Hálózati Infrastruktúra Tervezése és Kivitelezése

***2.csoport***

**Készítették:**

Berki Dorina

Csépányi Bárdos Letícia

Budai József

# Bevezető

**Projektleírás:**

Egy közepes méretű vállalat három telephelyének hálózati infrastruktúráját kell megtervezni, megvalósítani és tesztelni.

A három telephelyes vállalat hálózati infrastruktúrájának tervezése, megvalósítása és tesztelése során számos fontos szempontot kell figyelembe venni annak érdekében, hogy a rendszer támogassa a vállalat összes üzleti és technikai igényét. A cél egy stabil, biztonságos és skálázható hálózat kiépítése, amely képes biztosítani az üzleti műveletek zavartalan működését és az alkalmazottak hatékony munkavégzését, akár a telephelyeken, akár távoli elérés során.

**Hálózati tervezés**

A hálózati infrastruktúra tervezésekor az első lépés az egyes telephelyek igényeinek felmérése. Minden telephelyen szükséges biztosítani a megfelelő belső hálózati kapcsolatot (LAN), amely gyors és megbízható adatátvitelt tesz lehetővé. Az eszközök, mint a munkaállomások, nyomtatók és szerverek egyaránt csatlakoznak az adott telephelyen kialakított helyi hálózathoz, amit célszerű vezetékes és vezeték nélküli (Wi-Fi) kapcsolatokat kombinálni. A hálózati topológia tervezésekor az optimális eszközök, például réteges switch-ek és routerek használata javasolt, amelyek biztosítják az adatforgalom szétosztását és a kapcsolatok hatékony menedzselését.

A telephelyek közötti kapcsolatot a vállalat igényeinek megfelelően VPN-en keresztül célszerű megoldani. A VPN (Virtual Private Network) lehetővé teszi, hogy az adatok titkosítva, biztonságos módon közlekedjenek a távoli telephelyek között, miközben minimalizálja a kockázatot, amelyet a nyilvános internet jelenthet.

**Internetkapcsolat**

A vállalat számára stabil és gyors internetkapcsolatra van szükség minden telephelyen. Az internetkapcsolatnak biztosítania kell a külső kommunikációs csatornák, például e-mail és webes alkalmazások zökkenőmentes használatát, valamint lehetőséget kell biztosítania a felhő alapú szolgáltatások elérésére. A kapcsolat redundanciájának biztosítása érdekében érdemes több szolgáltatót bevonni, hogy a lehetséges hálózati hibák esetén is folyamatos legyen az internet-hozzáférés.

**VPN és távoli hozzáférés**

A távoli munkavégzés támogatása érdekében az alkalmazottak számára VPN hozzáférést kell biztosítani. A VPN-en keresztüli elérés lehetővé teszi a dolgozók számára, hogy bárhonnan biztonságosan csatlakozhassanak a vállalat hálózatához. Ennek megvalósításához szükséges egy központi VPN szerver telepítése, amely minden telephelyről elérhető, és képes kezelni a bejövő VPN kapcsolatokat. A titkosítás, hitelesítés és jogosultságkezelés kulcsfontosságú, hogy megakadályozzuk a nem kívánt hozzáféréseket és biztosítsuk az adatok védelmét.

**Biztonsági intézkedések**

A biztonság kiemelt szempont a tervezés során. Minden telephelyen tűzfalak alkalmazásával kell védeni a belső hálózatot a külső fenyegetésekkel szemben. A tűzfalak szűrik az adatforgalmat és blokkolják a gyanús vagy nem kívánt kapcsolatokat. Ezen kívül behatolás érzékelő rendszereket (IDS) és behatolás megelőző rendszereket (IPS) is implementálhatunk a hálózat védelme érdekében. A rendszeres frissítések, a jelszókezelési szabályok betartása és a többfaktoros hitelesítés szintén alapvető biztonsági intézkedések.

**Tesztelés és optimalizálás**

A hálózat kiépítése után fontos lépés a rendszer tesztelése. Ennek során ellenőrizni kell a hálózati eszközök működését, a VPN kapcsolatok biztonságát és stabilitását, valamint a rendszer válaszidejét és terhelhetőségét. A tesztelés során a különböző használati forgatókönyveket, például távoli hozzáférést, adatcserét és hibák kezelését kell figyelembe venni. Az optimalizálás érdekében folyamatosan figyelemmel kell kísérni a hálózati forgalmat, és szükség szerint finomhangolni a beállításokat a teljesítményt.

**Tartalomjegyzék**

[Bevezető 2](#_Toc194312086)

[Eszközök 6](#_Toc194312087)

[**1841 Router** 6](#_Toc194312088)

[**ASA** 7](#_Toc194312089)

[**2960-24TT Switch** 8](#_Toc194312090)

[Fizikai topológia 9](#_Toc194312091)

[Logikai topológia 11](#_Toc194312092)

[Eszközök konfigurálása 16](#_Toc194312093)

[Szerverek konfigurálása 17](#_Toc194312094)

[Active Directory szolgáltatások Cisco szerveren 19](#_Toc194312095)

[Csoportmunka felosztás 20](#_Toc194312096)

## Eszközök

## **1841 Router**

**Jellemzői:**

* **Processzor**: 266 MHz-es vagy gyorsabb RISC processzor ,
* **RAM**: 32 MB-tól 128 MB-ig bővíthető ,
* **Flash memória**: 32 MB vagy nagyobb ,
* **WAN interfészek**: Támogatja a moduláris WAN-csatlakozásokat, például T1/E1, xDSL és más kapcsolódási lehetőségeket ,
* **LAN interfészek**: 2 db 10/100 Mbps Ethernet port ,
* **Bővítési lehetőségek**: Támogatja a Cisco HWIC (High-Speed WAN Interface Card) modulokat ,
* **Biztonság**: Beépített VPN-támogatás, tűzfal és titkosítási képességek ,
* **Operációs rendszer**: Cisco IOS.

## **ASA**

A **Cisco ASA 5505** adaptív biztonsági készülék a kisvállalatok, fiókirodák és a nagyvállalati távmunkakörnyezetek számára modulárisan bővíthető, „plug-and-play” berendezés formájában kínál új generációs, teljes körű biztonsági szolgáltatásokat, így fokozott biztonságú tűzfalat, SSL és IPsec VPN-t, valamint médiatartalomban gazdag hálózati szolgáltatásokat.

A Cisco Adaptive Security DeviceManager nevű integrált webes felügyeleti eszközzel a Cisco ASA 5505 gyorsan telepíthető és könynyen felügyelhető. A készülékben nyolcportos 10/100 Fast Ethernet kapcsoló található, melynek portjai dinamikusan csoportosíthatók, így akár három különálló VLAN-hálózat is létrehozható, ami jobban elkülöníthetővé és biztonságosabbá teszi az otthoni, vállalati és internetes adatforgalmat.

Cisco ASA 5505 két porton Ethernet-kábeles tápellátással rendelkezik, ezzel lehetővé téve külön konfigurálást nem igénylő, biztonságos VoIP-protokollt használó Cisco IP-telefonok egyszerű csatlakoztatását, sőt a nagyobb hálózati mobilitás érdekében külső, vezeték nélküli hozzáférési pontok is kialakíthatók. A berendezés az ASA 5500 sorozat többi tagjához hasonlóan moduláris felépítésű, ami kiváló bővíthetőséget és értékállóságot biztosít. Ehhez a külső bővítőhely mellett több USB-port is rendelkezésre áll, amely további jövőbeni szolgáltatásbővítést tesz lehetővé.

A felhasználók számának növekedése esetén a Security Plus licenszbővítéssel a Cisco ASA 5505 nagyobb számú IPsec VPN felhasználót kiszolgálni képes megemelt kapacitás mellett. Ezt jól kiegészíti a teljes körű DMZ-támogatás, illetve a VLAN-trönkölés, amely a megoldást a kapcsolt hálózati környezetbe illeszti. Emellett a licenszbővítéssel az üzletmenet folytonossága is maximálisan biztosítható, mivel lehetővé válik a tartalék kapcsolat egy másik internetszolgáltatóval, állapotmentes aktív, illetve készenléti magas rendelkezésre állási szolgáltatásokkal együtt. A Cisco ASA 5505 fő előnye a piacvezető színvonalú biztonság és VPN-szolgáltatások mellett a hálózati funkciók gazdag választéka, a rugalmas távfelügyeleti lehetőségek, illetve a további bővíthetőség. Ezért ideális választásnak bizonyul az olyan cégek esetében, amelyek számára kulcsfontosságú a lehető legmagasabb biztonsági szintű kisvállalati, fiókirodai vagy távmunkamegoldás.

## **2960-24TT Switch**

A **2960-24TT Switch** egy Cisco által gyártott régebbi, de megbízható és jól ismert switch típus, amelyet elsősorban kisebb és közepes vállalkozások számára terveztek. A készülék 24 Ethernet porttal rendelkezik, amelyek 10/100/1000 Mbps sebességűek, és támogatja az Ethernet frame-ek gyors átvitelét. A "TT" jelölés arra utal, hogy a modell "Stackable" funkcióval rendelkezik, azaz több switch is összekapcsolható, így könnyedén bővíthető a hálózat a növekvő igényekhez.

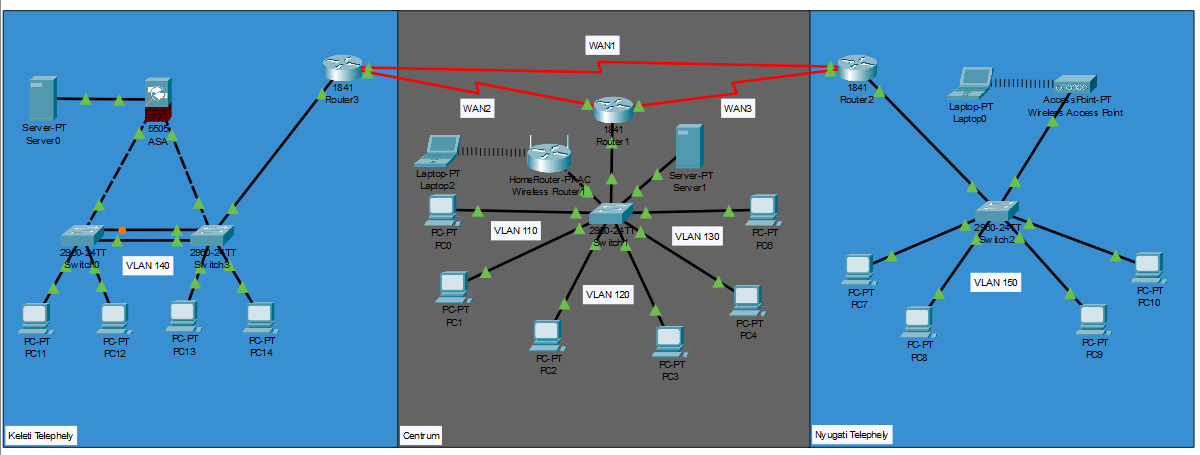
A Cisco 2960 sorozatú switch-ek az alapvető Layer 2 hálózati funkciókat biztosítják, mint például a VLAN-ok kezelése, port biztonság, valamint QoS (Quality of Service) szabályozás. Ezáltal képesek biztosítani a hálózaton belüli eszközök közötti stabil és gyors adatforgalmat. A készülék ideális megoldás azokon a helyeken, ahol alapvető hálózati szolgáltatásokra van szükség, de nem szükségesek a bonyolultabb Layer 3 routing funkciók.

A 2960-24TT Switch olyan funkciókat kínál, mint a port biztonság, a hálózati szegmentálás VLAN-okkal, és az IPv6 támogatás. A Cisco által használt Cisco IOS operációs rendszer biztosítja a könnyű kezelhetőséget és a hálózati forgalom hatékony irányítását. A switch többféle tápellátási lehetőséggel rendelkezik, beleértve a PoE (Power over Ethernet) lehetőséget is, amely lehetővé teszi az eszközök táplálását a hálózaton keresztül, így csökkentve a szükséges kábelezést.

Ez a modell robusztus és megbízható teljesítményt biztosít, amely ideális a kisebb irodákban vagy a nem kritikus üzleti környezetekben, ahol a költséghatékonyság és a könnyű skálázhatóság kulcsfontosságú tényezők. Az eszköz az egyszerű telepítés és karbantartás érdekében könnyen konfigurálható és kezelhető, még a kevésbé tapasztalt felhasználók számára is.

# 

# Fizikai topológia



Ez a hálózati diagram egy összetett számítógépes hálózatot ábrázol, három különböző helyszínt (telephelyet) kapcsol össze egy széles körű WAN hálózaton keresztül. A három helyszín a Keleti Telephely, a Centrum, és a Nyugati Telephely , amelyeket routerek kötnek össze.

**Keleti Telephely**

A bal oldali szegmens a Keleti Telephelyet ábrázolja. Itt található egy ASA tűzfal (jelölve 5505 típusként), amely védelmet nyújt a belső hálózat számára. A tűzfal mögött egy VLAN 140 hálózat van kialakítva, amelyhez két switch (2950-24TT modell) kapcsolódik. Ezek a switchek több PC állomást szolgálnak ki. Ezen kívül egy szerver (Server0) is jelen van, amely jelenlegi hálózati szolgáltatásokat nyújt a telephely számára. A telephely egy Router3 (1841 modell) köti össze a WAN hálózattal.

**Centrum**

A központi rész (Centrum) a teljes hálózat szíve, ahol egy Router1 (1841 modell) készült a különböző WAN kapcsolatok kezelését. Itt található egy fő switch , amelyhez több PC csatlakozik. Egy szerver (Server1) is jelen van, amely központi szolgáltatásokat nyújthat. Ezen kívül egy Wi-Fi router (HomeRouter-PTAC) működik , amely vezeték nélküli kapcsolatot biztosít az eszközök számára.

**Nyugati Telephely**

A jobb oldali szegmens a Nyugati Telephelyet mutatja, egy 1841 típusú router csatlakozik a WAN hálózathoz. Itt egy VLAN 150 van kialakítva egy switch (2960-24TT modell) segítségével .Több PC kapcsolódik a switch-hez, valamint egy vezeték nélküli hozzáférési pont (Access Point-PT) is elérhető, amelyhez laptopok csatlakoznak.

**WAN Hálózat**

A három telephelyet egy WAN hálózat köti össze, amely három különböző kapcsolaton keresztül (WAN1, WAN2, WAN3) biztosítja a kommunikációt . Ez lehet egy redundáns kapcsolat, amely biztosítja a folyamatos működést hálózati hiba esetén is.

# Logikai topológia

Az első ábra egy hálózati címzési terv. A vállalati hálózati struktúra szegmentálása fontos lépés a biztonságos és hatékony működés biztosításához. Az alábbiakban bemutatott VLAN (Virtual Local Area Network) és IP alhálózati beosztás segít a különböző részlegek és funkciók elkülönítésében, valamint a hálózati erőforrások jobb kihasználásában és védelmében.

**Centrum**

1. **Adminisztrációs VLAN (110)**

Az Adminisztrációs VLAN, melynek IP tartománya **192.168.110.0/24** és IPv6 címzése **fd00:110::/64**, a vállalat adminisztratív feladataihoz kapcsolódó eszközöket és hálózati erőforrásokat biztosít. Ezen a szegmensen találhatóak a fontos üzleti és pénzügyi adatok, ezért kiemelt figyelmet igényel a biztonsági intézkedések alkalmazása.

1. **IT VLAN (120)**

Az IT VLAN, **192.168.120.0/24** IP tartománnyal és **fd00:120::/64** IPv6 címzéssel, az informatikai rendszerek működtetéséhez szükséges eszközöket és szervereket tartalmazza. Az IT csapat ezen a VLAN-on kezeli a hálózati eszközöket, rendszereket és az informatikai infrastruktúrát, amelyek az egész vállalat számára kritikusak.

1. **Vendéghálózat (130)**

A Vendéghálózat, amely a **192.168.130.0/24** és **fd00:130::/64** IP tartományokat használja, a látogatók és vendégek számára biztosít internetkapcsolatot anélkül, hogy hozzáférnének a vállalati belső hálózathoz. Ez a szegmens biztosítja a vendégek számára a szükséges hálózati elérést, miközben védi a vállalat érzékeny adatokat.

**Telephelyek**

1. **Keleti telephely (140)**

A Keleti telephelyen található **192.168.140.0/24** IP tartomány és **fd00:140::/64** IPv6 címkészlet a Gyártási VLAN számára van fenntartva. Ezen a szegmensen a gyártási folyamatokhoz szükséges gépek és rendszerek működnek. A gyártás során keletkező adatokat elkülönítik a vállalat többi szegmenseitől, biztosítva a hatékony adatkezelést és a termelési folyamatok zavartalan működését.

1. **Nyugati telephely (150)**

A Nyugati telephelyen található **192.168.150.0/24** IP tartomány és **fd00:150::/64** IPv6 címek, amelyek az értékesítési VLAN-hoz tartoznak. Itt az értékesítési csapat számára biztosítanak különálló hálózati hozzáférést, amely lehetővé teszi számukra az ügyfelekkel való kapcsolattartást, a termékek és szolgáltatások értékesítését, miközben megvédik a vállalat egyéb, érzékeny területeit.

**VPN Hálózat**

1. **VPN hálózat (10.0.0.0/24)**

A **10.0.0.0/24** IP cím tartomány és **fd00:100::/64** IPv6 címkészlet a vállalat távoli dolgozóinak és partnereinek biztosít VPN hozzáférést. A VPN hálózaton keresztül a felhasználók biztonságosan csatlakozhatnak a vállalati rendszerhez, mintha a helyi hálózaton dolgoznának, miközben a távoli kapcsolatok védelme is biztosított.

**Összegzés**

A fent bemutatott VLAN és IP alhálózati struktúra biztosítja, hogy minden telephely és üzleti terület elkülönített, védett hálózati szegmensként működjön. Az egyes szegmensek szigorú elválasztása lehetővé teszi a hatékony erőforrás-kezelést, a biztonság növelését, és biztosítja, hogy a különböző munkafolyamatok ne befolyásolják egymást. A VPN hálózat pedig lehetővé teszi, hogy a távoli dolgozók biztonságosan csatlakozhassanak a vállalat hálózatához.

Az második ábra egy hálózati konfigurációs táblázat, amely a különböző routerek kapcsolódási pontjait és paramétereit tartalmazza. A táblázat öt oszlopot foglal magában: Router, Hálózat, Port, DCE/DTR és IP-Cím.

Az első oszlop, a "Router", a routerek nevét tartalmazza, például Router1, Router2 és Router3. Ez azt mutatja, hogy melyik router melyik hálózathoz csatlakozik.

A második oszlop, a "Hálózat", az adott router által használt WAN kapcsolatot mutatja. A hálózati kapcsolatok között szerepel a Wan1, Wan2 és Wan3, ami arra utal, hogy ezek különböző alhálózatokat vagy kapcsolatokat képviselnek.

A "Port" oszlop a használt interfészeket tünteti fel, például "S0/0/0" és "S0/0/1". Ezek a soros interfészek, amelyeket a routerek közötti kommunikációhoz használnak. Az ilyen típusú interfészek segítségével a routerek különböző hálózatokhoz kapcsolódnak és adatokat továbbítanak.

A "DCE/DTR" oszlop a kapcsolat típusát határozza meg, ahol a DCE (Data Circuit-Terminating Equipment) és a DTE (Data Terminal Equipment) szerepel. A DCE az adatátviteli vonal vezérléséért felelős eszközt jelenti, míg a DTE az adatküldő eszközt képviseli. A táblázat alapján például a Router1 DCE-ként van megadva a Wan2 és Wan3 kapcsolatoknál, míg a Router2 és Router3 különböző helyzetekben DTE vagy DCE szerepet töltenek be.

Az utolsó oszlop a "Cím", amely az adott interfész IP-címét tartalmazza.

Összegzésképpen a táblázat a routerek közötti kapcsolatokat és azok konfigurációs beállításait tartalmazza. Ez az információ különösen hasznos lehet hálózati adminisztrátorok számára, mivel segít a hálózat tervezésében, hibakeresésben és karbantartásban. A megfelelő interfészek és IP-címek hozzárendelése elengedhetetlen a stabil és hatékony hálózati kommunikáció érdekében.



**1. Hálózati Címzési Terv**



**2. Wan Címzési Táblázat**

# Eszközök konfigurálása

A hálózati eszközök konfigurálásakor fontos a megfelelő kapcsolat és biztonság biztosítása. Ezt különböző lépésekben érhetjük el:

1. **Router beállítások**:

* IP címek kiosztása (statikus vagy dinamikus).
* Portforwarding, tűzfal és NAT beállítások.
* Wi-Fi jelszó, SSID és titkosítási protokollok (WPA2, WPA3).

1. **Switch és access point konfigurálása**:

* VLAN beállítások, QoS (Quality of Service) beállítások.
* Kábelezési és hálózati sebesség optimalizálása.

1. **VPN beállítások**:

* VPN szerverek és ügyfelek konfigurálása.
* Telephelyek közötti biztonságos kommunikáció.

# Szerverek konfigurálása

A szerver konfigurációja a rendszer teljesítményének, biztonságának és megbízhatóságának biztosítása érdekében elengedhetetlen. A konfiguráció során számos tényezőt kell figyelembe venni, például a hardvert, a szoftvert és a hálózati beállításokat. Íme néhány fontos szempont a szerver konfigurálásához:

**Hardveres Konfiguráció**

A szerver hardveres konfigurálása határozza meg a rendszer teljesítményét. A legfontosabb tényezők:

* **Processzor (CPU):** A szerver teljesítménye nagyban függ a processzor teljesítményétől. Többmagos, nagy sebességű processzorok szükségesek a nagy terheléshez.
* **RAM:** Minél több memória áll rendelkezésre, annál gyorsabban végezhet el a szerver nagy mennyiségű adatfeldolgozást. Az ajánlott memória mennyiség a szerver céljától függ (pl. web, adatbázis, fájlszerver).
* **Tárhely:** A gyors SSD-k a rendszer sebességét növelhetik, míg a hagyományos HDD-k nagyobb kapacitást biztosítanak olcsóbban.
* **Hálózati kártyák:** Az adatátviteli sebesség kritikus lehet, így gyors, megbízható hálózati kártyák szükségesek.
* **Hálózati kártyák:** Az adatátviteli sebesség kritikus lehet, így gyors, megbízható hálózati kártyák szükségesek.

**Operációs Rendszer és Szoftverek**

A szerver operációs rendszere és a rajta futó szoftverek kiválasztása alapvetően meghatározza a szerver működését.

* **Linux vagy Windows Server:** Linux alapú rendszerek (pl. Ubuntu, CentOS, Debian) gyakran előnyben részesítettek szerver környezetekben, mivel stabilitást és biztonságot kínálnak. Windows Server rendszerekre van szükség, ha Microsoft-alapú alkalmazásokat futtatunk.
* **Webszerverek (pl. Apache, Nginx):** A webszerverek felelősek a weboldalak kiszolgálásáért. Az Nginx gyakran gyorsabb és erőforrás-kímélőbb, míg az Apache rugalmasabb és bővíthetőbb.
* **Adatbázisok (pl. MySQL, PostgreSQL):** A relációs adatbázisok alapvetően tárolják az alkalmazások adatokat. Az adatbázis választása a tárolt adatok típusától függ.
* **Virtuális gépek (VM) vagy konténerek (Docker):** Ha több alkalmazást kell futtatni egy gépen, virtualizációra vagy konténerekre lehet szükség a hatékony erőforrás-kezeléshez.

# Active Directory szolgáltatások Cisco szerveren

**Lépések az Active Directory telepítéséhez Cisco szerveren:**

1. **Hardver és szoftver előkészítése**
   1. Győződj meg róla, hogy a Cisco UCS vagy más Cisco szerver támogatja a Windows Server megfelelő verzióját.
   2. Telepíts Windows Server 2019/2022 operációs rendszert a szerverre.
   3. Állítsd be az IP-címet és a hálózati kapcsolatokat.
2. **Active Directory telepítése**
   1. Nyisd meg a Server Manager-t, és válaszd ki az "Add roles and features" (Szerepkörök és szolgáltatások hozzáadása) opciót.
   2. Válaszd ki az Active Directory Domain Services (AD DS) szerepkört, majd telepítsd.
   3. A telepítés után futtasd az AD DS konfigurációs varázslót a tartományvezérlő beállításához.
   4. Állíts be egy új erdőt (pl. brody.local) és hozz létre egy új tartományt.
3. **DNS és DHCP konfigurálása**
   1. Az AD-hoz szükséges egy DNS-szerver, amelyet a varázsló automatikusan telepít.
   2. Ha a szerver DHCP-t is kezel, konfiguráld a DHCP szerepkört, hogy az ügyfélgépek megfelelő IP-címet és DNS-beállításokat kapjanak.
4. **Felhasználók és csoportok létrehozása**
   1. Nyisd meg az Active Directory Users and Computers (ADUC) konzolt.
   2. Hozz létre új felhasználókat, csoportokat, biztonsági beállításokat.

# Csoportmunka felosztás