# Serverrollen

|  |  |
| --- | --- |
| **Serverrolle** | **Funktion** |
| Active Directory Certificate Services (AD CS) | Verwalten von öffentlichen Schlüsseln. Absicherung der Kommunikation |
| Active Directory Domain Services (AD DS) | Domaincontroller für AD. Speicherung und Verwaltung von Netzressourcen. |
| Active Directory Federation Services (AD FS) | Single-Sign-on. Eimalige Anmeldung über mehrere Dienste |
| Active Directory Lightweight Directory Services (AD LDS) | Light-Version von AD. Keine Benutzereinstellungen und Windows Domäne möglich. LDAP |
| Active Directory Rights Management Services (AD RMS) | Schützt Informationen von unautorisierter Verwendung |
| Application Server | Dies ist eine Sammlung von Diensten, welche für den Betrieb von Netzwerk-basierten  Applikationen (z.B. Web-Services) benötigt werden. Unter anderem kommt diese Rolle zum  Einsatz, eine Applikation das .NET Framework 3.0 erfordert.  .net, ASP.net und message queuing, //.auszuführen welche  net, http, sql server verwendet |
| DHCP Server | Dynamische IP-Vergabe |
| DNS Server | Namensauflösung |
| File Services | Speicherverwaltung und Verwaltung von Dateien und Ordnern. |
| Network Policy and Access Services | Diese Rolle umfasst Dienste für den Fernzugriff (remote access service) auf ein Netzwerk, den  Aufbau von VPNs, den Einsatz des Servers als Router, so  wie für den notwendigen Schutz des  Netzwerkes in einer solchen Umgebung. |
| Print Services | Verwalten von Druckern über eine zentrale Einheit |
| Terminal Services | Remote Desktop |
| Web Server (IIS) | Zur Bereitstellung von Webdiensten. IUSR = Standardbenutzer, IIS\_IUSRS = Standardgruppe. Es existieren Statische-, Dynamische-Seiten und Verzeichnislisten. Verzeichnis = C:\inetpub\ |
| Windows Server Update Services | Verwalten der Windows Updates innerhalb einer Domäne. |
| HyperV in Windows | Eine Virtualisierungstechnologie |

# Authentifizierungen

|  |  |
| --- | --- |
| **Authentifizierung** | **Erklärung** |
| Anonymous | Kein Login. Default |
| Basic | Benutzername & Passwort |
| Windows | Automatisch Login. Login Dialog nur im Fehlerfall |
| Digest | Sicherer als Basic. Benutzername und Passwort gehen nicht über das Netz. |

# Group Policies

* Richtlinien welche mit einem Standort, Domain oder einer OU verknüpft werden können.
* Sie dürfen sich gegenseitig nicht wiedersprechen.
* Riesige Auswahl an verschiedenen Einstellungen

# NTFS-Rechte

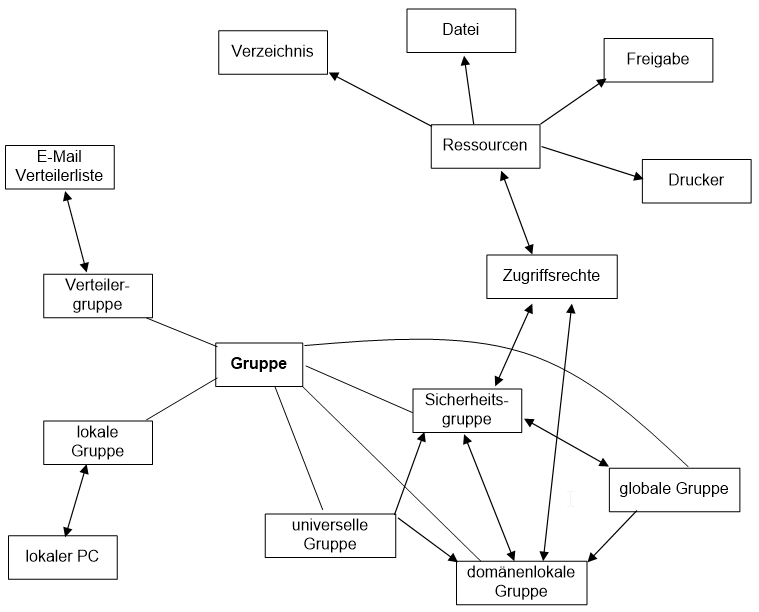
* Spielen bei Freigaben auch eine Rolle
* Zuerst Freigabeberechtigungen danach NTFS-Rechte

# Active Directory

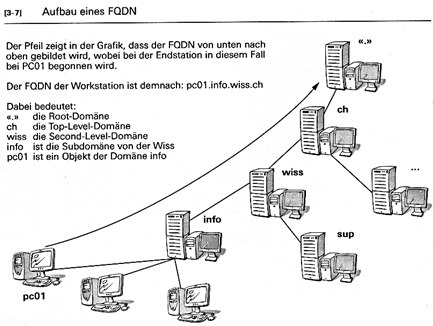
* OU: Organisationseinheit. Können in anderen OUs sein.
* Sammlung von Objekten
* Benutzerverwaltung
* Jedes Objekt hat Attribute: z.B. Name und Telefonnummer
* Schema legt fest, welche Attribute ein Objekt haben kann
* Nicht ohne DNS möglich
* Bei Fehler nicht mehr deinstallierbar oder behebbar

# Gruppen

|  |  |  |
| --- | --- | --- |
| **Gruppenart** | **Verwendbar/sichtbar in** | **Mögliche Mitglieder** |
| Domänenlokale Gruppen | Nur auf der eigenen Domäne sichtbar | Globale Gruppen, Benutzer |
| Globale Gruppe | Überall sichtbar | Benutzer aus der eigenen Domäne, andere Globale Gruppen |
| Universelle Gruppe | Verwendbar in allen Domänen der Gesamtstruktur | Globale Gruppe, Mitglieder aus allen Domänen |



# DNS

* Reverse Lookup Zone für 192.168.40.10 -> 10.40.168.192.in-addr.arpa
* Mehrere Zonen sind möglich
* FQDN = Fully qualified Domain Name

# AGDLP (Account, Global, Domain Local, Permisson)

Accounts in Globale Gruppen, diese in Domänen Lokale Gruppen und diesen gibt man dann die Berechtigung (Permissions).

# Passwortrichtlinien

* Genügend Komplex und lang
* Läuft nach einiger Zeit ab