INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Active-Directory

Das Active Directory ist die zentrale Steuer- und Konfigurationsschnittstelle in einem Windows-Netzwerk. Praktisch alles kann darüber verwalten und konfiguriert werden. Daher ist die korrekte und sinnvolle Konfiguration sehr wichtig. Dieser INFONEWS geht dabei auf die verschiedenen Aspekte ein und beantwortet unter anderem die folgenden Fragen:

- Aus welchen Bestandteilen besteht das AD?
- Welche Konfigurationen sind möglich?
- Wie funktionieren Gruppenrichtlinien?

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

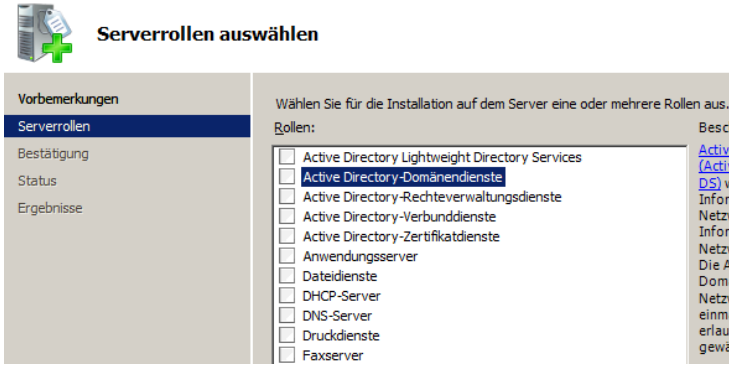
Telefon 052 320 91 20
Fax 052 320 91 21

2 Active Directory

Das Active Directory ist der zentrale Verzeichnisdienst in einem Windows-Netzwerk. Mit der Einführung von Windows Server 2008 wurde die Kernkomponente als Active Directory Domain Services (ADDS) bezeichnet. Das Active Directory (AD) ermöglicht es, ein Netzwerk analog einer realen Struktur oder der räumlichen Verteilung gliedern. Im AD können verschiedene Objekte gegliedert und verwaltet werden. Dazu gehören beispielsweise Benutzer, Gruppen, Computer, Dienste, Freigaben und viele weitere Elemente. Bereits mit Windows Server 2003 R2 wurden die Möglichkeiten massiv erweitert. Windows Server 2008 wurde nochmals stark erweitert.

3 Rollen

Das AD unter WS08 wurde in fünf Rollen aufgeteilt. Die folgenden Rollen stehen dabei zur Verfügung:



- Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) Diese Rolle ersetzt die Zertifikatdienste unter Windows Server 2003. Sie können mit dieser Rolle eine Public Key Infrastructure (PKI) aufbauen.
- Active Directory-Domänendienste (Active Directory Domain Services, AD DS) Hierbei handelt es sich um die Rolle eines Domänen Controllers für das Active Directory. Bevor Sie einen Server zum Domänencontroller für das Active Directory heraufstufen können, muss diese Rolle installiert sein.
- Active Directory-Verbunddienste (Active Directory Federation Services, AD FS) Mit den AD FS können Sie eine webbasierte Single Sign-On (SSO)-Infrastruktur aufbauen.
- Active Directory Lightweight Directory Services (AD LDS) Mit diesen Diensten können Applikationen, welche Informationen in einem Verzeichnis speichern, arbeiten. Im Gegensatz zu den Active Directory Domain Services, wird das Verzeichnis nicht als Dienst ausgeführt. Diese Dienste benötigen keinen reinen Domänencontroller. Auf einem Server können mehrere Instanzen laufen. Bei den AD LDS handelt es sich sozusagen um ein Mini-Active Directory ohne grosse Verwaltungsfunktionen. Unter Windows Server 2003 wurden diese Dienste noch Active Directory Application Mode (ADAM) genannt.
- Active Directory-Rechteverwaltungsdienste (Active Directory Rights Management Services, AD RMS) Mit dieser Technologie werden Daten mit digitalen Signaturen versehen, um sie vor einem unerwünschten Zugriff zu sichern. Besitzer von Dateien können basierend auf Benutzerinformationen exakt festlegen, was andere Benutzer mit den Dateien machen dürfen. Dokumente können zum Beispiel als "Nur Lesen" konfiguriert werden.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4 Betriebsmasterrollen

In einem AD sind alle Domänencontroller gleichberechtigt. Auf jedem Domänencontroller können Änderungen vorgenommen werden, die daraufhin zu den anderen Domänencontrollern repliziert werden. Allerdings gibt es fünf unterschiedliche Rollen, die ein Domänencontroller annehmen kann:

1. PDC-Emulator
2. Infrastrukturmaster
3. RID-Master
4. Schemamaster
5. Domänennamenmaster

Die verschiedenen Rollen, also PDC-Emulator, Infrastrukturmaster, RID-Master, Schemamaster und Domänennamenmaster, werden als Flexible Single Master Operation* (FSMOs) bezeichnet, jede dieser Rollen ist entweder einmalig pro Domäne (PDC-Emulator, Infrastrukturmaster, RID-Master) oder sogar einmalig pro Gesamtstruktur (Schemamaster, Domänennamenmaster). Fällt eine dieser Rollen aus, gibt es im Active Directory Fehlfunktionen, die schnell behoben werden müssen, da durch diese Fehlfunktionen der produktive Betrieb beeinflusst wird. Schon aus der Bezeichnung Flexible geht hervor, dass diese Rollen zwar einzelnen Domänencontrollern zugewiesen werden, aber auch recht flexibel verschoben werden können.

4.1 PDC-Emulator

Die Rolle des PDC-Emulators gibt es in jeder Domäne von Active Directory einmal. Der erste installierte Domänencontroller einer Active Directory-Domäne bekommt diese Rolle automatisch zugewiesen.

- Er ist für die Anwendung und Verwaltung der Gruppenrichtlinien zuständig. Steht der Domänencontroller, der diese Rolle hat, nicht mehr zur Verfügung, werden Gruppenrichtlinien fehlerhaft angewendet und können so gut wie nicht mehr verwaltet werden, da spezielle Verwaltungskonsolen, wie die Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC), gezielt die Verbindung zum PDC-Emulator aufbauen.
- Der PDC-Emulator ist darüber hinaus für Kennwortänderungen bei Benutzern verantwortlich.
- Er steuert auch die externen Vertrauensstellungen einer Domäne.
- Außerdem ist der PDC-Emulator der Zeitserver einer Domäne.

Alle hier beschriebenen Funktionen sind gestört, wenn der PDC-Emulator nicht mehr zur Verfügung steht.

Um den PDC-Emulator anzuzeigen, klicken Sie mit der rechten Maustaste auf die Domäne im Snap-In und wählen Sie im Kontextmenü den Eintrag Betriebsmaster aus. Es öffnet sich ein neues Fenster. Holen Sie die Registerkarte PDC in den Vordergrund. Hier wird Ihnen der aktuelle PDC-Emulator der Domäne angezeigt.

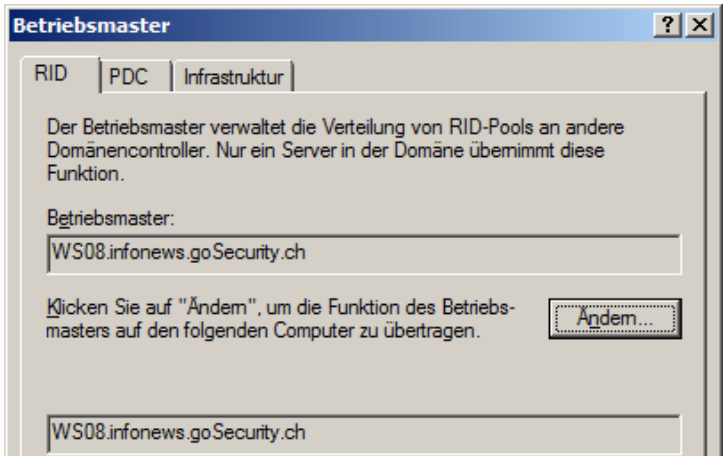
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4.2 RID-Master

Auch die Rolle des RID-Masters erhält der erste installierte Domänencontroller einer Domäne automatisch. Den RID-Master gibt es einmal in jeder Domäne einer Gesamtstruktur. Die Aufgabe des RID-Masters ist es, den anderen Domänencontrollern einer Domäne Relative Identifiers (RIDs) zuzuweisen. Wird ein neues Objekt in der Domäne erstellt, also ein Computerkonto, ein Benutzer oder eine Gruppe, wird diesem Objekt eine eindeutige Sicherheits-ID (SID) zugewiesen. Diese SID erstellt der Domänencontroller aus einer domänenspezifischen SID in Verbindung mit einer RID aus seinem RID-Pool. Ist der RID-Pool eines Domänencontrollers aufgebraucht ist, werden ihm vom RID-Master neue RIDs zugewiesen. Steht der RID-Master nicht mehr zur Verfügung und bekommen die Domänencontroller damit keine RIDs mehr, können keine neuen Objekte mehr in dieser Domäne erstellt werden, bis der RID-Master wieder einem Domänencontroller zur Verfügung gestellt wird. Jeder Domänen Controller erhält zunächst einen Pool von 500 RIDs. Stehen nur noch 100 RIDs zur Verfügung, fordert er neue RIDs vom RID-Master an. Steht der RID-Master nicht mehr zur Verfügung, können also pro Domänencontroller der Domäne immerhin noch bis zu 100 neue Objekte erstellt werden, was für die meisten Organisationen ausreichen wird.

Um den Domänencontroller anzuzeigen, der die Rolle des RID-Masters verwaltet, öffnen Sie wieder das Snap-In Active Directory-Benutzer und -Computer, klicken mit der rechten Maustaste auf die Domäne und wählen im Kontextmenü den Eintrag Betriebsmaster aus.



4.3 Infrastrukturmaster

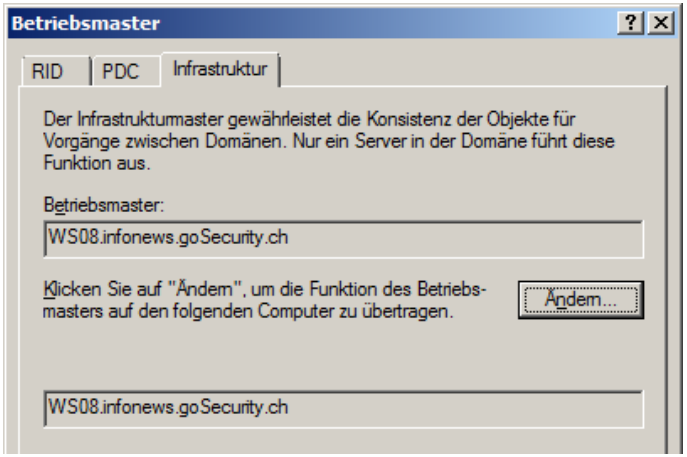
Auch den Infrastrukturmaster gibt es in jeder Domäne einer Gesamtstruktur einmal. Diese Rolle erhält ebenfalls wieder der erste installierte Domänencontroller einer Active Directory-Domäne. In einer Gesamtstruktur mit nur einer Domäne spielt dieser Betriebsmaster keine Rolle. Seine Bedeutung steigt jedoch beim Einsatz mehrerer Domänen oder Strukturen. Er hat in einer Domäne die

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Aufgabe, die Berechtigungen für die Benutzer zu steuern, die aus unterschiedlichen Domänen kommen. Da die Berechtigungsanfragen sonst sehr lange dauern würden, wenn zum Beispiel in den Berechtigungen einer Ressource Benutzerkonten oder Gruppen aus unterschiedlichen Domänen gesetzt sind, dient der Infrastrukturmaster einer Domäne sozusagen als Cache für diese Zugriffe, um die Abfrage der Berechtigungen zu beschleunigen. Er wird außerdem für die Auflösung von Verteilergruppen verwendet, wenn Sie Exchange einsetzen, da auch an dieser Stelle eine Gruppe Mitglieder aus verschiedenen Domänen der Gesamtstruktur enthalten kann.

Um sich den Infrastrukturmaster anzeigen zu lassen, öffnen Sie das Snap-In Active Directory-Benutzer und -Computer. Klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie die Option Betriebsmaster aus. Wechseln Sie auf die Registerkarte Infrastruktur.

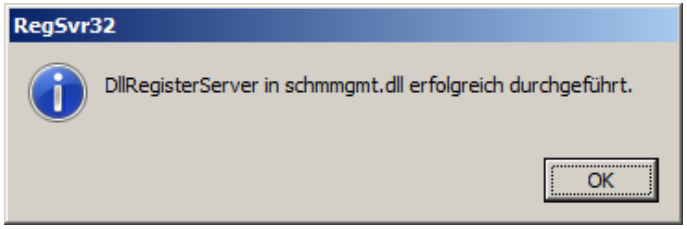


4.4 Schemamaster

Die Struktur eines Verzeichnisses, wie das AD eines ist, wird Schema genannt. Im Schema ist genau definiert, welche Informationen auf welche Art gespeichert werden sollen. Das AD speichert die Daten, das Schema definiert, wie sie gespeichert werden. Es gibt Objekte und es gibt Attribute. Die Attribute sind Objekten zugeordnet. Jeder Verzeichniseintrag ist ein Objekt. Beim AD sind Objekte also Benutzer, Computer, Freigaben oder Drucker. Das AD verfügt über ein erweiterbares Schema. Dieses gibt die Möglichkeit, zusätzliche Informationen im Verzeichnis flexibel zu speichern. Durch das erweiterbare Schema lassen sich jederzeit zusätzliche Objekteigenschaften hinzufügen. Diese Funktion wird beispielsweise von Exchange Server 2000/2003/2007 genutzt. Damit das Schema erweitert werden kann, wird der Schemamaster benötigt. In jeder Gesamtstruktur gibt es nur einen Schemamaster. Nur auf diesem Schemamaster können Änderungen am Schema vorgenommen werden. Steht der Schemamaster nicht mehr zur Verfügung, können auch keine Erweiterungen des Schemas stattfinden und die Installation schlägt fehl. Der erste installierte Domänencontroller der ersten Domäne und Struktur einer Gesamtstruktur erhält die Rolle des Schemamasters. Alle Änderungen des Schemas werden ausschließlich auf dem Schemamaster durchgeführt. Der Schemamaster hat ansonsten keine Auswirkungen auf den laufenden Betrieb. Solange das Schema nicht durch eine spezielle Applikation erweitert wird, spielt dieser Betriebsmaster keine Rolle.

Damit der Schemamaster angezeigt werden kann, müssen Sie zunächst das Snap-In registrieren, welches das Schema anzeigt. Aus Sicherheitsgründen wird dieses Snap-In zwar installiert, jedoch nicht angezeigt. Geben Sie über Start/Ausführen den Befehl *regsvr32 schmmgmt.dll*

ein. Sie erhalten daraufhin die Information, dass die dll im System erfolgreich registriert wurde.



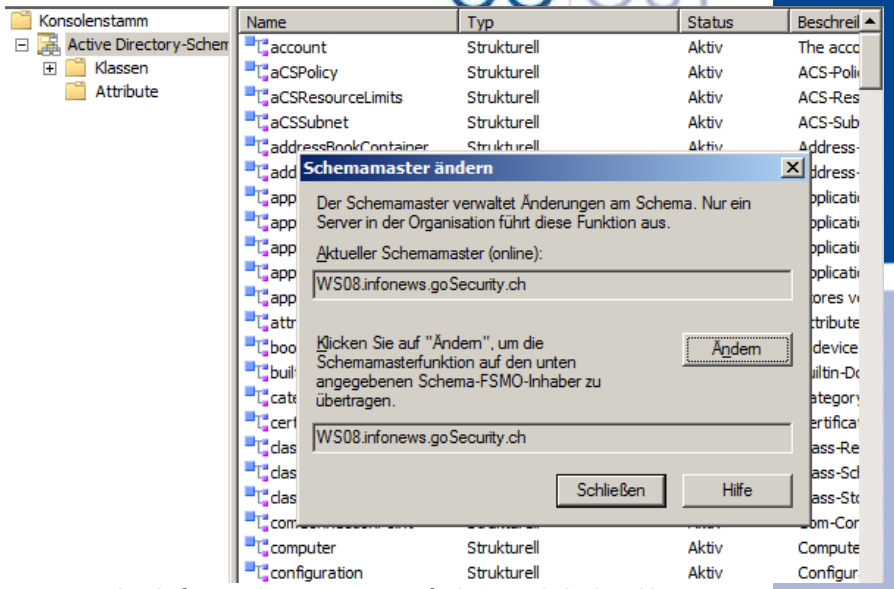
Anschliessend kann via der MMC das Snap-In Active-Directory-Schema hinzufügen.

4.5 Empfehlungen

Standardmäßig besitzt der erste installierte Domänencontroller einer Gesamtstruktur alle fünf FSMO-Rollen seiner Domäne und der Gesamtstruktur. Jeder erste Domänencontroller weiterer Domänen verwaltet die drei Betriebsmasterrollen seiner Domäne (PDC-Emulator, RID-Master, Infrastrukturmaster). Vor allem in größeren Active Directorys empfiehlt Microsoft jedoch die Verteilung der Rollen auf verschiedenen Domänencontrollern. Zur optimalen Verteilung der FSMO-Rollen gibt es folgende Empfehlungen:

- Der Infrastrukturmaster sollte nicht auf einem globalen Katalog liegen, da ansonsten Probleme bei der Auflösung von Gruppen, die Mitglieder aus verschiedenen Domänen haben, auftreten können. Bei Unternehmen mit nur einer Domäne müssen Sie diese Richtlinie nicht beachten. Installieren Sie einen zusätzlichen Domänencontroller in der Domäne, überprüft

  der Assistent für das Active Directory, ob sich



der Infrastrukturmaster auf einem globalen Katalog befindet. Ist das der Fall, schlägt der Assistent das Verschieben der Rolle auf den neuen Domänencontroller vor.

- Domänennamenmaster und Schemamaster sollten auf einem gemeinsamen Domänencontroller liegen, der auch globaler Katalog ist.
- PDC-Emulator und RID-Master kommunizieren viel miteinander und sollten daher auf einem gemeinsamen Domänencontroller Hegen, der auch globaler Katalog ist.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

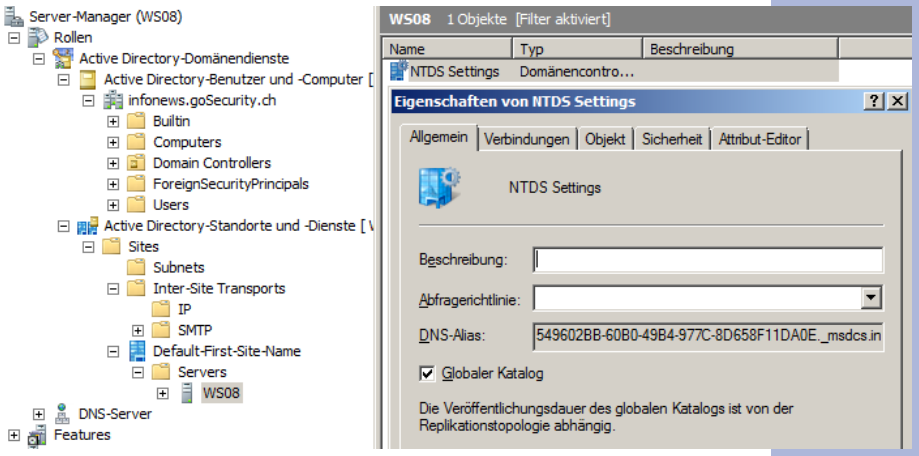
5 Globaler Katalog

An jedem Standort im AD sollte ein globaler Katalog-Server installiert sein. Der globale Katalog ist eine weitere Rolle, die ein Domänen Controller einnehmen kann. Im Gegensatz zu den beschriebenen FSMO-Rollen kann (und sollte auch) die Funktion des globalen Katalogs mehreren Domänencontrollern zugewiesen werden. Dem globalen Katalog kommt in einer Active Directory-Domäne eine besondere Bedeutung zu. Er enthält einen Index aller Domänen einer Gesamtstruktur. Aus diesem Grund wird er von Serverdiensten wie Exchange Server 2007 und Suchanfragen verwendet, wenn Objekte aus anderen Domänen Zugriff auf eine Ressource der lokalen Domäne enthalten.

Der globale Katalog spielt darüber hinaus eine wesentliche Rolle bei der Anmeldung von Benutzern. Steht der globale Katalog in einer Domäne nicht mehr zur Verfügung, können sich keine Benutzer mehr anmelden, wenn keine speziellen Vorbereitungen getroffen worden sind. Ein Domänencontroller mit der Funktion des globalen Katalogs repliziert sich nicht nur mit den Domänencontrollern seiner Domäne, sondern enthält eine Teilmenge aller Domänen in der Gesamtstruktur. Der erste installierte Domänencontroller einer Gesamtstruktur ist automatisch ein globaler Katalog. Alle weiteren globalen Kataloge müssen hingegen manuell hinzugefügt werden. Der globale Katalog dient auch zur Auflösung von universalen Gruppen. Sie sollten aber nicht alle Domänen Controller zu globalen Katalogen machen, da dadurch der Replikationsverkehr zu diesen Domänencontrollern stark zunimmt. An jedem Standort sollten zwei bis drei Domänencontroller diese Aufgabe übernehmen.

Nachträglich können Sie wie folgt einen Domänencontroller zum globalen Katalog konfigurieren:

1. Um einen Domänencontroller als globalen Katalog zu konfigurieren, benötigen Sie das Snap-In Active Directory-Standorte und -Dienste aus dem Server-Manager.
2. Öffnen Sie dieses Snap-In und rufen Sie die Eigenschaften der Option NTDS Settings über Sites/ <Name des Standortes>/Servers/<Servername> auf.
3. Auf der Registerkarte Allgemein aktivieren Sie das Kontrollkästchen Globaler Katalog.



Haben Sie diese Konfiguration vorgenommen, repliziert sich der Server zukünftig mit weiteren Domänencontrollern und enthält nicht nur Informationen seiner Domäne, sondern einen Index der Gesamtstruktur.

6 Struktur-Elemente

6.1 Struktur (Baum, Tree)

Eine Struktur ist eine hierarchische Anordnung von Domänen, welche den gleichen, zusammenhängenden DNS Namensbereich verwenden (Contiguous DNS Namespace). Pro Tree innerhalb eines Forests sind also alle AD-Domänen angeordnet, die innerhalb eines DNS Namensbereichs wie z.B. firma.ch, sub1.firma.ch, sub2.firma.ch etc. angesiedelt sind.

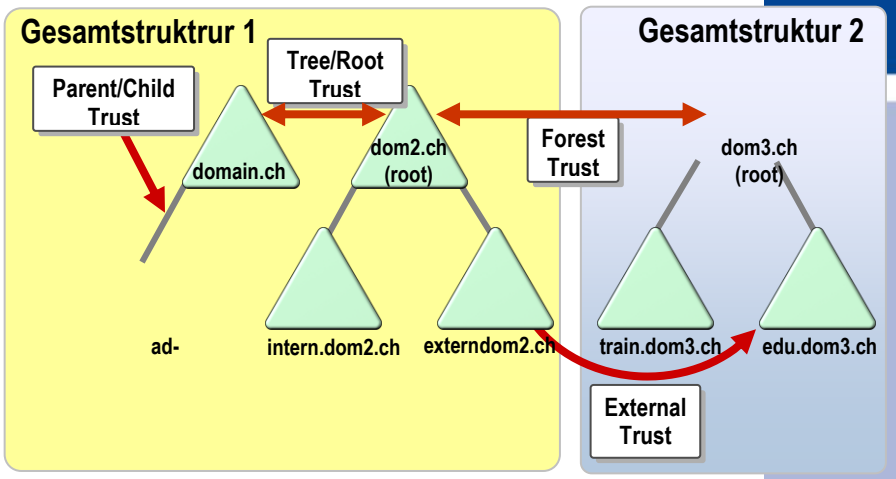
Sämtliche untergeordneten Domänen in einem Forest besitzen eine bidirektionale, transitive Vertrauensstellung mit ihrer jeweils übergeordneten Domäne. Vertrauensstellungen bewirken zum Beispiel, dass Benutzern einer Domäne auf Servern in einer anderen Domäne Zugriffsrechte erteilt werden können.

6.2 Gesamtstruktur

Eine Gesamtstruktur besteht aus einer oder mehreren Strukturen (Trees), welche unterschiedliche Namenspace verwenden können. Sämtliche Strukturen der Gesamtstruktur verwenden ein gemein-sames Schema und einen gemeinsamen globalen Katalog.

Hinweis: Ein Tree hat abgesehen vom unterschiedlichen DNS Namespace keine weitere eigenständige Funktionalität im AD. Alle Domänen in unterschiedlichen Trees sind gleichwertig und mittels bidirektionaler transitiver Trusts baumartig miteinander verbunden. Einzige Ausnahme ist die Forest Root Domain, welche als erste Domäne eines Forests erzeugt wird und in sich spezielle Gruppen wie die „Enterprise Admins“ und „Schema Admins“ beherbergt.

6.3 Vertrauensstellungen



Seit Windows Server 2003 sind folgende Vertrauensstellungen möglich:

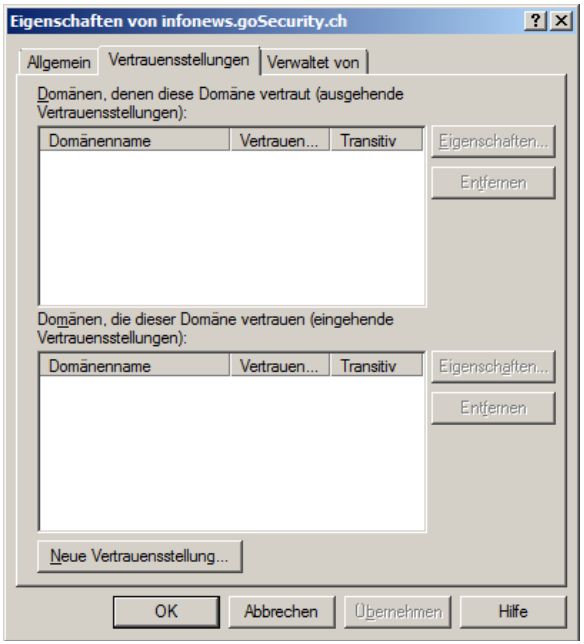
Trust Typ	Beschreibung
Parent/Child	Besteht zwischen sämtlichen Domänen der Gesamtstruktur. Dieser Typ ist transitiv und gegenseitig (two-way). Diese Trusts werden standardmässig erstellt und können nicht entfernt werden.
Tree/Root	Besteht zwischen sämtlichen Strukturen der Gesamtstruktur. Dieser Typ ist transitiv und gegenseitig (two-way). Die Trusts werden standardmässig erstellt und können nicht entfernet werden.
External	Besteht zu Domänen, die nicht Mitglied der Gesamtstruktur sind. Dieser Typ ist NICHT transitiv und ist ein- oder gegenseitig (one-way or two-way).
Forest	Besteht zwischen Windows 2003 Ge-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

	samtstrukturen, welche sich im Windows 2003 Server Funktionsmodus befinden. Dieser Typ ist transitiv oder nicht transitiv und einseitig oder gegenseitig (one-way or two-way).

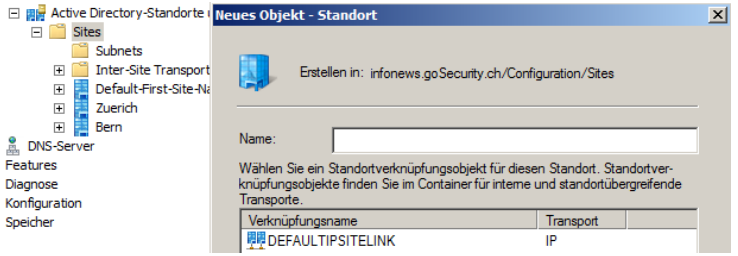
Eine manuelle Vertrauensstellung kann unter den Eigenschaften der Domaine im Snap-In "Active Directory-Domänen und -Vertrauensstellungen" vorgenommen werden. Im Register "Vertrauensstellungen" kann der Punkt "Neue Vertrauensstellung" ausgewählt werden:



6.4 Standorte

Mittels Standorten lässt sich die physische Topologie eines Netzwerks abbilden. Microsoft empfiehlt, verschiedene Standorte, die miteinander verbunden sind, jeweils als eigene Site zu definieren. Standorte werden festgelegt, um den Replikations- und AD-Netzwerkverkehr optimal steuern zu können. So ist es zum Beispiel möglich, den Replikationsverkehr ausserhalb der Geschäftszeiten erfolgen zu lassen. Auch werden bei definierten Sites Benutzeranmeldungen zuerst von Domänencontrollern desselben Standorts übernommen.

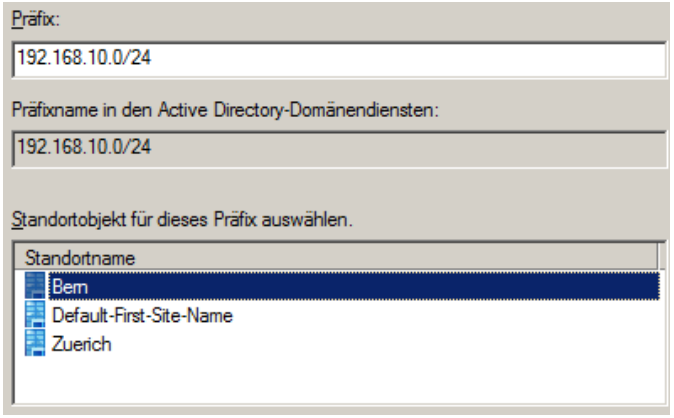
Standort hinzufügen: Unter Sites, Rechte Maustaste - Neuer Standort auswählen. Folgendes Fenster öffnet sich:



Als zweites wird unter Subnets, Rechte Maustaste, Neues Subnetz ein neues Subnetz definiert und mit dem entsprechenden Standort verknüpft.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

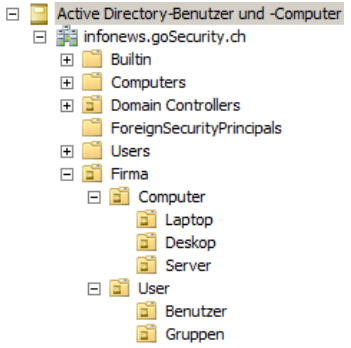
Telefon 052 320 91 20
Fax 052 320 91 21



Wird an diesem Standort ein Server zu einem Domain Controller heraufgestuft, wird anhand der IP-Adresse des Servers dieser automatisch mit dem richtigen Standort verknüpft.

7 Organisation des ADs

In der Domäne sollten die Objekte in einer sinnvollen Struktur gepflegt werden. Dazu sollte in der Domäne als erstes eine neue OU erstellt werden. Diese kann beispielsweise "Firma" lauten. Darunter werden weitere Elemente platziert. Es lohnt sich, hier einige Zeit in die Planung zu investieren. Oft macht es wenig Sinn, die gesamte Firmenstruktur eins-zu-eins abzubilden. Vereinfacht werden die Funktionen nur mit der OU Computer mit den Unter-OUs Desktop, Laptop und Server sowie die OU User mit den Untergruppen Benutzer und Gruppen gezeigt:



Hinweise:

- Standardmässig werden Computer, die zur Domäne hinzugefügt werden, in der OU Computers platziert. Hier sollten aber keine Geräte platziert werden, da keine Gruppenrichtlinien verknüpft werden können.

  Mit dem Befehl *redircmp.exe <definierter Name DN>*, Beispiel: *redircmp "OU=Clients, DC=Domäne, DC=Erweiterung*" kann ein Ort für neu erstellte Computer zugewiesen werden. Wird ein Computer, z.B. via Wizard oder lokal auf dem Gerät via Hinzufügen zu einer Domäne in eine Domäne integriert, wird das Objekt an diese Stelle platziert

- Standardmässig werden neu angelegte Benutzer in der OU Users platziert. Hier sollten aber ebenfalls keine Benutzer platziert werden, da keine Gruppenrichtlinien verknüpft werden können.

  Mit dem Befehl *redirusr.exe <definierter Name DN>*, Beispiel: *redirusr "OU=Users, DC=Domäne, DC=Erweiterung*" wird analog den

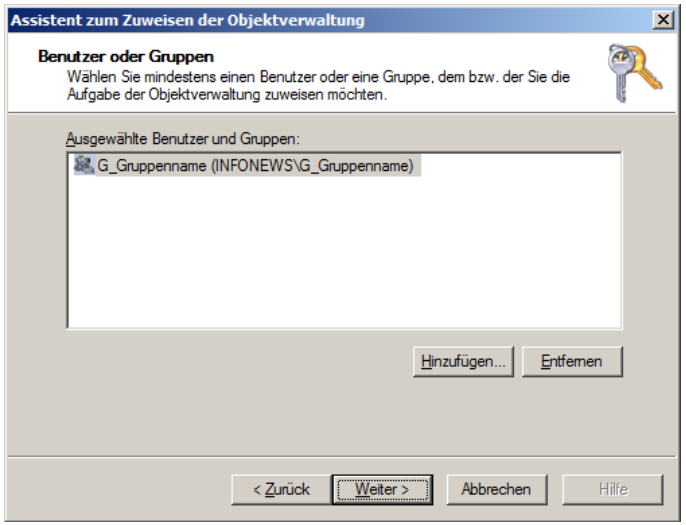
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

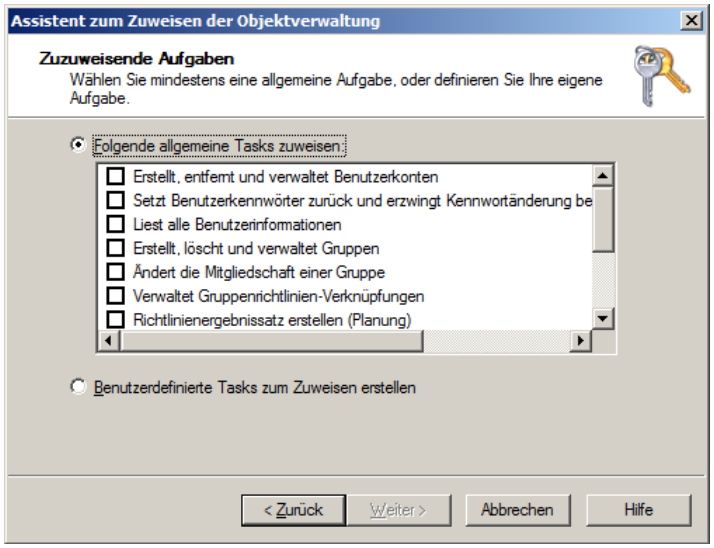
Computern für Benutzer ein neuer Ort zugewiesen.

7.1 Delegierung

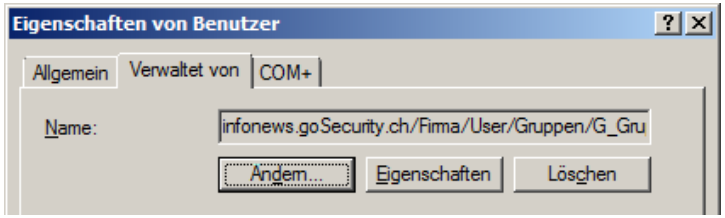
Jede OU kann an einen Benutzer, bzw. besser an eine Gruppe delegiert werden. Dazu muss mit der rechten Maustaste auf die entsprechende OU geklickt und "Objektverwaltung zuweisen" ausgewählt werden. Mit Hilfe eines Wizards kann anschliessend die entsprechende Gruppe hinzugefügt werden:



Im nächsten Schritt können die erlaubten Aufgaben ausgewählt werden:



Zusätzlich sollte unter den Eigenschaften im Register "Verwaltet von" die entsprechende Gruppe hinzugefügt werden:



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

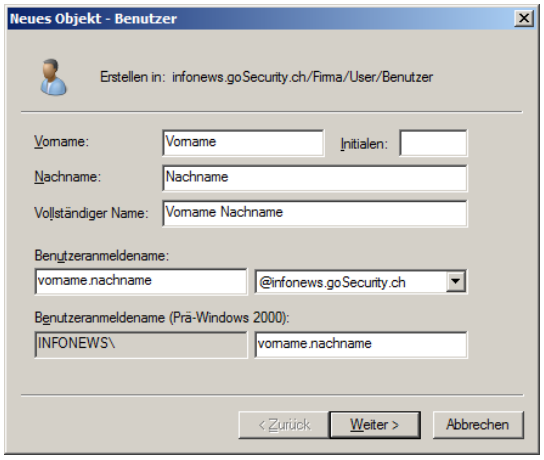
Telefon 052 320 91 20
Fax 052 320 91 21

7.2 AGDLP-Regeln

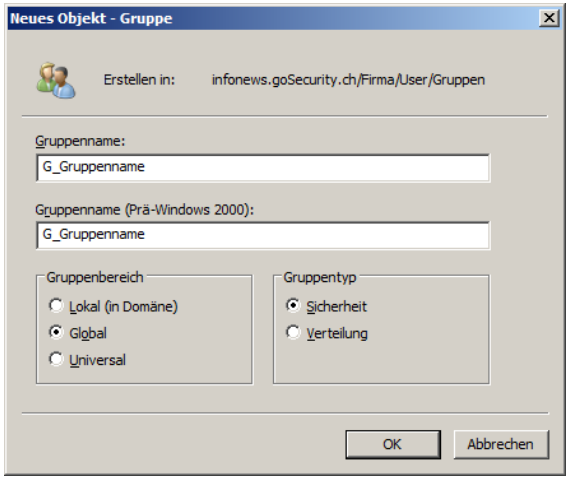
Zur Vergabe von Rechten in einem Firmennetzwerk ist ein strukturiertes, immer gleich aufbauendes Vorgehen sinnvoll. Damit wird sichergestellt, dass auch bei grösseren Mengen von Benutzern die Rechtevergabe übersichtlich bleibt. Auch lässt sich bei später folgenden Umbauten der Migrationsaufwand erheblich reduzieren, wenn die Rechtevergabe nach AGDLP aufgebaut ist.

1. Schritt:
   Im ersten Schritt erhält der Benutzer (A = Accounts) eine Mitgliedschaft in einer globalen Gruppe (G = Global Group)

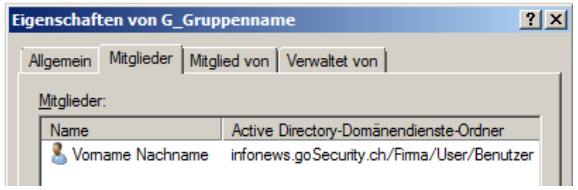
   Benutzer erstellen:



Gruppe erstellen:



Zuweisung des Benutzers in diese Gruppe:



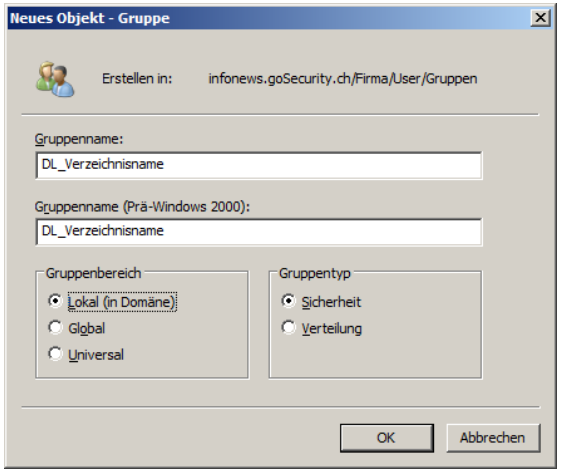
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

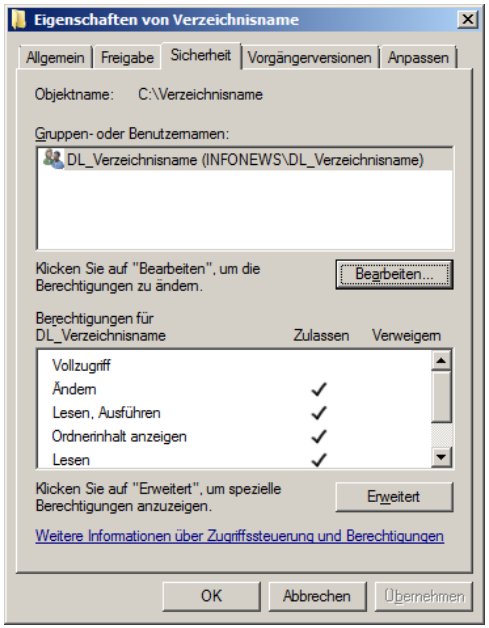
2. Schritt:
Im zweiten Schritt wird die globale Gruppe in eine lokale Gruppe (DL = Domain Local Group) platziert.

Gruppen erstellen:



Zuweisen der Globalen Gruppe in die Domain Local Gruppe:

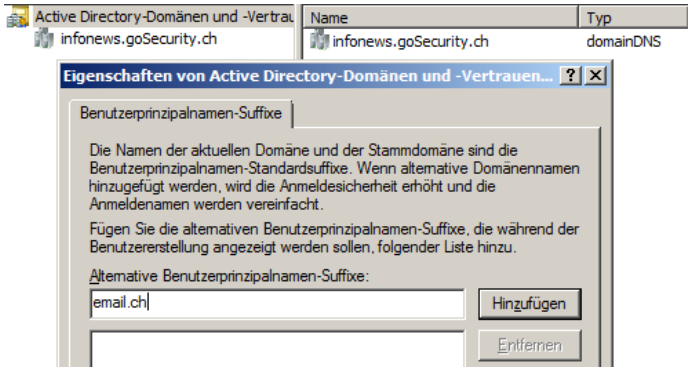
3. Schritt:
Im dritten Schritt erfolgt die Vergabe von Zugriffsberechtigungen (P = Permission) an die lokale Gruppe:



Anmeldung an der Domäne
Es ist von Vorteil, dass sich Benutzer immer mit deren UPN (User Principal Name) an der Domäne anmelden. Die UPN zeigt definiert sich fast wie die Emailadresse: benutzername@domainname. Daher wäre es von Vorteil, dass die Emailadresse verwendet werden kann. Nur lautet der Name der Domäne oft nicht identisch zur Emailadresse. Unter dem Dienstprogramm "Active Directory-Domänen und -Vertrauensstellungen" kann in den Eigenschaften ein zusätzliches Suffix definiert werden:

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



Die Benutzer können im Anschluss das neu definierte Suffix oder das Original-Suffix für die Anmeldung an die Domäne verwenden.

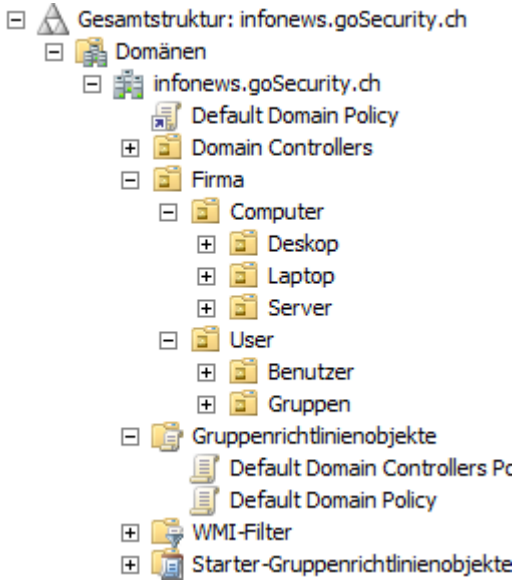
Mit dieser Erweitertung reduziert sich der Supportaufwand. Gemäss einer US-Studie kostet die Entsperrung eines Benutzerkontos $75. Mitgerechnet wurde hier die Zeit des Benutzers und des Administrators sowie dass beide aus ihrer Arbeit herausgerissen werden.

8 Gruppenrichtlinien

8.1 Gruppenrichtlinien verwalten

Eine wichtige Aufgabe bei der Administration von Netzwerken ist die Verwaltung von Benutzer- und Computereinstellungen. Damit sind nicht nur Desktop-Einstellungen oder IP-Adressen gemeint, sondern auch sicherheitsrelevante Einstellungen und die Konfiguration von Programmen, wie Internet Explorer, Windows-Explorer oder Office-Programme. Für diese Verwaltungsarbeiten stehen die Gruppenrichtlinien (Group Policies), oft auch als Gruppenrichtlinienobjekte (Group Policy Object, GPO) bezeichnet, zur Verfügung. Mit Gruppenrichtlinien lassen sich zahlreiche Einstellungen in einem AD automatisch vorgeben.

Die Verwaltung von Gruppenrichtlinien über die Gruppenrichtlinienverwaltungskonsole ist nahezu identisch zu Windows Server 2003. Die Gruppenrichtlinienverwaltungskonsole (GPMC) muss unter Windows Server 2008 nicht mehr heruntergeladen werden. Sie können diese als Funktion über den Server-Manager hinzufügen (Features hinzufügen). Auf Domänencontrollern wird dieses Feature standardmäßig bereits automatisch installiert.



8.2 Grundlagen

Allgemein wird oft von Gruppenrichtlinien gesprochen. Damit sind meistens die GPOs gemeint. Ein GPO ist eine Gruppenrichtlinie, in der Einstellungen vorgenommen

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

und gespeichert wurden. Diese Einstellungen legen für Benutzer-PCs oder Benutzerkonten fest, wie sich die Systeme verhalten. Diese Einstellungen werden innerhalb eines Containers, der GPO, gespeichert. Damit diese Einstellungen jedoch auch angewendet werden, muss die GPO mit Organisationseinheiten oder einer ganzen Domäne verknüpft werden. Erst wenn eine GPO mit einer Organisationseinheit verknüpft ist, werden die Einstellungen innerhalb der GPO auf die entsprechende OU angewendet. In diesem Fall spricht man von Gruppenrichtlinienverknüpfungen.

8.3 Neuerungen in den Gruppenrichtlinien

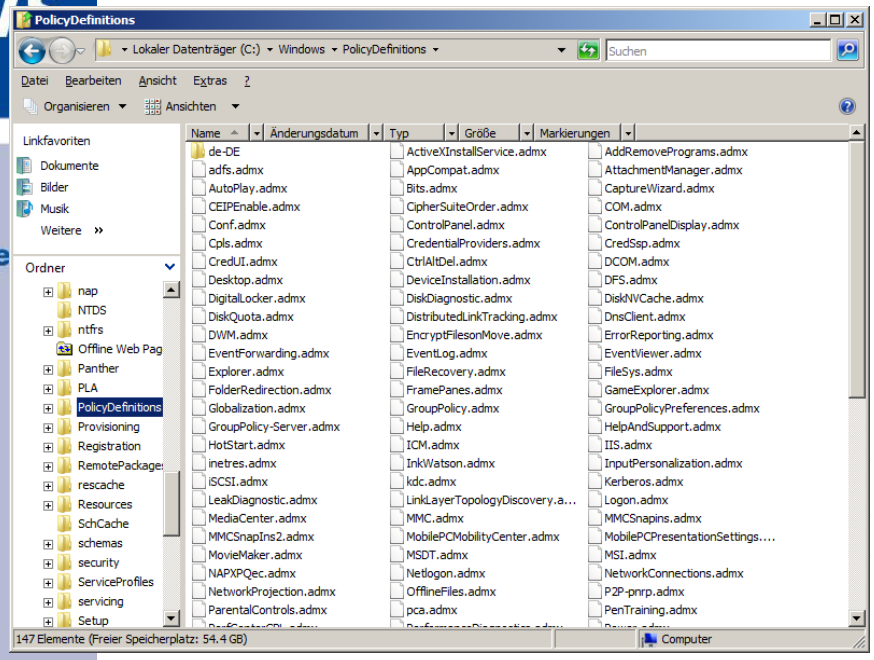
Windows Server 2008 bietet zahlreiche Neuerungen in den Gruppenrichtlinien, die natürlich ihre gesamte Funktionsbreite erst durch Einsatz von Windows Server 2008 und Windows Vista darlegen. Windows Server 2008 unterstützt als Neuerung zum Beispiel die Konfiguration der Energiesparoptionen für Windows Vista. Auch der Zugriff auf USB-Sticks kann in Windows Server 2008, zusammen mit Windows Vista, konfiguriert werden. Viele Änderungen hat Microsoft bezüglich der Einstellmöglichkeiten des Internet Explorers integriert. Auch die Steuerung von Druckerinstallationen und der Druckerverwaltung in Windows wurde erneuert.

8.4 Neue administrative Vorlagen

Unter Windows XP und Windows Server 2003 gab es für unterschiedliche Sprachversionen von Windows unterschiedliche Versionen der Vorlagendateien (*.adm-Dateien). Da dies vor allem für internationale Unternehmen nicht sehr effizient ist, hat Microsoft das Design der Vorlagendateien angepasst. Änderungen in Gruppenrichtlinien müssen dadurch nicht in jeder Sprachversion eingestellt werden, sondern nur noch einmal zentral im Unternehmen. Die alten Vorlagen-Dateien (*.adm) können unter Windows Server 2008 weiterhin verwendet werden. Windows Server 2008 verwendet für seine neuen Vorlagendateien sprachneutrale *.admx-Dateien. Diese bauen auf XML auf. Diese *.admx-Dateien werden nicht mehr für jede einzelne Gruppenrichtlinie hinterlegt, sondern zentral im Policy-Ordner. Die Gruppenrichtlinientools - der Gruppenrichtlinienverwaltungs-Editor und die Gruppenrichtlinienverwaltung (GPMC) - bleiben weitestgehend unverändert. In den meisten Situationen werden Sie nicht einmal bemerken, dass es nur *.admx-Dateien gibt. Die Vorlagendateien von Windows Server 2008 (*.admx) liegen im Verzeichnis C:\Windows\PolicyDefi-nitions.

8.5 Standardgruppenrichtlinien

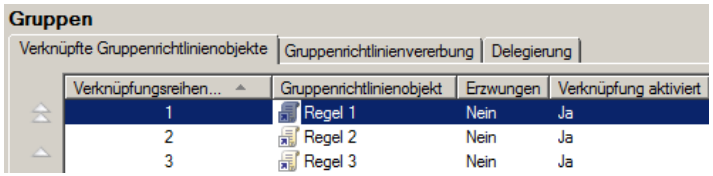
Nach der Erstellung eines ADs gibt es bereits zwei Gruppenrichtlinienobjekte. Diese Richtlinien sollten möglichst nicht verändert werden. Wenn Sie neue Einstellungen vornehmen wollen, sollten Sie möglichst eigene Gruppenrichtlinien definieren und die Einstellungen der Standardrichtlinien so belassen wie sie sind.



- Default Domain Controllers Policy
  Diese GPO ist mit dem Container Domain Controllers verknüpft. In dieser Richtlinie werden spezielle Einstellungen vorgegeben, die für Domänencontroller notwendig sind. Aus diesem Grund sollten Sie auch keine Domänencontroller aus dem Container Domain Controllers in eine andere OU verschieben.
- Default Domain Policy
  In dieser Richtlinie werden spezielle Einstellungen für die ganze Domäne gesetzt. Diese Richtlinie ist mit dem Domänenobjekt verknüpft und hat daher für alle OUs in der Domäne Gültigkeit.

8.6 Priorisierung einer GPO-Verknüpfung

Wenn Sie die Richtlinie erstellt und verknüpft haben, klicken Sie die Domäne in der Gruppenrichtlinienverwaltung an. Auf der rechten Seite werden Ihnen alle Gruppenrichtlinien angezeigt, die direkt mit der Domäne verknüpft sind. An dieser Stelle kann die Reihenfolge der Ausführung verändert werden.



8.7 Erzwingen einer Richtlinie

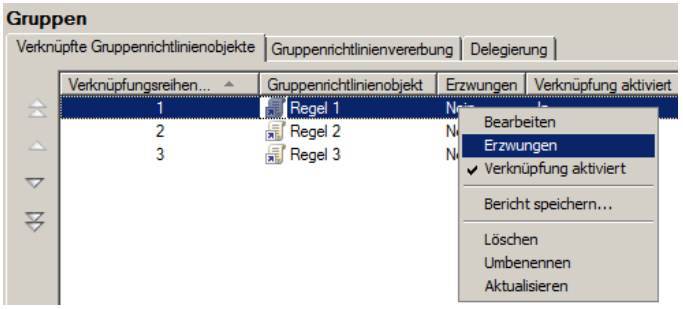
Durch die Vererbung von Gruppenrichtlinien besteht die Möglichkeit, dass die Einstellung einer Gruppenrichtlinie durch eine andere Gruppenrichtlinie, die in einer untergeordneten OU definiert ist, überschrieben wird. Wenn Sie zum Beispiel eine Richtlinie, in der die Komplexität der Kennwörter mitgegeben wird, mit der ganzen Domäne verknüpfen, dann wird diese Einstellung an alle Organisationseinheiten und die darin enthaltenen Benutzer weitergegeben. Ist jetzt aber mit einer untergeordneten Organisationseinheit eine weitere Gruppenrichtlinie verknüpft, die in der Anwendungsreihenfolge nach der Richtlinie für die Domäne angewendet wird, besteht die Möglichkeit, dass die Einstellungen der vererbten Richtlinie der Domäne überschrieben werden.

Für Benutzer innerhalb eines Containers gilt immer die zuletzt angewendete Richtlinie. Wenn also in der Domänenrichtlinie eine Einstellung gesetzt wird, die in der OU

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

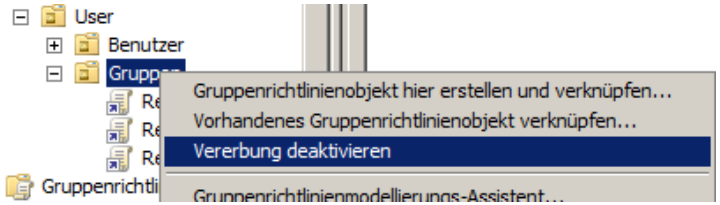
Telefon 052 320 91 20
Fax 052 320 91 21

des Benutzers zurückgenommen wird, dann gilt das auch für den Benutzer. Wenn Domänenadministratoren sicherstellen wollen, dass gewisse Gruppenrichtlinien nicht überschrieben werden können, besteht die Möglichkeit, die Einstellungen dieser Richtlinie zu erzwingen. In diesem Fall kann von untergeordneten Organisationseinheiten die Durchsetzung dieser Gruppenrichtlinie nicht verhindert werden. Sie können eine Gruppenrichtlinie erzwingen lassen, indem Sie auf der rechten Seite der Gruppenrichtlinienverwaltung auf der Registerkarte Verknüpfte Gruppenrichtlinienobjekte die Verknüpfung mit der rechten Maustaste anklicken. Wählen Sie im daraufhin geöffneten Kontextmenü die Option Erzwungen aus.



8.8 Vererbung deaktivieren

Für manche Gruppenrichtlinien ist es unter Umständen sinnvoll, die standardmäßige Vererbung zu deaktivieren. Wenn Sie zum Beispiel in allen OUs einer Domäne die Internet Explorer-Einstellungen weitergeben wollen, in einer OU aber nicht, dann können Sie in dieser OU die Verwendung der Richtlinie deaktivieren, auch wenn diese mit der ganzen Domäne verknüpft ist. Haben Sie zum Beispiel einige Mitarbeiter, die einen eigenen Proxyserver verwenden, zum Beispiel die Entwicklungsabteilung oder die IT-Abteilung, können Sie eine eigene Gruppenrichtlinie für diese OU erstellen und sie mit dieser OU verknüpfen. Die Vererbung der übergeordneten Richtlinie können Sie für diese OU deaktivieren. Wenn Sie die entsprechende OU in der Gruppenrichtlinienverwaltung anklicken, können Sie auf der rechten Seite der Konsole auf der Registerkarte Gruppenrichtlinienvererbung erkennen, welche Verknüpfungen von übergeordneten OUs auf diese OU übernommen - also vererbt - werden.



Nachdem die Vererbung deaktiviert wurde, wird die entsprechende OU mit einem blauen Kreis mit weissen Ausrufezeichen gekennzeichnet:

8.9 Delegierung

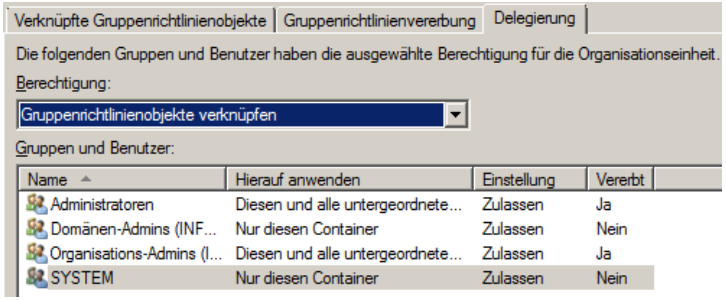
Nebst der Verwaltung von Objekten kann auch die Konfiguration von Gruppenrichtlinien delegiert werden. Dazu muss der entsprechende Benutzer, bzw. besser die entsprechende Gruppe zugelassen werden. Ebenfalls kann angegeben werden, worauf diese Gruppe Zugriff hat:

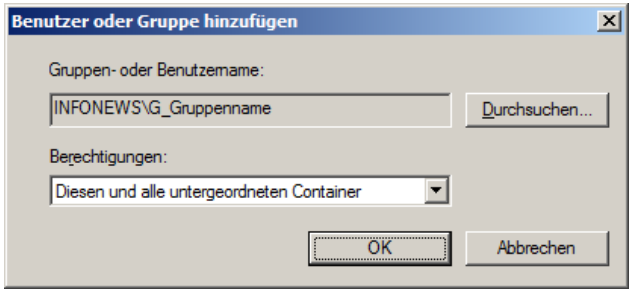
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



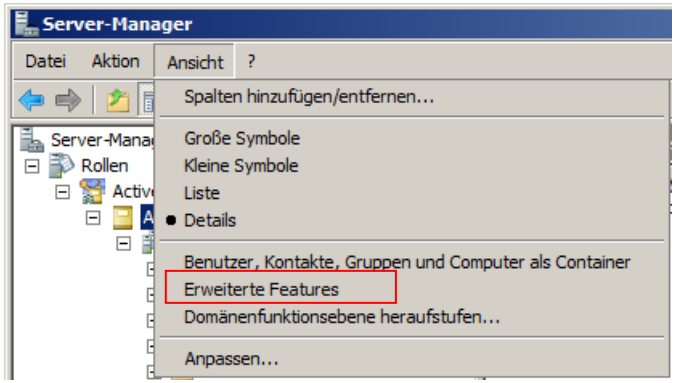


9 WS08: Neuerungen im AD

9.1 Richtlinien für Kennwörter

Es ist ein offenes Geheimnis. In den Vorgängerversionen konnte nur eine Kennwortrichtlinie definiert werden. Dies war in vielen Fällen unpraktisch, gerade wenn Geräte ins AD integriert wurden, die andere Vorgaben verlangen. Dies kann beispielsweise eine Kasse sein, die sechs Zahlen benötigt. Für ein Benutzerkennwort ist dies auf jeden Fall ungenügend.

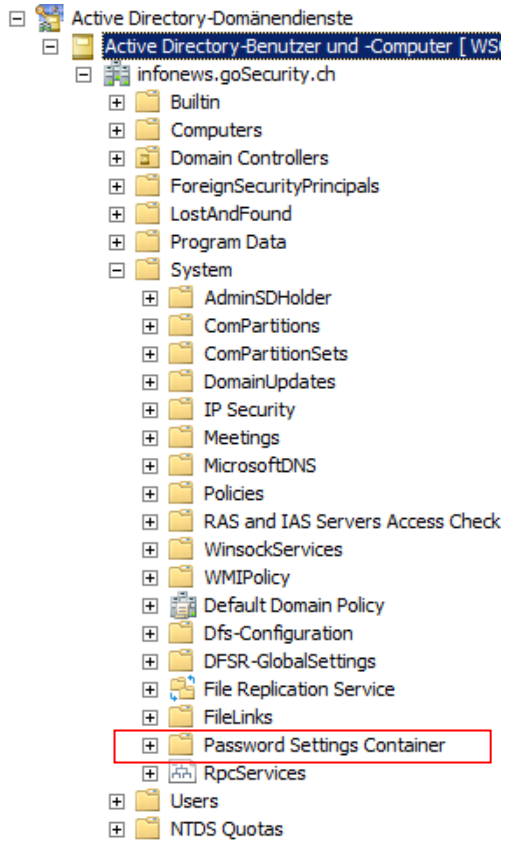
Unter Windows Server 2008 können jetzt mehrere Richtlinien für Kennwörter definiert werden. Diese Funktion steht aber nur zur Verfügung, wenn die Domäne im Funktionsmodus Windows Server 2008 betrieben wird. Kennwortrichtlinien können jetzt einzelnen OUs zugewiesen werden, d.h. sie müssen nicht mehr dem Domänenobjekt zugewiesen sein. Microsoft hat für diese Funktion zwei neue Objekt-Klassen in das Schema des ADs integriert:
- Password Settings Container
- Password Settings



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Ebenfalls wichtig ist für diese neue Funktion ist die OU Password Setting Container, der unterhalb der OU System im Snap-In Active Directory-Benutzer und - Computer angezeigt wird. Damit diese überhaupt angezeigt werden, muss die Ansicht der erweiterten Funktionen aktiviert sein (Menübefehl Ansicht/Erweiterte Features).



In dieser OU werden nach Erstellung die Password Settings Objects (PSO) gespeichert. Eine PSO enthält alle notwendigen Einstellungen zur Konfiguration von Kennwortrichtlinien.

9.2 Schreibgeschützte Domänencontroller

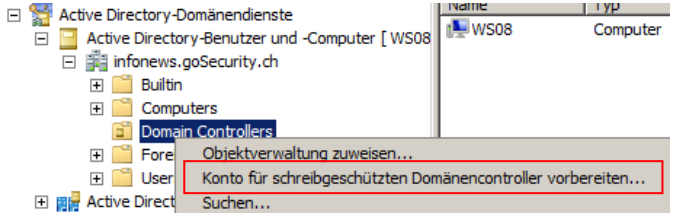
Eine Neuerung sind schreibgeschützte Domänencontroller (Read-Only Domain Controller, RODC). Diese Domänencontroller erhalten zwar die replizierten Informationen von den anderen DCs, können aber selber keine Änderungen entgegennehmen. Somit ist es möglich, diese RODCs in einer Niederlassung mit einem kleineren physischen Schutz platziert werden. Ein RODC kennt zwar alle Objekte im AD, speichert aber nur diejenigen Kennwörter, die explizit festgelegt wurden. Ist ein Benutzer bzw. dessen Kennwort nicht bekannt, muss der DC angefragt werden.

Wichtig: mindestens ein DC in einer Gesamtstruktur muss ein Windows Server 2008 sein. Die anderen dürfen WS03-DCs sein. Jedoch ist die Replikation zwischen WS03 und einem RODC weniger zuverlässig. Aus diesem Grund sollte die Replikation zu einem RODC am besten immer über einen WS08-DC erfolgen.

Hinweis: Bevor ein RODC konfiguriert wird, sollte auf dem Schema-Master der Gesamtstruktur der Befehl adprep /rodcprep ausgeführt werden.

Zur Konfiguration stehen zwei Möglichkeiten zur Verfügung. Bei der Installation des ADs kann ausgewählt werden, ob es sich um einen RODC handelt. Üblicherweise wird jedoch auf einem bestehenden DC die Installation vorbereitet. Dazu wird in der OU Domain Controllers der

Befehl "Konto für schreibgeschützten Domänencontroller vorbereiten" ausgewählt:



Nun führt der Assistent durch die Installation. Am Ende wird ein Computerkonto für den RODC erstellt. In der Niederlassung kann anschliessend ein Administrator diesen Server installieren. Der Server bekommt automatisch die Funktion des RODCs zugewiesen.

Anmeldung: meldet sich ein Benutzer nun an, wird überprüft, ob das Kennwort des Anwenders bereits auf den Server repliziert wurde. Falls nicht, wird die Anfrage an einen vollwertigen DC weitergeleitet. Ist die Anmeldung erfolgreich, wird dem RODC ein Kerberosticket zugewiesen. Der RODC stellt anschliessend diesem Benutzer ein eigenes Kerberosticket aus. Gruppenmitgliedschaften und Gruppenrichtlinien werden übrigens nicht jedes Mal vom DC geholt, sondern sind bereits auf dem RODC gespeichert. Ob das Passwort des Benutzers nun in die Datenbank des RODCs aufgenommen wird, ist abhängig von der jeweiligen Gruppenmitgliedschaft.

Hinweis: Die Kennwörter von Administratorenkonten werden in keinem Fall auf einem schreibgeschützten DC gespeichert. Geht die Verbindung zwischen DC und RODC verloren, findet keine Anmeldung mehr an der Domäne statt. Der RODC verhält sich dann wie ein normaler Mitgliedsserver, d.h. es sind nur lokale Anmeldungen möglich.

9.3 AD manuell starten und stoppen

Unter Windows Server 2008 ist endlich möglich, den AD-Dienst im laufenden Betrieb zu stoppen und wieder zu starten. Dies kann beispielsweise bei der Offlinedefragmentation des ADs sinnvoll sein oder wenn Updates installiert werden.

9.4 AD Snapshot-Viewer

Mit dem AD Snapshot-Viewer können versehentlich gelöscht Objekte der Domäne angezeigt werden. Wiederherstellen ist zwar nicht möglich, jedoch kann das entsprechende Element angezeigt und die Objektinformationen neu erstellt werden.

Vorgehen:

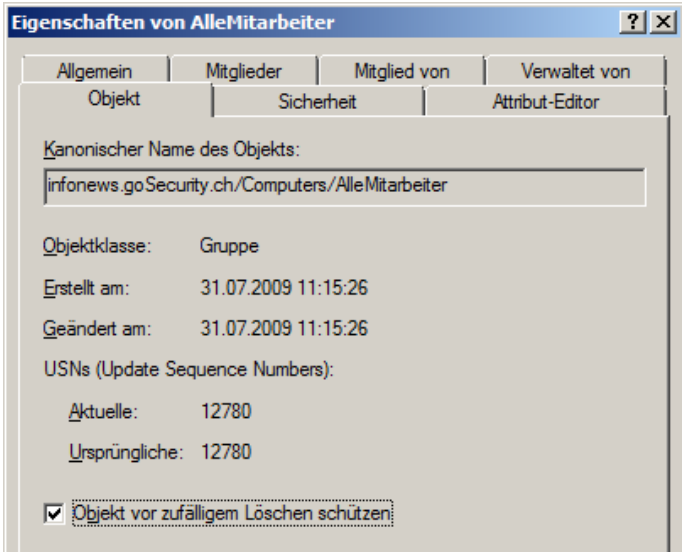
1. mit dem Tool ntdsutil.exe müssen regelmässig Snapshots angelegt werden
2. mit ntdsutil.exe können anschliessend die Snapshots angezeigt werden.
3. mit dem Befehl dsamain.exe kann ein Snapshot als LDAP-Server bereitgestellt werden.
4. mit ldp.exe kann nun der Snapshot untersucht werden

9.5 Versehentliches Löschen verhindern

Unter WS08 sind AD-Objekte vor versehentlichem Löschen geschützt. Werden die Eigenschaften eines Objekts angezeigt, ist der entsprechende Punkt im Register Objekt sichtbar (Vorher muss "Erweiterte Features" aktiviert sein):

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



Hinweis: Dieser Schutz gilt auch für Administratoren.

10 Zusätze

- Übertragen der Betriebsmasterrollen: http://technet.microsoft.com/de-de/library/cc778806(WS.10).aspx
- Übernehmen der Betriebsmasterrollen: http://technet.microsoft.com/de-de/library/cc757500(WS.10).aspx
- Verwalten von Vertrauensstellungen: http://technet.microsoft.com/de-de/library/cc758857(WS.10).aspx

11 Quellen

- Betriebsmaster http://technet.microsoft.com/de-de/library/cc773108(WS.10).aspx
- Microsoft Press: MS Windows Server 2008 - Das Handbuch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21