Active Directory

Windows-Netzwerk steuern und konfigurieren

Das Active Directory ist der zentrale Verzeichnisdienst in einem Windows-Netzwerk. Mit der Einführung von Windows Server 2008 wurde die Kernkomponente in «Active Directory Domain Services» (ADDS) umbenannt. Das Active Directory (AD) ermöglicht es, ein Netzwerk analog einer realen Struktur oder der räumlichen Verteilung zu gliedern. Im AD können verschiedene Objekte gegliedert und verwaltet werden. Dazu gehören beispielsweise Benutzer, Gruppen, Computer, Dienste, Freigaben und viele weitere Elemente.

Autor: Andreas Wisler

Bereits mit Windows Server 2003 R2 wurden die Möglichkeiten massiv erweitert. Noch einmal stark ausgebaut wurden sie in Windows Server 2008 sowie Windows Server 2008 R2, welches im Oktober 2009 auf den Markt kam.

Rollen

Das AD ist in fünf Rollen aufgeteilt. Die folgenden Rollen stehen 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. 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.

Domänencontroller

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
Aufgaben: Anwendung und Verwaltung der Gruppenrichtlinien, Kennwortänderungen, externen Vertrauensstellungen, Zeitserver
2. Infrastrukturmaster
Aufgabe: Berechtigungen für die Benutzer steuern, die aus unterschiedlichen Domänen kommen
3. RID-Master
Aufgabe: Vergibt anderen Domänencontrollern Relative Identifiers (RIDs)
4. Schemamaster
Aufgabe: Verwaltet das Schema, das heisst die möglichen Objekte
5. Domänennamenmaster
Aufgabe: Kontrolle, ob doppelte Namen vergeben werden, legt als Einziger neue Attribute an

Die verschiedenen Rollen, also PDC-Emulator, Infrastrukturmaster, RID-Master, Schema-

master 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.

Globaler Katalog

An jedem Standort im AD sollte ein globaler Katalog-Server installiert sein. Der globale Katalog ist eine weitere Rolle, die ein Domänencontroller 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.

Organisation des ADs

In der Domäne sollten die Objekte in einer sinnvollen Struktur gepflegt werden. Daher ist es empfohlen, in der Domäne als erstes eine neue OU zu erstellen. 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. Ein weiterer Vorteil ist, dass auf alle selber erstellten Organisationseinheiten (OU, organizational unit) Gruppenrichtlinien (Vorgaben an Geräte und Benutzer) gesetzt werden können. (Siehe Abbildung 1)

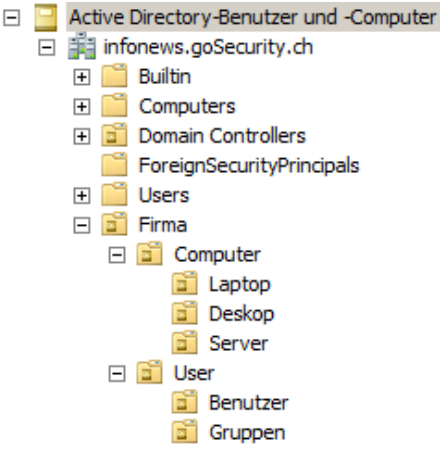

Abbildung: 1

Gruppenrichtlinien

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.

Zum einfachen Verwalten steht die Gruppenrichtlinienverwaltungskonsole (GPMC) zur Verfügung. (Siehe Abbildung 2)

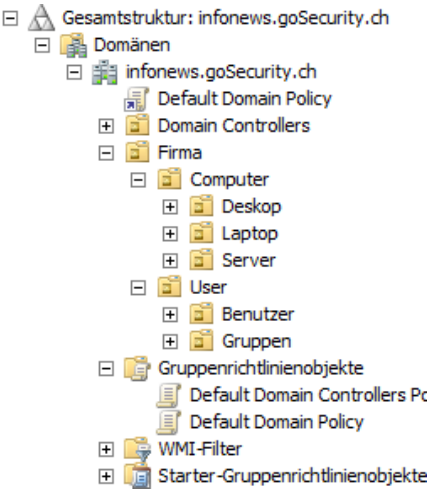

Abbildung: 2

In jeder GPO können Einstellungen festgelegt werden, wie sich ein Benutzer-PC oder ein Benutzerkonto verhält. Für die verschiedenen Betriebssysteme stehen zwischen 9'700 und 11'400 Einstellungsmöglichkeiten

Zum Autor

Andreas Wisler, (Tel.: 052 320 91 20), Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. System Hardening rundet das Profil ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

zur Verfügung! Damit diese Einstellungen jedoch auch angewendet werden, muss die GPO mit einer Organisationseinheit oder der ganzen Domäne verknüpft werden. Erst wenn eine GPO mit einer Organisationseinheit verknüpft ist, werden die Einstellungen innerhalb der GPO auf die entsprechende OU angewendet.

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 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.

Windows Server 2008: Neuerungen im AD

Richtlinien für Kennwörter: 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, das heisst 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

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 respektive 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.

Fazit

Mit dem Active Directory steht Ihnen ein mächtiges Werkzeug zur Konfiguration und Steuerung Ihres Windows-Netzwerkes zur Verfügung. Der Aufbau und die Definitionen benötigen allerdings einiges an Aufwand. Dieser sollte auf jeden Fall betrieben werden, ansonsten können sich Fehler schnell rächen. ◆