Active Directory Tartomány Kiépítése Windows Server 2016-on

Ez az útmutató lépésről lépésre vezet a VirtualBoxban futó Windows Server 2016 rendszeren egy teljes körű tartományi infrastruktúra felépítéséhez. Az Active Directory (AD) a modern hálózati rendszerek gerincét képezi, lehetővé téve a központosított felhasználókezelést, biztonsági házirendek alkalmazását és erőforrás-hozzáférés szabályozását.

A gyakorlat során elsajátítja az alapvető rendszergazdai feladatokat, beleértve a hálózati konfigurációt, szerepkör-telepítést, tartományvezérlő promóciót és felhasználókezelést. Minden lépés részletesen dokumentálva van, így akár önálló tanuláshoz, akár osztálytermi gyakorláshoz használható.

Az AD Telepítés Folyamata

01

Előkészületek

Hálózati és rendszerbeállítások konfigurálása: statikus IP-cím, számítógép átnevezése

02

AD DS Szerepkör

Active Directory-tartományszolgáltatások bináris fájljainak telepítése a Kiszolgálókezelőn keresztül

03

Tartományvezérlő Promóció

Az erdő (Forest) és tartomány (Domain) létrehozása új tartományvezérlőként

04

Ellenőrzés

DNS és AD eszközök működésének tesztelése és validálása

05

Adminisztráció

Szervezeti egységek (OU) és felhasználók létrehozása a struktúra kialakításához

Az Active Directory egy hierarchikus adatbázis, amely tárolja a hálózati objektumokat - felhasználókat, számítógépeket, csoportokat, megosztásokat - és kezeli a hozzájuk való hozzáférést. A tartományvezérlő (Domain Controller) ezeket az információkat tárolja és kezeli, biztosítva a hitelesítést és engedélyezést a hálózaton belül.

Gyakorlati Feladat: A "Példa Kft." Tartományának Kiépítése

A gyakorlat célja, hogy valós vállalati környezetet szimuláljunk létrehozva egy új tartományt **pelda.local** néven, és megvalósítva a cég alapvető felhasználói struktúráját. Ez a konfiguráció szolgál alapul további hálózati szolgáltatások és biztonsági beállítások tanulmányozásához.

Tartomány Struktúra

Új erdő és tartomány létrehozása pelda.local néven

Felhasználói Bázis

Igazgatóság szervezeti egység és felhasználók létrehozása

Hálózati Konfig

Statikus IP-cím és DNS beállítások konfigurálása

Az útmutató végrehajtása után rendelkezésére áll egy működőképes tartományvezérlő, amely képes hitelesíteni felhasználókat, kezelni számítógép fiókokat és alkalmazni csoport házirendeket. Ez a konfiguráció szimulálja a valós vállalati környezetek alapvető elemeit.

1. lépés: Hálózati beállítások és Előkészítés

Az Active Directory működésének alapfeltétele a fix, statikus IP-cím beállítása. A tartományvezérlő nem használhat dinamikus (DHCP) címet, mivel más klienseknek mindig tudniuk kell, hol található a DNS és hitelesítési szolgáltatás.

1

VirtualBox Hálózat

VirtualBox gép beállításainál a hálózati kártya legyen **Belső hálózat** (Internal Network) módban

2

Gép Átnevezés

Kiszolgálókezelő → Helyi kiszolgáló → Számítógép neve módosítása **SRV-01**-re

3

IP Konfiguráció

Ethernet adapter IPv4 beállításai: 192.168.10.10 / 255.255.255.0 / DNS: 127.0.0.1

Részletes Konfigurációs Lépések

VirtualBox Beállítás

Indítsa el a VirtualBox kezelőfelületét, válassza ki a Windows Server 2016 virtuális gépet, majd a Beállítások → Hálózat menüpontban állítsa a hálózati kártyát "Belső hálózat" módba. Ez biztosítja, hogy a virtuális gép egy privát hálózaton legyen más virtuális gépekkel.

Számítógép Átnevezés

Jelentkezzen be a Windows Server 2016 rendszerbe, nyissa meg a **Kiszolgálókezelőt** (Server Manager), majd kattintson a **Helyi kiszolgáló** (Local Server) fülre. A számítógép neve melletti hivatkozásra kattintva módosítsa a gép nevét **SRV-01**-re. Az újraindítás után a gép ezen a néven lesz elérhető a hálózatban.

Statikus IP Beállítás

Navigáljon a Vezérlőpult → Hálózati és megosztási központ → Adapterbeállítások módosítása menüpontba. Az Ethernet kártya jobb egérgombbal → Tulajdonságok → Internet Protocol Version 4 (TCP/IPv4) menüben konfigurálja a következő értékeket: IP-cím: **192.168.10.10**, Alhálózati maszk: **255.255.255.0**, Elsődleges DNS: **127.0.0.1**. Fontos, hogy a DNS szerver a saját gépre mutasson, mivel a tartományvezérlő maga is DNS szolgáltatást nyújt.

Fontos megjegyzés: A statikus IP-cím kritikus fontosságú az AD működéséhez. Ha a tartományvezérlő IP-címe változna (DHCP esetén), a kliensek nem tudnák megtalálni a hitelesítési és DNS szolgáltatásokat, ami teljes hálózati leállást okozhat.

2. lépés: AD DS Szerepkör Telepítése

Az Active Directory-tartományszolgáltatások (AD DS) telepítése a Kiszolgálókezelő segítségével történik. Ez a szerepkör tartalmazza az összes szükséges komponenst a tartományvezérlő működéséhez, beleértve az AD adatbázist, DNS szolgáltatást és hitelesítési protokollokat.

1 Kiszolgálókezelő Indítás

Nyissa meg a Server Manager-t, és kattintson a Kezelés (Manage) menüben az **Szerepkörök és szolgáltatások hozzáadása** (Add Roles and Features) lehetőségre

2 Szerepkör Kiválasztás

A varázslóban kattintgassa végig a Tovább gombokat, amíg el nem ér a Kiszolgálói szerepkörökhöz (Server Roles) lépéshez

3 AD DS Jelölés

Keresse meg és jelölje be az **Active Directory-tartományszolgáltatások** (Active Directory Domain Services) szerepkört a listában

4 Függőségek Telepítése

A felugró ablakban kattintson a **Szolgáltatások hozzáadása** (Add Features) gombra a szükséges függőségek automatikus telepítéséhez

5 Telepítés Elindítása

Kattintson a Tovább gombokon át a végleges Telepítés (Install) gombig, majd várja meg a telepítés befejezését

Telepítési Részletek

A telepítés során a rendszer másolja a szükséges bináris fájlokat, regisztrálja a szolgáltatásokat, és konfigurálja az AD DS komponenseit. Ez a folyamat néhány percet vesz igénybe, és nem igényel rendszerújraindítást. A telepítés sikeres befejezése után a Server Managerben megjelenik egy értesítés a következő lépésről.

- Az AD DS szerepkör tartalmazza az Active Directory Domain Services-t
- DNS szolgáltatás telepítése opcionális, de ajánlott
- Remote Server Administration Tools (RSAT) automatikusan települ
- A telepítés nem konfigurál automatikusan tartományt

Gyakori Hibák

Ha a telepítés nem sikerül, ellenőrizze a következőket:

- Elég lemezterület áll rendelkezésre (minimum 10 GB)
- A hálózati kártya engedélyezve van
- Nincs más szerepkör konfliktus
- Felhasználói fiók rendszergazdai jogosultsággal rendelkezik

3. lépés: Tartományvezérlő Promóció

A szerepkör telepítése után a szerver még csak a fájlokat kapta meg - nem "tudja", hogy ő egy tartományvezérlő. A promóció (előléptetés) folyamata konfigurálja az AD-t, létrehozza az erdőt és tartományt, és aktiválja a tartományvezérlő funkciókat.

1

Varázsló Indítás

Kattintson a Server Manager jobb felső sarkában megjelenő sárga felkiáltójel melletti zászlóra, majd válassza az **Kiszolgáló előléptetése tartományvezérlővé** (Promote this server to a domain controller) opciót

2

Üzembe Helyezés

A Telepítési konfiguráció (Deployment Configuration) ablakban válassza az **Új erdő felvétele** (Add a new forest) lehetőséget, mivel ez az első tartományvezérlő a hálózatban

3

Tartománynév

Adja meg a gyökértartomány nevét **pelda.local** formátumban. A .local kiterjesztés belső hálózatokhoz ajánlott, mivel nem létezik nyilvános DNS-ben

4

DSRM Jelszó

Adjon meg egy erős jelszót a Directory Services Restore Mode (DSRM) módban való bejelentkezéshez - például **P@ssword123**. Ez a jelszó kritikus fontosságú a vészhelyzetekhez

5

DNS Beállítások

A DNS-beállítások ablakban ellenőrizze, hogy nincs figyelmeztetés, majd kattintson Tovább. A rendszer automatikusan konfigurálja a DNS-t

6

AD Működési Szint

A Domain and Forest Functional Level (AD működési szint) ablakban hagyja az alapbeállításokat. Windows Server 2016 szintet válassza, ha csak modern klienseket használ

7

Prüfungs Opciók

A Additional Options ablakban adja meg a NetBIOS tartománynév (például PELDA), majd kattintson Tovább

8

Telepítés

Az ellenőrzés után kattintson a **Telepítés** (Install) gombra. A szerver automatikusan újraindul, és a boot után már tartományvezérlőként működik

Promóció Folyamat Részletei

Erdő és Tartomány

Az **Erdő** (Forest) a legmagasabb szintű AD struktúra, amely egy vagy több tartományt tartalmazhat. A **Tartomány** (Domain) egy logikai egység, amely felhasználókat, számítógépeket és más objektumokat tartalmaz. Ebben a gyakorlatban egy egyszerű erdő-tartomány struktúrát hozunk létre.

DSRM Mód

A Directory Services Restore Mode egy biztonsági módozat, amelyet AD visszaállításhoz vagy hibaelhárításhoz használunk. Ez a jelszó különbözik a normál rendszergazdai jelszótól, és csak AD-recovery műveletekhez szükséges.

Fontos: A promóció folyamata nem vonható vissza. Ha hibát követ el, csak a rendszer újratelepítésével javítható. Mindig ellenőrizze a beállításokat a Telepítés gomb megnyomása előtt!

4. lépés: Felhasználók és Szervezeti Egységek Létrehozása

Miután a gép újraindult és tartományvezérlőként működik, jelentkezzen be tartományi rendszergazdaként (például SRV-01\PéldaKft\Administrator). Ekkor megkezdheti a hálózati objektumok létrehozását és szervezését.

Szervezeti Egység (OU)

Az OU egy tároló objektum az AD-ben, amely segít a felhasználók, csoportok és számítógépek logikai szervezésében. Az OU-k lehetővé teszik a Group Policy (csoport házirend) célpontozását és a jogosultság delegálását.

Felhasználói Fiók

Az Active Directory-felhasználók objektumok, amelyek hitelesítési információkat és jogosultságokat tartalmaznak. Minden felhasználó rendelkezik egy egyedi bejelentkezési névvel és jelszóval, amelyet a tartományvezérlő hitelesít.

Attribútumok

A felhasználói fiókokhoz különböző attribútumokat rendelhet, például név, e-mail cím, telefonszám, csoporttagság. Ezek az adatok használhatók csoport házirendek feltételekhez és kereséshez.

OU és Felhasználó Létrehozása

ADUC Eszköz Megnyitás

Server Manager → Eszközök (Tools) → **Active Directory-felhasználók és -számítógépek** (Active Directory Users and Computers) menüpont kiválasztása

Új OU Létrehozás

Kattintson jobb egérgombbal a **pelda.local** tartománynév-re a bal oldali fastruktúrában, majd válassza az Új (New) → Szervezeti egység (Organizational Unit) menüpontot

OU Név Megadása

A Name mezőbe írja be az **Igazgatosag** nevet, majd kattintson OK gombra. Az új OU megjelenik a tartomány struktúrájában

Felhasználó Létrehozása az Igazgatóság OU-ban

1. Kattintson jobb egérgombbal az **Igazgatosag** mappára
2. Válassza az Új (New) → Felhasználó (User) lehetőséget
3. A varázslóban adja meg a Vezetéknév: **Kovács**
4. Utónév: **János** mezők kitöltése
5. Bejelentkezési név: **kovacs.janos** formátumban
6. Kattintson Tovább gombra

1. Adjon meg egy erős jelszót: **Kezdo1234**
2. Tegye ki a pipát a "Felhasználónak meg kell változtatnia a jelszót a következő bejelentkezéskor" opció mellől
3. Ez megkönnyíti a tesztelést, de éles környezetben NE tegye
4. Kattintson Tovább, majd Befejezés gombra
5. A felhasználó megjelenik az Igazgatosag OU-ban

A felhasználó létrehozása után további attribútumokat is konfigurálhat, például e-mail címet, telefonszámot, csoporttagságot vagy szervezeti információkat. Ezek az adatok később hasznosak lehetnek csoport házirendek feltételes alkalmazásához vagy keresési szűrőkhöz.

5. lépés: Ellenőrzés és Tesztelés

Az AD telepítés sikeres befejezését több módon is ellenőrizhetjük. A következő tesztek megerősítik, hogy a DNS, AD és hitelesítési szolgáltatások működnek.

1

nslookup Teszt

Indítsa el a parancssort (cmd.exe) rendszergazdaként, majd írja be a **nslookup pelda.local** parancsot. Ha a válasz tartalmazza az 192.168.10.10 IP-címet, a DNS működik

2

ADUC Ellenőrzés

Nyissa meg az Active Directory-felhasználók és -számítógépek eszközt, és keresse meg a létrehozott **kovacs.janos** felhasználót az Igazgatosag OU-ban

3

DNS Console

Server Manager → Eszközök → DNS menüpont kiválasztása. Ellenőrizze, hogy a pelda.local zóna létezik és tartalmaz rekordokat

4

DCPROMO Ellenőrzés

Parancssorból futtassa a **dcdiag /v** parancsot a tartományvezérlő diagnosztikájához. Ez részletes információt ad a működésről

nslookup Parancs Részletes Tesztelése

Parancs Futatása

Nyissa meg a parancssort a Start menüben vagy a Win+R paranccsal. Írja be a következő parancsot és nyomja meg az Enter-t:

```
nslookup pelda.local
```

A rendszernek a következőhöz hasonló választ kell adnia:

```
Server:  UnKnown
Address:  127.0.0.1

Name:    pelda.local
Address:  192.168.10.10
```

Válasz Értelmezése

A **Server: 127.0.0.1** azt jelzi, hogy a DNS lekérdezést a helyi gép kezeli. A **Name: pelda.local** és **Address: 192.168.10.10** sorok megerősítik, hogy a tartománynév megfelelően feloldódik a statikus IP-címre.

Ha hibaüzenetet kap (például "DNS request timed out"), ellenőrizze a DNS beállításokat és az IP-konfigurációt.

További Ellenőrzési Lépések

Event Viewer

Navigáljon a Server Manager → Eszközök → Event Viewer (Eseménynapló) menüpontba, és ellenőrizze a System és Directory Service naplókat hibák után

Services

Services.msc-ben győződjön meg róla, hogy az "Active Directory Domain Services", "DNS Server" és "Netlogon" szolgáltatások futnak

Ping Teszt

Parancssorból pingelje meg a tartomány nevét: **ping pelda.local**. Sikeres ping esetén a rendszer az 192.168.10.10 címet fogja használni

Tanári Tippek a Hibaelhárításhoz

A gyakorlatvezetés során előfordulhatnak tipikus problémák, amelyek gyors azonosítást és megoldást igényelnek. Az alábbiakban összegyűjtöttük a leggyakoribb hibákat és azok megoldásait.

❌ DNS Hiba: Promóció Nem Indul

Probléma: A tartományvezérlő promóciós varázsló nem indul el, vagy hibát jelez a DNS beállításokkal kapcsolatban.

Ok: A DNS szerver beállítása nem megfelelő - lehet, hogy a gép DHCP-t használ, vagy a DNS szerver nem a saját IP-címére mutat.

Megoldás: Ellenőrizze a hálózati adapter IPv4 beállításait. A DNS szervernek vagy a saját IP-címre (192.168.10.10) vagy a loopback címre (127.0.0.1) kell mutatnia. Ha DHCP van beállítva, változtassa statikusra.

⚠️ VirtualBox RAM: Lassú Teljesítmény

Probléma: A Windows Server 2016 rendkívül lassan működik, vagy bizonyos műveletek időtúllépést kapnak.

Ok: A virtuális géphez nem rendeltünk elegendő memóriát. A Server 2016 GUI módhoz legalább 2 GB RAM szükséges, de ajánlott 4 GB vagy több.

Megoldás: Állítsa le a virtuális gépet, majd a VirtualBox beállítások → Rendszer → Alap menüpontban növelje a RAM mennyiségét 4096 MB-ra. Indítsa újra a gépet.

🔐 Jelszó Komplexitás: Telepítési Hiba

Probléma: A promóció során hibaüzenet jelenik meg, hogy a jelszó nem elég erős vagy nem felel meg a komplexitási követelményeknek.

Ok: A Windows Server alapértelmezésben megköveteli, hogy a jelszavak tartalmazzanak kisbetűt, nagybetűt, számot és speciális karaktert is.

Megoldás: Használjon komplex jelszót, például **P@ssword123** vagy **Kezdo1234!**. Győződjön meg róla, hogy legalább 8 karakter hosszú, és tartalmaz mindegyik karaktertípust. Ne használjon egyszerű jelszavakat, mint "password" vagy "12345678".

Egyéb Gyakori Problémák és Megoldások

Hálózati Kapcsolat

Ha a virtuális gép nem tud kapcsolódni a hálózathoz, ellenőrizze a VirtualBox hálózati beállításait. Belső hálózat helyett próbálkozzon NAT móddal, vagy ellenőrizze, hogy a VirtualBox Host-only Adapter telepítve van-e.

Tűzfal Blokkolás

A Windows Firewall blokkolhatja az AD szolgáltatásokat. A tesztelés idejére ideiglenesen tiltsa le a tűzfalat, vagy hozzon létre kivételeket az AD portokhoz (TCP 389, 53, 88, 135, 445).

Idő Szinkronizáció

Az AD érzékeny az időeltolódásra - maximum 5 perc eltérés engedélyezett. Ellenőrizze, hogy a virtuális gép dátuma és ideje pontos-e, különösen ha snapshot-ot használ.

NetBIOS Engedélyezés

Egyes régi alkalmazások NetBIOS-t igényelnek. Ha problémák lépnek fel, ellenőrizze, hogy a hálózati adapter TCP/IP beállításaiban engedélyezve van-e a NetBIOS.

Tip: A gyakorlat során készítsen snapshot-ot a VirtualBox-ban minden fontos lépés után. Így ha hibát követ el, gyorsan vissza tud térni egy működő állapothoz, anélkül, hogy újra kellene telepíteni a rendszert.

Dokumentáció és Források

A további tanuláshoz javasoljuk a következő erőforrásokat:

- Microsoft Active Directory dokumentáció (docs.microsoft.com)
- Windows Server 2016 adminisztrációs útmutatók
- VirtualBox felhasználói kézikönyv a virtuális gép konfigurációjához
- Online kurzusok és oktató videók az AD alapjairól