(1) Grundlagen W2K Server

1. **Versionen von W2K Server:**
   - W2K Server → kleine und große Unternehmen
   - W2K Advanced Server → große Unternehmen
   - W2K DataCenter Server → stärkster Server

2. **Verzeichnisdienste in W2K Server:**
   - Active Directory in W2K Server (Verzeichnisdienst in W2K Netzwerken)
     - Hierarchisch verteilte Datenbank basierend auf MS Access
     - Aufgabe: Ressourcen (User, Groups, Computer, etc.) selektiv verfügbar machen
     - Sicherheit: Authentifizierungsprotokolle & Sicherheitskonzept im AD
     - Verwaltung: Fernwartung mittels Remote-Verbindung möglich
     - Flexibiltät: Hoch wegen Verschachtelung
     - Performance: Hoch wegen Begrenzung von Datenmengen

3. **Sicherheitsfunktionen:**
   - Sicherheit auf logischer Ebene durch Anmeldeauthentifizierung/Zugriffsberechtigung (durch Kerberos Anmeldeprotokoll)

4. **Verwaltungsfunktionen:**
   - Remote Installationsdienste
   - ACL = Access Control List
   - Group Policies (Gruppenrichtlinien)
   - Telnet Server
   - Terminal Services

5. **Skalierbarkeit, Zuverlässigkeit und Hardwareunterstützung:**

6. **Netzwerkinfrastruktur:**
   - DHCP (Dynamic Host Configuration Protocol)
     - Vergabe von IP-Adressen an Workstations; Autorisierung in AD erforderlich
   - DNS (Domain Name System)
     - Grundvoraussetzung für AD; IP-Adresse wird automatisch im DNS registriert → Zuordnung von Workstation-Namen zu IP-Adressen innerhalb DNS-Datenbank

7. **Dateiverwaltung und Dateisystem:**
   - DFS (Distributed File System) → einzige Verzeichnisstruktur für Datenbestände
   - Datenträgerkontigente → Zuordnung von Speicherplatz (NTFS = **N**ew **T**echnologie **F**ile **S**ystem)
   - NTFSv5 → neue Funktionalität (Vergabe von Laufwerksnamen statt Buchstaben)

(2) Installation W2K Server

1. **Hardware:**
   - Minimale Anforderungen (Pentium II mit 200MHz, 128 MB RAM, 1GB HDD Speicher, NTFS Dateisystem, Netzwerkkarte)

2. **Dateisystem:**
   - Unterstützt FAT, FAT32, NTFSv5 (nur hier Sicherheitsmerkmale & AD)

3. **Lizenzierung:**
   - Pro Workstation & Server benötigt man eine Lizenz (Server erlaubt Anzahl zulässiger Verbindungen

4. **Vorbereitungen:**
   - Hardware muss W2K kompatibel sein / W2K unterstützt Plug & Play

(3) DNS – Domain Name System in W2K Server

1. **Domain Name System:**
   - Konzeption zur Namensauflösung → Zuordnung IP-Adresse zu Hostname
   - Hierarchische Namensraum für Computer, Dienste und DNS-Subdomänen
   - DNS-Domäne hat selbst auch einen Namen
   - FQDN (**F**ull **Q**ualified **D**omain **N**ame) → setzt sich aus Host-Namen und Domänen-Namen zusammen (Bsp.: PC1.marketing.teamup.de = FQDN)

2. **Namensauflösung:**
   - DNS-Nameserver ermittelt zu einer IP-Adresse den Hostnamen bzw. umgekehrt
     - Forward-Lookup: Hostname ←→ IP-Adresse
     - Reverse-Lookup: IP-Adresse ←→ Hostname
     -
3. **Dynamisches DNS:**
   - Client kann dem Server seine IP & Host-Namen mitteilen, sofern diese sich geändert haben → weniger Verwaltungsaufwand
   - **DDNS → DHCP:** DHCP weist nach Aufforderung der Workstation/Client eine IP-Adresse sowie einen Host-Namen zu und teilt diese zur Registrierung dem DNS mit

4. **Zonen:**
   - Stammdomäne einer Zone ist die **Domäne** (Bsp.: **teamup.de** → *marketing*.**teamup.de**) [**Domäne** → *Subdomäne*] → Namenszuordnung von IP-Adresse wird in Zone 1 gespeichert
   - Subdomäne *service*.**teamup.de** → Namenszuordnungen werden in Zone 2 gespeichert

   → Vorteil: DNS ohne Zoneneinteilung verursacht eine sehr hohe Netzlast (daher besser Aufteilung des DNS in verschiedene Zonen → am besten hat eine Zone (eine Stammdomäne grundsätzlich) sowie mehrere DNS-Namensserver, um eine Ausfallsicherheit zu gewährleisten

(4) Active Directory

1. **Grundlagen zu Active Directory:**
   - AD ist ein Verzeichnisdienst mit der Aufgabe, Ressourcen im Netzwerk zu organisieren, verwalten, steuern bzw. dem User zur Verfügung zu stellen
   - Vorteile: Skalierbarkeit (Objekte verwaltbar) und zentrale Verwaltung
   - Unterstützung von TCP/IP, DNS, DHCP (Verzeichniszugriffe) / Kerberos (Authentifizierung) / http, Namensformate (URL, eMail)

2. **Logische Struktur:**
   - Hierarchischer Aufbau der Struktur (Untersuchung vor der Implementierung) der mit folgenden Komponenten umgesetzt wird:
     - Objekten → kleinste Einheit (PC, Drucker, etc.) werden später zu Klassen zusammengeführt
     - Organisationseinheiten (OU) → dient zur Gruppierung von Objekten
     - Domäne → wesentliche Einheit vom AD (nach innen und außen abgeschlossen) Zugriff auf Objekte nur nach Anmeldung möglich

3. **Vertrauensstellung:**
   - Beziehung zwischen zwei Domänen
   - Anmeldung an fremder Domäne über Authentifizierung aus der vertauenden Domäne möglich (Vertrauensbasis durch Bidirektionalen Austausch innerhalb W2K Netzwerken)

4. **Physische Struktur:**
   - Entfällt momentan

(5) Der Domänencontroller (DC)

1. **Allgemein:**
   - Führt W2K Server aus
   - Speichert komplettes AD der Domäne
   - Durch Replikation werden sämtliche Änderungen auf allen DC der Domäne verfügbar gemacht (kurzzeitiger Nachteil durch inkonsistente Daten)
   - Dient als Anmeldeserver → Benutzer können sich somit an der Domäne anmelden bzw. authentifizieren
   - Wenn DC gleichzeitig als DNS-Server dienen, dann können die Zonen ins AD integriert werden (→ Aktualisierung nach dem Multi-Master-Modell / AD-Sicherheit für Zonendateien)

2. **Installation des AD:**
   - Kommandozeile : Befehl dcpromo oder mittels Serverkonfigurationsassistent
   - **Stammdomäne** sowie Unterdomänen einrichten (**distributa.local**)
   -

(6) Active Directory Objekte

1. **Objekte:**
   - Kleinste Einheit, Name und Attribute (→ Aufgabe von AD diese in Orgaeinheiten zu gruppieren)

2. **Organisationseinheit:**
   - Gruppierung von Objekten (Verwaltung durch Domänenadministrator) → OU´s können in andere OU´s eingegliedert sein

3. **Benutzerkonten:**
   - Authentifizierung der User (Berechtigung für Zugriffe)
   - Sicherheitskennung (SID = Security Identifier + relative Kennung RID)
   - Serverbasiertes Benutzerprofil (Profil ist immer identisch, egal wo sich der User anmeldet) → es gibt grundsätzlich zwei Arten von Benutzerkonten:
     - lokale Benutzerkonten → liegt auf lokalem Rechner (Zugriffsrecht auf lokale Ressourcen)
     - Domänenbenutzerkonten → liegt in der AD (Zugriffsrecht auf Domänen-Ressourcen)

4. **Computerkonten:**
   - Werden im AD als Objekte dargestellt
   - Schützenswerte Elemente (SID)
   - Berechtigung für den Zugriff auf Computer definieren

(7) Gruppen:

1. **Gruppentypen:**
   - Lokale Gruppen (auf lokalem PC) und Sicherheitsgruppen (mittels Berechtigungen wird Zugriff auf Ressourcen gesteuert)

2. **Gruppenbereiche:**
   - Sicherheits- und Verteilergruppen (charakterisieren die Herkunft und den Wirkungsradius)

3. **AGDLP-Regel:**
   - Benutzer (**A**ccess) erhält Mitgliedschaft in globaler Gruppe (**G**lobal Group)
   - Globale Gruppe wird in lokale Gruppe platziert (**D**omain **L**ocal Group)
   - Vergabe von Zugriffsrechten (**P**ermission) an die lokale Gruppe

(8) Berechtigungen und Objektverwaltung:

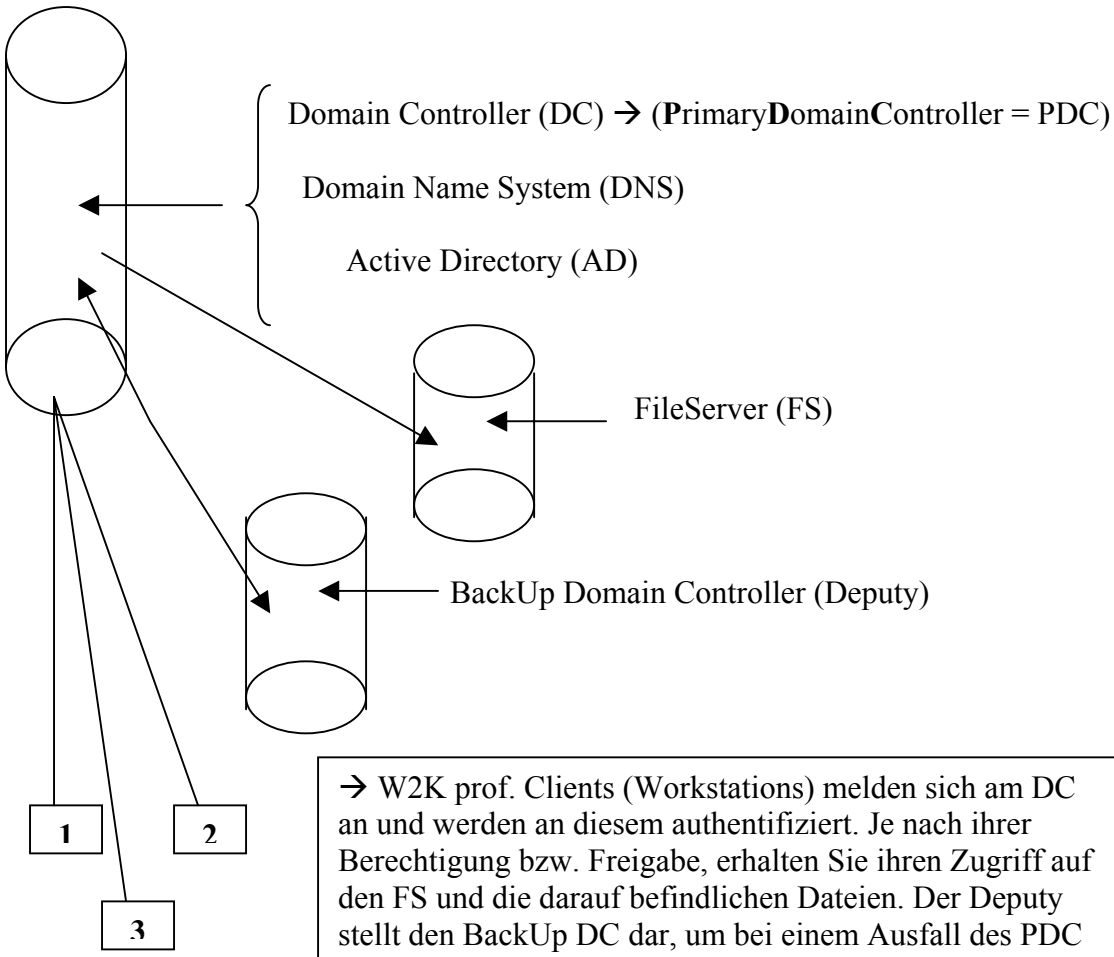
1. **NTFS-Berechtigungen:**
   - Manche Objekte werden nur durch AD-Berechtigungen geschützt (User, Gruppen)
   - Andere Objekte werden zusätzlich durch NTFS-Berechtigungen (Ordner) geschützt
   - NTFS-Berechtigungen werden auf untergeordnete Ordner vererbt

2. **Freigabeberechtigungen:**
   - Freigabe ist Grundvoraussetzung für Zugriffe aus dem Netzwerk
   - Freigaben existieren für Ordner und Drucker im AD, sowie auch für Dateien (NTFS)
   - Im AD existieren auch sogenannte ACL (Access Control List) für die vorhandene Ordnerstruktur → Objektschutz im AD (wer, wie, worauf zugreifen darf ...)

3. **Distributed File System (DFS):**
   - Das verteilte Dateisystem stellt eine einzelnes Dateisystem dar, welches hierarchisch aufgebaut ist
   - Ressourcen können über das gesamte Netzwerk verteilt sein, denn ein User greift über einen einzigen Punkt zu (DFS-Stammknoten)
   - Leichte Administration, da Zugriff lediglich über einen Punkt erfolgt
   - DFS-Stammknoten bildet die oberste Hierarchie und kann mehrere Unterknoten besitzen, die wiederum auf freigegebene Ordner verweisen

Schaubild: W2K Server Struktur innerhalb einer Firma

W2K Server → (DC / Deputy / FileServer)



→ W2K prof. Clients (Workstations) melden sich am DC an und werden an diesem authentifiziert. Je nach ihrer Berechtigung bzw. Freigabe, erhalten Sie ihren Zugriff auf den FS und die darauf befindlichen Dateien. Der Deputy stellt den BackUp DC dar, um bei einem Ausfall des PDC diesen zu ersetzten. (Replikation gewährleistet den Abgleich zwischen PDC und Deputy, so dass beide jederzeit ihre Funktion erfüllen können)