicht erlaubt vorsichtig vor. Wenn Sie die Standardeinstellung Nicht erlaubt festlegen, ist nur noch explizit zugelassene Software erlaubt. Jede Datei, die Sie öffnen möchten, muss über eine eigenständige Richtlinie verfügen, die das Öffnen der Datei erlaubt.*
- *Um zu verhindern, dass sich Administratoren und Benutzer selbst aus dem System aussperren, werden automatisch vier Registrierungspfadregeln erstellt, wenn die Standardsicherheitsstufe auf Nicht erlaubt festgelegt wird. Sie können diese Registrierungspfadregeln löschen oder ändern, was jedoch nicht empfohlen wird.*
- *Testen Sie Ihre Richtlinieneinstellungen in einer Testumgebung, bevor Sie sie auf Produktionssysteme übernehmen. Eine andere Möglichkeit zum Testen der Richtlinieneinstellungen besteht darin, zunächst ein „Test-Gruppenrichtlinienobjekt“ zu erstellen und mit einer „Testorganisationseinheit“ zu verknüpfen.*

IP-Sicherheitsrichtlinien

Mit Hilfe der IP-Sicherheitsrichtlinien kann in einer Domänenumgebung zwischen Computern eine verschlüsselte Kommunikation über IPSec (Internet Protocol Security) festgelegt werden.

Der Einsatz der IP-Sicherheitsrichtlinien ist abhängig davon, auf welche Art und Weise die Datenkommunikation in einer Organisation durchgeführt wird. So kann beispielsweise die erforderliche Sicherheit variieren, je nachdem, ob es sich bei dem Computer um einen Domänencontroller, Webserver, RAS-Server, Dateiserver, Datenbankserver, Intranet- oder Remote-Client handelt. Mit der Erstellung einer IP-Sicherheitsrichtlinie werden folgende drei abgestufte Standardrichtlinien eingerichtet:



IP-Sicherheitsrichtlinien

CLIENT (NUR ANTWORT, RESPOND ONLY)

Die Richtlinie CLIENT unterstützt nur die Verschlüsselung, sofern sie vom Server angefordert wird. Ansonsten wird die Kommunikation unverschlüsselt durchgeführt.

SERVER (SICHERHEIT ANFORDERN, REQUEST SECURITY)

Die Richtlinie SERVER führt eine verschlüsselte Kommunikation durch, erzwingt sie aber nicht. Diese Richtlinie ist dann von Bedeutung, wenn ein Client kein IPSec unterstützt.

SECURE SERVER (SICHERHEIT ERFORDERLICH, REQUIRE SECURITY)

Die Richtlinie SECURE SERVER (Require Security) setzt voraus, dass auf allen Clients, die mit dem Server kommunizieren möchten, IPSec unterstützt wird. In diesem Fall wird nur eine verschlüsselte Kommunikation zugelassen.

Darüber hinaus ist das Erstellen einer gesonderten individuellen Richtlinie über einen Assistenten möglich. Dabei muss zunächst der verwendete Authentifizierungsmechanismus ausgewählt werden. Kerberos wird dabei als Standardeinstellung vorgegeben. Danach können die Optionen für die Datenkommunikation konfiguriert werden.

Wenden Sie die IP-Sicherheitsrichtlinien zunächst in einer Testumgebung an. Eine fehlerhafte Konfiguration der IP-Sicherheitsrichtlinien kann dazu führen, dass die Computer nicht mehr miteinander kommunizieren können.

Nähere Einzelheiten zur Administration der Richtlinien finden Sie in der Online-Hilfe.

Für die Administration der IP-Sicherheitsrichtlinien stehen die Tools IP-Secpol.exe aus dem Windows Server 2003-Resource Kit sowie die Snap-In-Verwaltungsprogramme IP-Sicherheitsrichtlinienverwaltung und IP-Sicherheitsmonitor zur Verfügung.

IP-Sicherheitsrichtlinien verwenden IPSec (Internet Protocol Security)

Die IP-Sicherheitsrichtlinien arbeiten mit drei Sicherheitsfunktionen: Authentifizieren, Filtern und Verschlüsseln. Zunächst ist eine gegenseitige Authentifizierung der Systeme erfor-

derlich, bevor überhaupt eine Verbindung aufgebaut werden darf. Auf diese Verbindungen werden Filter angewendet, die definieren, welche Informationen zwischen zwei Systemen übertragen werden dürfen und welche Sicherheitsanforderungen daran gestellt sind. Eine dieser konfigurierbaren Anforderungen ist, dass die Informationen verschlüsselt werden müssen.

Der Verbindungsaufbau mit IPSec erfolgt immer in zwei Phasen. Die erste Phase handelt die Form der Authentifizierung aus. Windows 2000/2003 unterstützt mit Kerberos, X.509 und vordefinierten statischen Texten drei Varianten, um den Austausch von Schlüsseln zu sichern. Nachdem die Authentifizierung definiert ist, lässt sich in der zweiten Phase ein symmetrischer Schlüssel für die Verbindung aushandeln und austauschen. Erst danach kann die verschlüsselte Kommunikation durchgeführt werden.

IPSec schützt Daten im Netzwerk, sodass ihre Entschlüsselung für einen Angreifer unmöglich oder zumindest mit erheblichen Schwierigkeiten verbunden ist. Der Grad des bereitgestellten Schutzes wird durch die Stärke der in der IPSec-Richtlinienstruktur angegebenen Sicherheitsstufe bestimmt.

IPSec weist eine Reihe von Funktionen auf, durch die die folgenden Angriffe erheblich eingeschränkt oder verhindert werden:

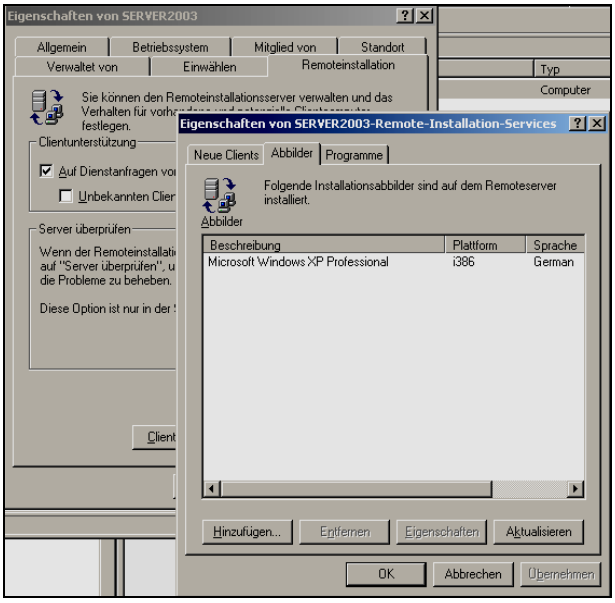
- Datenpakete über das Netzwerk abgreifen (sniffen)
  Durch den Einsatz des ESP-Protokolls (Encapsulating Security Payload) in IPSec wird die Datenvertraulichkeit durch die Verschlüsselung der IP-Pakete gewährleistet.
- Datenänderung
  IPSec verwendet Kryptografieschlüssel, die ausschließlich vom sendenden und vom empfangenden Computer gemeinsam verwendet werden, um für die einzelnen IP-Pakete eine kryptografische Prüfsumme zu erstellen. Durch jede Änderung der Paketdaten wird die Prüfsumme geändert, wodurch dem empfangenden Computer angezeigt wird, dass das Paket während der Übertragung geändert wurde.
- Angriffe mit Hilfe von Kennwörtern und Angriffe auf Anwendungsebene
  IPSec ermöglicht den Austausch und die Überprüfung von Identitäten, ohne dass diese Informationen für einen Angreifer analysierbar sind. Nach dem Einrichten der Identitäten verwendet IPSec Kryptografieschlüssel, die ausschließlich vom sendenden und von den empfangenden Computern gemeinsam verwendet werden, um eine kryptografische Prüfsumme für die einzelnen IP-Pakete zu erstellen. Durch die kryptografische Prüfsumme wird sichergestellt, dass nur die Computer, denen die Schlüssel bekannt sind, die jeweiligen Pakete gesendet haben können.
- Man-in-the-Middle-Angriff
  IPSec kombiniert die gegenseitige Authentifizierung mit gemeinsam genutzten Kryptografieschlüsseln.

8.2.3 Remoteinstallationsdienste

Mit der Richtlinie REMOTEINSTALLATIONSDIENSTE (Remote Installation Service, RIS) in den benutzerbezogenen WINDOWS-EINSTELLUNGEN können über das Netzwerk abbildbasierte Betriebssysteminstallationen benutzerbezogen gesteuert werden. Die Zuweisung der Richtlinie setzt voraus, dass die Windows-Komponente *Remoteinstallationsdienst* installiert ist. Über einen Assistenten können dann imagebasierte Betriebssysteminstallationen auf einem Server bereitgestellt werden.

RIS bietet folgende Verwendungszwecke:

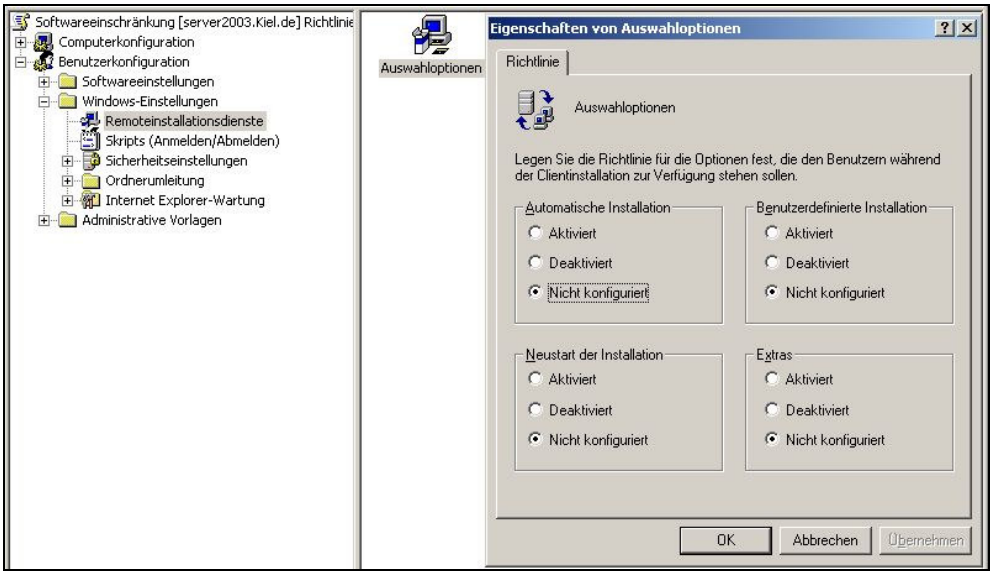
- Bedarfsgesteuerte Bereitstellung eines Betriebssystems für Benutzer. Startet ein Benutzer seinen PC, unabhängig davon, ob auf diesem ein Betriebssystem installiert ist, kann der RIS-Server antworten, indem er ein Betriebssystem über das Netzwerk installiert. Eine CD ist nicht erforderlich. Dazu muss der Computer Pre-Boot eXecution Environment (PXE) verwenden. Mit dieser Remotestarttechnologie kann der Computer einen Startablauf von einem Netzwerkadapter beginnen.
- Bereitstellen von Betriebssystemabbildern, die bestimmte Einstellungen und Anwendungen beinhalten, z. B. ein Abbild, das einen Standard für Desktops darstellt. Einer bestimmten Benutzergruppe kann ein bestimmtes Abbild (bzw. mehrere Abbilder) zur Verfügung gestellt werden, das für diese Gruppe definiert wurde.
- Erstellen automatisierter Installationsabbilder von Produkten aus der Windows Server 2003-Produktfamilie sowie Abbildern von Windows XP und Windows 2000.



Registerkarte REMOTEINSTALLATION des Remote-Servers

Nach der ersten Installation eines abbildbasierten Betriebssystems mit dem Remoteassistenten wird auf dem Server dem entsprechenden Computerkonto die Registerkarte REMOTEINSTALLATION hinzugefügt. Hier können die Installationen und auch zugewiesene Programme bzw. Tools verwaltet werden.

Für die Vorbereitung der Remoteinstallationsdienste ist zu beachten, dass die Installation von Abbildern nicht auf einem Festplattenlaufwerk durchgeführt wird, auf dem sich das Betriebssystem des Computers befindet.



Eigenschaften der Richtlinie REMOTEINSTALLATIONSDIENSTE

Die Richtlinie Remoteinstallationsdienste stellt auf der Eigenschaftenseite folgende Auswahloptionen zur Verfügung:

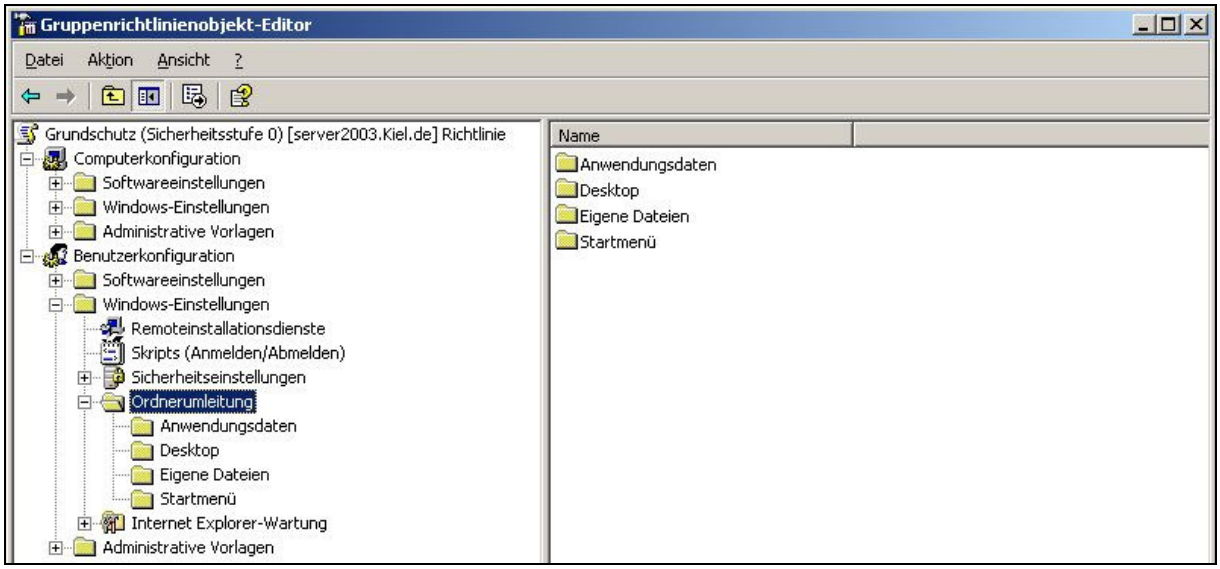
- AUTOMATISCHE INSTALLATION
  Die Aktivierung setzt voraus, dass bereits ein Computerkonto und ein Computername im Active Directory eingerichtet wurden.
- BENUTZERDEFINIERTE INSTALLATION
  Bei der benutzerdefinierten Installation kann der Benutzer das Computerkonto im Active Directory selbst einrichten.
- NEUSTART DER INSTALLATION
  Bei einem Installationsfehler kann festgelegt werden, dass die Installation durch einen Neustart wiederholt wird.
- EXTRAS/TOOLS
  Der Benutzer erhält mit der Installation Zugriff auf Tools für die Administration, die über

den Remoteinstallationsassistenten installiert wurden. Die Registerkarte REMOTE-INSTALLATION des Computerkontos des Remoteservers bietet die Möglichkeit, die Tools zu verwalten.

8.2.4 Ordnerumleitung

Benutzereinstellungen und Benutzerdateien werden standardmäßig im lokalen Benutzerprofil im Ordner DOKUMENTE UND EINSTELLUNGEN gespeichert. Auf die Dateien in lokalen Benutzerprofilen kann nur vom aktuellen Computer zugegriffen werden. Das ist problematisch für Benutzer, die mehr als einen Computer verwenden, da ihren Daten und Einstellungen nicht zentral gespeichert und gesichert werden.

Zur Lösung dieses Problems gibt es die Möglichkeit, entweder servergespeicherte Profile einzurichten oder die Richtlinie ORDNERUMLEITUNG der benutzerbezogenen WINDOWS-EINSTELLUNGEN zuzuweisen. Mit der Ordnerumleitung kann der Administrator den Pfad der Ordner ANWENDUNGSDATEN, DESKTOP, EIGENE DATEIEN und STARTMENÜ des lokalen Benutzerprofils an einen neuen Pfad umleiten. Für die Umleitung sollte ein freigegebenes Verzeichnis auf einem Server zur Verfügung stehen.



Gruppenrichtlinie Ordnerumleitung

Vorteile der Ordnerumleitung:

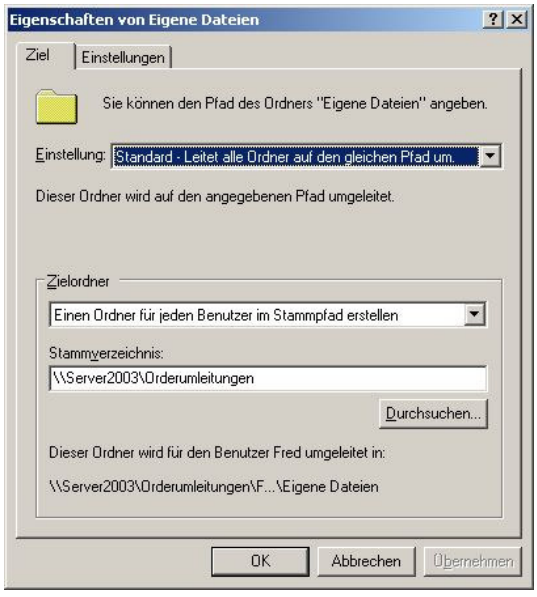
- Bei der Ordnerumleitung ist es nicht erforderlich, den Inhalt der umgeleiteten Ordner bei jedem An- oder Abmeldevorgang des Benutzers mit dem lokalen Client zu synchronisieren, sondern er wird im Netzwerk gespeichert. Somit wird der Netzverkehr deutlich verringert.

- Dem Benutzer stehen die eigenen Dokumente zur Verfügung, wenn er sich an verschiedenen Computern im Netzwerk anmeldet.
- Daten, die in einem freigegebenen Netzwerkordner gespeichert sind, können im Rahmen der routinemäßigen Systemverwaltung gesichert werden.
- Administratoren können mit Gruppenrichtlinien Datenträgerkontingente festlegen und somit den Speicherplatz für die Spezialordner eines Benutzers begrenzen.

Für die Umleitung der Ordner ist es erforderlich, dass auf dem Server ein Zielordner angelegt und freigegeben wird.

Die Kontextmenü-Option EIGENSCHAFTEN der Ordner ANWENDUNGSDATEN, DESKTOP, EIGENE DATeien und STARTMENÜ der Richtlinie ORDNERUMLEITUNG stellt ein Dialogfenster zur Verfügung, mit dem die Eigenschaften der entsprechenden Ordner konfiguriert werden können. Folgende Einstellungen stehen zur Verfügung:

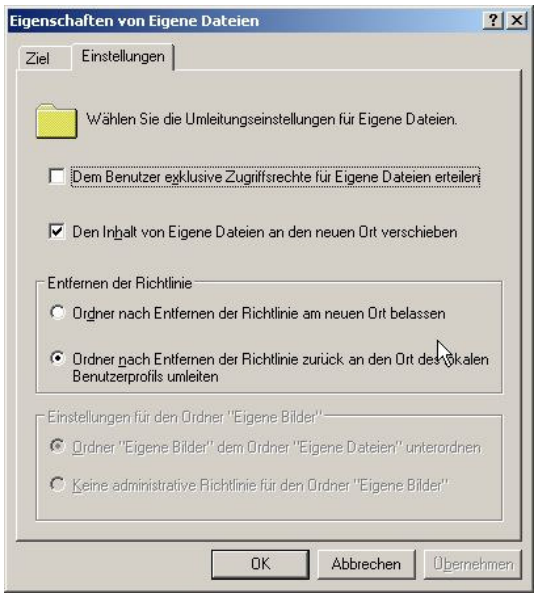
- STANDARD
  Alle Ordner werden auf den gleichen Pfad umgeleitet, der im Dialogfeld Stammverzeichnis angegeben wurde.
- ERWEITERT
  Alle Pfade für die Ordnerumleitung können gruppenkontenbezogen eingerichtet werden.



Registerkarte ZIEL des Ordners EIGENE DATEIEN

Bei der Richtlinie EIGENE DATEIEN stehen zusätzlich folgende Optionen zur Verfügung:

- EINEN ORDNER FÜR JEDEN BENUTZER IM STAMMPFAD ERSTELLEN
  Diese Option bewirkt, dass jeder Benutzer einen eigenen Ordner in dem angegebenen Stamm-verzeichnis erhält.
- AN FOLGENDEN PFAD UMLEITEN
  Diese Option bewirkt, dass die Benutzer den umgeleiteten Pfad gemeinsam nutzen, sodass die Dateien aller Benutzer in einem Ordner verwaltet werden.
- AN LOKALEN BENUTZERPROFILPFAD UMLEITEN
  Diese Option bietet die Möglichkeit, serverbasierte Ordner zurück in das lokale Benutzer-profil (Dokumente und Einstellungen) umzuleiten.
- IN DAS BASISVERZEICHNIS DES BENUTZERS KOPIEREN
  Diese Option bewirkt, dass der Ordner auf den Pfad umgeleitet wird, der als Basisver-zeichnis auf der Registerkarte Profil des Benutzerkontos eingetragen wurde.



Registerkarte EINSTELLUNGEN des Ordners EIGENE DATEIEN

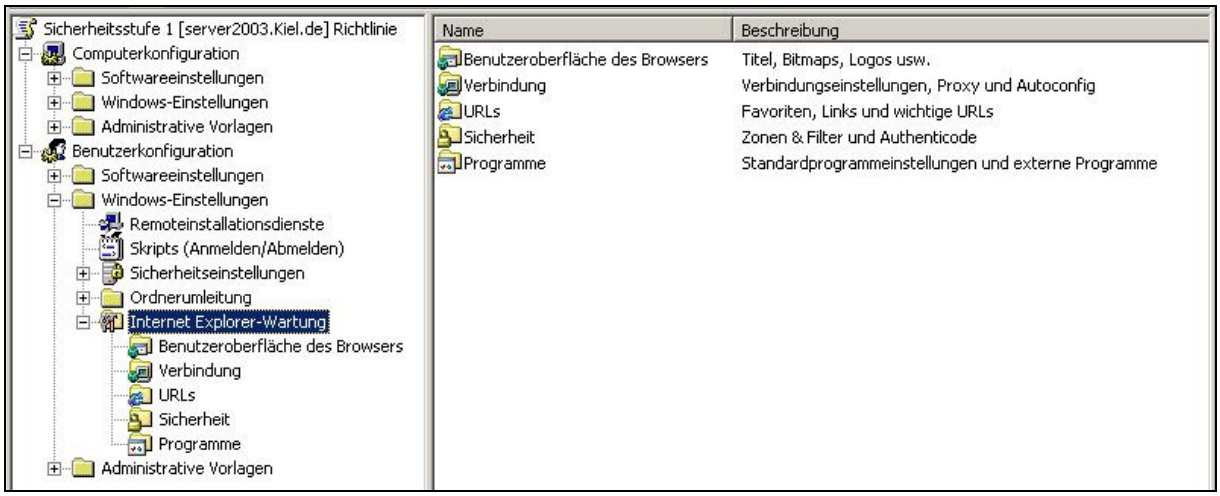
Auf der Registerkarte EINSTELLUNGEN stehen folgende Optionen zur Verfügung:

- DEM BENUTZER EXKLUSIVE ZUGRIFFSRECHTE FÜR <ORDNERNAME> ERTEILEN
  Diese Option bewirkt, dass ausschließlich der Benutzer über Berechtigungen auf den neu erstellten umgeleiteten Ordner verfügt. Auch die administrativen Benutzerkonten verfügen über keine Berechtigungen auf den umgeleiteten Ordner.

- DEN INHALT VON <ORDNERNAME> AN DEN NEUEN ORT VERSCHIEBEN
  Diese Option legt fest, dass die im lokalen Profil gespeicherten Dateien in den umgeleiteten Ordner verschoben werden.
- ENTFERNEN DER RICHTLINIE
  Diese Option bestimmt, wie mit der Ordnerumleitung zu verfahren ist, wenn die Richtlinie Ordnerumleitung deaktiviert oder gelöscht wird.

8.2.5 Internet Explorer-Wartung

Mit Hilfe der Richtlinien Internet Explorer-Wartung können folgende Einstellungen des Internet Explorers zentral vorgegeben werden:



Richtlinien für die Internet Explorer-Wartung

- BENUTZEROBERFLÄCHE DES BROWSERS
  Diese Option ermöglicht es, mit mehreren Richtlinien das Erscheinungsbild des Internet Explorers an die Bedürfnisse der Organisation anzupassen.
- VERBINDUNG
  Diese Option enthält Richtlinien, über die der Verbindungsaufbau mit dem Internet gesteuert werden kann. So kann beispielsweise die DFÜ-Einwahl vorgegeben werden.
- URLS
  Diese Option umfasst die Richtlinien FAVORITEN UND LINKS und WICHTIGE URLS. Mit Hilfe dieser Richtlinien lassen sich die Favoriten und URLs des Internet Explorer-Clients verwalten.

- SICHERHEIT

  Mit Hilfe dieser Option lassen sich die Sicherheitseinstellungen des Internet Explorers anpassen. Mit den AUTHENTICODE-EINSTELLUNGEN kann festgelegt werden, dass nur vertrauenswürdige Webseiten aufrufbar sind. Die Richtlinien SICHERHEITSZONEN und INHALTSFILTER können den Webzugriff noch weitergehend einschränken.

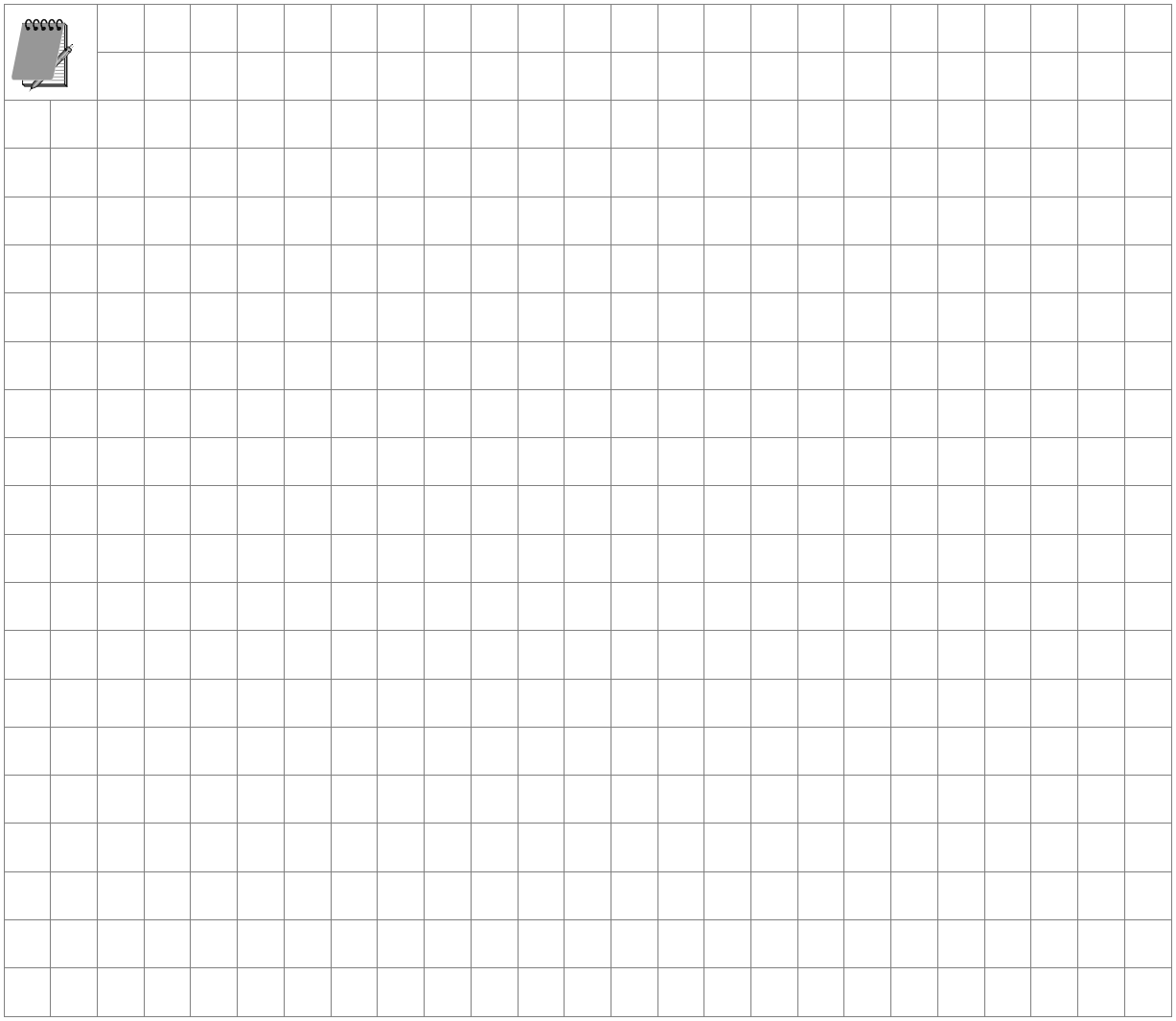
- PROGRAMME

  Diese Option legt fest, welche Internetprogramme standardmäßig für die allgemeinen Aufgaben im Zusammenhang mit dem Internet verwendet werden sollen, z. B. das Lesen von E-Mail-Nachrichten oder das Anzeigen von Newsgroups.

8.3 Sicherheitscheck

- *Nutzen Sie die Richtlinie **Softwareverteilung**, um Windows-Software und Servicepacks zentral auf den Clients zu installieren. Beachten Sie, dass die zu installierende Software die Windows Installer-Technologie (MSI-Pakete) unterstützt.*
- *Richten Sie einen **Fileserver** ein, auf dem die Software und Servicepacks vorinstalliert werden.*
- *Nutzen Sie das Tool **Custom Installation Wizard** aus dem **Office Resource Kit**, um für die Installation nur ganz bestimmte Office-Komponenten auszuwählen.*
- *Verwenden Sie die Richtlinie **Skripts**, um Systemeinstellungen während des Startens oder Herunterfahrens des Clients oder während des An- oder Abmeldens am Client zu automatisieren.*
- *Administrieren Sie in der Gruppenrichtlinie Default Domain Policy nur die **Kontorichtlinien**.*
- *Beachten Sie bei der Aktivierung der **Überwachungsrichtlinien**, dass organisatorisch festgelegt ist, welche Person die Protokolle auswertet. Legen Sie auch fest, aufgrund welcher Sicherheitsaspekte welche Überwachungsrichtlinie aktiviert werden soll.*
- *Verwenden Sie die Richtlinie **Eingeschränkte Gruppen**, wenn Sie die Mitgliedschaft von Benutzer- und Gruppenkonten in Bezug auf ein Gruppenkonto erzwingen möchten.*
- *Aktivieren Sie die Richtlinie **Softwareeinschränkungen**, wenn ein Benutzer nur ganz bestimmte Programme aufrufen darf. Beachten Sie, dass diese Richtlinie nur in einer **Windows 2003/XP** Umgebung unterstützt wird.*
- *Setzen Sie die **Hashregel** ein, um zu verhindern, dass ausgewählte Programme bzw. ausführbare Dateien ausgeführt werden können.*
- *Die **Pfadregel** sollten Sie einsetzen, wenn Sie grundsätzlich nur die in einem Ordner/Pfad installierten Programme zur Ausführung bereitstellen wollen.*

- *Sofern Sie eine **verschlüsselte Kommunikation** über Ihr Netzwerk mit Hilfe der IP-Sicherheitsrichtlinien realisieren wollen, sollten Sie zunächst in einer Testumgebung die Anwendung und Funktionsweise der einzelnen Richtlinien erproben.*
- *Nutzen Sie die Richtlinie **Remoteinstallationsdienste**, wenn Sie abbildbasierte Betriebssysteminstallationen durchführen wollen. Beachten Sie, dass die Windows-Komponente Remoteinstallationsdienste installiert ist.*
- *Aktivieren Sie die Richtlinie **Ordnerumleitung**, um die Dateien im lokalen Benutzerprofil zentral auf einem Server zu speichern.*
- *Verwenden Sie die Richtlinie **Internet Explorer-Wartung**, wenn für die Internetnutzung eine zentrale Grundkonfiguration des Internet Explorers vorgegeben werden soll.*



9 Administrative Vorlagen

In diesem Kapitel erfahren Sie,

- wie sich die Richtlinien im Bereich ADMINISTRATIVE VORLAGEN von den Richtlinien der Knoten SICHERHEITSEINSTELLUNGEN und WINDOWS-EINSTELLUNGEN unterscheiden,
- welche Bedeutung die adm-Dateien haben und
- welche Funktion die Richtlinie LOOPBACK zur Verfügung stellt.

In diesem Kapitel werden **nicht** die zahlreichen Richtlinien der ADMINISTRATIVEN VORLAGEN aufgelistet und erklärt. Zum einen unterscheidet sich die Anzahl der eingesetzten Richtlinien je nach eingesetztem Betriebssystem, sodass man sowieso keine Vollständigkeit garantieren kann und zum anderen kann man die Liste in fast jedem Fachbuch nachlesen, das sich mit den Gruppenrichtlinien befasst. Außerdem bietet jede Richtlinie der ADMINISTRATIVEN VORLAGEN auf einer eigenständigen Registerkarte eine aussagekräftige Beschreibung.

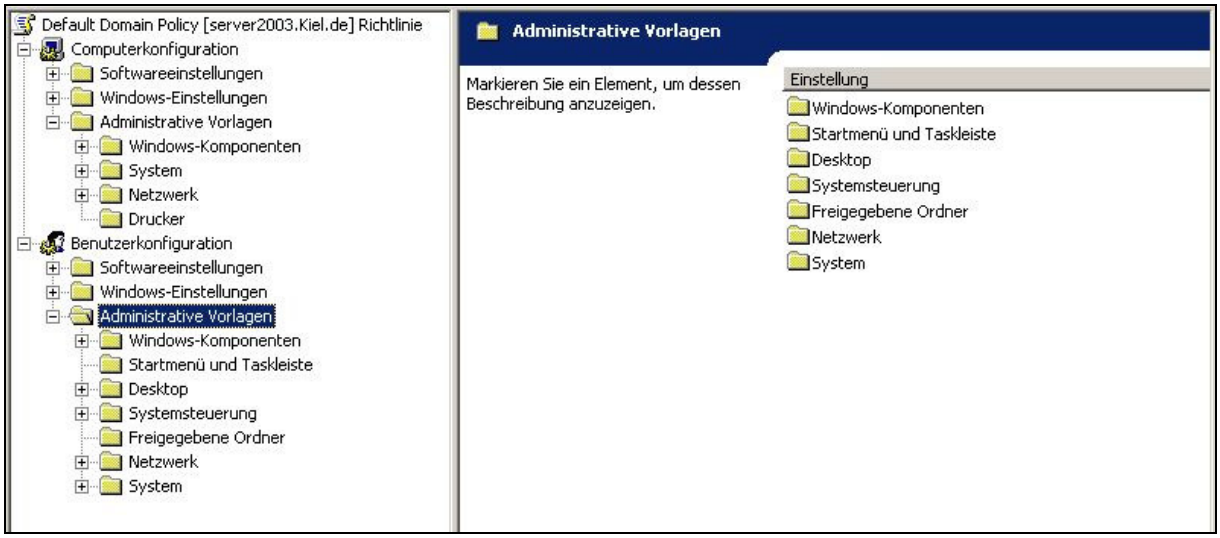
Dieses Kapitel beschreibt stattdessen die Struktur der ADMINISTRATIVEN VORLAGEN, die Besonderheiten bei der Verarbeitung der adm-Dateien und die Funktionsweise der Richtlinie LOOPBACK.

9.1 Struktur der Administrativen Vorlagen

Sowohl bei der Computer- als auch bei der Benutzerkonfiguration befindet sich die größte Anzahl an Richtlinien im Bereich der ADMINISTRATIVEN VORLAGEN einer Gruppenrichtlinie. Die Richtlinien der ADMINISTRATIVEN VORLAGEN enthalten diejenigen Einstellungen einer Gruppenrichtlinie, die in der Registrierungsdatenbank (Registry) gespeichert werden. Dabei werden alle Einstellungen einer Gruppenrichtlinie, die

- in der Computerkonfiguration aktiviert werden, beim Starten auf den Computer übertragen, der in den Wirkungsbereich der Gruppenrichtlinie fällt. Diese Einstellungen werden dann in dem computerspezifischen Bereich der Registrierung (im Schlüssel HKEY_LOCAL_MACHINE) des entsprechenden Computers gespeichert.
- in der Benutzerkonfiguration aktiviert werden, beim Anmelden des Benutzers übertragen, sofern sich dieser im Wirkungsbereich der Gruppenrichtlinie befindet. Diese Einstellungen werden dann in dem benutzerspezifischen Bereich der Registrierung (im Schlüssel HKEY_CURRENT_USER) des entsprechenden Computers gespeichert.

Die Richtlinien der benutzerbezogenen ADMINISTRATIVEN VORLAGEN gliedern sich in die Bereiche WINDOWS-KOMPONENTEN, STARTMENÜ UND TASKLEISTE, DESKTOP, SYSTEMSTEUERUNG, FREIGEGEBENE ORDNER, NETZWERK und SYSTEM. Die ADMINISTRATIVEN VORLAGEN der Computerkonfiguration sind in die Bereiche WINDOWS-KOMPONENTEN, SYSTEM, NETZWERK und DRUCKER aufgeteilt.



ADMINISTRATIVE VORLAGEN der Computer- und Benutzerkonfiguration

Auch wenn die verschiedenen Bereiche der ADMINISTRATIVEN VORLAGEN aussagekräftige Namen haben, gestaltet sich die Suche nach einer bestimmten Richtlinie oft schwierig, vor allem, wenn sie thematisch anders in die verschiedenen Bereiche eingeordnet wurden als gedacht. Für den Fall, dass die gesuchte Richtlinie schon aktiviert wurde, kann die Funktion FILTERUNG des Gruppenrichtlinien-Editors genutzt werden. Wird nach einer noch nicht konfigurierten Richtlinie gesucht, so kann die Schlagwortsuche der Hilfe im Gruppenrichtlinien-Editor hinzugezogen werden. Beide Verfahren werden im Kapitel 7.3 beschrieben.

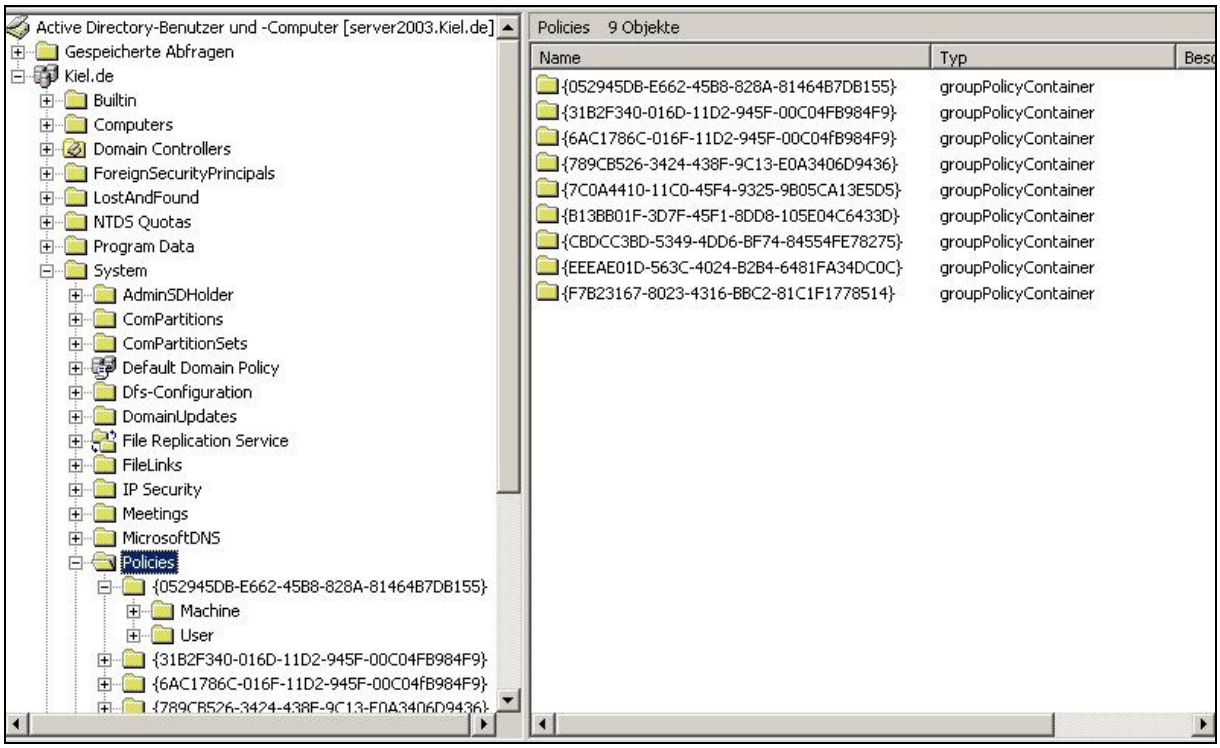
9.2 Verarbeitung von adm-Dateien

Möchte man die Verarbeitung von Richtlinien der Administrativen Vorlagen mit der Verwendung von adm-Dateien verstehen, so kommt man um die Definition der an der Verarbeitung beteiligten Objekte nicht herum. Dabei spielen die Speicherstrukturen *Gruppenrichtlinien-container* und *Gruppenrichtlinienvorlage* sowie die adm-Dateien und die Registry.pol-Dateien eine wichtige Rolle.

Gruppenrichtliniencontainer und Gruppenrichtlinienvorlage

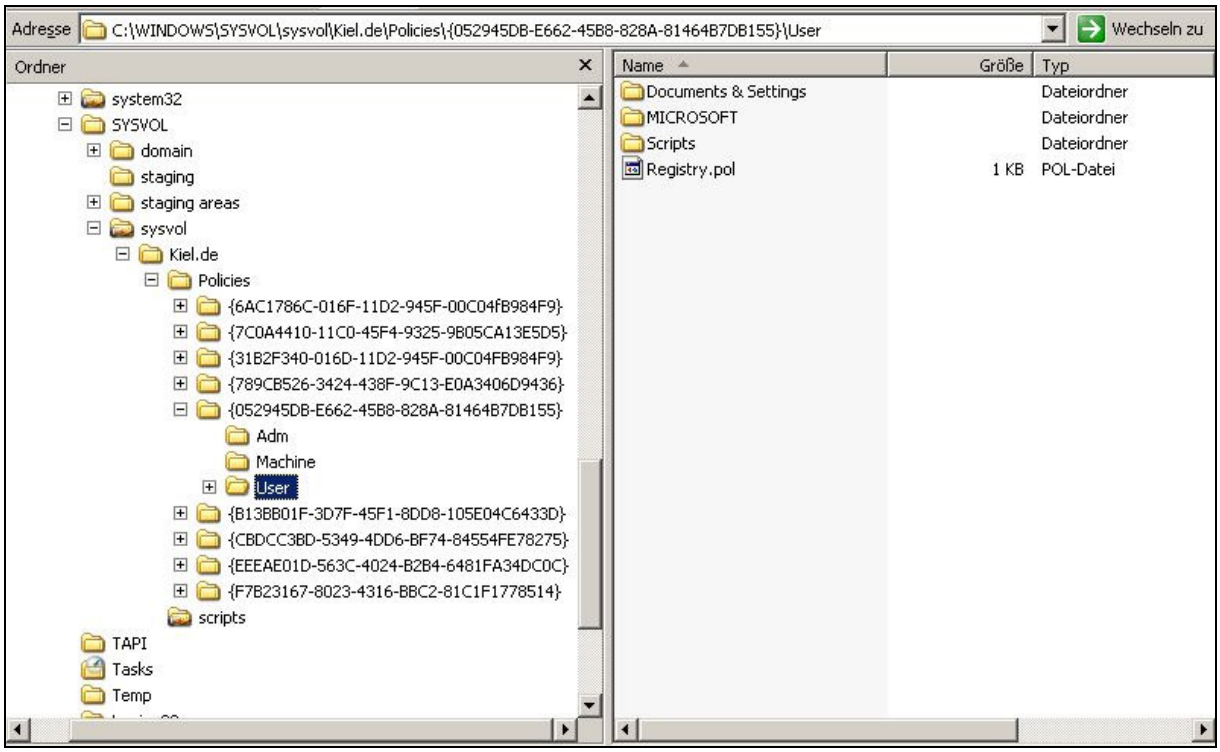
Wird eine neue Gruppenrichtlinie erstellt, so werden standardmäßig folgende Speicherstrukturen für diese neue Gruppenrichtlinie eingerichtet:

- Im Active Directory wird für die neue Gruppenrichtlinie in dem Container KIEL.DE/SYSTEM/POLICIES ein neuer Gruppenrichtliniencontainer **(Group Policy Container, GPC)** mit einer eindeutigen Kennung (GUID) eingerichtet (siehe Abbildung unten). Der Gruppenrichtliniencontainer speichert die Attribute der Gruppenrichtlinie und die Verweise auf die Gruppenrichtlinienvorlage. Er wird als Active Directory-Objekt mit all seinen Attributen zwischen den Domänencontrollern repliziert.



Gruppenrichtliniencontainer im Active Directory

- Im Dateisystem des Domänencontrollers wird für die neue Gruppenrichtlinie gleichzeitig eine weitere Speicherstruktur, die Gruppenrichtlininenvorlage **(Group Policy Template, GPT)**, eingerichtet (siehe folgende Abbildung). Die Gruppenrichtlinienvorlage wird in dem Verzeichnis <Stammverzeichnis:\Windows\Sysvol\Sysvol\<Domäne>\Policies> erstellt und erhält die gleiche GUID wie der Gruppenrichtliniencontainer. In diesem Verzeichnis und deren Unterverzeichnisse werden die Informationen der Gruppenrichtlinien gespeichert, u. a. auch die Registrierungseinstellungen in den unterschiedlichen Knoten der computer- und benutzerbezogenen ADMINISTRATIVEN VORLAGEN einer Gruppenrichtlinie.



Gruppenrichtlinienvorlage im Dateisystem des Domänencontrollers

Die Ordnerstruktur wird nur dann vollständig angezeigt, wenn die Option GESCHÜTZTE SYSTEMDATEIEN AUSBLENDEN *deaktiviert und die Optionen* INHALTE VON SYSTEMORDNER ANZEIGEN *sowie* ALLE DATEIEN UND ORDNER ANZEIGEN *aktiviert wurde.*

Wie hängen diese beiden Speicherstrukturen zusammen? Die getrennte Speicherung des Gruppenrichtlinienobjekts hat den Vorteil, dass die Einstellungen der Gruppenrichtlinie zentral, nämlich in der Gruppenrichtlinienvorlage im Dateisystem des Domänencontrollers, gespeichert werden. In dem Gruppenrichtliniencontainer werden lediglich Verweise auf die Gruppenrichtlinienvorlage gespeichert. Beim Replizieren der Gruppenrichtliniencontainer werden demnach keine Konfigurationsdaten, sondern nur die Verweise aktualisiert.

Ist z. B. für ein Benutzerkonto eine Gruppenrichtlinie EINSCHRÄNKUNG eingerichtet worden und der entsprechende Benutzer meldet sich am System an, dann erhält der Client eine Liste der Gruppenrichtlinien, die auf den Benutzer wirken, in diesem Fall den Hinweis auf den Gruppenrichtliniencontainer der Gruppenrichtlinie EINSCHRÄNKUNG im Active Directory. Dieser wiederum verweist auf den Pfad der Gruppenrichtlinienvorlage (der Gruppenrichtlinie EINSCHRÄNKUNG) im Dateisystem. Dort werden dann die konfigurierten Einstellungen ausgelesen.

Gibt es mehrere Domänencontroller, so werden die Gruppenrichtliniencontainer auf die anderen Domänencontroller repliziert. Anhand von Versionsnummern, die sowohl als Attribut aus dem Gruppenrichtliniencontainer als auch aus der Datei GPT.ini der Gruppenrichtlinienvorlage ausgelesen und verglichen werden können, wird sichergestellt,

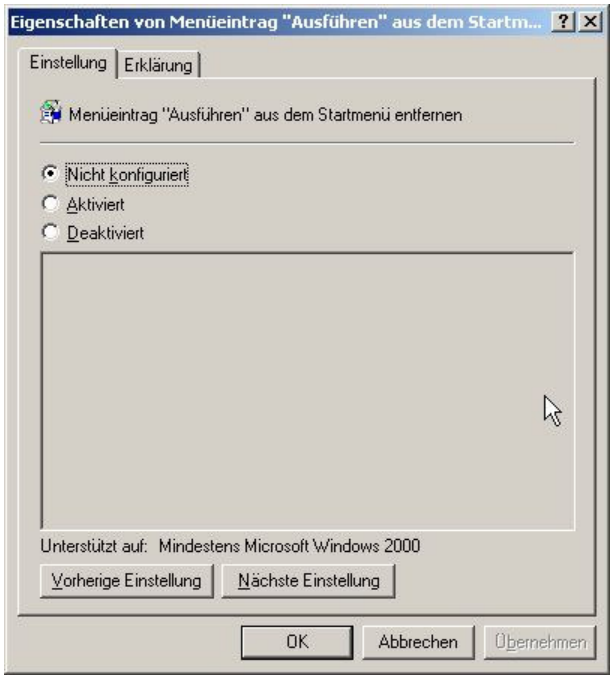
- dass der Gruppenrichtliniencontainer mit der aktuellsten Versionsnummer zu der entsprechenden Gruppenrichtlinienvorlage verweist und
- dass die Gruppenrichtlinienobjekte eines Domänencontrollers synchron sind.

Das Tool GPOTool.exe kann auf dem Domänencontroller eine Konsistenzprüfung der Versionsnummern von Gruppenrichtliniencontainern und Gruppenrichtlinienvorlagen durchführen und bei Inkonsistenzen auf den Fehler hinweisen (siehe Kapitel 11.2).

Adm-Dateien

Die adm-Dateien werden zur Darstellung der konfigurierbaren Einstellungen von Richtlinien in den ADMINISTRATIVEN VORLAGEN der Computer- bzw. Benutzerkonfiguration einer Gruppenrichtlinie benötigt. Mit ihrer Hilfe können Registrierungsschlüssel durch Gruppenrichtlinien zentral verwaltet werden.

Die Abbildung unten zeigt beispielsweise die Informationen zu der Richtlinie MENÜEINTRAG „AUSFÜHREN“ AUS DEM STARTMENÜ ENTFERNEN, die in der Vorlagendatei system.adm gespeichert sind.



Darstellung der Informationen der adm-Datei

Die adm-Dateien stellen sich als einfache Textdateien dar, die Informationen enthalten über

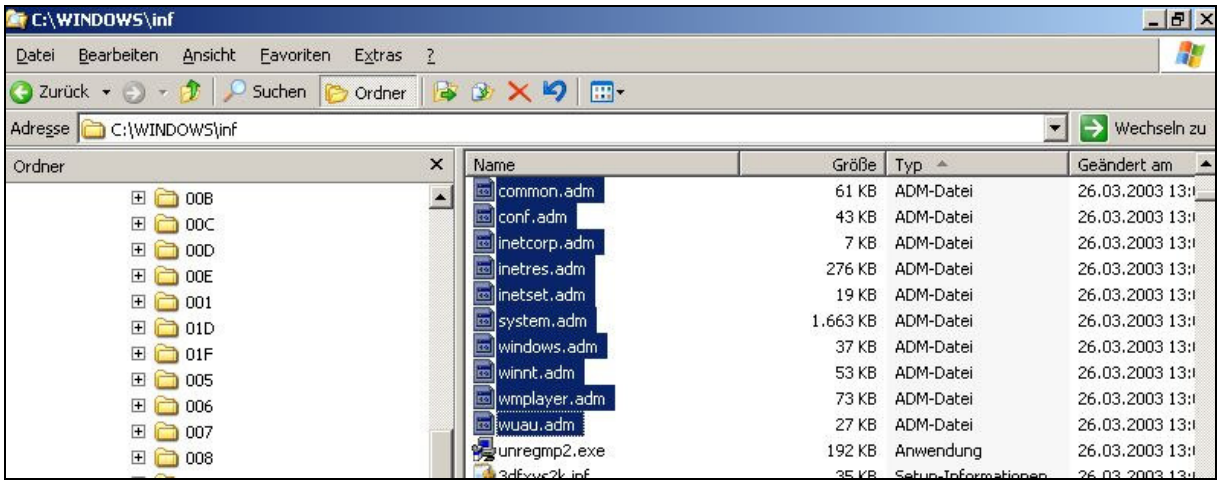
- den Pfad in der Registrierungsdatenbank, in der die entsprechende Einstellung konfiguriert werden kann,
- Optionen oder Einschränkungen für die Werte der jeweiligen Einstellungen,
- Kontrollkästchen, Eingabefelder und andere Methoden für die Parametereingabe,
- einen Standardwert, der ggf. angezeigt werden soll,
- einen Hilfetext zu den einzelnen Einstellungen und
- die Windows-Versionen, die die jeweilige Einstellung unterstützen.

Wird der Knoten ADMINISTRATIVE VORLAGEN beim Arbeiten im Gruppenrichtlinien-Editor erweitert und eine Richtlinie aufgerufen, dann werden die Informationen aus der adm-Datei ausgelesen und entsprechend dargestellt (siehe Abbildung oben).

Bei der Konfiguration der Richtlinie kann zwischen drei Möglichkeiten gewählt werden (siehe auch Kapitel 7.2):

- NICHT KONFIGURIERT: Diese Richtlinie hat keinen Einfluss auf die Benutzer- bzw. Computerkonten dieser Verwaltungseinheit. Wenn sie auf einer übergeordneten Ebene schon konfiguriert wurde, wird sie standardmäßig vererbt und übernommen.
- AKTIVIERT: Die Einstellungen werden für die betreffenden Benutzer- bzw. Computerkonten dieser Verwaltungseinheit übernommen und in die Registrierungsdatenbank des betroffenen Computers übernommen. Wenn die Richtlinie auf einer übergeordneten Ebene schon konfiguriert wurde, wird sie standardmäßig überschrieben.
- DEAKTIVIERT: Die Einstellungen werden für die betreffenden Benutzer- bzw. Computerkonten dieser Verwaltungseinheit **nicht** übernommen und bei Bedarf aus der Registrierungsdatenbank des betroffenen Computers gelöscht. Das bedeutet: Wenn die Richtlinie auf einer übergeordneten Ebene schon konfiguriert wurde, wird sie standardmäßig überschrieben.

Microsoft stellt für die unterschiedlichen Betriebssystemversionen jeweils einen definierten Satz von adm-Dateien zur Verfügung. Sie befinden sich standardmäßig in dem Verzeichnis <Stammverzeichnis:\Windows\inf> (siehe folgende Abbildung).



Richtlinienvorlagen im inf-Verzeichnis

Für das Betriebssystem Windows 2003 werden standardmäßig folgende adm-Dateien bereitgestellt:

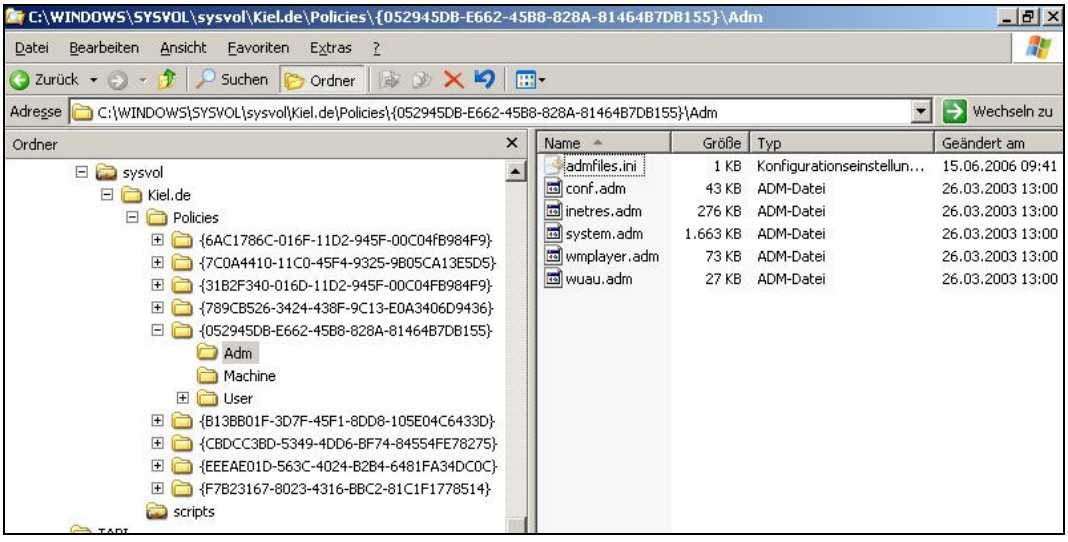
- **Common.adm:** Diese Vorlage enthält Einstellungen für das System des Betriebssystems Windows NT 4.0 und ist nur für die Ausführung mit poledit.exe gedacht.
- **Conf.adm:** Diese Vorlage stellt Richtlinien für NetMeeting (Erweiterung des Internet Explorers für Audio/Videoübertragung) zur Verfügung.
- **Inetcorp.adm:** Diese Vorlage enthält Einstellungen für den Internet Explorer und ist nur für die Ausführung mit poledit.exe gedacht.
- **Inetres.adm:** Diese Vorlage beinhaltet die Richtlinien für den Internet Explorer ab dem Betriebssystem Windows 2000.
- **Inetset.adm:** Diese Vorlage enthält spezielle Einstellungen für den Bereich Internet Explorer-Wartung.
- **System.adm:** Diese Vorlage enthält Einstellungen für das System und stellt die meisten Richtlinien bereit.
- **Windows.adm:** Diese Vorlage enthält Einstellungen für das System von Betriebssystemen 9x und ist nur für die Ausführung mit poledit.exe gedacht.
- **Winnt.adm:** Diese Vorlage enthält Einstellungen für die Konfiguration des Betriebssystems Windows NT 4.0 und ist nur für die Ausführung mit poledit.exe gedacht.
- **Wmplayer.adm:** Diese Vorlage beinhaltet Richtlinien für den Windows Media Player.
- **Wuau.adm:** Diese Vorlage enthält Einstellungen für Windows Update-Dienste, die nur für die Computerkonfiguration verwendet werden können.

Die Vorlagedateien Common.adm, Inetcorp.adm, Windows.adm und Winnet.adm beinhalten Registrierungsschlüssel, die nicht mit den Betriebssystemen Windows 2000, Windows XP und Windows Server 2003 kompatibel sind. Sie sollten diese Vorlagedateien nur nutzen, wenn Sie die entsprechenden Richtlinien für die Betriebssysteme Windows 9x und Windows NT 4.0 mit Hilfe von Gruppenrichtlinien zur Verfügung stellen müssen.

Zusätzlich zu dem vordefinierten Satz können weitere adm-Dateien für Windows-Komponenten oder Microsoft-Software, z. B. Microsoft Office, hinzugefügt werden. Diese können im Gruppenrichtlinien-Editor importiert werden (siehe auch Kapitel 7.4). Neben der Möglichkeit, vorgefertigte adm-Dateien in die Gruppenrichtlinie zu importieren, können diese auch selbst erstellt werden. Hierfür sind jedoch vertiefte Systemkenntnisse erforderlich.

Die Vorlagedateien finden sich nur im inf-Verzeichnis des Domänencontrollers. Jedes Mal, wenn eine neue Gruppenrichtlinie erstellt und im Bereich der ADMINISTRATIVEN VORLAGEN bearbeitet wird, dann werden die Standardvorlagen aus dem inf-Verzeichnis in den Unterordner ADM der Gruppenrichtlinienvorlage kopiert (siehe folgende Abbildung).

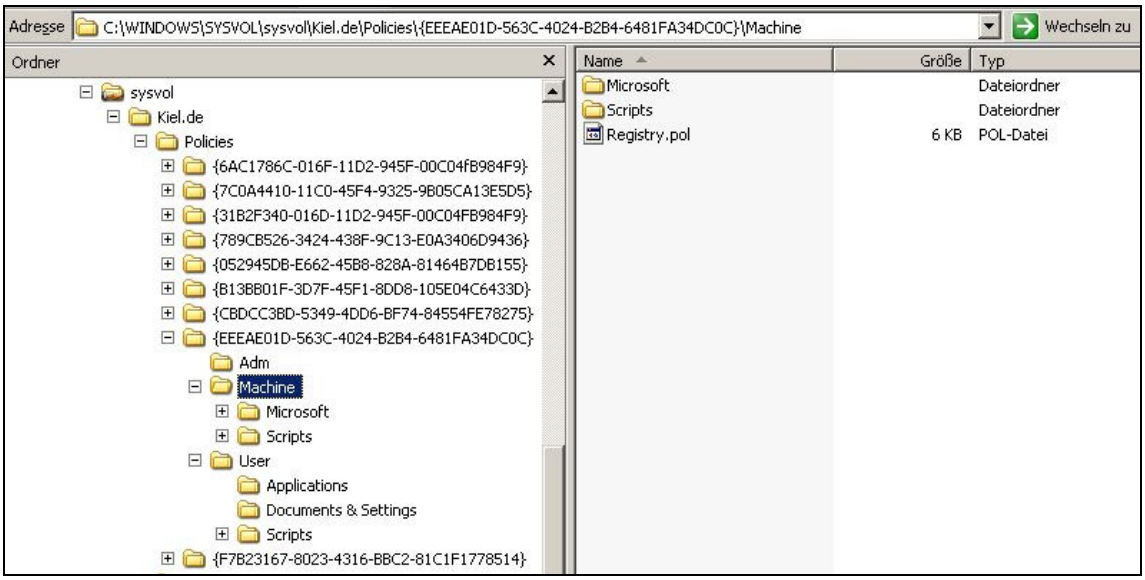
Bei dem Betriebssystem Windows 2000/2003 werden standardmäßig nicht alle Vorlagendateien aus dem Verzeichnis <Stammverzeichnis:\Windows\inf> in den Unterordner der Gruppenrichtlinienvorlage kopiert. Alle Vorlagedateien, die die Betriebssysteme 9x und NT 4.0 betreffen, werden zunächst ignoriert und müssen bei Bedarf nachträglich in die Gruppenrichtlinienvorlage importiert werden.



Unterordner ADM der Gruppenrichtlinienvorlage

Registry.pol-Datei

Neben den adm-Dateien in dem Unterordner Adm einer Gruppenrichtlinienvorlage spielen die Registry-.pol-Dateien in den Unterverzeichnissen Machine und User eine große Rolle. Sie speichern die Registrierungseinstellungen der computer- und benutzerbezogenen Administrativen Vorlagen, die später beim Starten eines Computers bzw. Anmelden eines Benutzers ausgeführt werden.



Registry.pol-Datei in der Gruppenrichtlinienvorlage

Die Unterordner MACHINE und USER einer Gruppenrichtlinienvorlage haben folgende Bedeutung:

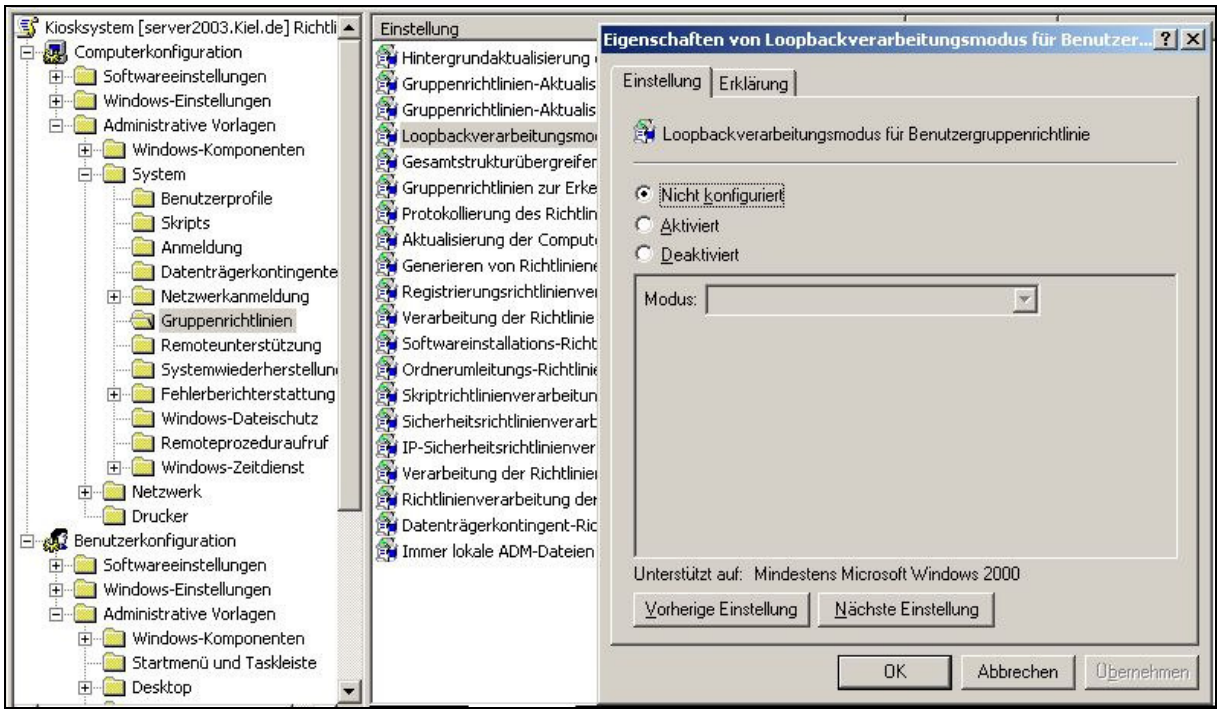
- MACHINE
  Dieser Ordner enthält eine Datei *Registry.pol*. Sie beinhaltet nur die Einstellungen derjenigen Richtlinien, die unter dem Knoten Computerkonfiguration einer Gruppenrichtlinie konfiguriert wurden. Wenn ein Computer gestartet wird und die Verbindung zu der Domäne aufnimmt, wird die Datei *Registry.pol* ausgewertet und in den Abschnitt HKEY_LOCAL_MACHINE der Registrierdatenbank des Computers übernommen. Je nach Konfiguration der entsprechenden ADMINISTRATIVEN VORLAGEN werden weitere Unterordner (MACHINE\APPLICATIONS, MACHINE\DOCUMENTS & SETTINGS, MACHINE\MICROSOFT\WINDOWS NT\SECEDIT, MACHINE\SCRIPTS\SHUTDOWN und MACHINE\SCRIPTS\STARTUP) erzeugt, in denen Informationen zu den entsprechenden Registrierungseinstellungen gespeichert werden.

- USER

  Dieser Ordner enthält ebenfalls eine Datei mit dem Namen *Registry.pol*. Sie enthält nur die Einstellungen derjenigen Richtlinien, die im Knoten Benutzerkonfiguration konfiguriert wurden. Wenn sich ein Benutzer am Client anmeldet, wird die Datei *Registry.pol* ausgewertet und in den Abschnitt HKEY_CURRENT_USER der Registrierdatenbank des Computers übernommen. Auch unterhalb des Ordners USER werden in Abhängigkeit von den Einstellungen der ADMINISTRATIVEN VORLAGEN die Unterordner USER\APPLICATION, USER\DOCUMENTS & SETTINGS, USER\MICROSOFT\REMOTEINSTALL, USER\SCRIPTS\LOGIN und \USER\SCRIPTS\LOGOFF erstellt.

Eine Registry.pol-Datei wird nur erzeugt, wenn Einstellungen in den Richtlinien der computer- bzw. benutzerbezogenen Administrativen Vorlagen konfiguriert wurden. Sind weder in den computer- noch benutzerbezogenen Administrativen Vorlagen Einstellungen vorgenommen worden, findet sich weder im Ordner Machine noch im Ordner User eine Registry.pol-Datei.

9.3 Loopbackverarbeitungsmodus

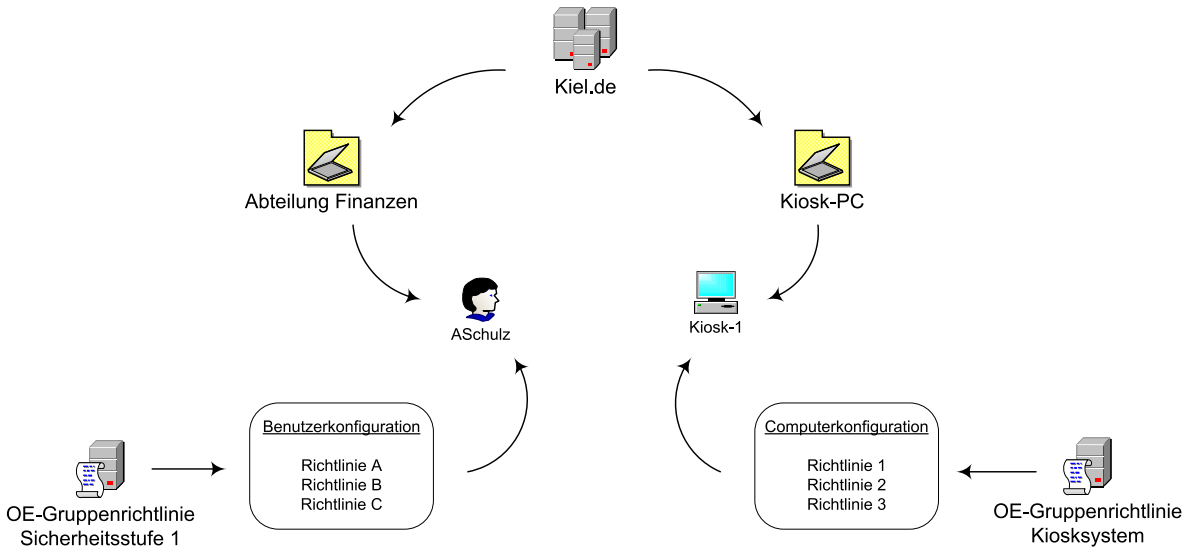


Richtlinie LOOPBACKVERARBEITUNGSMODUS

Die Richtlinie LOOPBACK ist eine spezielle Gruppenrichtlinieneinstellung im Knoten COMPUTERKONFIGURATION\ADMINISTRATIVE VORLAGEN\SYSTEM\GRUPPENRICHTLINIE. Sie kann sicherstellen, dass alle Benutzer, die sich an bestimmten Computern anmelden, über die gleichen Einstellungen verfügen, egal welcher Organisationseinheit sie zugeordnet sind und welche Gruppenrichtlinien mit diesen Organisationseinheiten verknüpft sind.

Die Wirkungsweise dieser Richtlinie soll an einem Beispiel dargestellt werden:

Der Computer KIOSK-1 ist der Organisationseinheit KIOSK-PC zugeordnet (siehe folgende Abbildung). Mit dieser Organisationseinheit ist die Gruppenrichtlinie KIOSKSYSTEM verknüpft. Der Benutzer ASCHULZ ist der Organisationseinheit ABTEILUNG FINANZEN zugeordnet, die mit der Gruppenrichtlinie SICHERHEITSSTUFE 1 verknüpft ist.



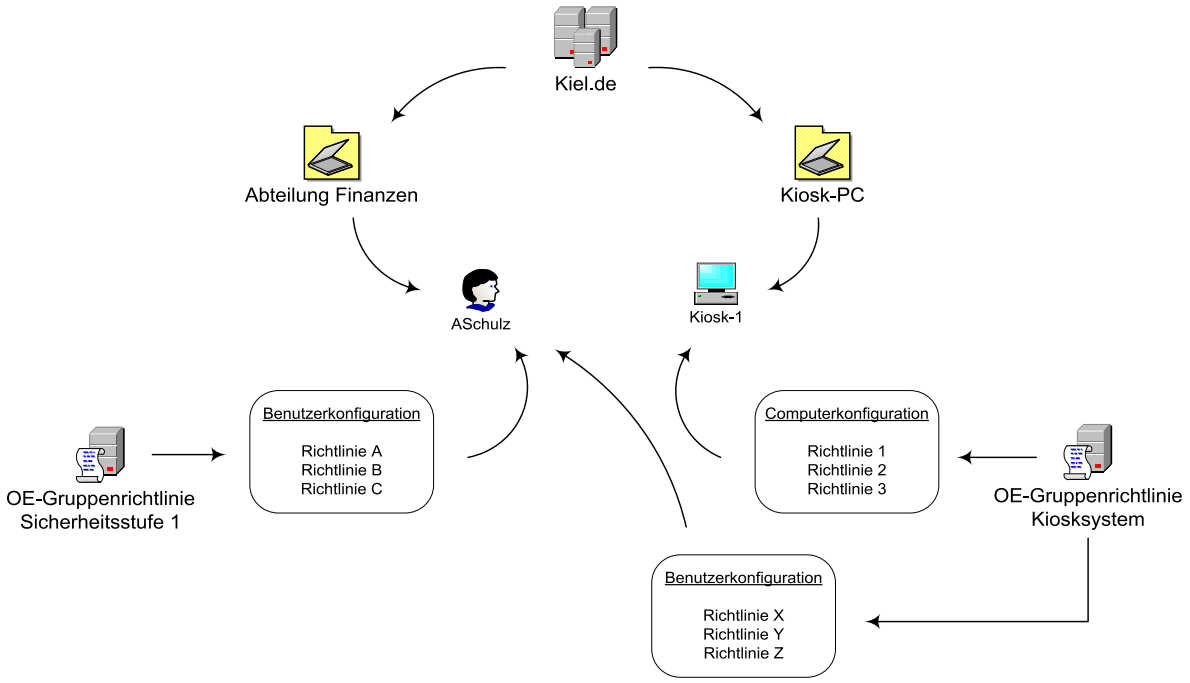
Wenn der Benutzer ASCHULZ den Computer KIOSK-1 startet und sich an ihm anmeldet, werden

- beim Starten des Computers die Richtlinien in der Computerkonfiguration der Gruppenrichtlinie KIOSKSYSTEM und
- beim Anmeldevorgang die Richtlinien in der Benutzerkonfiguration der Gruppenrichtlinie SICHERHEITSSTUFE 1

verarbeitet. Konfigurierte Richtlinien in der Benutzerkonfiguration der Gruppenrichtlinie KIOSKSYSTEM würden nicht berücksichtigt werden, da sich das Benutzerkonto nicht in der entsprechenden Organisationseinheit befindet.

Werden nun allerdings in der Gruppenrichtlinie KIOSKSYSTEM Einstellungen in den Richtlinien der Benutzerkonfiguration vorgenommen und der Loopbackverarbeitungsmodus aktiviert, ändert sich der Ablauf der Richtlinienverarbeitung wie folgt:

- Beim Starten des Computers werden die Richtlinien in der Computerkonfiguration der Gruppenrichtlinie KIOSKSYSTEM verarbeitet.
- Beim Anmeldevorgang des Benutzers ASchulz werden sowohl die Richtlinien in der Benutzerkonfiguration der Gruppenrichtlinie SICHERHEITSSTUFE 1 als auch in der Benutzerkonfiguration der Gruppenrichtlinie KIOSKSYSTEM verarbeitet (obwohl der Benutzer der Organisationseinheit KIOSK-PC nicht zugeordnet ist).



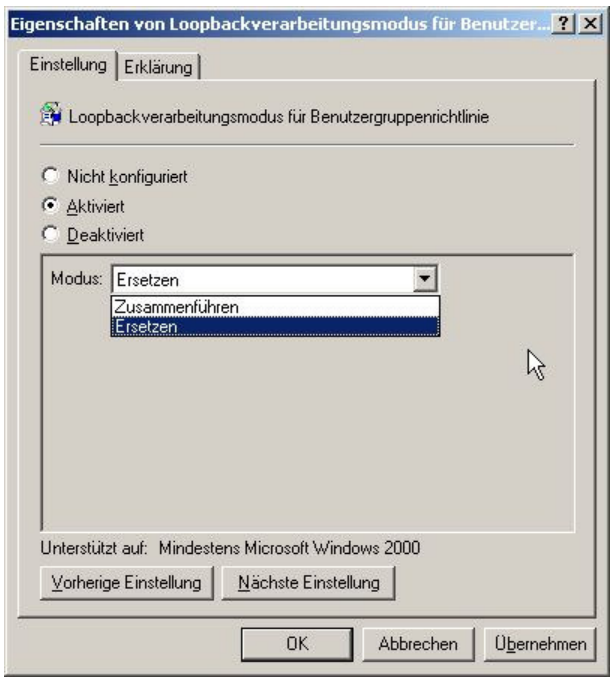
Die Aktivierung des Loopbackverarbeitungsmodus kann in folgenden Fällen sinnvoll sein:

- **Server und Domänencontroller**
  Alle administrativen Benutzerkonten sollen bei der Anmeldung an einem Server oder Domänencontroller über die gleichen Benutzereinstellungen verfügen, egal welcher Organisationseinheit sie zugeordnet sind und welche Einstellungen sie aus den entsprechend verknüpften Gruppenrichtlinien erhalten.
- **Terminal Server und öffentliche Systeme**
  Alle Benutzer, die sich an einem oder mehreren speziellen Systemen anmelden, z. B. an öffentlich zugänglichen PC (Kiosksysteme), sollen grundsätzlich über die gleichen Benutzereinstellungen verfügen.

Für den gezielten Einsatz der Richtlinie LOOPBACKVERARBEITUNGSMODUS kann bei der Konfiguration zwischen zwei Einstellungen gewählt werden:

- Modus ERSETZEN

  Die Einstellungen der Gruppenrichtlinien, die ein Benutzerkonto durch die Zuordnung zu einer bestimmten Organisationseinheit zugewiesen bekommt, werden nicht verarbeitet. Nur die Einstellungen der Richtlinien in der Benutzerkonfiguration der Loopback-Richtlinie werden beim Anmelden des Benutzers berücksichtigt.
  Für das Beispiel oben bedeutet das: Die konfigurierten Einstellungen der Computer- und Benutzerkonfiguration der Gruppenrichtlinie KIOSKSYSTEM werden verarbeitet, die Gruppenrichtlinie SICHERHEITSSTUFE 1 wird ignoriert.



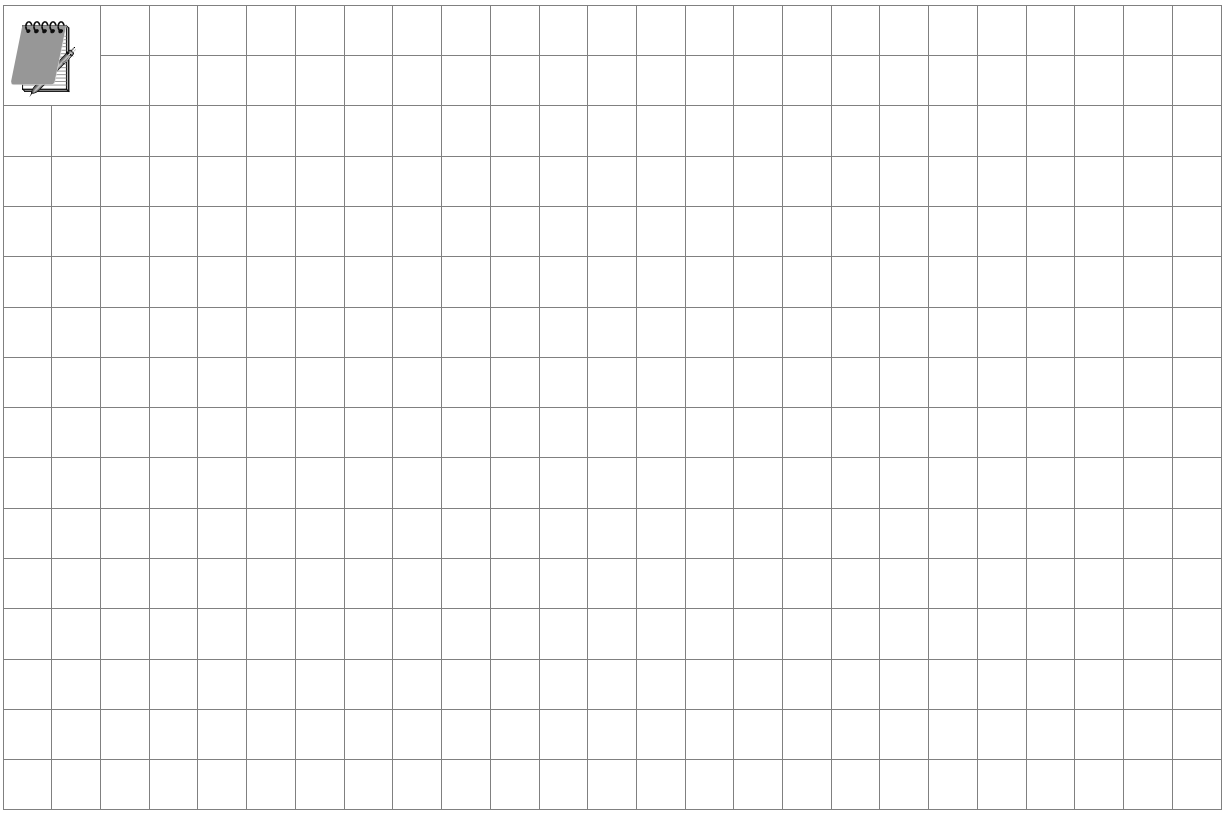
Optionen der Richtlinie LOOPBACKVERARBEITUNGSMODUS

- ModusVERBINDEN
  Die Einstellungen der Gruppenrichtlinien, die ein Benutzer durch die Zuordnung zu einer bestimmten Organisationseinheit zugewiesen bekommt, und die Einstellungen, die er durch die konfigurierten Richtlinien in der Benutzerkonfiguration der Loopback-Richtlinie erhält, werden zusammengeführt. Dabei haben die Einstellungen der Benutzerkonfiguration der Loopback-Gruppenrichtlinie eine höhere Priorität. Für das Beispiel oben bedeutet das: Die konfigurierten Einstellungen der Computer- und Benutzerkonfiguration der Gruppenrichtlinie KIOSKSYSTEM und die konfigurierten Einstellungen der Benutzerkonfiguration der Gruppenrichtlinie SICHERHEITSSTUFE 1 werden berücksichtigt.

Dabei haben die Einstellungen der Benutzerkonfiguration der Gruppenrichtlinie KIOSKSYSTEM eine höhere Priorität.

9.4 Sicherheitscheck

- *Machen Sie sich mit der Systematik der **Gruppenrichtlinienvorlagen (GPT)** im Verzeichnis< Stammverzeichnis:\Windows\SYSVOL\sysvol\<Domänenname>\ Policies> vertraut.*
- *Importieren Sie **Vorlagedateien (adm-Dateien)**, wenn Sie Einstellungen für Windows-Komponenten oder Microsoft Softwareprodukte zentral mit Gruppenrichtlinien zur Verfügung stellen möchten und die Vorlagendateien standardmäßig nicht installiert sind.*
- *Die für **Microsoft Office** verfügbaren ADM-Vorlagen finden Sie in dem entsprechenden Resource Kit.*
- *Konfigurieren Sie die Richtlinie **Loopback**, wenn Sie auf einem Client eine bestimmte Richtlinienkonfiguration erzwingen wollen.*



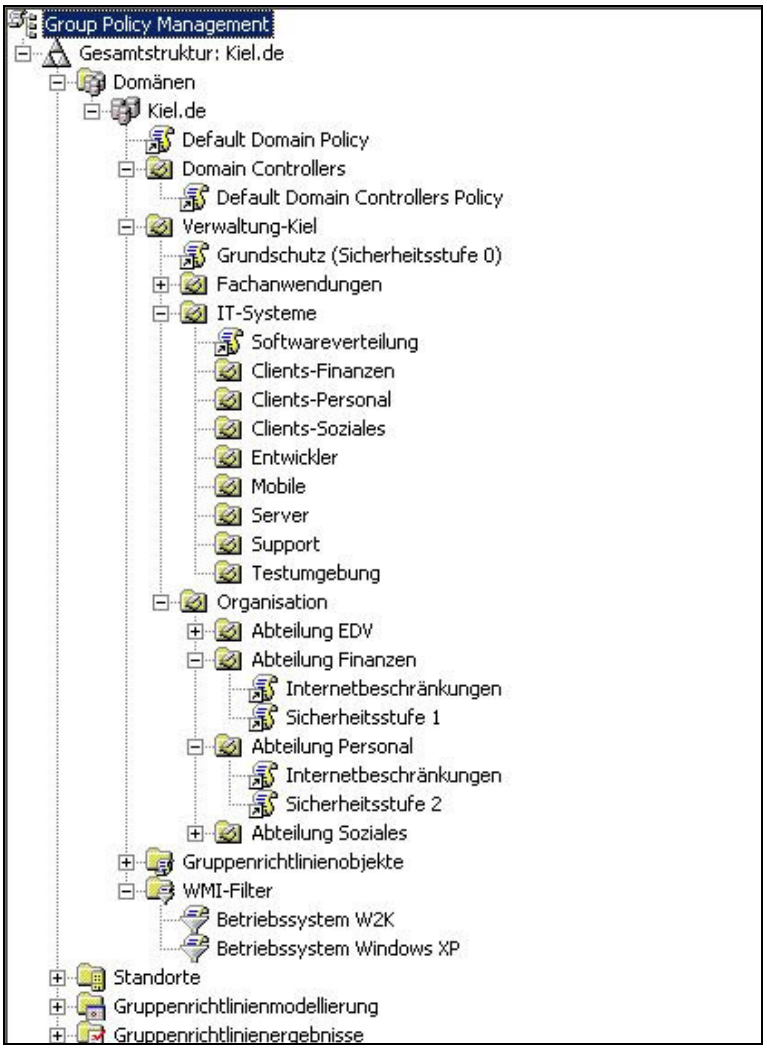
10 Beispielmodell

Dieses Kapitel soll Ihnen

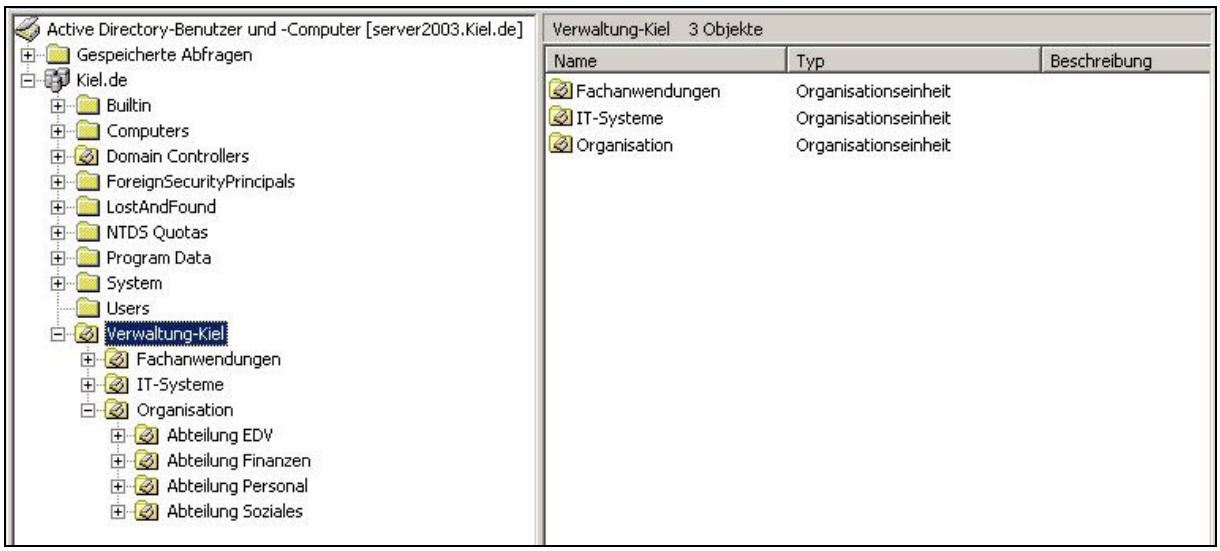
- ein Modell für den strukturierten Einsatz von Gruppenrichtlinien vorstellen.

An dem Beispiel einer fiktiven Organisation soll in diesem Kapitel ein Modell für den strukturierten Einsatz von Gruppenrichtlinien mit einem abgestuften Sicherheitsniveau vorgestellt werden. Zur Erläuterung wird zunächst beschrieben, wie das Active Directory-Design gewählt wird, um die Gruppenrichtlinien differenziert nach Sicherheitsstufen einzusetzen. Danach werden die eingesetzten Gruppenrichtlinien mit den entsprechenden Einstellungen dargestellt.

10.1 Planung des Active Directory-Design



Im ersten Schritt wird die Active Directory-Struktur entwickelt, die den Einsatz der Gruppenrichtlinien nach unterschiedlichen Sicherheitsstufen gewährleisten soll. In diesem Beispiel wird als oberste Ebene unterhalb der Domäne die Organisationseinheit VERWALTUNG-KIEL gewählt. Das hat den Vorteil, dass im Verwaltungsprogramm *Active Directory-Benutzer und -Computer* eine bessere Übersicht gegeben ist und sich die Container nicht mit den Standard-Containern vermischen (siehe Abbildung unten). Weiterhin besteht die Möglichkeit, eine Gruppenrichtlinie auf dieser Ebene zu verknüpfen. Sie betrifft dann alle Benutzer- und Computerkonten, die sich in dieser und allen unterordneten Organisationseinheiten befinden.



Active Directory der Beispielorganisation

Die zweite Ebene wird nach administrativen Gesichtspunkten in die Organisationseinheiten FACHANWENDUNGEN, IT-SYSTEME und ORGANISATION strukturiert.

In der Organisationseinheit FACHANWENDUNGEN werden die Sicherheitsgruppen für die Rechtezuweisung der unterschiedlichen Fachanwendungen erstellt und verwaltet. Der Hintergrund ist eine rein strukturelle Überlegung, Gruppenrichtlinien sollen mit dieser Organisationseinheit nicht verknüpft werden.

In der Organisationseinheit IT-SYSTEME werden die Clients der Organisation gespeichert und verwaltet. Mit dieser Organisationseinheit (oder mit einer der untergeordneten Organisationseinheiten) werden die Gruppenrichtlinien verknüpft, die auf die Computerkonten angewendet werden sollen (Einstellungen im Knoten Computerkonfiguration).

Die Organisationseinheit ORGANISATION wird zusätzlich nach organisatorischen Gesichtspunkten in die Organisationseinheiten ABTEILUNG EDV, ABTEILUNG FINANZEN, ABTEILUNG

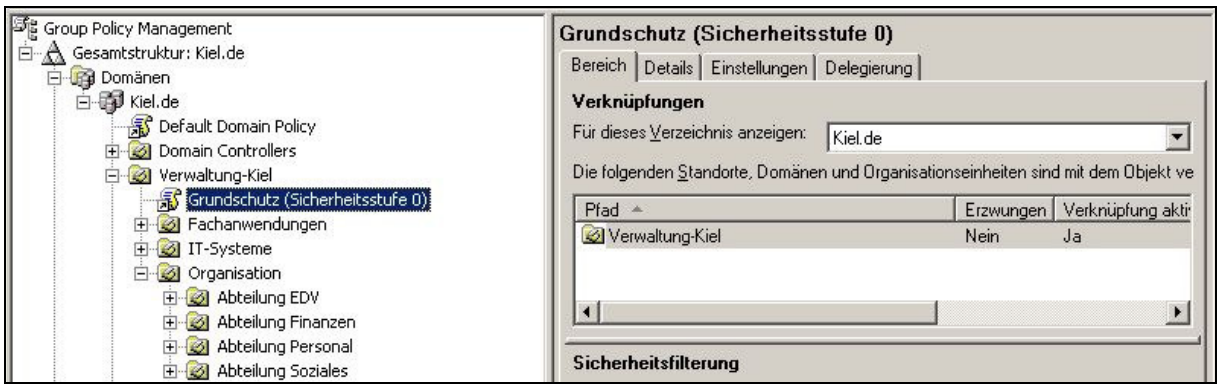
PERSONAL und ABTEILUNG SOZIALES strukturiert. Das hat den Vorteil, dass benutzerbezogene Gruppenrichtlinien (Einstellungen im Knoten Benutzerkonfiguration)

- sowohl mit der Organisationseinheit ORGANISATION verknüpft werden können und dann auf alle Benutzerkonten in dieser und allen untergeordneten Organisationseinheiten angewendet werden,
- als auch mit den einzelnen untergeordneten Organisationseinheiten verknüpft werden können und dann nur auf die Benutzerkonten angewendet werden, die sich in der entsprechenden Organisationseinheit befinden.

Nachfolgend werden die Gruppenrichtlinien sowohl mit den definierten Einstellungen als auch mit der Einbettung in die Active Directory-Struktur beschrieben. Mit der Funktion GRUPPENRICHTLINIENERGEBNISSE ist für jede Gruppenrichtlinie ein Bericht erstellt worden, um sowohl die Einstellungen als auch die korrekte Verarbeitung der Gruppenrichtlinie zu dokumentieren. Die in den nächsten Kapiteln abgebildeten Einstellungen sind über die Funktion BERICHT SPEICHERN dokumentiert worden.

10.2 Grundschutz

Die Gruppenrichtlinien für das Sicherheitsniveau „Grundschutz“ beinhalten Richtlinien, die für die gesamte Domäne bzw. für alle Computer- und Benutzerkonten gelten soll. Hierfür werden die Gruppenrichtlinien *Default Domain Policy* und *Grundschutz (Sicherheitsstufe 0)* eingesetzt, die mit der Domäne bzw. mit der Organisationseinheit VERWALTUNG-KIEL verknüpft sind.



Gruppenrichtlinien *Default Domain Policy* und *Grundschutz (Sicherheitsstufe 0)*

Folgende Anforderungen werden an das Sicherheitsniveau „Grundschutz“ der IT-Systeme definiert:

- Es sollen Kennwort- und Kontorichtlinien für alle Benutzerkonten gelten.
- Die Daten der Benutzer sollen im Ordner Eigene Dateien auf dem Server gespeichert werden.
- Ein Aufruf der Netzwerkumgebung darf nicht möglich sein.
- Systemprogramme dürfen nicht aufgerufen werden.
- Laufwerke (Diskette, CD-ROM, USB-Port) sollen deaktiviert werden.
- Die Richtlinien für den Grundschutz sollen mit Ausnahme der Kennwort- und Kontorichtlinien nicht für die administrativen Benutzerkonten gelten.

Default Domain Policy

Computerkonfiguration (Aktiviert)

Windows-Einstellungen

Sicherheitseinstellungen

Kontorichtlinien/Kennwortrichtlinien

Richtlinie	Einstellung
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen\ngespeicherte Kennwörter	10 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	90 Tage
Minimale Kennwortlänge	5 Zeichen
Minimales Kennwortalter	1 Tag

Kontorichtlinien/Kontosperrungsrichtlinien

Richtlinie	Einstellung
Kontensperrungsschwelle	3 ungültige Anmeldeversuche
Kontosperrdauer	0 Minuten
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten

In der Gruppenrichtlinie *Default Domain Policy* werden ausschließlich die Kennwort- und Kontosperrungsrichtlinien festgelegt. Weitere Einstellungen, die in dieser Gruppenrichtlinie standardmäßig konfiguriert sind, sind nicht geändert worden. Die Gruppenrichtlinie *Default Domain Policy* ist standardmäßig mit der Domäne verknüpft.

Grundschutz (Sicherheitsstufe 0)

Computerkonfiguration (Aktiviert)

Keine Einstellungen definiert

Benutzerkonfiguration (Aktiviert)

Windows-Einstellungen

Ordnerumleitung

Eigene Dateien

Einstellung: Standard (Leitet alle Ordner auf den gleichen Pfad um)

Pfad: \\Server2003\Ablage-EigeneDateien\%USERNAME%\Eigene Dateien

Optionen

Benutzer exklusive Zugriffsrechte für "Eigene Dateien" erteilen	Deaktiviert
Den Inhalt von "Eigene Dateien" an neuen Ort verschieben	Aktiviert
Verhalten bei Entfernen der Richtlinie	Inhalt wiederherstellen

Administrative Vorlagen

Desktop

Richtlinie	Einstellung
Desktopsymbol "Netzwerkumgebung" ausblenden	Aktiviert
Symbol "Arbeitsplatz" vom Desktop entfernen	Aktiviert

Startmenü und Taskleiste

Richtlinie	Einstellung
Menüeintrag "Ausführen" aus dem Startmenü entfernen	Aktiviert
Menüeintrag "Netzwerkverbindungen" aus dem Startmenü entfernen	Aktiviert
Programme im Menü "Einstellungen" entfernen	Aktiviert
Symbol "Netzwerkumgebung" aus dem Startmenü entfernen	Aktiviert
Symbol "Programmzugriff und -standards" aus dem Startmenü entfernen	Aktiviert
Verknüpfungen und Zugriff auf Windows Update entfernen	Aktiviert

Systemsteuerung

Richtlinie	Einstellung
Zugriff auf die Systemsteuerung nicht zulassen	Aktiviert

Windows-Komponenten/Windows Explorer

Richtlinie	Einstellung
Den Menüeintrag "Verwalten" im Windows Explorer-Kontextmenü ausblenden	Aktiviert
Optionen "Netzlaufwerk verbinden" und "Netzlaufwerk trennen" entfernen	Aktiviert
Zugriff auf Laufwerke vom Arbeitsplatz nicht zulassen	Aktiviert
Wählen Sie eine der folgenden Kombinationen	Nur Laufwerke A, B, C und D beschränken

In der Gruppenrichtlinie GRUNDSCHUTZ (SICHERHEITSSTUFE 0) sind folgende Richtlinien im Knoten BENUTZERKONFIGURATION/ADMINISTRATIVE VORLAGEN konfiguriert worden:

- die Ordnerumleitung für EIGENE DATEIEN auf den Server,
- das Ausblendung bzw. die Deaktivierung der Netzwerkumgebung,
- das Entfernen von Funktionen für das Ausführen von Systemprogrammen und
- der Zugriff auf die Laufwerke A: bis D:.

Die Gruppenrichtlinie GRUNDSCHUTZ (SICHERHEITSSTUFE 0) ist mit der Organisationseinheit VERWALTUNG-KIEL verknüpft worden.

*Die Deaktivierung der Laufwerke ist über die Gruppenrichtlinien nur eingeschränkt möglich. Für den USB-Port wird standardmäßig keine Richtlinie angeboten. Für eine flexible Administration und Reglementierung der Laufwerke und Schnittstellen wird empfohlen, eine Sicherheitssoftware, wie z. B. Devicelock, Devicecontrol, Deviceguard einzusetzen (siehe **backUP**-Magazin Nr. 5, Tz. 11.3).*

Die Verknüpfung der Gruppenrichtlinie GRUNDSCHUTZ (SICHERHEITSSTUFE 0) mit der Organisationseinheit VERWALTUNG-KIEL bewirkt, dass die Richtlinien auf alle Benutzerkonten angewendet werden, die dieser oder untergeordneter Organisationseinheiten zugeordnet sind. Darunter können dann auch die administrativen Benutzerkonten fallen (wenn sie den entsprechenden Organisationseinheit zugeordnet sind).

Um diesem Problem aus dem Weg zu gehen, können Sie eine Organisationseinheit anlegen, in die Sie die administrativen Benutzerkonten verschieben. Diese Organisationseinheit wird entweder außerhalb der Vererbungshierarchie der Organisationseinheiten VERWALTUNG-KIEL angelegt oder sie bleibt innerhalb der Vererbungshierarchie und die Vererbung der Richtlinien aus höheren Hierarchieebenen wird deaktiviert (siehe auch Kapitel 5.3 und 6.3).

10.3 Sicherheitsstufe 1

Mit dem Sicherheitsniveau „Sicherheitsstufe 1“ werden die Sicherheitsanforderungen an die IT-Systemumgebung der Organisation erweitert. Die diesem Sicherheitsniveau unterliegenden Benutzerkonten werden dadurch in Bezug auf ihre Funktionalitäten weiter eingeschränkt. Folgende Anforderungen werden festgelegt:

- Fehlerhaftes Anmelden am Client wird auf dem Domänencontroller protokolliert.

- Der Windows Explorer kann nicht aufgerufen werden.
- Die Taskleiste darf nicht geändert werden.
- Die Such- und Hilfefunktion steht nicht zur Verfügung.
- Windows-Standardprogramme dürfen nicht aufgerufen werden.

Zur Umsetzung der Anforderungen des Sicherheitsniveaus „Sicherheitsstufe 1“ werden die Gruppenrichtlinien *Default Domain Controllers Policy* und SICHERHEITSSTUFE 1 eingesetzt.

Default Domain Controllers Policy

Computerkonfiguration (Aktiviert)

Windows-Einstellungen

Sicherheitseinstellungen

Lokale Richtlinien/Überwachungsrichtlinie

Richtlinie	Einstellung
Anmeldeereignisse überwachen	Keine Überwachung
Anmeldeversuche überwachen	Fehlgeschlagen
Kontenverwaltung überwachen	Keine Überwachung
Objektzugriffsversuche überwachen	Keine Überwachung
Prozessverfolgung überwachen	Keine Überwachung
Rechteverwendung überwachen	Keine Überwachung
Richtlinienänderungen überwachen	Keine Überwachung
Systemereignisse überwachen	Keine Überwachung
Verzeichnisdienstzugriff überwachen	Keine Überwachung

Benutzerkonfiguration (Aktiviert)

Keine Einstellungen definiert

In der Gruppenrichtlinie *Default Domain Controllers Policy* werden die Richtlinien zur Überwachung der Anmeldeversuche (*Fehlgeschlagen)* aktiviert. Weitere Einstellungen sind in dieser Gruppenrichtlinie nicht durchgeführt worden. Die Ereignisse bei einem fehlerhaften Anmelden an einem Computer bzw. Client wird im Ereignisprotokoll SICHERHEIT auf dem Domänencontroller protokolliert.

Die Gruppenrichtlinie *Default Domain Controllers Policy* ist standardmäßig mit der Organisationseinheit DOMAIN CONTROLLERS verknüpft.

Diese Einstellung oben gilt für Windows 2000-Domänencontroller. Bei Windows 2003-Domänencontroller sind standardmäßig schon mehrere Überwachungsrichtlinien aktiviert (siehe Kapitel 8.2.2).

Um die restlichen Sicherheitsanforderungen des Sicherheitsniveaus „Sicherheitsstufe 1“ zu realisieren, ist eine zusätzliche Gruppenrichtlinie SICHERHEITSSTUFE 1 erstellt worden. In dieser Gruppenrichtlinie sind Einstellungen der Richtlinien in dem Knoten BENUTZERKONFIGURATION\ADMINISTRATIVE VORLAGEN\STARTMENÜ UND TASKLEISTE vorgenommen worden.

Sicherheitsstufe 1

Computerkonfiguration (Aktiviert)

Keine Einstellungen definiert

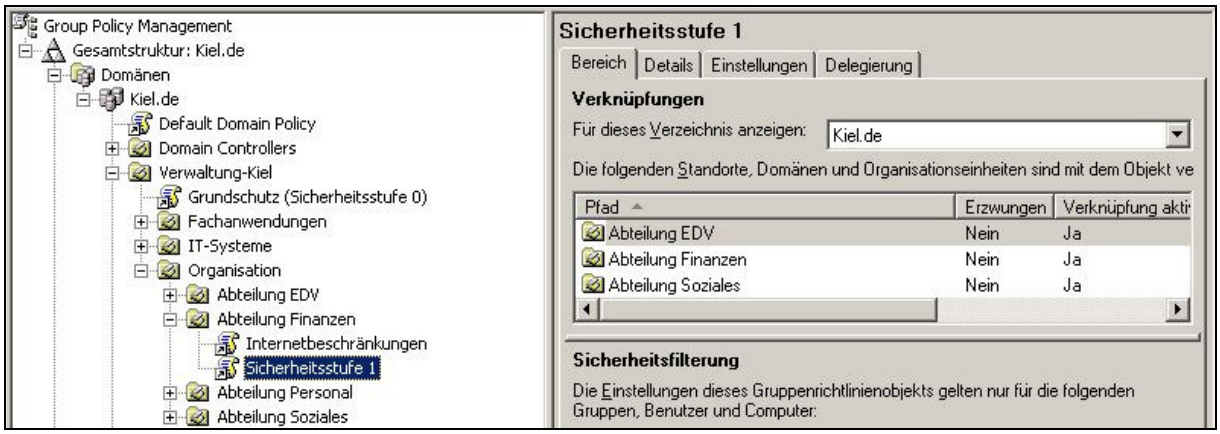
Benutzerkonfiguration (Aktiviert)

Administrative Vorlagen

Startmenü und Taskleiste

Richtlinie	Einstellung
Ändern der Einstellungen für die Taskleiste und das Startmenü verhindern	Aktiviert
Liste "Alle Programme" aus dem Startmenü entfernen	Aktiviert
Menüeintrag "Hilfe" aus dem Startmenü entfernen	Aktiviert
Menüeintrag "Suchen" aus dem Startmenü entfernen	Aktiviert
Standardprogrammgruppen aus dem Startmenü entfernen	Aktiviert
Zugriff auf Kontextmenüs für die Taskleiste deaktivieren	Aktiviert

Die Gruppenrichtlinie SICHERHEITSSTUFE 1 ist mit den Organisationseinheiten verknüpft worden, denen die Benutzerkonten zugewiesen sind, auf die die Richtlinien wirken sollen. In diesem Beispiel (siehe folgende Abbildung) werden die Einstellungen der Gruppenrichtlinie SICHERHEITSSTUFE 1, z. B. auf die Benutzerkonten der Organisationseinheit ABTEILUNG FINANZEN, angewendet.



Gruppenrichtlinie *Sicherheitsstufe 1*

10.4 Sicherheitsstufe 2

Das Sicherheitsniveau „Sicherheitsstufe 2“ erhöht die Sicherheitsanforderungen der „Sicherheitsstufe 1“. Das bedeutet, dass für Benutzerkonten im Bereich des Sicherheitsniveaus „Sicherheitsstufe 2“ sowohl die Richtlinien für die Sicherheitsstufe 1 als auch die Richtlinien für die Sicherheitsstufe 2 angewendet werden.

Folgende Anforderungen werden in der Sicherheitsstufe 2 ergänzend festgelegt:

- Es dürfen nur die Anwendungen Microsoft Word und Excel ausgeführt werden.

Sicherheitsstufe 2

Computerkonfiguration (Aktiviert)

Keine Einstellungen definiert

Benutzerkonfiguration (Aktiviert)

Administrative Vorlagen

Startmenü und Taskleiste

Richtlinie	Einstellung
Ändern der Einstellungen für die Taskleiste und das Startmenü verhindern	Aktiviert
Liste "Alle Programme" aus dem Startmenü entfernen	Aktiviert
Menüeintrag "Hilfe" aus dem Startmenü entfernen	Aktiviert
Menüeintrag "Suchen" aus dem Startmenü entfernen	Aktiviert
Standardprogrammgruppen aus dem Startmenü entfernen	Aktiviert
Zugriff auf Kontextmenüs für die Taskleiste deaktivieren	Aktiviert

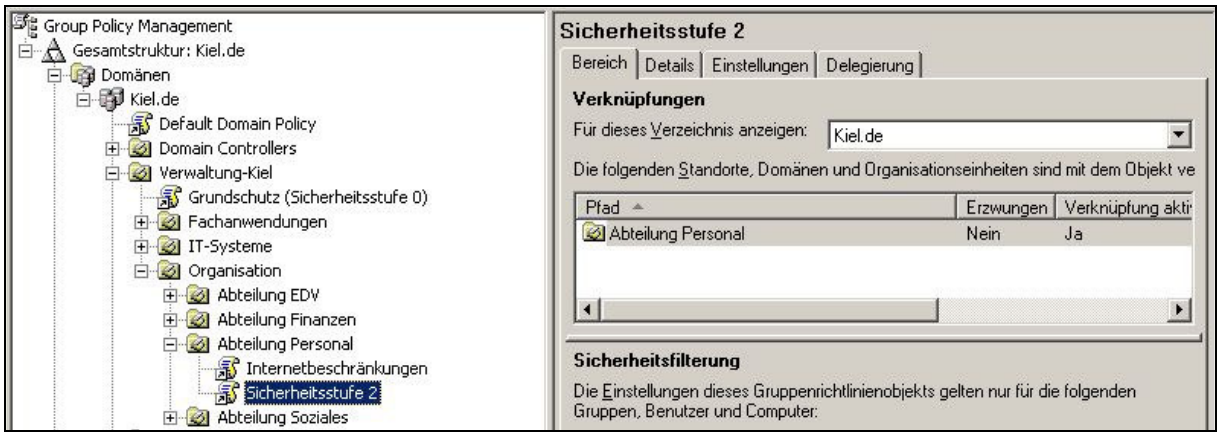
System

Richtlinie	Einstellung

Nur zugelassene Windows-Anwendungen ausführen	Aktiviert
Liste der zugelassenen Anwendungen	
Excel.exe	
Winword.exe	

Zur Umsetzung der Anforderungen des Sicherheitsniveaus „Sicherheitsstufe 2“ ist die Gruppenrichtlinie SICHERHEITSSTUFE 2 erstellt, konfiguriert und mit den Organisationseinheiten verknüpft worden, denen die Benutzerkonten zugewiesen sind, auf die die Richtlinien wirken sollen. In diesem Beispiel (siehe Abbildung unten) werden die Einstellungen der Gruppenrichtlinie SICHERHEITSSTUFE 2, z. B. auf die Benutzerkonten der Organisationseinheit ABTEILUNG PERSONAL, angewendet.

Die Einschränkung zur Ausführung von Windows-Anwendungen kann über die RICHTLINIEN FÜR SOFTWAREEINSCHRÄNKUNGEN in dem Knoten WINDOWS-EINSTELLUNGEN\SICHERHEITSEINSTELLUNGEN der Computer- und Benutzerkonfiguration wesentlich differenzierter durchgeführt werden (siehe auch Kapitel 8.2.2).



Gruppenrichtlinie *Sicherheitsstufe 2*

10.5 Internetbeschränkung

In der Organisation ist in einigen Abteilungen die Nutzung des Internetdienstes WWW erlaubt. Der Zugriff erfolgt über den Internet Explorer. Den Benutzern soll es nicht möglich sein, Sicherheitseinstellungen des Internet Explorers verändern zu können.

Internetbeschränkung

Computerkonfiguration (Aktiviert)

Keine Einstellungen definiert

Benutzerkonfiguration (Aktiviert)

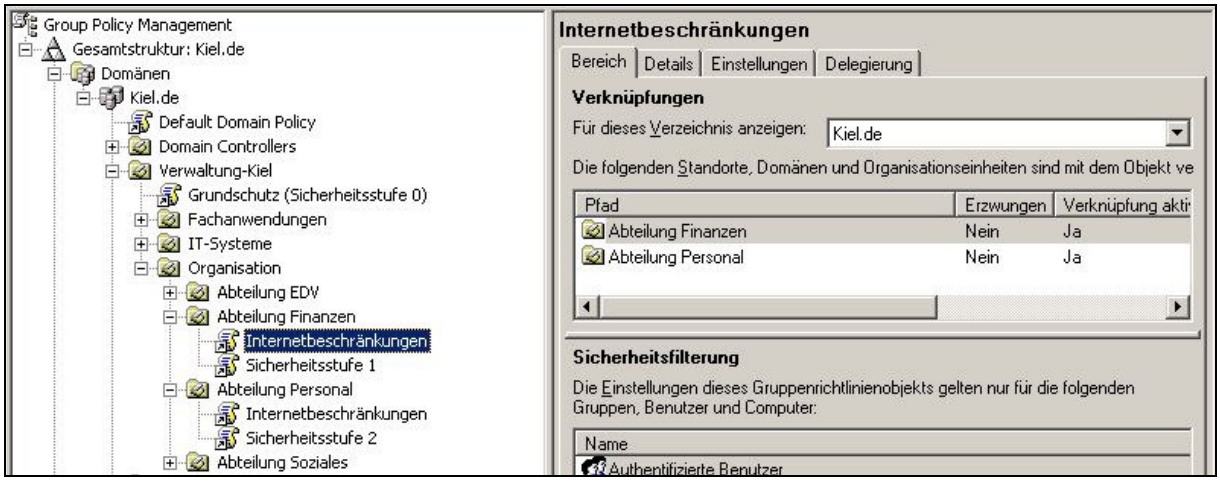
Administrative Vorlagen

Windows-Komponenten/Internet Explorer/Internetsystemsteuerung

Richtlinie	Einstellung
Programmseite deaktivieren	Aktiviert
Seite "Erweitert" deaktivieren	Aktiviert
Sicherheitsseite deaktivieren	Aktiviert
Verbindungsseite deaktivieren	Aktiviert

Für die Umsetzung der Sicherheitsvorgaben ist die Gruppenrichtlinie INTERNETBESCHRÄNKUNG angelegt worden. In ihr sind die Richtlinien in dem Knoten BENUTZERKONFIGURATION\ ADMINISTRATIVE VORLAGEN\WINDOWS-KOMPONENTEN\ INTERNET EXPLORER\INTERNETSYSTEMSTEUERUNG konfiguriert worden, die eine Veränderung von sicherheitskritischen Einstellungen verhindern.

In diesem Beispiel (siehe Abbildung unten) werden die Einstellungen der Gruppenrichtlinie INTERNETBESCHRÄNKUNG, z. B. auf die Benutzerkonten der Organisationseinheit ABTEILUNG PERSONAL und ABTEILUNG FINANZEN, angewendet.



Gruppenrichtlinie *Internetbeschränkung*

Für die Nutzung der Internetdienste sind darüber hinaus eine Reihe weiterer Sicherheitsmaßnahmen erforderlich, die in der Regel zentral über Firewallkomponenten umgesetzt werden.

10.6 Softwareverteilung

Um die Softwareinstallation von Betriebssystem-Updates und Service Packs auf den Clients zu erleichtern, soll diese zentral von einem Softwareverteilungsserver verteilt werden. Das gewährleistet, dass die in den Betriebssystemen aufgedeckten Sicherheitslücken auf allen Clients geschlossen werden (siehe auch Kapitel 8.1).

Softwareverteilung

WMI-Filterung

Name des WMI-Filters	Betriebssystem XP
Beschreibung	Nur auf Windows XP Professional anwenden

Computerkonfiguration (Aktiviert)

Softwareeinstellungen

Zugewiesene Anwendungen

Windows XP Service Pack 2 (1031)

Produktinformationen

Name	Windows XP Service Pack 2 (1031)

Bereitstellungsinformation

Allgemein	**Einstellung**
Bereitstellungsart	Zugewiesen
Bereitstellungsquelle	\\Server2003\Software\ServicePacks\SP2XP\i386\update\update.msi
Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt	Deaktiviert
Erweiterte Bereitstellungsoptionen	**Einstellung**
Sprache beim Bereitstellen dieses Pakets ignorieren	Deaktiviert
Diese 32-Bit-X86-Anwendung für Win64-Computer bereitstellen	Aktiviert
OLE-Klasse und Produktinformationen einbeziehen.	Aktiviert

Erweitert

Updates	**Einstellung**
Vorhandene Pakete aktualisieren	Aktiviert

Pakete, die von diesem Paket aktualisiert werden	**Gruppenrichtlinienobjekt**
Kein	

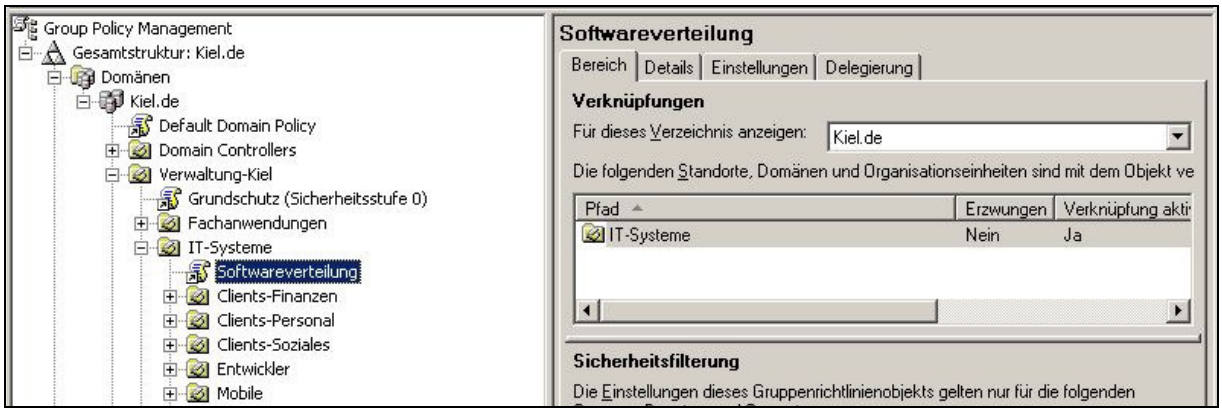
Pakete des aktuellen Gruppenrichtlinienobjekts, durch die dieses Paket aktualisiert wird	Kein

Benutzerkonfiguration (Aktiviert)

Keine Einstellungen definiert

Für die Softwareverteilung ist eine eigene Gruppenrichtlinie SOFTWAREVERTEILUNG angelegt worden. In dem Knoten COMPUTERKONFIGURATION/ SOFTWAREVERTEILUNG ist eine Softwareverteilungs-Richtlinie mit dem Service Pack 2 für Windows XP eingerichtet. Darüber hinaus ist der Gruppenrichtlinie ein WMI-Filter zugewiesen, der vor der Installation des Service Packs prüft, ob sich auf dem Client das Betriebssystem Windows XP befindet. Ist Windows XP nicht auf dem Client installiert, wird die Richtlinie nicht verarbeitet (siehe auch Kapitel 5.4 und 6.3)

In diesem Beispiel (siehe Abbildung unten) ist die Gruppenrichtlinie SOFTWAREVERTEILUNG mit der Organisationseinheit IT-SYSTEME verknüpft worden, deren Unterstrukturen die Computerkonten zugeordnet sind.

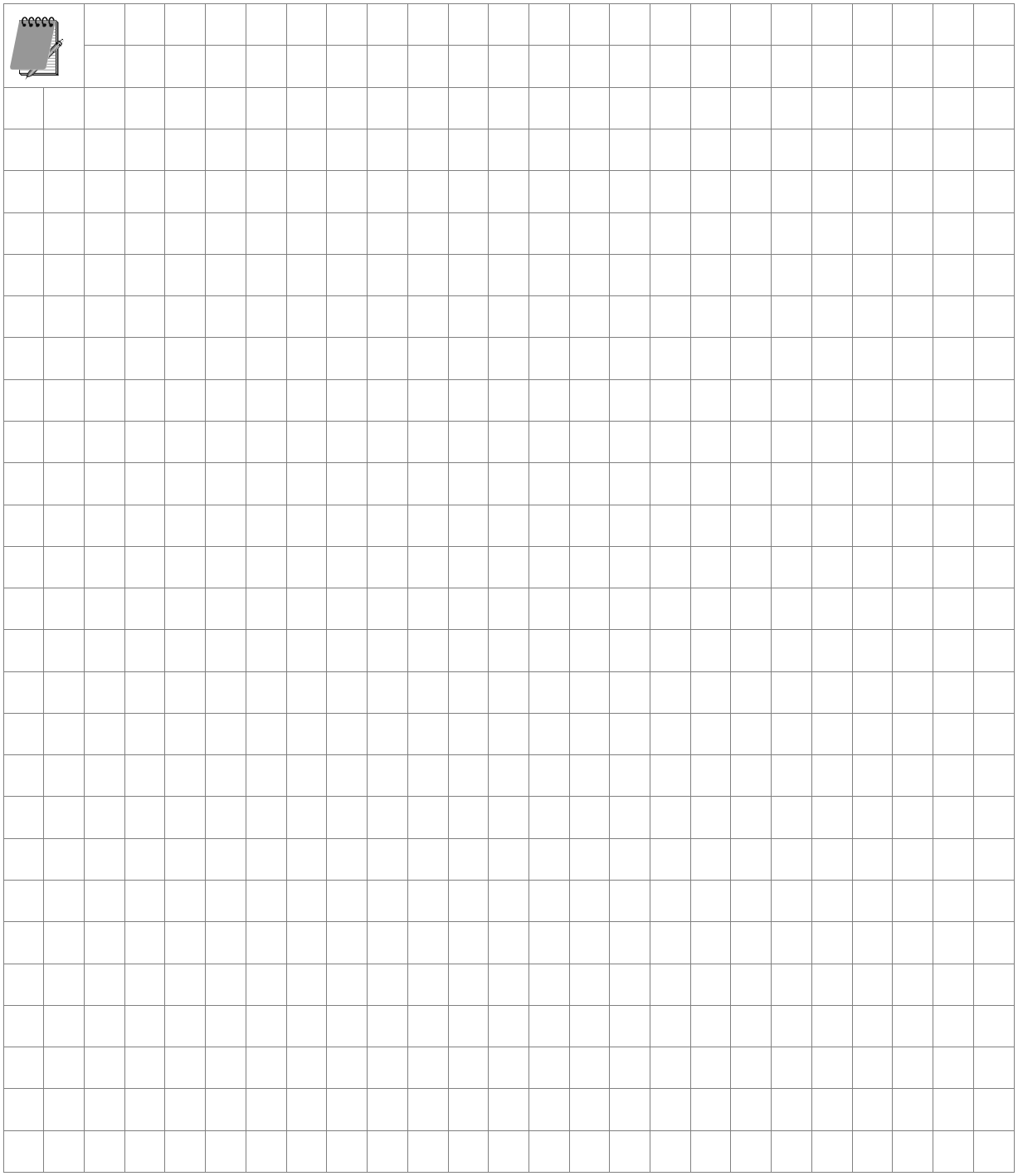


Gruppenrichtlinie *Softwareverteilung*

10.7 Sicherheitscheck

- *Entwickeln Sie für Ihre Organisation auch zunächst ein **Modell** in einer Testumgebung, in der Sie Ihr Active Directory-Design und die entsprechend eingebetteten Gruppenrichtlinien ausgiebig testen können.*
- *Gehen Sie bei der Entwicklung des Modells **schrittweise** vor: Konfigurieren Sie die Gruppenrichtlinien nacheinander und überprüfen Sie regelmäßig, ob die Richtlinien korrekt verarbeitet werden.*

- *Nutzen Sie auch weitere **Informationsquellen** für die Einarbeitung in das Thema Gruppenrichtlinien. Auf der Webseite „Gruppenrichtlinien“ (URL im Anhang) werden z. B. viele praktische Hinweise zur Konfiguration von Gruppenrichtlinien vorgestellt.*

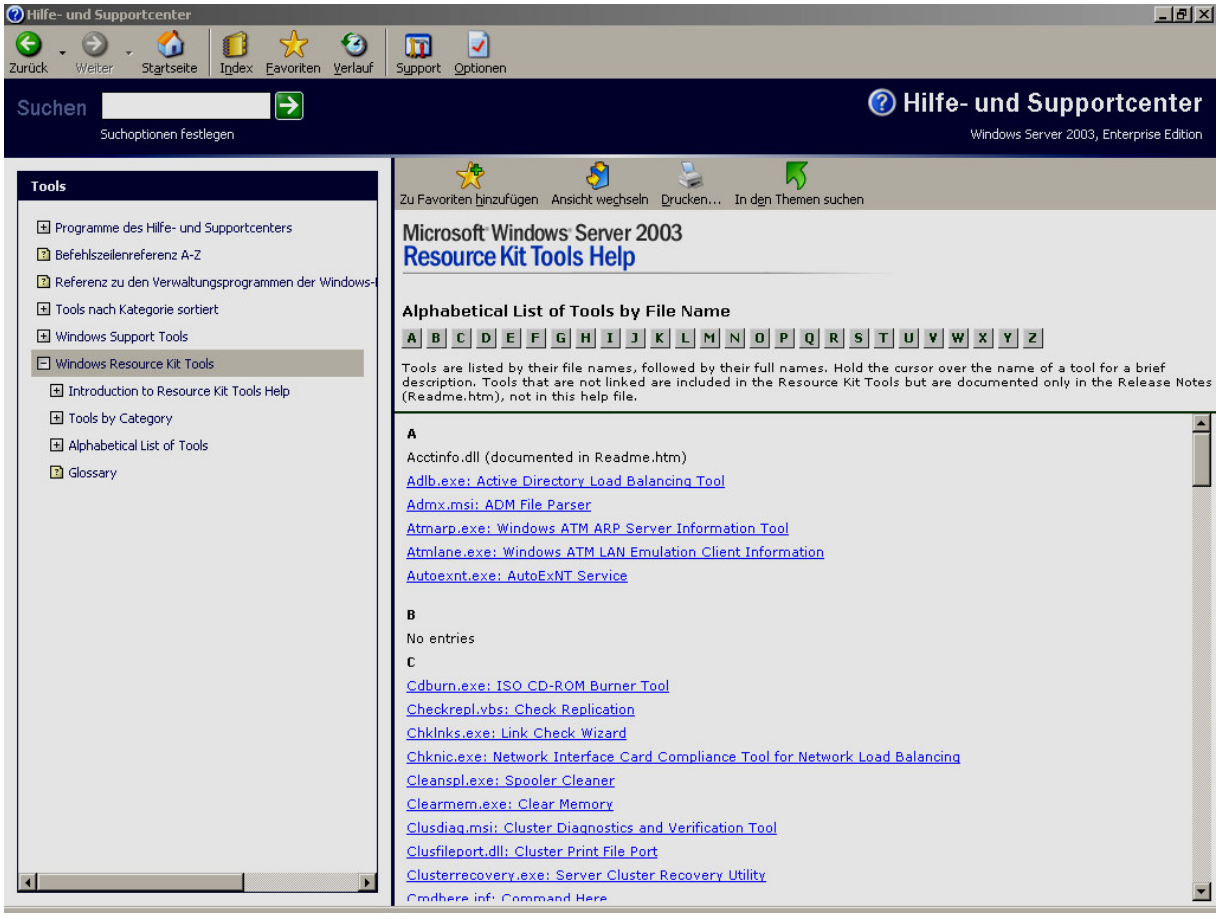


11 Tools

In diesem Kapitel erfahren Sie,

- welche Softwaretools für die Administration der Gruppenrichtlinien hilfreich sind.

Für Windows Server 2003, Windows 2000, Windows XP stehen Resource Kits zur Verfügung, die eine Sammlung nützlicher Tools für die Administration enthalten. Die Resource Kits können von der Microsoftseite (URL im Anhang) kostenlos heruntergeladen werden und sind nur in der englischen Version verfügbar. Die Tools werden in der Online-Hilfe beispielhaft beschrieben. Neben den Resource Kits gibt es zusätzlich die so genannten Support Tools. Sie sind jeweils eine Teilmenge des entsprechenden Resource Kit und befinden sich für die Betriebssysteme Windows Server 2003 / XP auf der Installations-CD im Ordner SUPPORT\TOOLS.



Windows Server 2003 Resource Kit

11.1 GPOTool

Im Resource Kit für Windows Server 2003 befindet sich in Bezug auf die Administration der Gruppenrichtlinienobjekte das Tool *GPOTool.exe*. Damit werden die Gruppenrichtlinienobjekte ausgewertet. Es werden der Name sowie die eindeutige Identifikationsnummer (GUID) und der Status über die Konsistenz des GPO angezeigt.

```
C:\GPOTool.exe
Searching for policies...
Found 4 policies
=====================================================
Policy {2658AB8E-D656-4656-B9E3-AF3C27417A28}
Friendly name: Grundschutz (Sicherheitsstufe 0)
Policy OK
=====================================================
Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Policy
Policy OK
=====================================================
Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Controllers Policy
Policy OK
=====================================================
Policy {6F0F90F7-40AA-4398-A65C-74082A4F3B0C}
Friendly name: Internetbeschränkung
Policy OK

Policies OK
```

GPOTool.exe

11.2 Gpresult

Gpresult zeigt Gruppenrichtlinieneinstellungen und den Richtlinienergebnissatz (Resultant Set of Policy, RSoP) für einen Benutzer oder Computer an. Diese Funktion steht standardmäßig in der Group Policy Management Console (GPMC) im Knoten GRUPPENRICHTLINIENERGEBNISSE zur Verfügung.

gpresult [/s Computer [/u Domäne\Benutzer /p Kennwort]] [/user Zielbenutzername] [/scope {user | computer}] [{/v | /z}]	
/s Computer	Gibt den Namen oder die IP-Adresse eines Remotecomputers an. Die Standardeinstellung ist der lokale Computer.

/u Domäne\Benutzer	Führt den Befehl mit den Kontoberechtigungen des Benutzers aus, der durch *Benutzer* oder *Domäne\Benutzer* angegeben ist. Standardmäßig werden die Berechtigungen des Benutzers verwendet, der aktuell an dem Computer angemeldet ist, der den Befehl ausgibt.
/p Kennwort	Gibt das Kennwort des im Parameter **/**u angegebenen Benutzerkontos an.
/user Zielbenutzer-name	Gibt den Benutzernamen des Benutzers an, dessen RSOP-Daten angezeigt werden sollen.
/scope {user|computer}	Zeigt entweder Ergebnisse für einen Benutzer (user) oder für einen Computer an. Gültige Werte für den Parameter **/**scope sind user oder computer. Wenn der Parameter **/**scope ausgelassen wird, zeigt gpresult sowohl Einstellungen für Benutzer als auch für Computer an.
/v	Gibt an, dass in der Ausgabe ausführliche Richtlinieninformationen angezeigt werden.
/z	Gibt an, dass in der Ausgabe alle verfügbaren Informationen zum Programm Gruppenrichtlinie angezeigt werden. Da dieser Parameter mehr Informationen erzeugt als der Parameter **/v**, sollte die Ausgabe bei Verwendung dieses Parameters in eine Textdatei umlenken (beispielsweise gpresult /z >richtlin.txt) werden.
/?	Zeigt die Hilfe der Parameterbeschreibung an.

```
(Auf der Arbeitsstation) C:\Gpresult /user Meier /v

Betriebssystem Microsoft (R) Windows (R) XP Gruppenrichtlinienergebnis-
Tool v2.0, Copyright (C) Microsoft Corp. 1981-2001

Am 24.05.2005 um 22:41:48 erstellt

RSOP-Ergebnisse für KIEL\meier auf APC : Protokollierungsmodus
-------------------------------------------------------------

Betriebssystemtyp: Microsoft Windows XP Professional
Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Betriebssystemversion: 5.1.2600
Domänenname: KIEL
Domänentyp: Windows 2000
Lokales Profil: E:\Dokumente und Einstellungen\Meier
Langsame Verbindung? Nein
```

```
COMPUTEREINSTELLUNGEN
---------------------

CN=APC,CN=Computers,DC=Kiel,DC=de
Zeit der letzten Gruppenrichtlinienanwendung: 24.05.2005 at 14:40:42
Gruppenrichtlinie wurde angewendet von: server2003.Kiel.de


Angewendete Gruppenrichtlinienobjekte
-------------------------------------

...........
.......
```

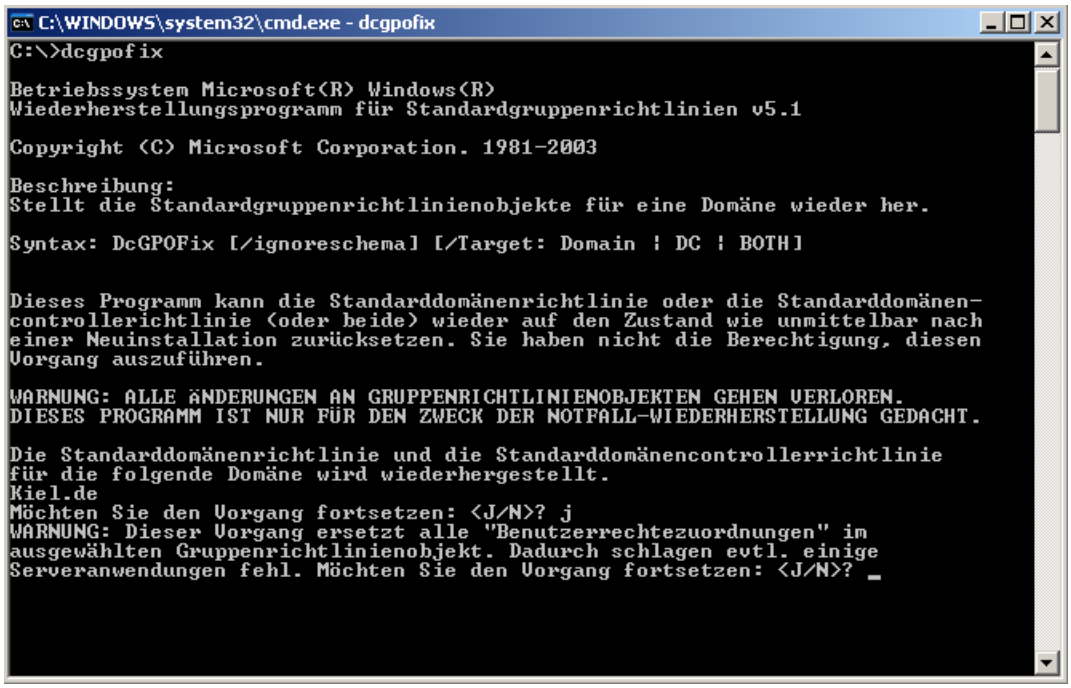
11.3 Dcgpofix

Dcgpofix stellt die Standard-Gruppenrichtlinienobjekte *Default Domain Policy* und *Default Domain Controllers Policy* mit ihrem ursprünglichen Status wieder her, d. h. im Standardstatus nach der Erstinstallation.

*Wenn **dcgpofix** ausführt wird, sind alle Änderungen, die an diesen Gruppenrichtlinienobjekten vorgenommen wurden, verloren.*

Um die Kompatibilität sicherzustellen, sollte nur die dcgpofix.exe verwendet werden, die mit dem aktuellen Betriebssystem installiert wurde.

dcgpofix [/ignoreschema][/target: {domain | dc | both}]	
/ignoreschema	Optional. Ignoriert die Versionsnummer des Active Directory-Schemas.
/target: {domain | dc | both}	Optional. Gibt die Zieldomäne, den Domänencontroller oder beides an. Wenn **/target** nicht angeben wird, verwendet **dcgpofix** standardmäßig den Parameter **both**.



dcgpofix

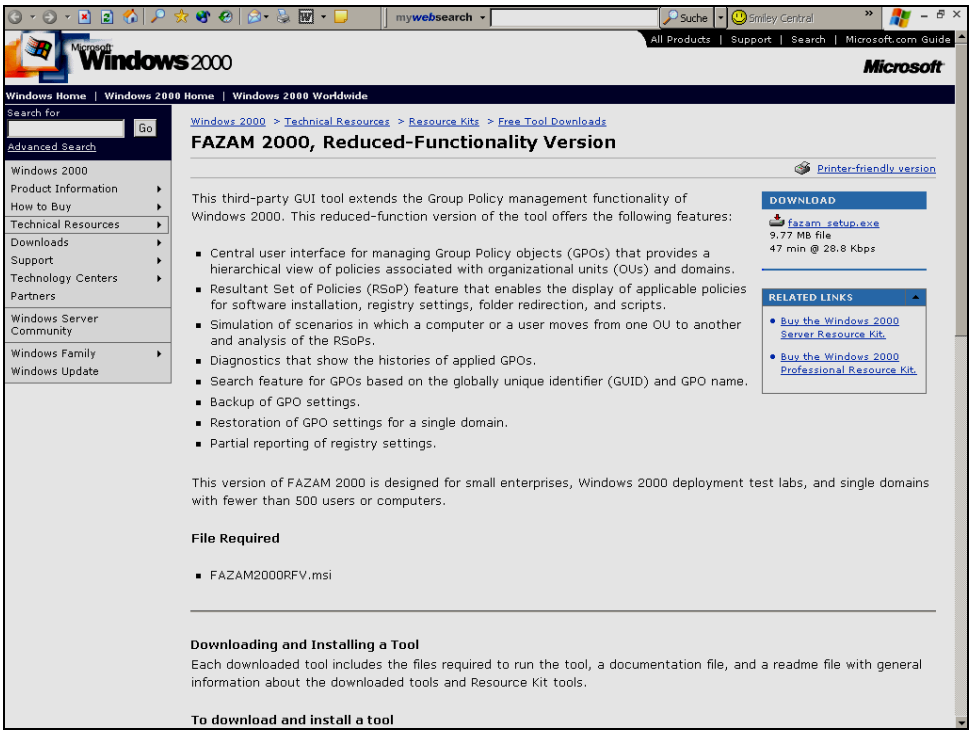
Dcgpofix.exe befindet sich im Ordner <*C:\Windows\Repair*> und lässt sich nur mit einem Benutzerkonto ausführen, das Mitglied der Gruppe DOMÄNEN-ADMINS oder ORGANISATIONS-ADMINS ist.

Folgende Richtlinien werden in den beiden Standard-Gruppenrichtlinien nicht zurückgesetzt:

- *Remoteinstallationsdienste (Remote Installation Services, RIS),*
- *Sicherheitseinstellungen und*
- *verschlüsselndes Dateisystem (Encrypting File System, EFS).*

11.4 FAZAM 2000

FAZAM ist ein eine spezielle Group Policy Management Console der Firma Fullamor, die insbesondere für Windows Server 2000/2003 angeboten wird. Der Funktionsumfang ist im Vergleich zu der von Microsoft entwickelten GPMC für den Windows Server 2003 sehr viel größer. Von der Microsoftseite (URL im Anhang) kann eine Version mit eingegrenztem Funktionsumfang heruntergeladen werden.



FAZAM 2000 Download

Einen Vergleich der Funktionalitäten zeigt die folgende Übersicht, die der Webseite „Gruppenrichtlinien“ entnommen wurde:

Fähigkeiten	**Windows 2000**	**GPMC** (1)	**Fazam 2000 v2**	**Fazam 2000 v3 (GPA)**
GPO Reporting		**x**	**x**	**x**
Backup und Recovery		**x**	**x**	**x**
GPO Replikation		**x**	**x**	**x**
Resultant Set of Policies (RSoP)	**x** (2)	**x** (2)	**x**	**x**
Remote Diagnose und Überwachung		**x** (3)	**x**	**x**
GPO Scripting		**x**	**x**	**x**
GPO Suche		**x**	**x**	**x**
Delegation von GPO Einstellungen			**x**	**x**
GPO Status/Funktionsüberwachung (Health Checking)			**x**	**x**
Heterogene OS Unterstützung			**x**	**x**
Live GPO Management		**x** (4)	**x**	**x**
Offline Änderungen an GPOs				**x**
Deaktivierung der GPO, während der Änderung				**x**
GPO Versionskontrolle				**x**
GPO Wiederherstellungsmöglichkeit (Rollback capability)				**x**

Änderungs-Verfolgung – wer, was, wann und warum				**x**
Systematische Dokumentierung der Änderung				**x**
Zeitliche Trennung von GPO Änderungen und Veröffentlichung				**x**
Copy der GPOs an Non-Trusted Domains		**x**		**x**
Copy der GPOs an Non-Connected Domains				**x**
AD Lockdown/Security				**x**
Beibehaltung der Baseline GPOs zum Vergleich				**x**

(1) GPMC benötigt zur Funktion Windows XP mit SP1, inklusive post SP1 Q326469 und dasn .NET framework.

(2) Benötigt einen Windows 2003 Domänen Controller in einer Windows 2000-Umgebung.

(3) Nur für Windows Server 2003 und Windows XP-Clients.

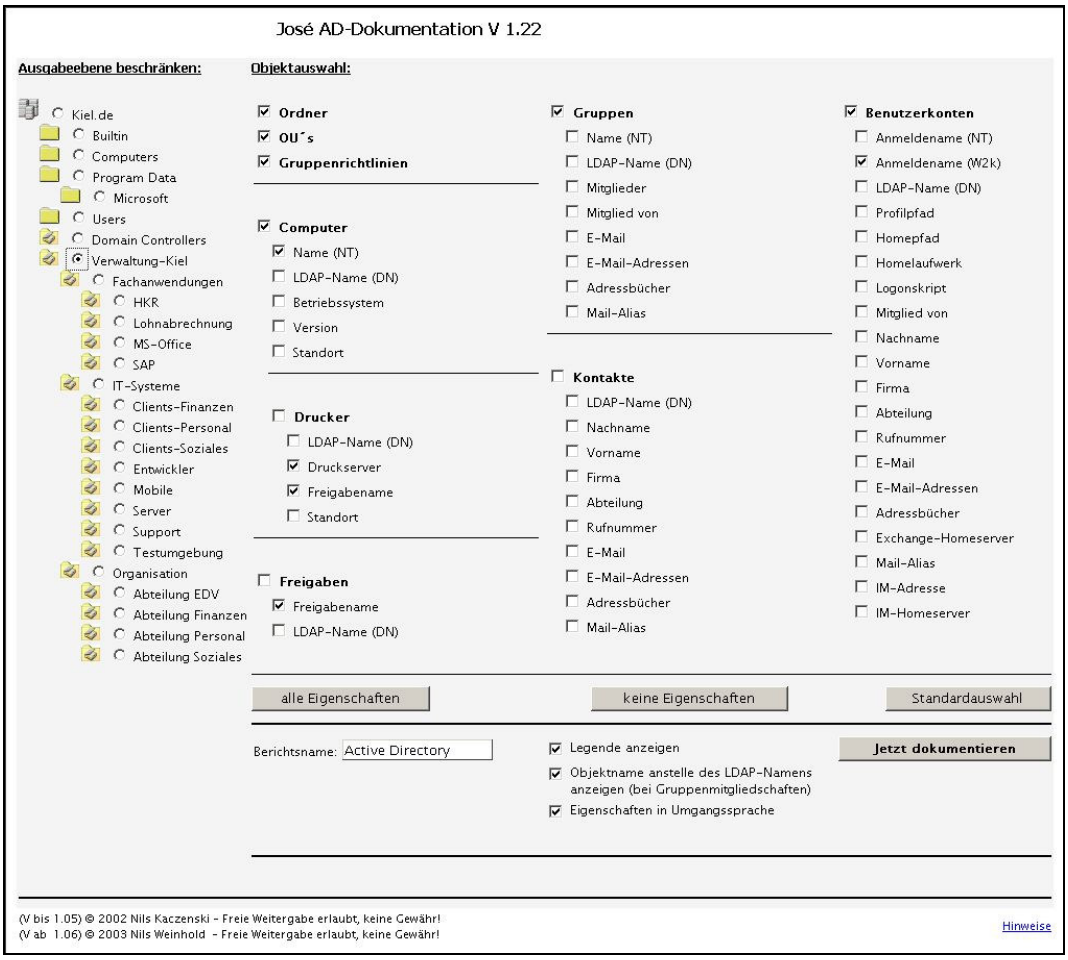
(4) Einige der GPMC-Funktionen stehen unter Windows 2000 Bedingungen evtl. nicht zur Verfügung.

11.5 Active Directory-Dokumentation

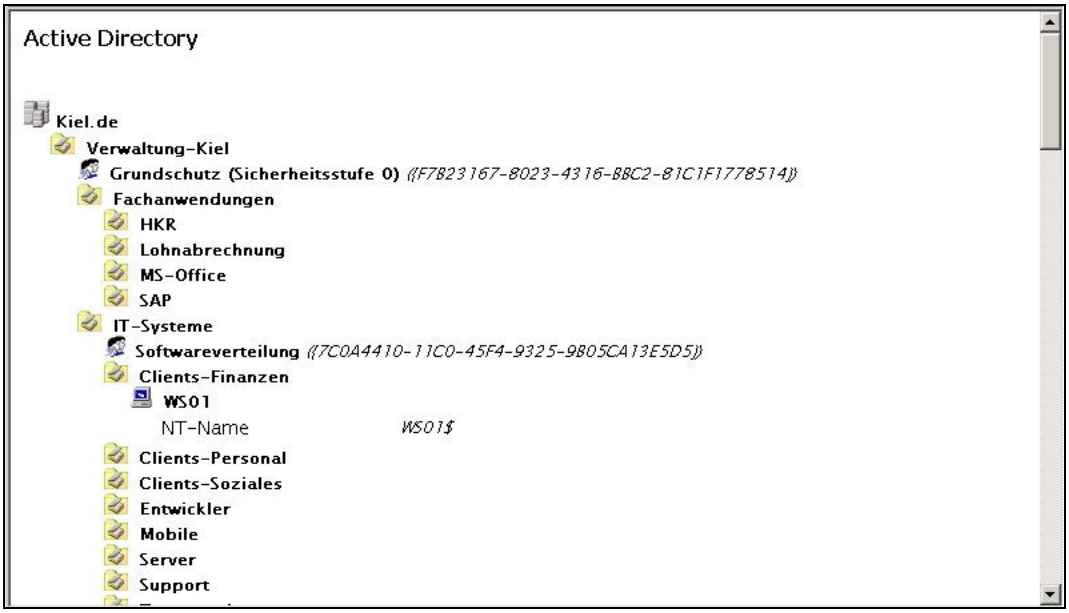
Zum Schluss soll an dieser Stelle noch ein Tool vorgestellt werden, dass das Design des Active Directory in Bezug auf die Organisationseinheiten, Benutzer- und Computerkonten, Gruppenrichtlinien und noch weiteren anderen Objekten untersucht und in Form eines HTML-Berichts auswertet. Der Bericht kann unterschiedlich ausführlich ausgewählt werden, je nachdem

- wie viele Objekte ausgewählt werden,
- wie viele Attribute zu den entsprechenden Objekten ausgewählt werden und
- ob nur eine Organisationseinheit oder das ganze Active Directory dokumentiert werden soll.

Der Bericht berücksichtigt nur den strukturellen Aufbau des Active Directory, nicht aber die Einstellungen der einzelnen Richtlinien (siehe folgende Abbildung). Das Tool ist kostenlos und kann von der Webseite des Entwicklers (URL im Anhang) heruntergeladen werden.



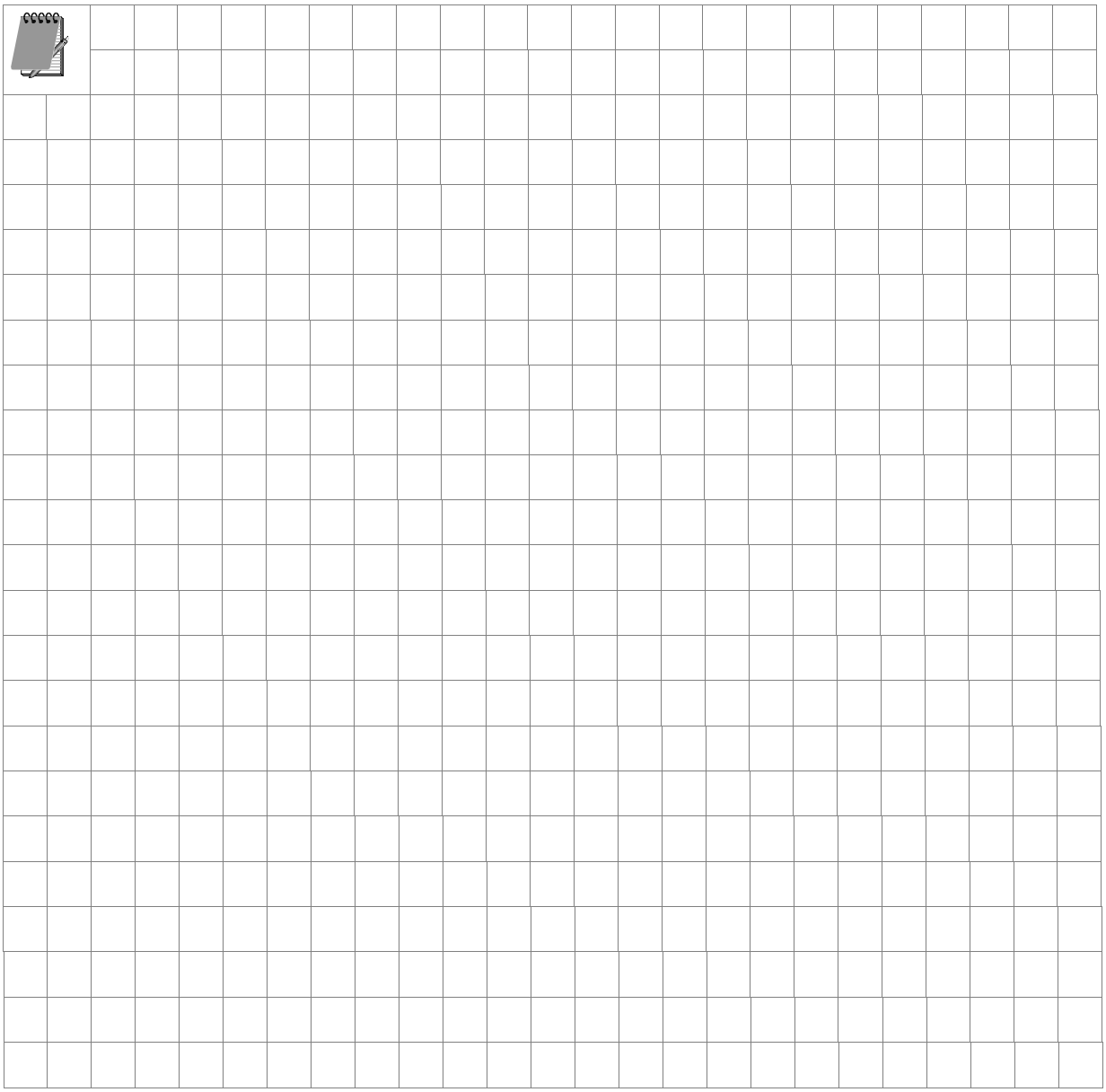
José Active Directory-Dokumentation



Bericht zu José Active Directory-Dokumentation

11.6 Sicherheitscheck

- *Üben Sie mit den Befehlen gpupdate und gpresult, um sich mit der Syntax vertraut zu machen.*
- *Verwenden Sie das Tool dcgpofix nur dann, um die Standard-Gruppenrichtlinien Default Domain Policy und Default Domain Controllers Policy auf die Standardeinstellungen zurückzusetzen.*
- *Verwenden Sie ein geeignetes Tool, um das Active Directory-Design zu dokumentieren.*



Anhang

- Literaturverzeichnis,
- Webseiten,
- Sicherheitsprotokoll-Ereignisse.

Literaturverzeichnis

- Netzwerkverwaltung mit Windows Server 2003 Gruppenrichtlinien
  Microsoft Press

- Windows Server 2003, Migration, Administration, Praxistipps
  Markt und Technik

- Microsoft Windows Server 2003 Terminaldienste
  Microsoft Press

- Microsoft Windows 2000 Active Directory planen und einführen
  Microsoft Press

Webseiten

- **Alles zum Thema Gruppenrichtlinien**
  http://www.gruppenrichtlinien.de
- **Downloadseite von Microsoft**
  http://www.microsoft.com/downloads
- **Hilfsmittel von Microsoft für die Skriptprogrammierung**
  http://www.microsoft.com/technet/scriptcenter
- **Leitfaden zur Verwendung der Gruppenrichtlinien-Verwaltungskonsole (GPMC)**
  http://www.microsoft.com/germany/technet/datenbank/articles/600540.mspx
- **Microsoft Downloadseite für das Tool FAZAM**
  http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/fazam2000-o.asp
- **Zurücksetzen von Benutzerrechten in der Standard-Gruppenrichtlinie einer Domäne**
  http://support.microsoft.com/?kbid=226243
- **MCSE-Forum zu Windows XP/2003**
  http://www.mcseboard.de
- **Windows-Forum**
  http://www.nthelp.de
- **Systemtools für die Administration**
  http://www.systemtools.com
- **Fehler im Ereignisprotokoll analysieren**
  http://www.eventid.net
- **Downloadseite des Tools José Active Directory-Dokumentation**
  http:// www.kaczenski.de

Beschreibung der Sicherheitsprotokoll-Ereignisse

Anmeldeereignisse überwachen

Ereignis-ID	Beschreibung
528	Ein Benutzer hat sich erfolgreich an einem Computer angemeldet.
529	Anmeldefehler. Ein Anmeldeversuch erfolgte mit einem unbekannten Benutzernamen oder einem bekannten Benutzernamen mit einem falschen Kennwort.
530	Anmeldefehler. Ein Anmeldeversuch erfolgte, wobei sich das Benutzerkonto außerhalb der zulässigen Zeit anzumelden versuchte.
531	Anmeldefehler. Ein Anmeldeversuch erfolgte mit einem deaktivierten Konto.
532	Anmeldefehler. Ein Anmeldeversuch erfolgte mit einem abgelaufenen Konto.
533	Anmeldefehler. Ein Anmeldeversuch erfolgte durch einen Benutzer, der sich nicht an diesem Computer anmelden darf.
534	Anmeldefehler. Der Benutzer hat beim Anmelden einen unzulässigen Anmeldetyp verwendet.
535	Anmeldefehler. Das Kennwort für das angegebene Konto ist abgelaufen.
536	Anmeldefehler. Der Anmeldedienst ist nicht aktiv.
537	Anmeldefehler. Der Anmeldeversuch ist aus anderen Gründen fehlgeschlagen. **Anmerkung:** In manchen Fällen ist der Grund für das Fehlschlagen der Anmeldung nicht bekannt.
538	Der Abmeldevorgang wurde für einen Benutzer durchgeführt.
539	Anmeldefehler. Das Konto wurde während des Anmeldeversuchs gesperrt.
540	Ein Benutzer hat sich erfolgreich an einem Netzwerk angemeldet.
541	Die Hauptmodusauthentifizierung per Internetschlüsselaustausch (Internet Key Exchange, IKE) wurde zwischen dem lokalen Computer und der aufgeführten Peerkennung (die eine Sicherheitszuordnung herstellt) durchgeführt, oder der Schnellmodus hat einen Datenkanal eingerichtet.
542	Ein Datenkanal wurde beendet.

543	Der Hauptmodus wurde beendet. **Anmerkung:** Dies kann auf das Ablaufen der Sicherheitszuordnung (standardmäßig acht Stunden), auf Richtlinienänderungen oder die Peerbeendigung zurückzuführen sein.
544	Die Hauptmodusauthentifizierung schlug aufgrund eines ungültigen Zertifikats des Peers oder einer unbestätigten Signatur fehl.
545	Die Hauptmodusauthentifizierung schlug aufgrund eines Kerberos-Fehlers oder eines ungültigen Kennwortes fehl.
546	Die IKE-Sicherheitszuordnung schlug fehl, weil der Peer eine ungültige Anfrage gesendet hat. Ein Paket mit ungültigen Daten wurde empfangen.
547	Bei einem IKE-Handshake ist ein Fehler aufgetreten.
548	Anmeldefehler. Die Sicherheitskennung (Security ID, SID) einer vertrauenswürdigen Domäne stimmt nicht mit der Kontodomänen-SID des Clients überein.
549	Anmeldefehler. Alle SIDs, die nicht vertrauenswürdigen Namespaces entsprechen, wurden während einer strukturübergreifenden Authentifizierung herausgefiltert.
550	Eine Benachrichtigung, die auf einen Dienstverweigerungsangriff hinweisen könnte.
551	Ein Benutzer hat den Abmeldevorgang gestartet.
552	Ein Benutzer hat sich mit expliziten Anmeldeinformationen erfolgreich an einem Computer angemeldet, wobei er bereits als ein anderer Benutzer angemeldet ist.
682	Ein Benutzer hat erneut eine Verbindung zu einer getrennten Terminalserversitzung hergestellt.
683	Ein Benutzer hat eine Terminalserversitzung getrennt, ohne sich abzumelden. **Anmerkung:** Dieses Ereignis wird generiert, wenn ein Benutzer mit einer Terminalserversitzung über das Netzwerk verbunden ist. Es wird auf dem Terminalserver angezeigt.

Anmeldeversuche überwachen

Ereignis-ID	Beschreibung
672	Ein AS-Ticket (Authentication Service, Authentifizierungsdienst) wurde erfolgreich ausgestellt und überprüft.
673	Ein TGS-Ticket (Ticket Granting Service, Ticket-genehmigender Dienst) wurde erteilt.
674	Ein Sicherheitsprinzipal hat ein AS- oder TGS-Ticket erneuert.
675	Die Präauthentifizierung ist fehlgeschlagen. Dieses Ereignis wird auf einem Schlüsselverteilungscenter (KDC) generiert, wenn ein Benutzer ein falsches Kennwort eingibt.
676	Die Anfrage für das Authentifizierungsticket ist fehlgeschlagen. Dieses Ereignis wird nicht unter Windows XP oder unter den Betriebssystemen der Windows Server 2003-Produktfamilie generiert.
677	Ein TGS-Ticket wurde nicht erteilt. Dieses Ereignis wird nicht unter Windows XP oder unter den Betriebssystemen der Windows Server 2003-Produktfamilie generiert.
678	Ein Konto wurde erfolgreich einem Domänenkonto zugeordnet.
681	Anmeldefehler. Die Anmeldung bei einem Domänenkonto wurde versucht. Dieses Ereignis wird nicht unter Windows XP oder unter den Betriebssystemen der Windows Server 2003-Produktfamilie generiert.
682	Ein Benutzer hat erneut eine Verbindung zu einer getrennten Terminalserversitzung hergestellt.
683	Ein Benutzer hat eine Terminalserversitzung getrennt, ohne sich abzumelden.

Kontenverwaltung überwachen

Ereignis-ID	Beschreibung
624	Ein Benutzerkonto wurde erstellt.
627	Ein Benutzerkennwort wurde geändert.
628	Ein Benutzerkennwort wurde festgelegt.
630	Ein Benutzerkonto wurde gelöscht.
631	Eine globale Gruppe wurde erstellt.
632	Ein Mitglied wurde zu einer globalen Gruppe hinzugefügt.
633	Ein Mitglied wurde aus einer globalen Gruppe entfernt.
634	Eine globale Gruppe wurde gelöscht.
635	Eine neue lokale Gruppe wurde erstellt.
636	Ein Mitglied wurde zu einer lokalen Gruppe hinzugefügt.
637	Ein Mitglied wurde aus einer lokalen Gruppe entfernt.
638	Eine lokale Gruppe wurde gelöscht.
639	Das Konto einer lokalen Gruppe wurde geändert.
641	Das Konto einer globalen Gruppe wurde geändert.
642	Ein Benutzerkonto wurde geändert.
643	Eine Domänenrichtlinie wurde geändert.
644	Ein Benutzerkonto wurde automatisch gesperrt.
645	Ein Computerkonto wurde erstellt.

646	Ein Computerkonto wurde geändert.
647	Ein Computerkonto wurde gelöscht.
648	Eine lokale Sicherheitsgruppe mit deaktivierter Sicherheit wurde erstellt. **Anmerkung:** SECURITY_DISABLED im formalen Namen bedeutet, dass mit Hilfe dieser Gruppe bei Zugriffsüberprüfungen keine Berechtigungen erteilt werden können.
649	Eine lokale Sicherheitsgruppe mit deaktivierter Sicherheit wurde geändert.
650	Ein Mitglied wurde zu einer lokalen Sicherheitsgruppe mit deaktivierter Sicherheit hinzugefügt.
651	Ein Mitglied wurde aus einer lokalen Sicherheitsgruppe mit deaktivierter Sicherheit entfernt.
652	Eine lokale Gruppe mit deaktivierter Sicherheit wurde gelöscht.
653	Eine globale Gruppe mit deaktivierter Sicherheit wurde erstellt.
654	Eine globale Gruppe mit deaktivierter Sicherheit wurde geändert.
655	Ein Mitglied wurde zu einer globalen Gruppe mit deaktivierter Sicherheit hinzugefügt.
656	Ein Mitglied wurde aus einer globalen Gruppe mit deaktivierter Sicherheit entfernt.
657	Eine globale Gruppe mit deaktivierter Sicherheit wurde gelöscht.
658	Eine universelle Gruppe mit aktivierter Sicherheit wurde erstellt.
659	Eine universelle Gruppe mit aktivierter Sicherheit wurde geändert.
660	Ein Mitglied wurde zu einer universellen Gruppe mit aktivierter Sicherheit hinzugefügt.

661	Ein Mitglied wurde aus einer universellen Gruppe mit aktivierter Sicherheit entfernt.
662	Eine universelle Gruppe mit aktivierter Sicherheit wurde gelöscht.
663	Eine universelle Gruppe mit deaktivierter Sicherheit wurde erstellt.
664	Eine universelle Gruppe mit deaktivierter Sicherheit wurde geändert.
665	Ein Mitglied wurde zu einer universellen Gruppe mit deaktivierter Sicherheit hinzugefügt.
666	Ein Mitglied wurde aus einer universellen Gruppe mit deaktivierter Sicherheit entfernt.
667	Eine universelle Gruppe mit deaktivierter Sicherheit wurde gelöscht.
668	Ein Gruppentyp wurde geändert.
684	Legen Sie die Sicherheitsbeschreibung von Mitgliedern administrativer Gruppen fest. **Anmerkung**: Auf einem Domänencontroller werden alle 60 Minuten im Hintergrund alle Mitglieder administrativer Gruppen durchsucht (z. B. Domänen-, Organisations- oder Schemaadministratoren) und eine festgelegte Sicherheitsbestimmung auf diese angewendet. Dieses Ereignis wird protokolliert.
685	Der Name eines Kontos wurde geändert.

Objektzugriffsversuche überwachen

Ereignis-ID	**Beschreibung**
560	Der Zugriff wurde auf ein bereits vorhandenes Objekt gewährt.
562	Ein Handle zu einem Objekt wurde geschlossen.
563	Es wurde versucht, ein Objekt zum Löschen zu öffnen. **Anmerkung:** Dies wird von Dateisystemen verwendet, wenn das Flag FILE_DELETE_ON_CLOSE in **Createfile()** verwendet wird.

564	Ein geschütztes Objekt wurde gelöscht.
565	Der Zugriff wurde auf einen bereits vorhandenen Objekttyp gewährt.
567	Eine Berechtigung, die mit einem Handle verknüpft ist, wurde verwendet. **Anmerkung:** Ein Handle wird mit bestimmten Berechtigungen erstellt (**Lesen**, **Schreiben** usw.). Bei Verwendung des Handles wird für jede verwendete Berechtigung eine Überprüfung generiert.
568	Es wurde versucht, eine feste Verbindung zu einer Datei, die überwacht wird, zu erstellen.
569	Die Ressourcenverwaltung im Autorisierungs-Manager versuchte einen Clientkontext zu erstellen.
570	Ein Client hat versucht, auf ein Objekt zuzugreifen. **Anmerkung:** Für jede Operation, die für das Objekt auszuführen versucht wird, wird ein Ereignis generiert.
571	Der Clientkontext wurde vom Autorisierungs-Manager gelöscht.
572	Der Verwaltungs-Manager hat die Anwendung gestartet.
772	Die Zertifikatverwaltung lehnte eine ausstehende Zertifikatanforderung ab.
773	Die Zertifikatdienste haben eine erneut gesendete Zertifikatanforderung erhalten.
774	Die Zertifikatdienste haben ein Zertifikat gesperrt.
775	Die Zertifikatdienste haben eine Anforderung zur Veröffentlichung der Zertifikatsperrliste erhalten.
776	Die Zertifikatdienste haben die Zertifikatsperrliste veröffentlicht.
777	Eine Zertifikatanforderungserweiterung wurde ausgestellt.
778	Ein oder mehrere Zertifikatanforderungsattribute wurden geändert.
779	Die Zertifikatdienste haben eine Beendigungsanforderung erhalten.

780	Die Sicherung der Zertifikatdienste wurde gestartet.
781	Die Sicherung der Zertifikatdienste wurde beendet.
782	Die Wiederherstellung der Zertifikatdienste wurde gestartet.
783	Die Wiederherstellung der Zertifikatdienste wurde beendet.
784	Die Zertifikatdienste wurden gestartet.
785	Die Zertifikatdienste wurden beendet.
786	Die Sicherheitsberechtigungen für die Zertifikatdienste wurden geändert.
787	Die Zertifikatdienste haben einen archivierten Schlüssel wiedergefunden.
788	Die Zertifikatdienste haben ein Zertifikat in die Datenbank importiert.
789	Der Überwachungsfilter für die Zertifikatdienste wurde geändert.
790	Die Zertifikatdienste haben eine Zertifikatanforderung erhalten.
791	Die Zertifikatdienste haben eine Zertifikatanforderung genehmigt und ein Zertifikat ausgestellt.
792	Die Zertifikatdienste haben eine Zertifikatanforderung abgelehnt.
793	Die Zertifikatdienste haben den Status einer Zertifikatanforderung als "Anstehend" festgelegt.
794	Die Zertifikatverwaltungseinstellungen für die Zertifikatdienste wurden geändert.
795	Es wurde ein Konfigurationseintrag in den Zertifikatdiensten geändert.
796	Es wurde eine Eigenschaft der Zertifikatdienste geändert.
797	Die Zertifikatdienste haben einen Schlüssel archiviert.

798	Die Zertifikatdienste haben einen Schlüssel importiert und archiviert.
799	Die Zertifikatdienste haben das Zertifizierungsstellenzertifikat veröffentlicht.
800	Eine oder mehrere Zeilen wurden von der Zertifikatdatenbank gelöscht.
801	Rollentrennung aktiviert.

Objektzugriffsversuche überwachen

Ereignis-ID	Beschreibung
592	Ein neuer Prozess wurde erstellt.
593	Ein Prozess wurde beendet.
594	Ein Handle eines Objekts wurde dupliziert.
595	Indirekter Zugriff auf ein Objekt erfolgreich.
596	Ein Datensicherungs-Hauptschlüssel wurde gesichert. **Anmerkung:** Der Hauptschlüssel wird von den Routinen **CryptProtectData** und **CryptUnprotectData** sowie vom verschlüsselnden Dateisystem (Encrypting File System, EFS) verwendet. Der Hauptschlüssel wird jedes Mal gesichert, wenn ein neuer Hauptschlüssel erstellt wird. (Die Standardeinstellung ist 90 Tage.) Im Normalfall wird der Hauptschlüssel auf einem Domänencontroller gesichert.
597	Ein Datensicherungs-Hauptschlüssel wurde von einem Wiederherstellungsserver wiederhergestellt.
598	Zu überwachende Daten waren geschützt.
599	Zu überwachende Daten waren ungeschützt.
600	Einem Prozess wurde ein primäres Token zugewiesen.

601	Ein Benutzer hat versucht, einen Dienst zu installieren.
602	Ein Planerauftrag wurde erstellt.

Rechteverwendung überwachen

Ereignis-ID	Beschreibung
576	Die angegebenen Berechtigungen wurden zu einem Zugriffstoken eines Benutzers hinzugefügt. **Anmerkung:** Dieses Ereignis wird beim Anmelden des Benutzers generiert.
577	Ein Benutzer hat versucht, einen privilegierten Systemdienstvorgang auszuführen.
578	Die Berechtigungen wurden für ein bereits geöffnetes Handle zu einem geschützten Objekt verwendet.

Richtlinienänderungen überwachen

Ereignis-ID	Beschreibung
608	Ein Benutzerrecht wurde zugewiesen.
609	Ein Benutzerrecht wurde entfernt.
610	Eine Vertrauensstellung mit einer anderen Domäne wurde erstellt.
611	Eine Vertrauensstellung mit einer anderen Domäne wurde entfernt.
612	Eine Überwachungsrichtlinie wurde geändert.
613	Ein IPSec-Richtlinien-Agent wurde gestartet.
614	Ein IPSec-Richtlinien-Agent wurde deaktiviert.
615	Ein IPSec-Richtlinien-Agent wurde geändert.

616	Ein IPSec-Richtlinien-Agent hat einen möglicherweise schwerwiegenden Fehler entdeckt.
617	Eine Kerberos-Richtlinie wurde geändert.
618	Eine Richtlinie für die Wiederherstellung von verschlüsselten Daten wurde geändert.
620	Eine Vertrauensstellung mit einer anderen Domäne wurde geändert.
621	Der Systemzugriff wurde einem Konto gewährt.
622	Der Systemzugriff wurde einem Konto entzogen.
623	Für den Benutzer gesetzte Benutzerrichtlinienüberwachung.
625	Die Benutzerrichtlinienüberwachung wurde aktualisiert.
768	Eine Kollision zwischen einem Namespaceelement in einer Gesamtstruktur und einem Namespaceelement in einer anderen Gesamtstruktur wurde erkannt. **Anmerkung:** Wenn sich ein Namespaceelement in einer Gesamtstruktur mit einem Namespaceelement in einer anderen Gesamtstruktur überschneidet, kann dies zu Mehrdeutigkeiten beim Auflösen eines Namens führen, der zu einem der beiden Namespaceelemente gehört. Diese Überschneidung wird auch als Kollision bezeichnet. Nicht alle Parameter sind für jeden Eintragstyp gültig. Beispielsweise sind Felder wie DNS-Name, NetBIOS-Name und SID nicht für Einträge vom Typ "Name der obersten Ebene" (TopLevelName) zulässig.
769	Informationseintrag zur vertrauten Gesamtstruktur hinzugefügt. **Anmerkung:** Diese Ereignismeldung wird generiert, wenn Informationen zur Gesamtstruktur-Vertrauensstellung aktualisiert werden und Einträge hinzugefügt werden. Pro hinzugefügtem, gelöschtem oder geändertem Eintrag wird eine Ereignismeldung generiert. Falls bei einer einzigen Aktualisierung der Informationen zur Gesamtstruktur-Vertrauensstellung mehrere Einträge hinzugefügt, gelöscht oder geändert werden, weisen alle generierten Ereignismeldungen einen einzigen eindeutigen Bezeichner auf, eine so genannte Vorgangskennung. Sie zeigt an, dass die generierten Ereignismeldungen auf einen einzigen Vorgang zurückzuführen sind. Nicht alle Parameter sind für jeden Eintragstyp gültig. Beispielsweise sind Parameter wie DNS-Name, NetBIOS-Name und SID nicht für Einträge vom Typ "Name der obersten Ebene" (TopLevelName) zulässig.

770	Informationseintrag zur vertrauten Gesamtstruktur entfernt. **Anmerkung:** Siehe die Anmerkung zu Ereignis 769.
771	Informationseintrag zur vertrauten Gesamtstruktur geändert. **Anmerkung:** Siehe die Anmerkung zu Ereignis 769.
805	Der Ereignisprotokolldienst hat die Sicherheitsprotokollkonfiguration für eine Sitzung gelesen.

Richtlinienänderungen überwachen

Ereignis-ID	Beschreibung
512	Windows wird gestartet.
513	Windows wird heruntergefahren.
514	Ein Authentifizierungspaket wurde von der lokalen Sicherheitsinstanz geladen.
515	Ein vertrauenswürdiger Anmeldevorgang wurde bei der lokalen Sicherheitsinstanz registriert.
516	Die für die Überwachung reservierten internen Ressourcen sind ausgelastet. Dies wird zu einem Verlust von Überwachungsereignissen führen.
517	Das Überwachungsprotokoll wurde gelöscht.
518	Ein Benachrichtigungspaket wurde von der Sicherheitskontenverwaltung (Security Accounts Manager, SAM) geladen.
519	Ein Prozess verwendet einen ungültigen Port für den lokalen Prozeduraufruf (Local Procedure Call, LPC), um die Identität eines Clients anzunehmen und zu antworten oder von einem Clientadressbereich zu lesen bzw. in diesen zu schreiben.
520	Die Systemzeit wurde geändert. **Anmerkung:** Diese Überwachung wird normalerweise zweimal durchgeführt.

Verzeichnisdienstzugriff überwachen

Ereignis-ID	Beschreibung
566	Ein allgemeiner Objektvorgang wurde durchgeführt.

Bestellformular ***backUP***-Magazine für IT-Sicherheit
***backUP*-Magazine erhalten Sie kostenlos!**
Fax: 0431-988-1223 **Mail:** mail@datenschutzzentrum.de **Internet:** http://www.datenschutzzentrum.de
Absender:
Magazine:
☐ **Nr. 1: IT-Sicherheitskonzepte** Planung – Erstellung – Umsetzung
☐ **Nr. 2: MS-Windows NT 4.0** Sicherheitsmaßnahmen und Restrisiken
☐ **Nr. 3: MS-Windows NT 4.0** Resource Kit und Security-Tools
☐ **Nr. 4: PC-Arbeitsplatz** So viel Datenschutz muss an jedem Arbeitsplatz sein!
☐ **Nr. 5: MS-Windows 2000** Sicherheitsmaßnahmen und Restrisiken
☐ **Nr. 6: Windows Gruppenrichtlinien** Planen und effektiv anwenden
☐ **Bitte nehmen Sie mich in den Verteiler *backUP*-Magazine auf.**