net.com
networking & communications

CARLO WESTBROOK

Active Directory für Windows Server 2008

Planung und praktischer Einsatz in Windows-Netzwerken

› Berücksichtigt Windows XP- und Vista-Clients
› Für den Einsatz ab Windows Server 2000 geeignet

ADDISON-WESLEY

Add-ons,
Management Tools u.v.m.

CD

Teil 2

Planung, Aktualisierung & Migration

Nach der Einführung in die Grundlagen und Funktionen der Active Directory-Domänendienste führt Sie der Teil 2 dieses Buches in insgesamt drei weiteren Kapitel in die Planung der Implementierung der Active Directory-Domänendienste sowie die Aktualisierung und Migration von bestehenden Active Directory-Gesamtstrukturen und -Domänen ein.

Der zweite Teil dieses Buches unterteilt sich in die folgenden Kapitel:

- **Kapitel 4 – Planung einer Infrastruktur der Active Directory-Domänendienste** Erfahren Sie die notwendigen Schritte und Details für die erfolgreiche Planung der Implementierung einer Infrastruktur der Active Directory-Domänendienste unter Windows Server 2008. (*ab Seite* 159)

- **Kapitel 5 – Aktualisierung vorhandener Gesamtstrukturen und Domänen** In diesem Kapitel werden Ihnen die möglichen Aktualisierungspfade sowie auch die durchzuführenden Schritte zur erfolgreichen Aktualisierung vorhandener Active Directory-Gesamtstrukturen und -Domänen beschrieben. (*ab Seite* 231)
- **Kapitel 6 – Migration von Gesamtstrukturen und Domänen** Erfahren Sie die möglichen Migrationspfade sowie die notwendigen Verwaltungsschritte für die Migration vorhandener Active Directory-Gesamtstrukturen und -Domänen zu Windows Server 2008. (*ab Seite* 245)

3 Sicherheit in Active Directory-Domänen-dienst-Umgebungen

In dem vorangegangenen Kapitel haben Sie grundlegendste Informationen zu Active Directory-Gesamtstrukturen und -Domänen erfahren. Es wurde Ihnen mitunter auch erläutert, dass Domänen im Microsoft-Umfeld eine gewisse Sicherheitsgrenze darstellen. Ein verantwortlicher Administrator kann die Grenzen einer Domäne klar definieren und damit ebenso festlegen, welcher Clientcomputer oder Benutzer im Vertrauen der Domäne steht. Im Gegensatz zu Arbeitsgruppencomputern, in denen die Benutzerkonten und Ressourcen auf jedem der darin teilhabenden Computer jeweils getrennt verwaltet werden müssen, erfolgt die Verwaltung von Computern, Benutzerkonten und Ressourcen in Domänenumgebungen in der Regel zentral, beispielsweise durch die Domänenadministratoren. Auch lassen sich die Rechtevergaben, aber auch bestimmte Einschränkungen für die einzelnen Domänenbenutzer durch Domänenrichtlinien sehr detailliert und bei Bedarf einheitlich definieren.

Damit diese sichere, zentrale Verwaltbarkeit funktioniert, kommen in einer Domäne der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) bestimmte Mechanismen sowie Objekte und auch Richtlinien zum Einsatz. In den nachfolgenden Seiten erfahren Sie mehr über die Identifikation von Sicherheitsprinzipalen, die Rechtevergabe sowie den Authentifizierungs- und Autorisierungsprozess.

3.1 Grundlagen

Um die Sicherheit in Domänenumgebungen zu verstehen, muss man sich zuerst einmal mit den notwendigen Grundlagen und Grundbegriffen befassen. Als Erstes wendet man sich hierbei der möglichen Eindeutigkeit und Identifizierbarkeit von Benutzern oder Computern innerhalb von Active Directory-Domänen zu.

3.1.1 Sicherheitsprinzipale

Eindeutigkeit von Objekten durch die SID

Die Identität von Benutzern oder Computern wird in den Domänen der Active Directory-Domänendienste (*AD DS*) anhand von Sicherheitsprinzipalen (engl. *Security Principals*) geregelt. Diese Sicherheitsprinzipale erhalten ihre Eindeutigkeit durch eine einzigartige Sicherheitskennung (engl. *Security Identifier, SID*). Diese Sicherheitskennung besteht prinzipiell aus zwei Teilen:

- der eindeutigen **Domänenkennung**
- der eindeutigen **Objektkennung** (Relative Identifier, RID)

Sicherheitskennung bleibt auch beim Umbenennen von Objekten eindeutig

Die Domänenkennung wird beim Einrichten einer Domäne als eindeutige Kennung festgelegt. Die eindeutige Objektkennung (als *Relative Identifier, RID*) wird vom RID-Master einer jeweiligen Domäne definiert, an die vorhandenen Domänencontroller in Form von RID-Pools ausgegeben und beim Anlegen eines Objekts (in Kombination mit der Domänenkennung) für dieses vergeben.

Der Anzeige- oder Objektname eines Objekts in Active Directory ist dabei unerheblich. Selbst beim Umbenennen von Objekten bleibt die Sicherheitskennung die gleiche.

Anhand der Sicherheitskennung (*SID*) eines Objekts in einer Active Directory-Domäne ist es möglich, beispielsweise den Zugriff auf Ressourcen gezielt zu vergeben oder gar zu verweigern.

Beispiel für eine Sicherheitskennung (SID)

Die Sicherheitskennungen (*SIDs*) innerhalb von Domänen sind nach einem bestimmten Schema definiert. Eine Sicherheitskennung enthält dabei die folgenden Bestandteile:

`S-1-5-21-1454471165-494733854-2908337755-501`

Bestandteile der Sicherheitskennung Die Sicherheitskennung unterteilt sich dabei wie folgt:

`S` – Kennzeichnet die Zeichenkette als SID

`1` – Die Revisionsebene

`5` – Identifizierungsautorität

`21-1454471165-494733854-2908337755` – Domäne/Computer

`501` – Relativer Identifizierer (RID)

Standardmäßige Sicherheitskennungen

In Active Directory gelten bestimmte Regeln für die Vergabe von Sicherheitskennungen. So erhält das bei der Installation von Domänen standardmäßig eingerichtete Administrator-Objekt immer die gleiche Endung.

In der folgenden Tabelle finden Sie einige der wichtigsten, vordefinierten Sicherheitskennungen im Umfeld einer Infrastruktur der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*):

Sicherheitskennung	Zuordnung
S-1-5-Domäne-500	Administrator – Benutzerkonto
S-1-5-Domäne-501	Gast – Benutzerkonto
S-1-5-Domäne-502	KRBTGT – Dienstkonto
S-1-5-Domäne-512	Domänen-Admins – Gruppe
S-1-5-Domäne-513	Domänenbenutzer – Gruppe
S-1-5-Domäne-514	Domänengäste – Gruppe
S-1-5-Domäne-515	Domänencomputer – Gruppe
S-1-5-Domäne-516	Domänencontroller – Gruppe
S-1-5-Domäne-519	Organisations-Admins – Gruppe
S-1-5-Domäne-520	Richtlinien-Ersteller-Besitzer – Gruppe
S-1-5-32-544	Administratoren – Gruppe
S-1-5-32-545	Benutzer – Gruppe

Tabelle 3.1 *Standardmäßige Sicherheitskennungen*

Das bei der Installation standardmäßig angelegte Administrator-Objekt einer Domäne oder eines lokalen Computersystems erhält am Ende immer die gleiche Kennung (*500*) und ist somit grundsätzlich auch für potenzielle Angreifer ermittelbar. Selbst ein Umbenennen des Administratornamens verschleiert dieses Objekt gegenüber Dritten nur bedingt. Es existieren Tools, mit denen man in der Lage ist, das Konto des Administrators – unbemerkt – ausfindig zu machen. Es ist deshalb umso wichtiger, für dieses Konto ein strenges Kennwort zu vergeben und die damit vollzogenen, erfolgreichen wie auch fehlgeschlagenen Anmeldeversuche zu überwachen.

Löschen von Objekten

Wenn ein Objekt in einer Domäne gelöscht wird, kann es für weitere Anmeldevorgänge oder Ressourcenzugriffe nicht mehr verwendet werden. Sollte man nun ein neues Objekt mit dem gleichen Namen des vorweg gelöschten Objekts anlegen, so erhält das neue Objekt trotzdem keinen Zugriff auf die Ressourcen, die dem ursprünglichen Objekt zugeordnet waren. Das neue Objekt erhält beim Anlegen wiederum eine neue Sicherheitskennung, die nicht der des alten, gelöschten Objekts entspricht. Somit greift die Eindeutigkeit der Objekte, und der Zugriff wird dem neuen Objekt verwehrt.

Mitunter vor dem Löschen erst deaktivieren

In der Praxis empfiehlt es sich oft, nicht mehr benötigte Objekte, beispielsweise Benutzerkonten, erst einmal zu deaktivieren, bevor man diese dauerhaft löscht. Im Bedarfsfall kann man sie einfach wieder aktivieren, ohne sie durch umfangreiche Wiederherstellungsvorgänge wieder bereitzustellen. Einen Zeitpunkt für die Löschung sollte man aber schon ins Auge fassen, um mit der Zeit keine unnötigen „Objektleichen“ anzusammeln.

3.1.2 Zugriffskontrolllisten

Der Zugriff auf Ressourcen wird in einer Domäne der Active Directory-Domänendienste in der Regel anhand einer *Zugriffskontrollliste* (engl. *Access Control List, ACL*) festgelegt. Innerhalb einer Zugriffskontrollliste sind Zugriffskontrolleinträge (engl. *Access Control Entries, ACEs*) enthalten, in denen der Zugriff auf die betreffende Ressource anhand der Sicherheitskennung (*SID*) eines Objektes mitsamt der zugehörigen Zugriffsrechte (beispielsweise Lese- oder Schreibzugriff) geregelt werden.

ACLs wie auch im NTFS-Dateisystem

Zugriffskontrolllisten, wie sie innerhalb von Active Directory-Domänen für die kontrollierte Vergabe von Zugriffsrechten auf Objekte eingesetzt werden, finden beispielsweise auch im *NTFS-Dateisystem* ihren Nutzen. Auch dort werden die Zugriffe auf Dateien und Ordner über Zugriffskontrolllisten geregelt.

Es existieren zwei verschiedene Arten von Zugriffskontrolllisten (*ACLs*):

- *Discretionary Access Controll List* (*DACL*)
- *System Access Control List* (*SACL*)

Die beiden Zugriffskontrolllisten unterscheiden sich hierbei in der jeweiligen Verwendung.

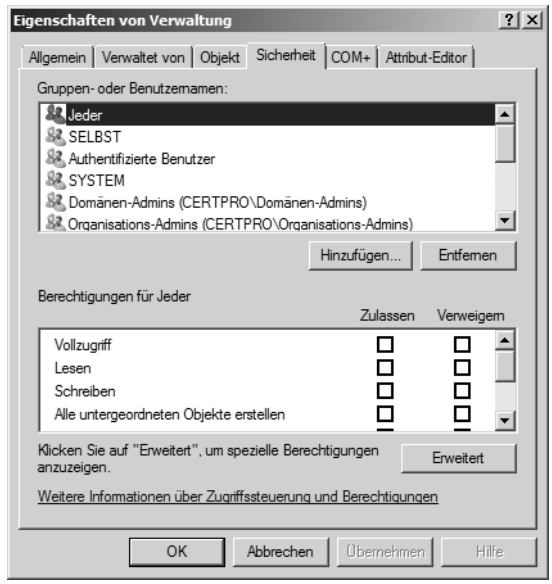


Abbildung 3.1 *Beispiel für eine „diskrete" Zugriffskontrollliste (DACL) in den Active Directory-Domänendiensten (AD DS) unter Windows Server 2008*

Discretionary Access Control List (DACL)

Steuerung der Zugriffsberechtigung

Eine *Discretionary Access Control List* (*DACL*) wird als *diskrete Zugriffskontrollliste* für die Steuerung von Zugriffen auf Ressourcen verwendet. In dieser Zugriffskontrollliste werden Objekte (beispielsweise Benutzer, Gruppen oder Computer) in Form von sogenannten

Zugriffskontrolleinträgen (engl. *Access Control Entries, ACEs*) eingetragen, um ihnen darüber beispielsweise die Berechtigung des Lese- oder Änderungszugriffs auf eine Ressource (sprich: Datei, Ordner oder Objekt) zu genehmigen oder gar zu verweigern.

System Access Control List (SACL)

Überwachung der Zugriffe

Im Gegensatz zur DACL wird eine *Systemzugriffskontrollliste* (engl. *System Access Control List, SACL*) für die Definition von Überwachungseinträgen für Ressourcen verwendet. Auch in SACLs werden sogenannte Zugriffskontrolleinträge (engl. *Access Control Entries, ACEs*) definiert, über die jedoch die Zugriffsüberwachung gesteuert wird. So kann man beispielsweise den Änderungs- oder Löschzugriff von bestimmten Benutzern oder Gruppen auf eine spezielle Datei, einen Ordner oder ein Objekt innerhalb eines Computersystems überwachen. Der dabei festgestellte Zugriff wird als Eintrag in der Ereignisanzeige des betreffenden Computersystems dokumentiert.

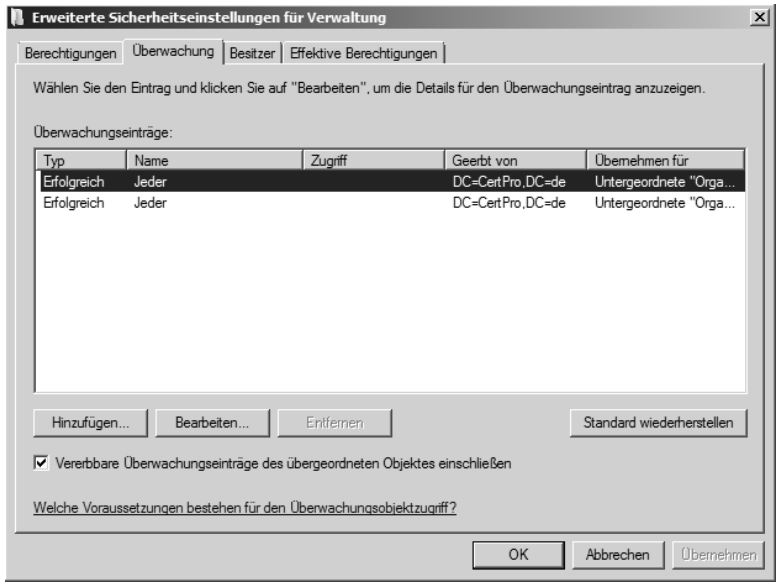


Abbildung 3.2 *Beispiel für eine Überwachungsrichtlinie (SACL)*

3.1.3 Authentifizierung & Autorisierung

Erfolgreich authentifiziert ist nicht gleich auch autorisiert

Um die Zugriffe auf Ressourcen innerhalb von Active Directory-Domänen steuern zu können, werden den darin enthaltenen Objekten (beispielsweise Benutzern oder Gruppen) eindeutige Sicherheitskennungen (engl. *Security Identifier, SIDs*) zugeordnet. Um die Eindeutigkeit zu gewährleisten, muss sich ein Benutzer anhand eines ihm zugeordneten Anmeldenamens und eines zugehörigen Kennworts gegenüber einem der Domänencontroller einer Domäne anmelden. Wenn der

betreffende Domänencontroller die Anmeldedaten nun erfolgreich mit den Einträgen in der Active Directory-Domänendienste-Datenbank abgleichen konnte, so ordnet man diesen Vorgang der erfolgreichen Authentifizierung zu.

Obgleich der Benutzer sich gegenüber der Domäne erfolgreich authentifizieren konnte, wird vom Domänencontroller des Weiteren überprüft, ob der Benutzer überhaupt autorisiert ist, sich beispielsweise zu bestimmten Anmeldezeiten oder gar von der betreffenden Arbeitsstation aus in der Domäne anzumelden. Dieser Vorgang wird als Autorisierung bezeichnet. Bei fehlender Autorisierung kann einem Benutzer trotz vorangegangener, erfolgreicher Authentifizierung die Anmeldung in einer Active Directory-Domäne verweigert werden.

Es wird ersichtlich, dass sich der Anmeldeprozess innerhalb einer Active Directory-Domäne, aber auch innerhalb eines Computersystems in zwei Prozesse aufteilt:

- *Authentifizierung*
- *Autorisierung*

Die Authentifizierung ist nicht auf den Benutzernamen in Verbindung mit einem Benutzerkennwort beschränkt. Wenn die notwendigen Voraussetzungen geschaffen sind, kann für den Authentifizierungsprozess auch ein digitales Zertifikat, das auf einer *SmartCard* oder einem *SecureToken* gespeichert ist, verwendet werden.

Um nach erfolgreicher Authentifizierung und Autorisierung den Zugriff auf Ressourcen steuern zu können, bedarf es noch einer weiteren Komponente: eines *Zugriffstokens*.

3.1.4 Zugriffstoken

Eindeutigkeit des Benutzers mitsamt allen zugeordneten Gruppen

Ein Zugriffstoken (engl. *Access Token*) wird bei einer Domänenanmeldung von einem Domänencontroller erstellt und enthält neben der eindeutigen Sicherheitskennung (*SID*) des Benutzers auch alle Sicherheitskennungen von Benutzergruppen, denen der Benutzer zugeordnet ist. Darüber hinaus sind in dem Zugriffstoken beispielsweise auch Benutzerrechte aufgeführt, die dem Benutzerkonto zugestanden wurden.

Das Ausstellen des betreffenden Zugriffstokens erfolgt unter Windows durch die lokale Sicherheitsautorität (engl. *Local Security Authority, LSA*) eines Domänencontrollers bei Domänenanmeldung oder bei lokaler Anmeldung durch die lokale LSA eines Computersystems.

3.1.5 Kerberos V5-Protokoll

Standard-Authentifizierungsprotokoll

In Active Directory-Domänen, die auf den Active Directory-Domänendiensten (*Active Directory Domain Services, AD DS*) basieren, wird seit der Einführung von Windows 2000 das Kerberos-Protokoll für die Authentifizierung von Benutzern eingesetzt. Nach erfolgreicher Authentifizierung und Autorisierung über das Kerberos-Protokoll erhält der Benutzer seitens eines auf den Domänencontrollern ab Windows 2000 vorhandenen *Schlüsselverteilungscenters* (engl. *Key Distribution Center, KDC*) ein sogenanntes *Ticket-genehmigendes Ticket* (engl. *Ticket-Granting Ticket, TGT*) ausgestellt. In diesem TGT ist auch ein Zugriffstoken enthalten, in dem die Sicherheitskennung (*SID*) des Benutzers sowie aller Sicherheitsgruppen enthalten ist, denen der Benutzer zugeordnet wurde.

TGT und für den Zugriff noch ein Dienstticket

Wenn der Benutzer nachfolgend auf eine Ressource (beispielsweise eine Freigabe auf einem Dateiserver) innerhalb der Domäne zugreifen möchte, so erfragt er für den Zugriff wiederum bei dem KDC ein *Dienstticket* (engl. *Service Ticket*) für die notwendige Zugriffsgenehmigung. Das KDC stellt dem Benutzer anschließend das beantragte Dienstticket aus, das der Benutzer nun beim Zugriffsversuch an den betreffenden Dateiserver sendet. Der Dateiserver vergleicht nun die im übersandten Dienstticket enthaltenen Sicherheitskennungen des Benutzers und aller Gruppen mit der für den Ressourcenzugriff konfigurierten, diskreten Zugriffskontrollliste (*DACL*). Anschließend genehmigt oder verweigert der Server den Zugriff anhand der darin enthaltenen Zugriffskontrolleinträge (*ACEs*).

Hierzu ein Beispiel:

Ein Benutzer meldet sich in der Active Directory-Domäne mit seinem Benutzernamen und Kennwort an und möchte nach erfolgter Authentifizierung und Autorisierung nun auf eine Freigabe auf einem Dateiserver zugreifen.

Die einzelnen Schritte beschreiben sich dabei (vereinfacht) wie folgt:

1. Der Benutzer sendet seine Anmeldedaten zur Authentifizierung über seinen Clientcomputer an den Domänencontroller.
2. Der Domänencontroller überprüft die Anmeldedaten und stellt dem Benutzer ein ticketgenehmigendes-Ticket (Ticket-Granting Ticket, TGT) aus.
3. Der Domänencontroller sendet das TGT an den Clientcomputer zurück.
4. Der Clientcomputer sendet nun die Anfrage für den Zugriff auf die Dateifreigabe an den Domänencontroller.

5. Der Domänencontroller stellt für den Clientcomputer ein Dienstticket (Service Ticket) aus und sendet dieses an ihn zurück.
6. Der Clientcomputer übersendet das Dienstticket für den Zugriff auf die Dateifreigabe an den Dateiserver.

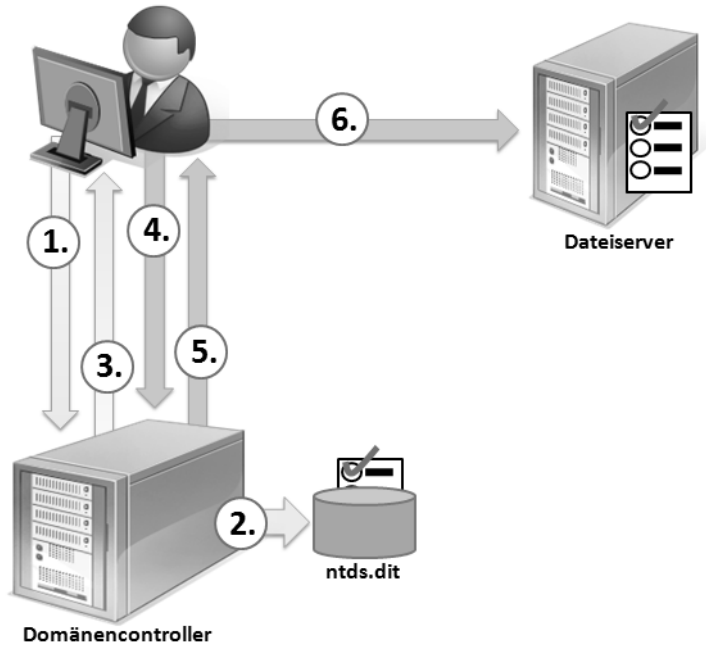


Abbildung 3.3
Beispiel für die Authentifizierung und Zugriffssteuerung über Kerberos

Zeitnahe Entscheidung

Wie in dem oben gezeigten Beispiel deutlich wird, ermöglicht das Kerberos-Protokoll eine zeitnahe Entscheidung über die Genehmigung oder gar die Verweigerung des Zugriffs auf Ressourcen. Vor der Ausstellung eines Diensttickets für den Zugriff auf Ressourcen liest das KDC die aktuellen, dem Benutzer zugeordneten Sicherheitskennungen (*SIDs*) aus dem vorweg ausgestellten TGT und trägt diese in das Zugriffstoken ein.

Kerberos-Konfiguration unter Windows Server 2008

Kerberos für alle Computersysteme ab Windows 2000

Unter Windows Server 2008 können verschiedene Einstellungen für die Verwendung des Kerberos-Protokolls innerhalb einer Domäne vorgenommen werden. Standardmäßig nimmt man diese Einstellungen in der *Default Domain Policy* einer Domäne vor, die auf alle Clients, Mitgliedsserver und Domänencontroller der jeweiligen Domäne angewendet wird.

Bei der Installation des ersten Domänencontrollers einer Domäne wird ein spezielles Konto mit dem Namen *krbtgt* erstellt. Dieses Konto dient dem Domänencontroller für die Ver- und Entschlüsselung der durch das KDC ausgestellten TGTs. Dieses Konto kann nicht gelöscht oder umbenannt werden. Auch wird diesem Konto ein Kennwort gemäß den Kennwortrichtlinien der Domäne zugeordnet. Dieses Kennwort wird dann im vordefinierten Zeitzyklus der Domäne automatisch erneuert. Jeder schreibgeschützte Domänencontroller (RODC) erhält beim Einrichten ein ebensolches Konto namens *krbtgt*. Durch die Verwendung eines eigenen krbtgt-Kontos wird in der Netzwerkumgebung eines RODC somit ein anderes Kennwort für die Ver- und Entschlüsselung der TGTs verwendet, als auf einem beschreibbaren Domänencontroller in der betreffenden Domäne – und somit die Sicherheit erhöht.

In der nachfolgenden Grafik sehen Sie die möglichen Einstellungen für die Kerberos-Authentifizierung:

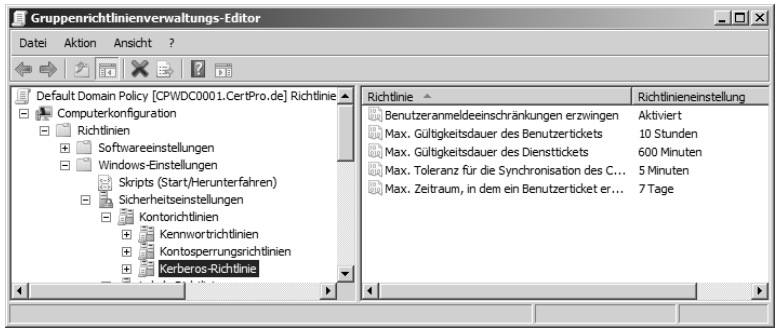


Abbildung 3.4 *Kerberos-Einstellungen in der Default Domain Policy unter Windows Server 2008*

Ports für die Kerberos-Authentifizierung

Die Kerberos-Authentifizierung wird zwischen den Clients, Servern und Domänencontrollern über spezielle Kommunikationsports durchgeführt. Diese müssen insbesondere bei der Firewall-Konfiguration innerhalb einer Domänenumgebung berücksichtigt werden.

Die nachfolgende Tabelle enthält die für die Authentifizierung über das Kerberos-Protokoll benötigten Kommunikationsports:

Port	Wird verwendet für
53 (TCP) und 53 (UDP)	Namensauflösung über DNS
88 (TCP) und 88 (UDP)	Kommunikation zum KDC
123 (TCP) und 123 (UDP)	Zeitsynchronisation
464 (TCP)	Kerberos-Kennwortänderungen unter Windows 2000

Tabelle 3.2 *Kommunikationsports für die Kerberos-Authentifizierung*

Tools für die Kerberos-Verwaltung und -Problembehandlung

In Windows Server 2008 sind einige Tools für die Verwaltung und auch die Problembehebung im Zusammenhang mit der Kerberos-Authentifizierung enthalten. Weitere Tools findet man im *Resource Kit* zu Windows Server 2003. Die nachfolgende Tabelle gibt Ihnen einen Überblick über die wichtigsten Kerberos-Tools:

Tabelle 3.3 *Tools für die Kerberos-Verwaltung und -Problembehandlung*

Tool	Beschreibung
Klist.exe	Kerberos List (Kommandozeilentool) Dient der Anzeige sowie dem Löschen von genehmigten Kerberos-Tickets.
Kerbtray.exe	Kerberos Tray (grafisches Tool) Dient der Anzeige sowie dem Löschen von genehmigten Kerberos-Tickets.
Tokensz.exe	Kerberos Token Size Dient zum Ermitteln der Größe eines Kerberos-Tokens.

3.1.6 NTLM-Protokoll

Neben der Kerberos-Authentifizierung unterstützt der Windows Server 2008 auch die NT-LanManager-Authentifizierung (NTLM). Dieses Authentifizierungsprotokoll ist aus Abwärtskompatibilitätsgründen zu Computern unter Windows 95, 98 und NT 4.0 weiterhin verwendbar.

Damit Clients unter Windows 95 oder 98 die NTLM-Authentifizierung verwenden können, muss auf diesen Computern die Active Directory-Clienterweiterung (*DSClient.exe*) installiert sein. Wenn dies nicht der Fall ist, verwenden diese alten Betriebssysteme statt des NTLM sogar nur das reine LanManager-Protokoll (*LM*).

Situationen für die Verwendung des NTLM-Protokolls

Das NTLM-Protokoll wird in folgenden Situationen verwendet:

- Beim Zugriff auf einen unter Windows Server 2008 betriebenen, einzeln stehenden Server (Stand-alone-Server) außerhalb einer Domäne.
- Von Clientsystemen unter Windows 2000 oder XP ersatzweise beim Anmeldeprozess an einem Active Directory-Domänencontroller unter Windows Server 2008, wenn die Authentifizierung über Kerberos nicht möglich war.
- Von Client- und Serversystemen unter Windows NT 4.0 bei der Authentifizierung gegenüber einem Domänencontroller unter Windows Server 2008.

- Von Clientsystemen unter Windows 95 oder 98 mit installierten Active Directory-Clienterweiterungen (DSClient.exe).
- Beim Zugriff auf Ressourcen über die IP-Adresse anstellen von Computernamen.

Vergleich von LM, NTLM und NTLMv2

Das NT-LanManager-Protokoll findet seine Ursprünge im reinen LanManager-Protokoll, das bereits zu Zeiten von Windows 95, also zu Zeiten vor Windows NT 4.0, zum Einsatz kam. Zur damaligen Zeit waren das Thema Sicherheit und auch die Kennwortattacken noch lange nicht in aller Munde. Die Sicherheitsanforderungen an die Authentifizierungsprotokolle sind mit den Jahren stark gewachsen. In diesem Zusammenhang erhalten Sie in der nachfolgenden Aufzählung einen Überblick über die verschiedenen – nicht empfohlenen – Alternativen zur Kerberos-Authentifizierung:

LanManager(LM)-Protokoll

Nicht mehr zeitgemäß

Das LanManager-Protokoll stellt das unsicherste Protokoll für die Benutzerauthentifizierung im Windows-Umfeld dar. Hierbei werden die Benutzerkennwörter bei einer maximalen Kennwortlänge von 14 Zeichen in zwei kurze Kennwortteile mit je sieben Zeichen aufgeteilt. Groß-/Kleinschreibung sowie auch einige Sonderzeichen werden dabei jedoch nicht berücksichtigt. Das Kennwort wird lediglich mit dem einfachen DES-Algorithmus (*Data Encryption Standard*) verschlüsselt. Von der Verwendung des LanManager(LM)-Protokolls in Active Directory-Domänen wird aus Sicht der IT-Sicherheit klar abgeraten. Lediglich alte Betriebssysteme wie Windows 95 oder 98 ohne installierte Active Directory-Clienterweiterungen verwenden das LM-Protokoll zur Benutzerauthentifizierung. Im Bedarfsfall sollte man diese alten Betriebssysteme gegen neuere Versionen ersetzen.

Die *Active Directory-Clienterweiterung* (engl. *Active Directory Client Extension*) für Clientsysteme unter Windows 95, Windows 98 und Windows NT 4.0 können Sie im Internet kostenfrei herunterladen unter:

http://support.microsoft.com/kb/288358

NT-LanManager Version 1(NTLMv1)-Protokoll

Der Nachfolger des einfachen LanManager-Protokolls, das NT-LanManager(NTLM)-Protokoll in der Version 1, wurde mit Windows NT 4.0 (bis einschließlich Service Pack 3) eingesetzt. Das Kennwort wird dabei anhand des RSA-MD4-Algorithmus (Message Digest 4) mit einer Verschlüsselungstiefe von 128 Bit gesichert.

NT-LanManager Version 2(NTLMv2)-Protokoll

Eine Weiterentwicklung des NTLM-Protokolls stellt das NT-LanManager-Protokoll in der Version 2 dar. Hierbei werden die Kennwörter durch ein *Challenge-Response*-Verfahren ergänzt, welches das Erraten der Kennwörter für Angreifer erschwert. Dieses Protokoll kann ab Windows NT 4.0 mit Service Pack 4 oder höher eingesetzt werden.

Verhindern der Zwischenspeicherung von LM-Hashes

Auslesen leicht gemacht

Aus Abwärtskompatibilitätsgründen ist es auf den Domänencontrollern einer Domäne möglich, den LanManager-Hash von Benutzerkennwörtern zwischenzuspeichern. Wenn ein Domänencontroller entsprechend konfiguriert ist, erhält jeder, der über einen Lesezugriff auf die Datenbank der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) verfügt, die Möglichkeit, die gespeicherten Benutzerkennwörter anhand des LanManager-Hashes zu entschlüsseln.

Zwischenspeichern von LM-Hashes unter Windows Server 2008 standardmäßig deaktiviert

Da dies eine sehr große Gefährdung für die Domänensicherheit darstellt, wurde eine Sicherheitsrichtlinie auf den Domänencontrollern unter Windows Server 2008 so vordefiniert, dass das Zwischenspeichern der LM-Hashes der Benutzerkennwörter standardmäßig deaktiviert ist.

Sie finden Sie Sicherheitsrichtlinie innerhalb der Gruppenrichtlinienobjekte einer Active Directory-Domäne unter Windows Server 2008 unter folgendem Namen:

Netzwerksicherheit: Keine Speicherung von LAN-Manager-Hashes bei der nächsten Kennwortänderung

in folgendem Pfad:

Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

Konfiguration der LanManager-Authentifizierungsebene

Darüber hinaus kann man die LanManager-Authentifizierungsebene innerhalb einer Active Directory-Domäne festlegen, um die Verwendung der LanManager(*LM*)- oder NT-LanManager(*NTLM*)-Authentifizierung zu verhindern, hingegen aber die NT-LanManager Version 2(*NTLMv2*)-Authentifizierung zu erlauben.

Sie finden die Richtlinie in der *Default Domain Policy* einer Active Directory-Domäne unter Windows Server 2008 unter dem Namen:

Netzwerksicherheit: LanManager-Authentifizierungsebene

im folgenden Pfad:

Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

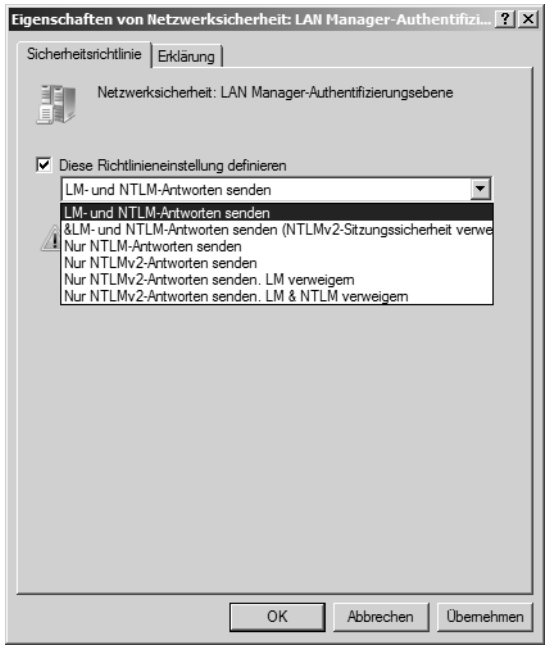


Abbildung 3.5
Konfiguration der LanManager-Authentifizierungsebene in der Default Domain Policy unter Windows Server 2008

Für die Richtlinie *Netzwerksicherheit: LanManager-Authentifizierungsebene* können Sie die folgenden Einstellungen konfigurieren, um Einfluss auf die möglichen Authentifizierungsmethoden der Clientcomputer und Server gegenüber den Domänencontrollern zu nehmen:

Tabelle 3.4
Konfigurierbare LanManager-Authentifizierungsebenen

Ebene	Einstellung	Beschreibung
0	LM- und NTLM-Antworten senden	Clients (und Server) verwenden die LM- und NTLM-Authentifizierung, jedoch niemals die NTLMv2-Sitzungssicherheit; Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung.
1	LM- und NTLM-Antworten senden (NTLMv2-Sitzungssicherheit verwenden, wenn ausgehandelt)	Clients verwenden die LM- und NTLM-Authentifizierung bzw. die NTLMv2-Sitzungssicherheit, wenn dies vom Server unterstützt wird; Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung.
2	Nur NTLM-Antworten senden	Clients verwenden nur die NTLM-Authentifizierung bzw. die NTLMv2-Sitzungssicherheit, wenn dies vom Server unterstützt wird; Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung.

Ebene	Einstellung	Beschreibung
3	Nur NTLMv2-Antworten senden	Clients verwenden nur die NTLMv2-Authentifizierung bzw. die NTLMv2-Sitzungssicherheit, wenn dies vom Server unterstützt wird; Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung.
4	Nur NTLMv2-Antworten senden\LM verweigern	Clients verwenden nur die NTLMv2-Authentifizierung und verwenden die NTLMv2-Sitzungssicherheit, wenn dies vom Server unterstützt wird; Domänencontroller verweigern die LM-Authentifizierung (nur die NTLM- und NTLMv2-Authentifizierung wird akzeptiert).
5	Nur NTLMv2-Antworten senden\LM & NTLM verweigern	Clients verwenden nur die NTLMv2-Authentifizierung und verwenden die NTLMv2-Sitzungssicherheit, wenn dies vom Server unterstützt wird; Domänencontroller verweigern die LM- und NTLM-Authentifizierung (nur die NTLMv2-Authentifizierung wird akzeptiert).

Um die größtmögliche Sicherheit im Zusammenhang mit der NT-LanManager-Authentifizierung zu erreichen, empfiehlt es sich (nach eingehender Überprüfung der möglichen Kompatibilität mit älteren Clientbetriebssystemen und Anwendungen im Netzwerk) mitunter, die Sicherheitsebene 5 der LanManager-Authentifizierungsebene zu konfigurieren. Hierdurch wird die Authentifizierung über die unsicheren LanManager- und NT-LanManager-Protokolle verhindert.

Unter Windows Server 2008 ist die *LanManager-Authentifizierungsebene* standardmäßig auf den Wert der *Ebene 3* voreingestellt. Bei Bedarf sollte man diese Richtlinie auf die Ebene 4 oder gar 5 konfigurieren. Überprüfen Sie jedoch vor der Konfiguration der Richtlinie, ob eventuelle Probleme mit älteren Client-Betriebssystemen oder -Anwendungen zu erwarten sind, die mit den hohen Sicherheitsebenen ggf. nicht kompatibel sind.

Nachdem wir uns mit den Authentifizierungsprotokollen in der Umgebung der Active Directory-Domänendienste (Active Directory Domain Services, AD DS) befasst haben, wenden wir uns nun den Active Directory-Domänen und den darin u. a. für die Authentifizierung eingesetzten Active Directory-Domänencontrollern zu. Diese Server müssen wegen den in der Verzeichnisdatenbank gespeicherten Domänenbenutzerkonten und Benutzerkennwörtern besonders geschützt werden.

3.2 Domänensicherheit

Erhöhte Sicherheit in Windows Server 2008

Die Sicherheit der gespeicherten Objekte in einer Active Directory-Domänendienste-Umgebung stellt in Unternehmensnetzwerken einen immens wichtigen Aspekt dar. Letztlich wird der Zugriff auf die internen Unternehmensdaten (Personal- und Kundendaten, Buchhaltungsdaten etc.) durch bestimmte Sicherheitsmechanismen geregelt. Die Konzeption einer Active Directory gibt den verantwortlichen Administratoren die notwendigen Mittel in Form von Richtlinien und Bedingungen zur Hand, um die Sicherheit dieser Daten zu gewährleisten. Auch ist Microsoft von der ursprünglichen Konzeption einer Domäne, wie sie noch zu Windows NT 4.0-Zeiten herrschte, abgegangen. Die Einfachheit der Verwaltung sollte hierbei jedoch erhalten bleiben, der Aspekt der Sicherheit allerdings um ein Vielfaches erhöht werden. Dies ist Microsoft mit dem Windows Server 2008 sicherlich gut gelungen.

3.2.1 Vordefinierte Sicherheit

Kennwörter mit „null" Zeichenlänge werden nicht mehr akzeptiert

Bereits mit der Einführung von Windows Server 2003 forderte eine Domäne beim Einrichten bereits *komplexe Kennwörter*, die durch potenzielle Angreifer nicht mehr so einfach zu knacken sind. Im Gegensatz zu den vorherigen Betriebssystemen werden Kennwörter mit null Zeichenlänge standardmäßig nicht mehr akzeptiert.

Damit die Sicherheit in den Active Directory-Domänen unter Windows Server 2008 gewahrt werden kann, hat Microsoft bereits viele Voreinstellungen in den nach der Installation einer Domäne standardmäßig vorhandenen Gruppenrichtlinienobjekten (*Default Domain Policy* und *Default Domain Controllers Policy*) vorgenommen. Es existieren noch weitere Sicherheitsfunktionen, die allesamt die Sicherheit in den Unternehmensnetzwerken gewährleisten können. In diesem Zusammenhang sind insbesondere auch die Domänencontroller zu erwähnen, die eine besondere Rolle in den Active Directory-Domänen einnehmen.

An den standardmäßigen, nach der Einrichtung der Active Directory-Domänendienste vorhandenen Gruppenrichtlinienobjekten, *Default Domain Policy* und *Default Domain Controllers Policy*, sollten in der Praxis möglichst keine Änderungen vorgenommen werden. Stattdessen sollte man eigens erstellte Gruppenrichtlinienobjekte definieren und auf gleicher Ebene einer Active Directory-Domäne verknüpfen. Somit steht einer möglicherweise notwendigen Wiederherstellung der standardmäßigen Gruppenrichtlinienobjekte mithilfe des Kommandozeilenbefehls DCGpofix.exe nicht mehr viel entgegen.

3.3 Domänencontroller-Sicherheit

Neue Sicherheitsfunktionen in Windows Server 2008

Die Sicherheit für Domänencontroller spielt in Umgebungen der Active Directory-Domänendienste eine besonders große Rolle. Wenn ein Angreifer es schaffen würde, einen Domänencontroller erfolgreich zu attackieren, so würde er unter Umständen sogar an die darauf gespeicherten Domänenbenutzerkonten und Benutzerkennwörter gelangen. Es ist deshalb besonders wichtig, sich der Schutzbedürftigkeit solcher Systeme bewusst zu sein.

Es existieren ein paar wichtige, sicherheitsrelevante Grundregeln für den Einsatz von Active Directory-Domänencontrollern. Zu diesen zählen u. a.:

- **Deaktivierung aller nicht benötigten Dienste auf einem Domänencontroller** Durch den Verzicht auf unnötig ausgeführte Dienste verringert sich auch die Angriffsfläche gegenüber einem potenziellen Hacker. Mit dem Sicherheitskonfigurations-Assistenten (engl. *Security Configuration Wizard, SCW*), der in Windows Server 2008 bereits enthalten ist, kann man Sicherheitsvorlagen einheitlich auf die Domänencontroller einer Domäne anwenden, um den Zugriff auf unnötige Dienste, Protokolle und Kommunikationsports zu verhindern.
- **Aktivierung der Überwachungsrichtlinien** Durch die Aktivierung der Überwachungsrichtlinien können beispielsweise mögliche, unerlaubte Änderungsversuche an den Benutzerkennwörtern oder den Benutzerkonten und Sicherheitsgruppen der Active Directory-Domäne erkannt werden.
- **Aktivierung der Firewall** Die in Windows Server 2008 integrierte Firewall sollte auf allen Domänencontrollern sowie auch auf allen vorhandenen Client- und Serversystemen aktiviert sein. Hierdurch wird der Zugriff auf ungewünschte Kommunikationsports und Dienste verhindert.

3.3.1 Der Sicherheitskonfigurations-Assistent

In Windows Server 2008 ist der Sicherheitskonfigurations-Assistent (engl. *Security Configuration Wizard, SCW*), der bereits schon Bestandteil des Service Packs 1 für Windows Server 2003 war, integriert. Mit diesem Assistenten kann man bereits vordefinierte oder auch speziell angepasste Sicherheitsvorlagen einheitlich auf die Domänencontroller in einer Active Directory-Domäne anwenden. Darüber hinaus ist es beispielsweise auch möglich, die konfigurierten Sicherheitsvorlagen in fertige Gruppenrichtlinienobjekte für eine Active Directory-Domäne zu transformieren.

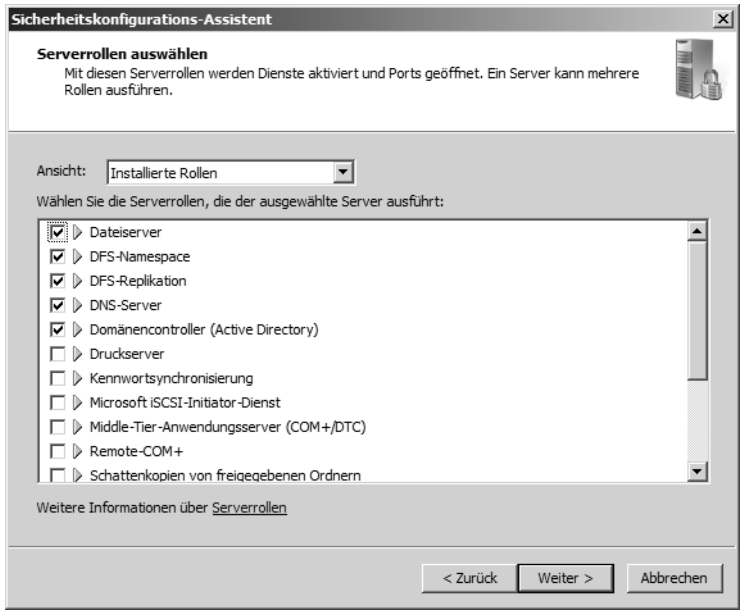


Abbildung 3.6 *Konfiguration von Serverrollen im Sicherheitskonfigurations-Assistenten von Windows Server 2008*

Konfiguration der Sicherheit anhand von definierbaren Sicherheitsrichtlinien

Mit dem Sicherheitskonfigurations-Assistent (*SCW*) kann man die Sicherheitskonfiguration von Servern wie beispielsweise den Domänencontrollern anhand von definierbaren Sicherheitsrichtlinien analysieren und das Ergebnis im HTML-Format anzeigen lassen. Zum Speichern der vorgenommenen Konfigurationen setzt der Sicherheitskonfigurations-Assistent (*SCW*) eine auf XML-Dateien basierte Sicherheitskonfigurationsdatenbank ein.

Enthaltene Tools

Kommandozeilentool für weitere Funktionen

Zum Ausführen sämtlicher Funktionen verfügt der *Sicherheitskonfigurations-Assistent (SCW)* über eine grafische Oberfläche, die man über die Schaltfläche START und dann VERWALTUNG aufrufen kann. Viele der Konfigurationsschritte jedoch, wie zum Beispiel das Transformieren von Sicherheitsvorlagen in Gruppenrichtlinien, werden mit einer Kommandozeilenversion des SCW, dem Tool *SCWcmd.exe*, durchgeführt.

Weitere Informationen zum Sicherheitskonfigurations-Assistent (SCW) finden Sie unter Hilfe und Support in Windows Server 2008.

3.3.2 Sicherheitsrichtlinien für Domänencontroller

Bereits mit der Einführung von Active Directory mit Windows 2000 war es möglich, spezielle Sicherheitsrichtlinien für die Domänencontroller einer Domäne festzulegen. Da mögliche Änderungen an der Active Directory-Datenbank auf den Domänencontrollern vorgenommen werden, ist es wichtig, sich diese Sicherheitsrichtlinien genauer anzuschauen.

Standardmäßige Gruppenrichtlinienobjekte

Nach der Einrichtung der Active Directory-Domänendienste (Active Directory Domain Services, AD DS) auf einem Domänencontroller stehen in der betreffenden Active Directory-Domäne zwei bereits vordefinierte Gruppenrichtlinienobjekte zur Verfügung:

- **Default Domain Policy**
  Dieses Gruppenrichtlinienobjekt ist standardmäßig direkt mit der Domäne verknüpft und enthält Richtlinien für alle Objekte in der betreffenden Active Directory-Domäne.
- **Default Domain Controllers Policy**
  Dieses Gruppenrichtlinienobjekt ist standardmäßig mit der Organisationseinheit (Organizational Unit, OU) Domaincontrollers der Domäne verknüpft. Hiermit werden spezielle Richtlinien auf die in der Domäne vorhandenen Domänencontroller angewendet.

Die in den vordefinierten Gruppenrichtlinienobjekten enthaltenen Richtlinien werden standardmäßig an in der Domäne enthaltene Objekte weitergereicht, sprich: *vererbt*. Beispielsweise enthält die Domäne eine vordefinierte Anzahl an Organisationseinheiten und Containerobjekten, in denen die Active Directory-Objekte enthalten sind. Die nun in der *Default Domain Policy* definierten Richtlinien werden standardmäßig automatisch auf alle in der Domäne vorhandenen Objekte angewendet. Hierdurch wird den Domänenadministratoren die zentrale Verwaltbarkeit und Steuerung der enthaltenen Objekte in der betreffenden Active Directory-Domäne ermöglicht.

Da die Verknüpfung der *Default Domain Controllers Policy* standardmäßig auf die Organisationseinheit (Organizational Unit, OU) *Domain Controllers* angewendet wird, gelten die darin definierten Richtlinien auch nur für solche Computersysteme der Domäne, deren Computerobjekte in der betreffenden Organisationseinheit gespeichert sind.

Neue Überwachungsrichtlinien in Windows Server 2008

Detaillierte Überwachung möglich

Wie bereits in der Einführung dieses Buches beschrieben, wurden in Windows Server 2008 neue Richtlinien für die Überwachung des Verzeichnisdienstzugriffs auf die Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) implementiert.

Diese Unterkategorien der eigentlichen Überwachungskategorie für den Verzeichnisdienstzugriff (engl. *Directory Service Access, kurz: DS-Access*) umfassen:

- Verzeichnisdienständerungen
- Verzeichnisdienstreplikation
- Detaillierte Verzeichnisdienstreplikation
- Verzeichnisdienstzugriff

Sie können die neuen Unterkategorien der Überwachungsrichtlinien für den Verzeichnisdienstzugriff mit dem folgenden Befehl auf einem Domänencontroller unter Windows Server 2008 anzeigen lassen:

```
Auditpol /get /category:"DS-Zugriff"
```

Die Anführungszeichen bei der Benennung der Überwachungskategorie können weggelassen werden, wenn der dabei anzugebende Name aus nur einem einzigen Wort besteht.

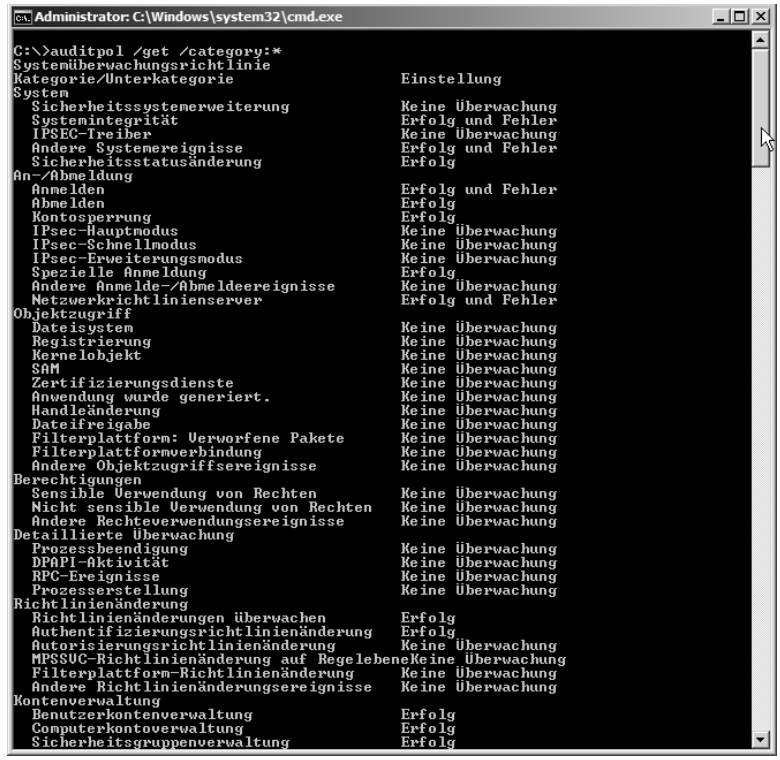
Die neuen Unterkategorien der Überwachungsrichtlinien für den Verzeichnisdienstzugriff (DS-Zugriff) werden in der Konsole für die Gruppenrichtlinienverwaltung nicht angezeigt. Um diese anzuzeigen oder auch zu konfigurieren, müssen Sie das Kommandozeilentool *auditpol.exe* verwenden.

Anzeige der vorhandenen Überwachungskategorien

Um alle vorhandenen Überwachungskategorien anzeigen zu lassen, verwenden Sie wiederum das Kommandozeilentool Auditpol.exe wie folgt:

```
Auditpol /get /category:*
```

Abbildung 3.7
Anzeige der Überwachungskategorien



Die folgende Tabelle enthält die für die Überwachung der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) auf den Domänencontrollern unter Windows Server 2008 relevanten, voreingestellten Richtlinien:

Tabelle 3.5
Konfigurierbare, voreingestellte Richtlinien für die Überwachung der Active Directory-Domänendienste unter Windows Server 2008

Kategorie	Unterkategorie	Standardeinstellung
An-/Abmeldung	Anmelden	Erfolg und Fehler
	Abmelden	Erfolg
	Kontosperrung	Erfolg
	Spezielle Anmeldung	Erfolg
	Andere Anmelde-/Abmeldeereignisse	Keine Überwachung
	Netzwerkrichtlinienserver	Erfolg und Fehler
Richtlinienänderung	Richtlinienänderungen überwachen	Erfolg
	Authentifizierungsrichtlinienänderung	Erfolg

Kategorie	Unterkategorie	Standardeinstellung
Kontenverwaltung	Benutzerkontenverwaltung	Erfolg
	Computerkonten-verwaltung	Erfolg
	Sicherheitsgruppen-verwaltung	Erfolg
DS-Zugriff	Verzeichnisdienst-änderungen	Keine Überwachung
	Verzeichnisdienst-replikation	Keine Überwachung
	Detaillierte Verzeichnis-dienstreplikation	Keine Überwachung
	Verzeichnisdienstzugriff	Erfolg
Kontoanmeldung	Ticketvorgänge des Kerberos-Diensts	Erfolg
	Andere Kontoanmelde-ereignisse	Keine Überwachung
	Kerberos-Authentifizie-rungsdienst	Erfolg
	Überprüfung der Anmelde-informationen	Erfolg

Verzeichnisdienständerungen überwachen

Konfiguration über die Kommandozeile

Wie in der oberen Tabelle zu erkennen, sind die Überwachungsrichtlinien für Verzeichnisdienständerungen auf den Domänencontrollern unter Windows Server 2008 standardmäßig nicht aktiviert. Bei Bedarf kann man diese Überwachungsrichtlinien in der *Default Domain Controllers Policy* der Domäne mit dem Befehl `Auditpol.exe` aktivieren.

Zum Aktivieren der Überwachungsrichtlinien für erfolgreiche Verzeichnisdienständerungen in der *Default Domain Controllers Policy* der Domäne geben Sie auf einem der Domänencontroller unter Windows Server 2008 den folgenden Befehl ein:

```
Auditpol/set/subcategory:"Verzeichnisdienständerungen"/
success:enable
```

Abbildung 3.8 *Aktivierung der Überwachungsrichtlinie für Verzeichnisdienständerungen unter Windows Server 2008*

Nach der Aktivierung der Überwachungsrichtlinien für Verzeichnisdienständerungen in der *Default Domain Controllers Policy* der Domäne werden diese nun auf alle Domänencontroller unter Windows Server 2008 angewendet.

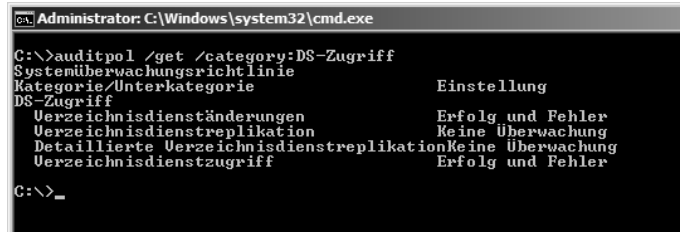


Abbildung 3.9 *Überprüfung der aktuellen Überwachungskonfiguration unter Windows Server 2008 mithilfe von auditpol.exe*

Anzeige der Ursprungswerte bei Änderungen

Bei Änderungen von Attributwerten eines hierzu überwachten Objektes in der Datenbank der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) werden in der Ereignisanzeige unter Windows Server 2008 nun auch der jeweilige Ursprungswert sowie auch der neue Attributwert angezeigt. Dies ermöglicht einem Administrator, den ursprünglichen Attributwert eines Objektes nach einer versehentlichen Änderung wieder herzustellen.

Natürlich wird ebenso auch erfasst, von welchem Benutzerkonto aus die Änderung ausgeführt wurde.

Die Überwachung fehlgeschlagener Verzeichnisdienständerungen sollte bei Bedarf zusätzlich aktiviert werden. Verwenden Sie zum Aktivieren der Überwachung dieser Ereignisse wiederum den folgenden Befehl:

```
Auditpol /set /subcategory:"Verzeichnisdienständerungen"
/failure:enable
```

Zum Deaktivieren der Überwachung setzen Sie im Rahmen der gleichen Syntax des Befehls `Auditpol.exe` statt des Wertes `enable` einfach den Wert `disable`.

Aktivieren der Überwachung in zwei Stufen

Die Aktivierung der Überwachungsrichtlinien alleine reicht zur Überwachung von Änderungen an den Objekten in der Datenbank der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) jedoch noch *nicht* aus. Es muss *zusätzlich* noch festgelegt werden, welche Active Directory-Objekte in welchem Umfang überwacht werden sollen.

Diese Überwachungsstrategie in zwei Stufen gleicht der Überwachung von Dateien und Ordnern in NTFS-Datenträgern. Auch dort muss nach der Aktivierung der Überwachungsrichtlinie jeweils genau festgelegt werden, welche Dateien und Ordner in Bezug auf bestimmte Änderungen überwacht werden sollen. Erst danach werden die entsprechend definierten Ereignisse in den Ereignisprotokollen dokumentiert.

Aktivierung der Überwachung einzelner Active Directory-Objekte

Mit der Aktivierung der Überwachungsrichtlinien für den Verzeichnisdienstzugriff (*DS Access*) besteht nun die Möglichkeit, beispielsweise die Änderungen an Benutzerobjekten in der Active Directory-Domäne zu überwachen. Eine erweiterte Überwachung der Verzeichnisdienstzugriffe findet jedoch noch nicht statt.

Festlegen der zu überwachenden Objekte

Damit die Überwachung der Active Directory-Objekte erfolgen kann, muss nun festgelegt werden, welche der Objekte in der Active Directory-Domänendienste-Datenbank überhaupt überwacht werden sollen. Dies legt man in der *Systemzugriffskontrollliste* (engl. *System Access Control List, SACL*) der zu überwachenden Organisationseinheiten oder der einzelnen Objekte in der Active Directory-Domänendienste-Datenbank fest.

Um die Überwachung der Änderungen an einzelnen Objekten in einer Organisationseinheit (engl. *Organizational Unit, OU*) festzulegen, gehen Sie wie folgt vor:

1. Klicken Sie auf START, VERWALTUNG, und öffnen Sie die Konsole ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
2. Klicken Sie in der Menüleiste auf ANSICHT und dann auf ERWEITERTE FEATURES.
3. Klicken Sie mit der rechten Maustaste auf die zu überwachende Organisationseinheit (engl. *Organizational Unit, OU*) oder das zu überwachende Active Directory-Objekt und dann auf EIGENSCHAFTEN.
4. Wechseln Sie in den Eigenschaften auf das Register SICHERHEIT, und klicken Sie auf ERWEITERT.
5. Wechseln Sie zum Register ÜBERWACHUNG, und klicken Sie auf HINZUFÜGEN.

Alternativ können Sie auch einen vorhandenen Überwachungseintrag auswählen und die darin bereits festgelegten Einstellungen über einen Klick auf die Schaltfläche BEARBEITEN anzeigen lassen. Hier können Sie die gewünschten Änderungen an den vorhandenen Einstellungen vornehmen.

6. Wählen Sie die zu überwachende Benutzergruppe (beispielsweise die Gruppe „Jeder“) oder den gewünschten Benutzer aus, und klicken Sie auf OK.
7. Bestimmen Sie die zu überwachenden Zugriffe (Erfolg und/oder Fehler), und klicken Sie anschließend auf OK.

8. Schließen Sie das Dialogfeld *Erweiterte Sicherheitseinstellungen* mit einem Klick auf die Schaltfläche OK.
9. Schließen Sie das Dialogfeld *Eigenschaften von ..*mit einem erneuten Klick auf die Schaltfläche OK.

Nach dieser Konfiguration wird der entsprechend definierte Verzeichnisdienstzugriff (*DS-Zugriff*) nun überwacht und bei Eintreten des entsprechenden Ereignisses in der Ereignisanzeige des jeweiligen Domänencontrollers dokumentiert.

Die Domänenadministratoren sind somit in der Lage, sämtliche Änderungen an den in der Datenbank der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) vorhandenen Objekte zu überwachen und bei Bedarf anschließend rückgängig zu machen.

Abbildung 3.10
Konfiguration der Überwachungsrichtlinien

Dokumentation der Änderungen in der Ereignisanzeige

Erfassung der Änderungen in den Ereignisanzeigeprotokollen

Die Änderungen, die durch die aktivierten Überwachungsrichtlinien für die Verzeichnisdienstzugriffe (*DS Access*) auf Domänencontrollern erfasst werden, speichert das betreffende Serversystem in Ereignisanzeigeprotokollen.

Abbildung 3.11
Anzeige von überwachten Ereignissen

Archivierung der Ereignisprotokolle

Archivierung von Ereignissen möglich

Die Erfassung der Änderungen von Objekten in der Datenbank der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) kann unter bestimmten Umständen von rechtlicher Bedeutung sein. Damit die Ereignisse in den Ereignisanzeigeprotokollen der Active Directory-Domänencontroller nicht versehentlich überschrieben werden, müssen diese Protokolle regelmäßig archiviert werden. Auch sollten die Ereignisprotokolle so konfiguriert werden, dass sie beim Erreichen einer vordefinierten Größe zum Erfassen neuer Einträge nicht einfach überschrieben werden. Die genaue Vorgehensweise zur entsprechenden Konfiguration der Ereignisprotokolldateien wird Ihnen in der Hilfe von Windows Server 2008 erklärt.

3.4 Zusammenfassung

Wie Sie in den vorangegangenen Seiten erfahren haben, kommen in Umgebungen der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) verschiedene Protokolle zum Authentifizieren von Benutzern und Computern zum Einsatz. Neben dem Kerberos-Protokoll wird auch weiterhin die Authentifizierung auf Ebene des NT-LanManager-Protokolls unterstützt. Beschrieben wurden auch die vordefinierten Sicherheitseinstellungen, die in einer Active Directory-Domäne unter Windows Server 2008 automatisch aktiviert sind.

Wie beschrieben, bietet der Sicherheitskonfigurations-Assistent (engl. *Security Configuration Wizard, SCW*) durch den Einsatz entsprechender Sicherheitsvorlagen die Möglichkeit, Domänencontroller und auch andere Server und Clientcomputer auf nur die notwendigen Rollen, Funktionen und angebotenen Kommunikationsports zu beschränken. Hierdurch kann die Sicherheit in Unternehmensumgebungen gegenüber potenziellen Angreifern erheblich verstärkt werden.

Im nächsten Kapitel wenden wir uns der Planung einer Infrastruktur der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) zu.