**Active Directory**

Das Active Directory ist ein Verzeichnisdienst von Microsoft. Durch den Verzeichnisdienst werden Information über Objekte in einem Netzwerk gespeichert. Diese Objekte können Benutzer, Drucker, Telefone etc. sein. Durch ihn ist die Strukturierung und die Administration von Objekten vereinfacht worden. Durch das Active Directory ist eine wirklichkeitsgetreue Darstellung einer Organisation möglich.

**Active Directory Objekte**

Die gespeicherten Daten, also Informationen über Benutzer, Drucker etc., werden im AD in Objekten gespeichert. Ein Objekt ist ein individueller Attributsatz mit Informationen. Spezielle Objekte, welche andere Objekte enthalten können, nennt man Container. Eine Domäne ist zum Beispiel ein Container, da sie Benutzer, Drucker etc. beinhaltet.

**AD-Schema**

Das Schema definiert Objekte, die in das AD aufgenommen werden können. Das Schema ist daher eine Definitionsliste, die beschreibt welche Art von Objekten und welche Art von Informationen zu einem AD-Objekt gespeichert werden können.

Das Schema wird unterteilt in Schemaklassen und Schemaattribute. Die Schemaklassen beschreiben die Objekte, die in AD erstellt werden können. Jede Schemaklasse hat eine Auflistung von Schemaattributen.

Das AD enthält Basisklassen und Attribute. Diese können dann erweitert werden, um den Spezifikationen nachzukommen.

**AD-Komponenten**

Diese werden benötigt, um den Strukturaufbau zu ermöglichen. Es gibt dabei logische Komponenten und physische Komponenten.

**Logischer Aufbau**

Domänen

Die Domäne ist die wichtigste Komponente zur Strukturierung. In ihr können Millionen von Objekten gespeichert werden. Bei den diesen handelt es sich um Objekte, die von den Netzwerkbenutzern jeden Tag gebraucht werden, so also Benutzer, Drucker etc.

Eine Domäne enthält nur Informationen über die Objekte, die in ihr enthalten sind. Sie stellt auch eine Sicherheitsbarriere dar. Durch Berechtigungen wird klargestellt welcher Benutzer Zugriff auf welche Objekte der Domäne hat und in welchem Umfang dieser Zugriff erfolgt.

Die Domänenstruktur spiegelt die Struktur des Unternehmens wieder. Daher kann man anhand der Struktur erkennen wie das Unternehmen aufgebaut ist.

Organisationseinheiten

Eine OU ist ein Container mit dessen Hilfe innerhalb einer Domäne in logische administrative Gruppen gegliedert werden kann. Domänen können beliebig viele OUs haben und eine OU kann eine andere OU beinhalten, auf diese Weise entsteht eine Hierarchie innerhalb der Domäne.

Jede OU kann eigene Berechtigungen haben. Wenn aber zwei oder mehr OUs eine übergeordnete OU haben, erben diese standardgemäß die Berechtigungen der Übergeordneten.

Strukturen (Tree)

Eine Struktur ist eine hierarchische Anordnung von Domänen. Die Domänen einer Struktur nutzen einen gemeinsamen zusammenhängenden Namespace. Bei dem Namen einer untergeordneten Domäne handelt es sich um den Eigennamen an welchem der Name der übergeordneten Domäne angehängt wird.

Gesamtstruktur (Forest)

Als Gesamtstruktur werden mehrere Strukturen bezeichnet, welche separat und vollständig voneinander sind. Alle Domänen eines Forest basieren auf einem gemeinsamen Schema, besitzen denselben Global Catalog, sind durch Vertrauensstellungen verknüpft und agieren unabhängig.

**Physische Struktur**

Die physischen Komponenten sind Standorte und Domänencontroller.

Standorte

Ein Standort ist ein Subnetz oder eine Kombination aus mehreren IP-Subnetzen.

Die Standorte sind nicht Teil des Namespace. Wenn der Namespace durchsucht wird, werden Objekte von Domänen und OUs angezeigt, jedoch nicht die Gliederung nach Standorten. Die Standorte enthalten nur Computer und Verbindungsobjekte, welche zur Replikation zwischen den Standorten genutzt werden.

Domänencontroller

Ein Domänencontroller ist ein Computer auf welchem ein Replikat des Domänenverzeichnissen (der lokalen Domänendatenbank) gespeichert ist. Ein Domänencontroller kann nur einer Domäne zugehören, diese wiederrum kann aber mehrere Domänencontroller haben, welche alle ein vollständiges Replikat besitzen. Der Domänencontroller authentifiziert außerdem Anmeldeversuche und verwaltet Sicherheitsrichtlinien für Domänen.

Änderungen der Informationen werden an einem Domänencontroller vorgenommen. Dieser repliziert dann die Änderungen auf allen anderen Controllern innerhalb der Domäne. Eine größere Anzahl an Domänencontrollern wird für die Fehlertoleranz benötigt.

**FSMO-Rollen**

Einige Funktionen werden mit dem Single Master Prinzip durchgeführt. Dafür werden Controllern FSMO-Rollen zugewiesen. Eine Domäne darf nur 1 jeder FSMO-Rollen besitzen, aber die Rollen können beliebig aufgeteilt werden.

Gesamtstrukturweite Rollen:

Schema-Master

Der Schema Master ist für Änderungen des Schemas im Active Directory verantwortlich. Daher wird er bei Änderungen oder durch das hinzufügen von Objekten ins Schema benutzt.

Domain Naming Master

Dieser ist für die Namensgebung zuständig. Falls versucht wird, eine neue Domäne oder einen Domänencontroller in die Struktur einzubinden, funktioniert das nur, wenn der Domain Naming Master den Namen der neuen Domäne kontrolliert und freigegeben hat.

Domänenweite Rollen:

RID (Relative ID)-Master

Die SID muss eindeutig sein deswegen legt der RID-Master für jeden anderen Domänencontroller RID-Pools aus welchen dann bei neu erstellten Objekten gewählt wird.

PDC (Primary Domain Controller) -Emulator

Da die Speicherung von Daten in die Datenbank 20 Minuten dauern kann, werden geänderte Benutzerpasswörter auf dem PDC gespeichert. Wenn ein DC einen fehlerhaften Anmeldeversuch feststellt, frägt er erst beim PDC nach, bevor er den Benutzer zurückweist.

Der PDC ist auch globaler Zeitgeber für alle Server und Clients.

Domain Infrastructure Master

Der Infrastructure Master sorgt dafür, dass bei der Änderung von Objekten, welche in irgendeiner Weise mit anderen Objekten zusammenhängen, diese auch die Änderung mitbekommen. Das Ganze muss Domänenübergreifend Funktionieren.

**Global Catalog**

Der Global Catalog beinhaltet Informationen zu Objekten aus allen Domänen. Dieser Katalog wird auf einen Domänencontroller, meist auf dem ersten Controller der ersten Domäne gespeichert. Dieser wird dann als globaler Katalogserver bezeichnet. Durch den Globalen Katalog können Informationen im Verzeichnis gefunden werden, egal welche Domäne diese erhält. Zudem stellt der globale Katalog einem Controller Informationen über Gruppenmitgliedschaften eines Benutzers, welcher sich anmeldet, zur Verfügung.

**Replikation**

Durch die Replikation wird sichergestellt, dass Informationen, die an einem Domänencontroller durchgeführt wurden, auch auf allen anderen Controllern vorgenommen werden. Die Änderungen werden auf Controllern innerhalb eines Standortes, aber auch außerhalb repliziert.

Welche Informationen werden repliziert?

Die Informationen im Verzeichnis werden in Partitionen unterteilt und jede dieser Partitionen stellt eine Einheit der Replikation dar.

* **Schemapartition**

Auf dieser Partition befindet sich das Schema, also die Regeln für die Objekte und Attribute. Dieses Schema ist in der Gesamtstruktur gleich und wird auf die Controller repliziert

* **Konfigurationspartition**

Diese Partition beschreibt den logischen Aufbau der Domänen. Diese sind auch in der Gesamtstruktur gleich.

* **Domänenpartition**

Diese Partition beschreibt alle Objekte der Domäne. Diese Informationen sind Domänenspezifisch und werden nur auf Controllern der Domäne repliziert.

* **Anwendungsverzeichnispartition**

Hier werden dynamische, anwendungsspezifische Daten des Active Directory gespeichert.

Wie werden Informationen repliziert?

**Standortinterne Replikation**

Bei der Replikation innerhalb eines Standortes kommt ein Dienst namens Konsistenzprüfung (KCC) zum Einsatz. Der Dienst wir auf allen Controllern ausgeführt und er definiert den Pfad der Verzeichnisaktualisierung so, dass diese von einem zum nächsten Controller weitergeleitet wird. Die Topologie entspricht einer Ringstruktur, daher gibt es immer zwei Replikationspfade pro Domänencontroller. Dies bringt den Vorteil, dass wenn ein Domänencontroller nicht verfügbar ist, immer noch alle anderen die Aktualisierung mitbekommen.

Falls eine Domäne mehr als sieben Controller besitzt, dann werden mehr Verbindungsobjekte erstellt. Durch diese wird sichergestellt, dass kein Controller mehr als 3 Hops vom nächsten entfernt ist.

**Standortübergreifende Replikation**

Für die Replikation auf mehreren Standorten, müssen die Standorte durch Standortverknüpfungen manuell verbunden sein. Ein KCC pro Standort erstellt alle Verbindungen zwischen Standorten.

Über diese Verbindungen geschieht dann die Replikation

**Vertrauensstellung**

Eine Vertrauensstellung besteht zwischen Domänen. Bei der Anmeldung übernimmt die vertrauende Domäne die Echtheitsbestätigung der vertrauten Domäne. Das heißt, wenn eine Vertrauensstellung zwischen Domäne A und Domäne B herrscht und sich ein Benutzer bei Domäne A authentifiziert, dieser auch automatisch auf der Domäne B authentifiziert ist. Der Benutzer hat aber auf Domäne B nicht die gleichen Berechtigungen wie auf Domäne A.

Vertrauensstellungen können manuell erstellt werden oder sie werden automatisch erstellt. Die Vertrauensstellungen können transitiv sein, d.h. dass wenn A->B vertraut und B->C vertraut A->C vertraut.

Zudem können sie bidirektional oder auch nicht sein. Das bedeutet, dass wenn A->B vertraut, B->A auch vertraut.

**Gruppenrichtlinien**

Gruppenrichtlinien sind Zusammenstellungen von Benutzer- und Computerkonfigurationseinstellungen welche mit Computer, Domänen und OUs verknüpft werden können.

Durch diese Richtlinien kann unter anderem eingestellt werden, welche Programme welcher Benutzer anwenden kann.

Diese Richtlinien können lokal oder nicht-lokal sein. Lokale werden von den nicht-lokalen überschrieben.

Die Gruppenrichtlinien werden in folgender Reihenfolge angewendet:

* Lokale GPO
* Mit Standort verknüpfte GPOs
* Mit Domänen verknüpfte GPOs
* Mit Organisationseinheit verknüpfte GPOs

**Gruppen**

Benutzern sollte man niemals direkt Rechte geben oder ihnen diese verweigern. Es sollten Gruppen erstellt werden, die bestimmte Rechte haben.

Globale Gruppen

Diese Gruppen können Benutzerkonten oder andere globale Gruppen beinhalten. Diese werden benutzt, um die Organisationsgruppen zu zeigen wie z.B.: Manager. Diese Gruppen sind global in der Gesamtstruktur bekannt. Sie können aber nur Mitglieder aus der eigenen Domäne besitzen.

Lokale Gruppen

Diese existieren nur in der jeweiligen Domäne und beschreiben nicht die Mitglieder, sondern die Rechte. In ihre werden nur in Ausnahmefällen Benutzerkonten gespeichert. In ihr befinden sich hauptsächlich globale Gruppen. Aus Lokalen Gruppen werden automatisch Domänenlokale Gruppen. Der Vorteil ist dabei, dass die Gruppe nur einmal pro Domäne definiert werden müssen.

Universale Gruppen

Die Universellen Gruppen sind überall bekannt und können von jedem verwendet werden. Daher eigenen sie sich zur organisatorischen Beschreibung als auch zur Rechtevergabe. Änderungen müssen sofort in den Global Catalog gespeichert werden.

**HSM**

Das HSM ist ein System, welches Daten, auf welche längere Zeit nicht zugegriffen wird, auf nicht so schnelle Datenträger exportiert. Der Grund ist, dass diese Datenträger die gleiche Speicherkapazität besitzen aber billiger sind. Wenn auf die Daten zugegriffen werden möchte, werden diese erst wieder auf den schnellen Datenträger übertragen. Dieser Prozess wird als Recall bezeichnet.

**DFS**

Durch das DFS ist es möglich, auf Verzeichnisse zuzugreifen, ohne den tatsächlichen Speicherort zu kennen. Das DFS trennt dabei physikalischen Speicherort einer Datei von dem Namen, dadurch ist es möglich eine Verzeichnisstruktur zu erzeugen, obwohl die Verzeichnisse auf verschiedenen Speicherorten liegen. Dies ist nötig, da oft Dateien verschoben werden und die ganze Struktur neu verändert wird.

**EFS**

EFS ist ein Verschlüsselungsdienst, welchem es möglich ist, eine oder mehrere Dateien in einem Ordner zu verschlüsseln. Ohne die entsprechenden Schlüsselinformationen lässt sich die Datei nicht entschlüsseln.

Zudem ermöglich das EFS eine Benutzergebundene Verschlüsselung. Dateien werden mit einem Schlüssel versehen, auf den nur ein oder mehrere Benutzer Zugriff haben.

**Kerberos**

Kerberos ist eine Authentifikationsdienst, welcher dazu dient, eine sichere Authentifikation zu ermöglichen. Die Authentifizierung übernimmt dabei der geschützte Kerberos-dienst.

Die Authentifizierung läuft folgendermaßen ab:

Kerberos authentifiziert den Server gegenüber dem Client und den Client gegenüber dem Server, zudem authentifiziert er sich selbst gegenüber den beiden um seine Identität zu bestätigen. Danach meldet sich der Client am Kerberos-Server an und fordert ein Ticket. Dazu muss er dem Server ein Passwort mitgeben. Mit diesem Ticket kann er dann Dienste bzw. weiter Tickets anfordern.

Wenn ein Dienst angefordert wird, wird das Ticket an den Dienst gesendet, welcher dann überprüft ob der Benutzer berechtigt ist. Auch hier wird ein Sitzungsschlüssel vereinbart um die Identität von Client, Server und Kerberos-Server zu bestätigen.

**LDAP**

LDAP ist ein Netzwerkprotokoll, welches bei der Abfrage von Informationen eines Verzeichnisdienstes zum Einsatz kommt. LDAP beschreibt dabei die Kommunikation zwischen dem Client und dem Verzeichnisdienst. Wenn ein Client den Dienst anstößt, erzeugt er dabei eine LDAP-Abfrage, diese wird zum Server gesendet, welcher dann eine Antwort formuliert.

Das Protokoll unterstützt alle Funktionen welche notwendig sind: Anmeldungen, Suchanfragen und Änderungen von Daten.

**DNS**

Der DNS ist ein Dienst, der in TCP/IP-Netzwerken der dazu Dient benutzerfreundliche Namen auszufinden. Das DNS kann benutzerfreundliche Namen, welche aus den Domänennamen zusammengestellt sind, in andere Information auflösen, wie die IP-Adresse. Dies ist nötig, da Computer in einem Netzwerk nur über nummerische Adressen kommunizieren.

**Objektbenennung**

Das Active Directory verwendet den Netzwerkdienst LDAP zur Abfrage der AD-Datenbank. LDAP-Standards bestimmen daher wie Objekte benannt werden. Das Active Directory verwendet verschiedene Namenskonventionen für die Objekte

Definierte Namen

Jedes Objekt verfügt über einen definierten Namen, mit welchem das Objekt eindeutig identifiziert wird. Dieser Name enthält genügend Informationen, um das Objekt im Verzeichnis zu finden. Der Name hat den Namen des Objektes, die OUs und die Domäne enthalten.

Bsp: CN=Beispiel,OU=Werbung,DC=Windows,DC=Com

CN steht für Common Name und steht für den allgemeinen Namen.

OU steht für Oragnization Unit und zeigt den Namen der Organisationseinheit.

DC steht für Domain Component und zeigt den Namen der Domäne.

Relativ definierte Name

Der relative Name dient dazu, dass ein Objekt auch dann gefunden wird, wenn der ganze definierte Name nicht bekannt ist. Daher ist der relativ definierte Name im obigen Beispiel „Beispiel“.

Global eindeutige Kennung

Dies ist ein 128-Bit-Zahlenwert welcher bei der Erstellung des Objektes gesetzt wird. Diese Zahl ist eindeutig in der Gesamten Struktur und wird nie geändert egal ob das Objekt verändert oder verschoben wird. Falls also der Definierte Name des Objektes nicht zur Verfügung steht kann das Objekt trotzdem durch die GUID gefunden werden.

Benutzerprinzipalname

Der Benutzerprinzipalname ist der Name eine Benutzerkontos. Er besteht aus dem eigentlichen Benutzernamen und dem Domänennamen. Daher wäre ein Beispiel dafür: [Beispiel@Windows.com](mailto:Beispiel@Windows.com).