Active Directory – Überblick

Agenda

- Einführung
- Physische vs. logische Struktur
- Standorte, Dienste und Replikation
- Vertrauensstellungen
- Active Directory-Objekte
- Management und Administrationswerkzeuge

Einführung

- Active Directory = Active Directory Domain Services (AD DS)
  - Spezielle Rolle eines Windows Servers
  - Es kann mehrere (gleichberechtigte) Domänencontroller geben
- Verzeichnisdienst: Organisation verschiedenster Objekte, wie Benutzer, Gruppen, Computer,…
- Möglichkeit der Zugriffskontrolle und Überwachung
- 4 Hauptmerkmale:
  - Lightweight Directory Access Protocol (LDAP)
  - Kerberos-Protokoll
  - Common Internet File System (CIFS)
  - Domain Name System (DNS)

Physische Komponenten

- Verzeichnisdatenspeicher
  - Datenbank ntds.dit
    - Standardpfad: %Systemroot%\NTDS
    - Kopiervorlage: %Systemroot%\System32, wird beim dcpromo in Standardpfad kopiert und ggf. durch Replikation aktualisiert
  - Transaktionsprotokolle
  - Aufteilung sinnvoll um Performance zu erhöhen
- Globaler Katalog
  - Pro Gesamtstruktur genau 1 Globaler Katalog, aber mehrere Globale Katalog Server möglich (Ausfallsicherheit!!!)
  - Dient zum Abfragen von AD-Objekten und zur Authentifizierung von Benutzern aus anderen Domänen der gleichen Gesamtstruktur
  - Eigene AD-Partition (Port 3268 TCP)
  - Schreibgeschützt: Kann nur vom System verändert werden
  - ⚠ GC und Infrastructure Master nicht auf der gleichen Maschine, außer alle Domänencontroller der Domäne sind GCs

Physische Komponenten

- Betriebsmaster

Betriebsmaster sind spezielle Domänencontroller für bestimmte Schreibvorgänge in die Verzeichnis-Datenbank. Die einzelnen Funktionen werden als Rolle definiert (FSMO = Flexible Single-Master Operation).

Gesamtstrukturrollen:

- Schemamaster
  - Schreibrechte für das AD-Schema
  - Administrator muss Mitglied der Sicherheitsgruppe „Schema-Admins“ sein
- Domänennamenmaster
  - Hinzufügen und Entfernen sämtlicher Verzeichnispartitionen in der Gesamtstruktur
    - Hinzufügen/Entfernen von Domänen
    - Hinzufügen/Entfernen von Anwendungsverzeichnispartitionen

Physische Komponenten

- Betriebsmaster

  Domänenrollen:

  - RID-Master
    - Verwaltung des RID-Pools (Relative Identifier) und Vergabe von RIDs an Domänencontroller
    - RID = SID + Domänenkennung
  - PDC-Emulator
    - Primärer Domänencontroller für Betriebssysteme vor Windows 2000
    - Entfällt, da Server 2008 nicht mit Windows 2000 Server kompatibel ist
  - Infrastrukturmaster
    - Aktualisiert domänenübergreifende Verweise zwischen Benutzern und Gruppen
    - Objektänderungen werden in Gruppenmitgliedschaftslisten aktualisiert

Physische Komponenten

- Schema
  - Definiert Klassen und Attribute, die in der AD DS gespeichert werden können
  - Jedes AD-Objekt ist eine Instanz einer Klasse
  - Das Schema gewährleistet, dass alle Objekte in der Gesamtstruktur einheitlich erstellt und damit von allen Domänencontrollern verwaltet werden können.

Logische Komponenten

- AD DS-Partitionen

Die in der Verzeichnisdatenbank gespeicherten Informationen werden in mehrere logische Partitionen unterteilt, die jeweils unterschiedliche Informationstypen speichern. Die AD DS-Partitionen werden auch als Namenskontexte (Naming Contexts, NC) bezeichnet.

  - Folgende Kontexte:
    - *Domain*
      enthält die Domänenobjekte, Gruppen, Users, Computers, usw.
    - *Configuration*
      enthält die Konfiguration der Domäne / Forest und ihre OU Struktur
    - *RootDSE*
      LDAP Standardeinstiegspunkt
    - *Schema*
      hält das Schema der AD Datenbank
    - *NDNC*
      Non-Domain Naming Content, enthält anwendungsspezifische Informationen

Tools: LDP.exe, ADSIedit.msc, repadmin.exe, nltest.exe

Logische Komponenten

- Gesamtstruktur
  - Eine Gesamtstruktur ist eine integrierte Einheit mit folgenden Eigenschaften:
    - Gemeinsames Schema
    - Gemeinsame Konfigurationsverzeichnispartition
    - Gemeinsamer Globaler Katalog
    - Gemeinsamer Satz von gesamtstrukturweiten Betriebsmastern und Administratoren
    - Gemeinsame Konfiguration von Vertrauensstellungen

Logische Komponenten

- Domänenstruktur

Unterteilung einer Gesamtstruktur in kleinere Komponenten

- Stamm-, untergeordnete und nebengeordnete Domäne
- Domänengrenzen sind Replikationsgrenzen für Domänenverzeichnispartition und Domäneninformationen im Ordner SYSVOL
- Einfachere Verwaltbarkeit durch Delegation
- Domänen bieten besseren Zugriffsschutz auf Ressourcen (Vertrauensstellungen, Policies)

Gründe für mehrere Domänen:

- Eigener Namensraum
- Anforderungen an Kennwortrichtlinien
- Eingeschränkter Zugriff auf bestimmte Ressourcen

Logische Komponenten

- Domänen- und Gesamtstrukturfunktionsebene
  - Abwärtskompatibilität vs. neue Features

Wesentliche Verbesserungen bei Server 2008

- Domänenfunktionsebene:
  - Unterstützung der DFS-Replikation (Distributed File System) für SYSVOL
  - Unterstützung für AES 128 und 256 (Advanced Encryption Services) für das Kerberos Protokoll
  - Informationen zur letzten interaktiven Anmeldung (Uhrzeit, Computername, Anzahl fehlgeschlagener Anmeldeversuche)
  - Detaillierte Kennwortrichtlinien

Logische Komponenten

- Domänen- und Gesamtstrukturfunktionsebene
  - Abwärtskompatibilität vs. neue Features

Wesentliche Verbesserungen bei Server 2008

- Gesamtstrukturebene:
  - Vertrauensstellung mit einer anderen Gesamtstruktur
  - Domänenumbenennung
  - Replikation verknüpfter Werte (Es werden nur noch die Änderungen repliziert)
  - Möglichkeit der Bereitstellung von RODCs (Read-Only Domänencontroller)
  - Deaktivieren und Umdefinieren von Attributen und Klassen im Schema

Vertrauensstellungen

- Verbindungen zwischen mehreren Domänen oder Gesamtstrukturen
- Unidirektional (eingehend, ausgehend), bidirektional, transitiv
- Externe Vertrauensstellung:
  - Uni- oder bidirektional; NICHT transitiv!
  - Wird gewählt bei Zugriff auf Ressourcen einer bestimmten Domäne innerhalt einer Gesamtstruktur
- Gesamtstrukturvertrauensstellung
  - Bidirektional und transitiv
  - Kerberos-Authentifizierung
  - Zugriff auf Ressourcen von jeder Domäne in jede Domäne
  - Domänenweite und selektive Authentifizierung möglich

Standorttopologie

- Kombination aus logischen und physischen Komponenten
  - Logische Abbildung des physikalischen Netzwerks eines Unternehmens
  - „Standorte“ als spezielle Organisationseinheiten zur Verwaltung des Netzwerkverkehrs
  - Durch die Installation von AD DS ergibt sich eine Topologie, in der jede Domäne mit jeder anderen Domäne innerhalb einer Gesamtstruktur eine Verbindung herstellt und regelmäßig überprüft

Standorttopologie

- Gründe für eine Anpassung der Topologie:
  - Kleine Bandbreite: Die Replikation zwischen Standorten wird komprimiert, um Bandbreite über die WAN-Strecken zu sparen. Außerdem kann die Replikation zeitlich geplant werden.
  - Unzuverlässige Anbindung: Der Datenverkehr zur Clientanmeldung verbleibt innerhalb eines Standorts, wenn der lokale Domänencontroller erreichbar ist.
  - AD DS-fähige Anwendungen, wie Distributed File System (DFS) oder Exchange, können mithilfe von Standorten den Datenverkehr des Clientzugriffs begrenzen oder das Messagerouting basierend auf der Standortkonfiguration verwalten.

Replikation

- In einer Gesamtstruktur werden unterschiedlichste Daten zwischen Domänencontrollern repliziert.
- AD Replikation
  - Replikation der Daten des Active Directory: Benutzer, Computer und Gruppen. Diese Replikation wird als Multimasterreplikation bezeichnet. Betreibt man die DNS-Zone Active Directory integriert, wird diese ebenfalls repliziert.
- Sysvol Replikation
  - Replikation der Domäne, des Namensraums und der Berechtigungen über den „Dateireplikationsdienst“ bzw. DFS-R. Hier wird der im Filesystem angesiedelte Teil des AD repliziert.
- Replikation der Standortinformationen
  - Diese Aufgabe übernimmt der KCC (Knowledge Consistency Checker).

Replikation

- Replikation des GCs
  - Replikation der wichtigsten Attribute in den Globalen Katalog. Wird nichts konfiguriert repliziert das AD per Multimasterreplikation (RPC) innerhalb der Domänen. Per Definition kann über IP oder SMTP repliziert werden. Diese Einstellungen gelten primär für WAN Strecken. SMTP ist nur dann zu empfehlen, wenn „unsichere“ WAN Strecken eingesetzt werden. „Unsicher“ heißt für Microsoft in diesem Fall, dass die Strecken des Öfteren unterbrochen sein könnten.
  - Beim Hinzufügen von neuen Attributen zum GC muss beachtet werden, dass diese ebenfalls auf alle anderen GCs im Forest repliziert werden und zusätzliche Last auf WAN-Strecken erzeugen kann.
- DNS Replikation
  - Replikation der AD-Partitionen *ForestDnsZones* und *DomainDnsZones.*

Struktur und Objekte

- Organisationseinheiten (OUs)
  - Hierarchische Struktur
  - Erleichtert die Administration
  - Delegation möglich auf OU-Ebene
  - Keine Standard-Container verwenden
    - Organisationsstruktur immer neu abbilden
    - Standard-OUs nicht verändern

Struktur und Objekte

Beanspruchen den Großteil der administrativen Aufgaben:

- Benutzerobjekte
- Gruppenobjekte
- Computerobjekte

Struktur und Objekte

- Benutzerobjekte
  - Drei unterschiedliche Objekttypen:
    - Benutzerobjekte (Sicherheitsprincipal)
    - inetOrgPerson (Sicherheitsprincipal)
    - Kontaktobjekt (Kommunikation)

Attribut	Beispiel-Wert
CN	Administrator
instanceType	0x4 = (WRITE)
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=…
objectClass	Top; person; organizationalPerson; user
objectSid	S-1-5-21-678375784-9234653470-…
sAMAccountName	Administrator

Struktur und Objekte

- Gruppenobjekte
  - 2 Gruppentypen:
    - Sicherheitsgruppe

      Dient zur Zuweisung von Berechtigungen auf Netzwerk-ressourcen (Sicherheitsprinzipal).
    - Verteilergruppe

      Kein Sicherheitsprinzipal, dient zum Versand von Emails z.B. mit Microsoft Exchange

Struktur und Objekte

- Gruppenobjekte
  - Gruppenbereiche:
    - Lokal (in Domäne)
      Zum Zuweisen von Rechten auf Ressourcen der lokalen Domäne (ab Windows 2000)
    - Global
      Zum Zuweisen von Rechten auf Ressourcen in allen Domänen der Gesamtstruktur und zwischen vertrauten Gesamtstrukturen (ab NT4.0)
    - Universal
      Zum Zuweisen von Rechten auf Ressourcen in allen Domänen der Gesamtstruktur und zwischen vertrauten Gesamtstrukturen (ab Windows 2000)

Struktur und Objekte

- Lokal (in Domäne): Mitgliedschaft
  - Benutzerkonten von jeder beliebigen Domäne in der Gesamtstruktur
  - Globale oder universelle Gruppen von jeder beliebigen Domäne in der Gesamtstruktur
  - Benutzerkonten oder globale oder universelle Gruppen von jeder beliebigen Domäne in der Gesamtstruktur
  - Verschachtelte domänenlokale Gruppen von der lokalen Domäne

Struktur und Objekte

- Global: Mitgliedschaft
  - Benutzerkonten von der Domäne, in der die Gruppe erstellt wurde
  - Verschachtelte globale Gruppen von der gleichen Domäne

Struktur und Objekte

- Universal: Mitgliedschaft
  - Benutzerkonten von jeder beliebigen Domäne in der Gesamtstruktur
  - Globale Gruppen von jeder beliebigen Domäne in der Gesamtstruktur
  - Verschachtelte universelle Gruppen von jeder beliebigen Domäne in der Gesamtstruktur

Struktur und Objekte

- Verschachtelung (A – G – (U) – DL – P Prinzip)
  - **A**(ccounts) go in
  - **G**(lobal Groups) nested in
  - (**U**(niveral Groups) nested in)
  - **D**(omain Local Groups) that are granted
  - **P**(ermissions).

Struktur und Objekte

- Computerobjekte
  - Computerkonto wird beim erstmaligen Eintritt in die Domäne erzeugt und beinhaltet Informationen über Name, Betriebssystem, Sicherheitsrichtlinien, GUID
  - Computer muss sich genauso authentifizieren, wie Benutzer (Authentifizierung erfolgt beim Rechnerstart)
  - GUID wird bei jedem Neustart an DC übertragen und beide Maschinen erzeugen einen Kerberos verschlüsselten Kanal (Secure Channel) mit automatisch generiertem Passwort

Management und Administrationswerkzeuge

- Microsoft Management Console (MMC)
  - Active Directory Benutzer und Computer
  - Active Directory Domänen und Vertrauensstellungen
  - Active Directory Standorte und Dienste
- Powershell
- Systemtools
  - ADSIEdit.msc
  - Ldp.exe
  - Ntdsutil.exe

Vielen Dank für die Aufmerksamkeit

Stefan Berge
Hochschulrechenzentrum

+49 521 106-12610
stefan.berge@uni-bielefeld.de