Active Directory Domain Services (AD DS)

- **Was ist AD DS überhaupt?**

  - AD DS sind die **Kernfunktionen von Active Directory**, mit denen man die Benutzer und Computer verwalten kann und Systemadministratoren Daten in logischer Hierarchien organisieren können.
  - AD DS und die zugehörigen Dienste bilden die Grundlage für Unternehmensnetzwerke, in denen **Windows-Betriebssysteme** ausgeführt werden.
  - Der zentrale Speicher für alle Domänenobjekte (Benutzerkonten, Computerkonten und Gruppen), ist die AD DS-Datenbank.
  - Es gibt ein durchsuchbares hierarchisches Verzeichnis und eine Methode zum Anwenden von Konfigurations- und Sicherheitseinstellungen für Objekte.

- **Logische und Physische Komponenten von AD DS:**

  - In einer AD DS-Datenbank sind verschiedene Typen an **logischer Komponenten** enthalten, sie sind **Strukturen**, mit denen man ein AD DS-Design implementiert, welches für die eigene Organisation geeignet ist.
  - Folgende Typen **logischer Komponenten** gibt es in einer AD DS-Datenbank:

    - **Partition**:
      → Ein Teil der AD DS-Datenbank. Die Datenbank besteht zwar aus nur einer Datei namens „Ntds.dit“, Aber unterschiedliche Partitionen enthalten unterschiedliche Daten. Es gibt die Schemapartition, welche eine Kopie des Active Directory-Schemas enthält. Dann die Konfigurationspartition, welche die Konfigurationsobjekte für die Gesamtstruktur enthält, sowie die Domänenpartition, die Benutzer, Computer, Gruppen und andere domänenspezifische Objekte enthält. Auf mehreren Domänencontrollern werden Kopien der Partitionen gespeichert und dort mithilfe der Verzeichnisreplikation aktualisiert.

    - **Schema**:
      → Ein Satz, welcher Definitionen von Objekttypen und Attributen beinhaltet, mit denen man die in AD DS erstellten Objekte definiert.

    - **Domäne:**
      → Ein logischer Verwaltungscontainer für Objekte wie Benutzer und Computer. Eine Domäne ist einer bestimmten Partition zugeordnet und kann mithilfe von über- oder untergeordneten Beziehungen zu anderen Domänen organisiert werden.

- **Domänenstruktur:**
  → Eine hierarchische Sammlung von Domänen, die eine gemeinsame Stammdomäne sowie einen zusammenhängenden DNS-Namespace (Domain Name System) verwenden.

- **Gesamtstruktur**:
  → Eine Sammlung von einer oder mehreren Domänen, die über einen gemeinsamen AD DS-Stamm, ein gemeinsames Schema sowie einen gemeinsamen globalen Katalog verfügen.

- **OE (Organisationseinheit):**
  → Ein Containerobjekt für Benutzer, Computer und Gruppen, welches durch die Verknüpfung von Gruppenrichtlinienobjekten, ein Framework zum Delegieren von Administratorrechten und Verwaltung bereitstellt.

- **Container:**
  → Ein Objekt, welches ein organisationsbezogenes Framework für die Verwendung in AD DS zur Verfügung stellt. Man kann Standard- oder benutzerdefinierte Container erstellen.

- Konkrete Objekte oder Objekte, die konkrete, reale Komponenten beschreiben, sind **physische Komponenten**. Folgende gibt es im AD DS:

  - **Domänencontroller:**
    → Dieser enthält eine Kopie der AD DS-Datenbank sowie vom Datenspeicher. Jeder Domänencontroller kann bei den meisten Vorgängen Änderungen verarbeiten und auf alle anderen Domänencontroller in der Domäne replizieren.

  - **Datenspeicher:**
    → Die AD DS-Datenbank verwendet die Microsoft Jet-Datenbanktechnologie und speichert die Verzeichnisinformationen in der Datei „Ntds.dit“ und den zugehörigen Protokolldateien. Diese Dateien werden standardmäßig im Ordner „C:\Windows\NTDS“ gespeichert.

  - **Globaler Katalogserver:**
    → Ein Domänencontroller, welcher den globalen Katalog hostet. Eine partielle, schreibgeschützte Kopie aller Objekte in einer Gesamtstruktur mit mehreren Domänen. Ein globaler Katalog beschleunigt die Suche nach Objekten.

  - **RODC (Schreibgeschützter Domänencontroller):**
    → Eine besondere, schreibgeschützte Installation von AD DS.

- **Standort:**
  → Ein Container für AD DS-Objekte wie Computer und Dienste, welche speziell für einen physischen Standort erforderlich sind.

- **Subnetz:**
  → Ein Bestandteil der IP-Netzwerkadressen.

- **Es gibt AD DS-Optionen zum Ausführen folgender Aktionen:**

  - Installieren, Konfigurieren und Aktualisieren von Apps
  - Verwalten der Sicherheitsinfrastruktur
  - Aktivieren von Remote Access Service und DirectAccess
  - Ausstellen und Verwalten digitaler Zertifikate

- **Benutzer, Gruppen und Computer:**

  - **Benutzer:**
    - Benutzerkonten sind Objekte, die alle Informationen enthalten, die die Benutzer beschreiben, wie Name, Kennwort oder Gruppenmitgliedschaften.
    - Ebenfalls enthält ein Benutzerkonto Einstellungen, die man entsprechend der Anforderungen konfigurieren kann.
    - Benutzerobjekte in AD DS können an verschiedenen Stellen erstellt und verwaltet werden:

      → Active Directory-Verwaltungscenter
      → Active Directory-Benutzer und –Computer
      → Windows Admin Center
      → Windows PowerShell
      → Dsadd-Befehlszeilentool

  - **Gruppen:**
    - Gruppen sind ebenfalls Objekte. In diesen befinden sich dann Benutzerobjekte, die man der jeweiligen Gruppe zugewiesen hat.
    - Gruppen sind super praktisch, wenn es darum geht Rechte zuzuweisen. Wenn z.B. mehrere Benutzer die gleiche Zugriffsebene für einen Ordner benötigen, ist es effizienter, eine Gruppe zu erstellen, welche die entsprechenden Benutzerkonten enthält, und man dann der Gruppe die erforderlichen Berechtigungen zuweist. Somit muss man nicht jeden Benutzer gesondert verwalten, sondern kann einfach die Benutzerobjekte der passenden Gruppe hinzufügen.

- Es gibt **zwei Typen** von Gruppen:

- **Sicherheitsgruppen:**
  → Gruppen mit aktivierter Sicherheit und werden zum Zuweisen von Berechtigungen für verschiedene Ressourcen verwendet. Wenn man eine Gruppe zum Verwalten der Sicherheit verwenden möchte, muss es sich um eine Sicherheitsgruppe handeln.

- **Verteilergruppen:**
  → Gruppen ohne aktiver Sicherheit. Üblicherweise werden diese für E-Mail-Anwendungen verwendet.

- Der Gruppentyp bestimmt die Funktion der Gruppe.
- Der Geltungsbereich einer Gruppe bestimmt sowohl den Umfang der Funktionen, als auch die Berechtigungen und die Gruppenmitgliedschaft. Es gibt vier **Gruppengeltungsbereiche**:

- **Lokal:**
  → Für eigenständige Server oder Arbeitsstationen.
  → Für Server, die Domänenmitglied aber keine Domänencontroller sind.
  → Für Arbeitsstationen, die Domänenmitglied sind.
  → Lokale Gruppen sind nur auf den Computern verfügbar, auf denen sie vorhanden sind.
  → Wichtige **Merkmale** einer lokalen Gruppe:

    - Sie können Funktionen und Berechtigungen nur lokalen Ressourcen zuweisen.
    - Mitglieder können von jeder Stelle der AD DS-Gesamtstruktur stammen.

- **Lokal (in Domäne):**
  → Zum Verwalten des Zugriffs auf Ressourcen.
  → Zum Zuweisen von Verwaltungsrechten und Zuständigkeiten.
  → Sie befinden sich in einer AD DS-Domäne.
  → Wichtige **Merkmale** einer lokalen Domänengruppe:

    - Sie können Funktionen und Berechtigungen nur lokalen Domänenressourcen zuweisen.
    - Mitglieder können von jeder Stelle der AD DS-Gesamtstruktur stammen.

- **Global:**
  → Hauptsächlich, um Benutzer mit ähnlichen Merkmalen zu konsolidieren.
  → Wichtige **Merkmale** einer globalen Gruppe:

- Sie können überall in der Gesamtstruktur Funktionen und Berechtigungen zuweisen.

- Mitglieder können nur aus der lokalen Domäne stammen und Benutzer, Computer und globale Gruppen aus der lokalen Domäne beinhalten.

- **Universell:**
  - → Meistens in Netzwerken mit mehreren Domänen.
  - → Wichtige **Merkmale** von universellen Gruppen:

    - Sie können überall in der Gesamtstruktur Funktionieren und Berechtigungen zuweisen, ähnlich wie bei globalen Gruppen.
    - Mitglieder können von jeder Stelle der AD DS-Gesamtstruktur stammen.

- **Computer:**
  - Computerobjekte sind (genau wie Benutzer) Sicherheitsprinzipiale.
  - **Merkmale** von Computerobjekten:

    - → Sie verfügen über ein Konto mit einem Anmeldenamen und einem Kennwort, das von Windows regelmäßig und automatisch geändert wird.
    - → Sie authentifizieren sich bei der Domäne.
    - → Sie können zu Gruppen gehören, auf Ressourcen zugreifen und mithilfe von Gruppenrichtlinien konfiguriert werden.

  - Der Lebenszyklus eines Computerkontos beginnt, wenn man das Computerobjekt erstellt und in die Domäne einbindet. Nach dem Einbinden des Computerkontos in Ihre Domäne zählen folgende Aufgaben zu den alltäglichen Verwaltungsaufgaben:

    - → Konfigurieren von Computereigenschaften
    - → Verschieben des Computers zwischen Organisationseinheiten
    - → Verwalten des Computers selbst
    - → Umbenennen, Zurücksetzen, Deaktivieren, Aktivieren und schließlich Löschen des Computerobjekts

  - Wenn ein Computer der Domäne beitritt, wird ein Computerobjekt standartmäßig im „Computer“ Container gespeichert.
  - Der „Computer“ Container ist keine Organisationseinheit, sondern ein Objekt der Container-Klasse. Der allgemeine Name lautet „**CN-Computers**“.

- Unterschiede zwischen einem Container und einer Organisationseinheit:

  → Ein Container „Computer“ kann nicht unterteilt.
  → Mit einem Container kann auch kein Gruppenrichtlinienobjekt verknüpft werden.

- Empfehlenswert ist es, sich benutzerdefinierte Organisationseinheiten zum Hosten von Computerobjekten zu erstellen und nicht den Container „Computer“ zu verwenden.

- **AD DS-Gesamtstrukturen und –Domänen:**

  - Eine **Gesamtstruktur** ist ein Container der obersten Ebene in AD DS. Jede Gesamtstruktur ist eine Sammlung von einer oder mehreren Domänenstrukturen, die über ein gemeinsames Verzeichnisschema und einen globalen Katalog verfügen.
  - Für alle Domänen in einer Gesamtstruktur gilt:

    - Gemeinsamer Stamm
    - Gemeinsames Schema
    - Globaler Katalog

  - Eine **AD DS-Domäne** ist ein logischer Verwaltungscontainer für Benutzer, Gruppen und Computer.
  - Eine **Domänenstruktur** ist eine Sammlung von einer oder mehreren Domänen, die gemeinsam einen zusammenhängenden Namespace verwenden. Die Stammdomäne der Gesamtstruktur ist die erste Domäne, die in der Gesamtstruktur erstellt wird.
  - In der **Gesamtstruktur-Stammdomäne** sind folgende Objekte vorhanden:

    - Schema-Masterrolle
    - Domänennamen-Masterrolle
    - Gruppe „Unternehmensadministratoren“
    - Gruppe „Schemaadministratoren“

  - In **jeder Domäne** sind folgende Objekte vorhanden (einschließlich der Gesamtstruktur-Stammdomäne):

    - RID-Masterrolle
    - Infrastruktur-Masterrolle
    - PDC-Emulator-Masterrolle
    - Gruppe „Domänenadministratoren“

- Eine AD DS-Domäne ermöglicht:

  - **Authentifizierung**. Wenn ein in eine Domäne eingebundener Computer gestartet wird oder sich ein Benutzer an einem in die Domäne eingebundenen Computer anmeldet, wird er von AD DS authentifiziert. Bei der Authentifizierung wird anhand der Anmeldeinformationen überprüft, ob der Computer oder Benutzer über die richtige Identität in AD DS verfügt.

  - **Autorisierung.** Windows verwendet Technologien für die Autorisierung und Zugriffssteuerung, um zu ermitteln, ob authentifizierten Benutzern der Zugriff auf Ressourcen erlaubt ist.

- **Organisationseinheiten (OEs):**

  - Eine **Organisationseinheit** ist ein Containerobjekt innerhalb einer Domäne, welche man zum Konsolidieren von Benutzern, Computern, Gruppen und anderen Objekten verwenden kann.
  - Man kann **GPOs** (Gruppenrichtlinienobjekte) direkt mit einer OE verknüpfen, um die ein einer OE enthaltenen Benutzer und Computer zu verwalten.
  - Ebenfalls kann man einen **OE-Manager** zuweisen und einer OE eine COM+-Partition zuordnen.
  - Eine OE in AD DS kann man an folgenden Stellen erstellen:

    - Active Directory-Verwaltungscenter
    - Active Directory-Benutzer und -Computer
    - Windows Admin Center
    - Windows PowerShell mit dem Active Directory PowerShell-Modul

  - Mit OEs kann man die hierarchischen, logischen Strukturen in einer Organisation darstellen.
  - Es gibt zwei Gründe wie man eine OE erstellt:

    - Zum **Konsolidieren** von Objekten und zum Vereinfachen der Objektverwaltung, da GPOs auf die Gesamtheit angewendet werden.
    - Zum **Delegieren** der administrativen Objektkontrolle innerhalb der OE.

- **Verwaltungstools für AD DS:**

  - Es gibt verschiedene Tools für die Verwaltung von AD DS.

  - Das **Active Directory-Verwaltungscenter** stellt eine grafische Benutzeroberfläche bereit, die auf Windows PowerShell basiert. Diese erweiterte Oberfläche ermöglicht mithilfe einer aufgabenorientierten Navigation das Ausführen der **AD DS-Objektverwaltung** und ersetzt die Funktionalität „Active Directory-Benutzer und -Computer“.
  - Zu den **Aufgaben**, die Sie mit dem **Active Directory-Verwaltungscenter** ausführen können, gehören:

    - Erstellen und Verwalten von Benutzer-, Computer-und Gruppenkonten
    - Erstellen und Verwalten von Organisationseinheiten
    - Herstellen einer Verbindung zu mehreren Domänen und Verwalten dieser Domänen in einer einzigen Instanz des Active Directory-Verwaltungscenters
    - Suchen und Filtern von AD DS-Daten durch das Erstellen von Abfragen
    - Erstellen und Verwalten differenzierter Kennwortrichtlinien
    - Wiederherstellen von Objekten aus dem Active Directory-Papierkorb
    - Verwalten von Objekten, die für die dynamische Zugriffssteuerungsfunktion erforderlich sind

  - **Windows Admin Center** ist eine webbasierte Konsole, mit der man Servercomputer und Computer, auf denen Windows 10 ausgeführt wird, verwalten kann. In der Regel verwendet man Windows Admin Center anstelle der Remoteserver-Verwaltungstools (RSAT) zum Verwalten von Servern.

  - **RSAT (Remote Server Administration Tools)** ist eine Sammlung von Verwaltungstools, mit deren Hilfe Sie Windows Server-Rollen und -Features remote verwalten können.

  - **Active Directory-Modul für Windows PowerShell** unterstützt die AD DS-Verwaltung und zählt zu den wichtigsten Verwaltungskomponenten. Server-Manager und das Active Directory-Verwaltungscenter basieren auf Windows PowerShell und verwenden Cmdlets zum Ausführen der Aufgaben.

  - **„Active Directory-Benutzer und -Computer“** ist ein MMC-Snap-In (Microsoft Management Console), das die gängigsten Ressourcen (einschließlich Benutzer, Gruppen und Computer) verwaltet. Auch wenn viele Administratoren mit diesem Snap-In vertraut sind, wird es durch das Active Directory-Verwaltungscenter ersetzt, das mehr Funktionen bietet.

- Mit dem MMC-Snap-In **„Active Directory-Standorte und -Dienste“** werden Replikation, Netzwerktopologie und zugehörige Dienste verwaltet.

- Mit dem MMC-Snap-In **„Active Directory-Domänen und -Vertrauensstellungen“** werden Vertrauensstellungen auf den Funktionsebenen von Domänen und Gesamtstruktur konfiguriert und verwaltet.

- Mit dem MMC-Snap-In **„Active Directory-Schema“** werden die Definitionen von AD DS-Attributen und -Objektklassen überprüft und geändert. Diese müssen nur selten überprüft oder geändert werden. Daher ist das Snap-In „Active Directory-Schema“ standardmäßig nicht registriert.