 **Budapesti Műszaki SZC Bláthy  
Ottó Titusz Informatikai Technikum**

Hálózattervezési és kivitelezési vizsgaremek

(Szálkapari Zrt.)

Kis Tibor

Lócska Gergő István

Szamosi Krisztián Benjamin

2/14E – IT | 2024.

Tartalom

[1. Bevezetés 4](#_Toc166531863)

[2. Költségvetés 5](#_Toc166531864)

[3. Hálózati fizikai struktúrája 6](#_Toc166531865)

[4. Hálózati logikai struktúrája 7](#_Toc166531866)

[5. Alkalmazott hálózati konfigurációk 8](#_Toc166531867)

[5.1 Forgalomirányítás 8](#_Toc166531868)

[5.2 IP címek kiosztása 8](#_Toc166531869)

[6. Etherchannel 9](#_Toc166531870)

[7. VPN 10](#_Toc166531871)

[8. ASA 11](#_Toc166531872)

[9. Szabályok 12](#_Toc166531873)

[10. Vezeték nélküli hálózat 13](#_Toc166531874)

[11. Windows szerver konfigurálása 14](#_Toc166531875)

[11.1 DHCP 14](#_Toc166531876)

[11.2 Active Directory beállítása 14](#_Toc166531877)

[11.3 Biztonsági mentés 16](#_Toc166531878)

[12. Linux szerver konfigurálása 18](#_Toc166531879)

[12.1 Telepítés 18](#_Toc166531880)

[12.2 DNS 18](#_Toc166531881)

[12.3 SSH 18](#_Toc166531882)

[12.4 Samba 19](#_Toc166531883)

[12.5 Apache 19](#_Toc166531884)

[13. Jövőbeni fejlesztések 21](#_Toc166531885)

[14. Csapatmunka 22](#_Toc166531886)

[15. Melléklet 23](#_Toc166531887)

# Bevezetés

Cégünk a Szálkapari Zrt. amely bútorok tervezésével, raktározásával, értékesítésével foglalkozik. Cégünk három telephellyel rendelkezik Magyarország és Szlovákia területein. Pozsony városában helyezkedik el az áruház, a raktár Sopronban, végül, de nem utolsó sorban a központi iroda pedig Győrben erősíti a céget. A jelenlegi cégfelépítés, területi elhelyezkedés adóoptimalizálás miatt vált szükségessé.

# Költségvetés

A cég hálózata a következő eszközöket igényli:

|  |  |  |
| --- | --- | --- |
| **Eszköz** | **Mennyiség (darab)** | **Összeg USD** |
| PC (személyi számítógép) | 20 db | 27 855 $ |
| Laptop | 5 db | 6963 $ |
| Switch 2960 | 7 db | 8715 $ |
| Router 2911 | 8 db | 37 800 $ |
| Linksys WRT300N | 3db | 120 $ |
| Multilayer switch 3650 | 2 db | 18 572 $ |
| Server | 3 db | 15 833 $ |
| Access Point | 1 db | 130 $ |
| Nyomtató | 4 db | 1522 $ |
| ASA 5506 (tűzfal) | 1 db | 1261 $ |

**Összköltség az eszközökre: 118771 $ - 42 757 560 HUF**Továbbá felmerülő költségek:  
- Eszközök telephelyekre történő szállítása: Maximum keret 500.000 HUF   
- Eszközök beszerelése, konfigurálás, munkadíj: Maximum keret: 7.196.400 HUF  
  
**A teljes hálózat kialakításának bekerülési értéke: 50 453 960 HUF**

# Hálózati fizikai struktúrája

A vállalati hálózatban a kommunikáció létrejöttéhez a forrás és cél állomás összeköttetéséhez meg kell teremtenünk a csatornát, azt az átviteli közeget, amelyen keresztül az információ biztonságosan továbbítva lesz. Megvalósításunkban kétféle típust alkalmaztunk, a fizikai, vagy vezetékes, illetve a vezeték nélküli technológiát.

Telephelyeinken az adott létesítés idején legyakrabban alkalmazott technika lelhető fel. Mind csavart érpáras, de régebbi telephelyeken CAT5e az újabbakon már CAT6 típusúakat, változatos gyártóktól.

Távközlési szolgáltatónk jóvoltából a telephelyeinket nagysebességű béreltvonali összeköttetést tudunk használni.

Mobil eszközök számára az egyes helyszíneken a felhasználók számára hozzáférési pontokat (Access Point, AP) alakítottunk ki.

# Hálózati logikai struktúrája

Az elosztási réteg minden telephelyen több, logikailag különálló részre osztott. Alhálózatokat, VLAN-okat hoztunk létre szegmentált IP címzés alkalmazásával. Ennek több ismert oka van.

* Fizikai elhelyezkedés
* Logikai csoportosítás
* Terhelés csökkentése
* Biztonság
* Szórások hatókörének korlátozása

# Alkalmazott hálózati konfigurációk

## Forgalomirányítás

A telephelyeken illetve azok között a dinamikus forgalomirányítást OSPF területek kialakításával oldottuk meg. Két területet hoztunk létre. Egy Area 0-t a gerinchálózatnak és egy Area 1-et a telephely belső hálózatára. Egy jellemző kódsor a két routerre:

*Gyor\_R0*

router ospf 1

network 130.10.10.0 0.0.0.3 area 0

network 130.10.10.8 0.0.0.3 area 0

network 10.10.10.0 0.0.0.3 area 1

network 10.10.20.0 0.0.0.3 area 1

*Gyor\_R1*

router ospf 1

network 192.168.1.0 0.0.0.31 area 1

network 192.168.1.32 0.0.0.31 area 1

network 192.168.1.64 0.0.0.7 area 1

network 192.168.1.72 0.0.0.7 area 1

network 192.168.1.80 0.0.0.7 area 1

network 10.10.10.0 0.0.0.3 area 1

## IP címek kiosztása

A teljes hálózaton alkalmaztunk Szerver PC általi, forgalomirányító általi és statikusan beállított IP cím kiosztást. Így történt mind az IPv4 mind az IPv6 címekre. Egy jellemző routeren kiadott parancssorozat az IPv4 címkiosztásra:

*Gyor\_R1*

ip dhcp pool poolvlan10

network 192.168.1.0 255.255.255.224

default-router 192.168.1.1

dns-server 192.168.1.75

domain-name butor.loc

exit

ip dhcp excluded-address 192.168.1.1 192.168.1.3

Ugyanezen az eszközön az IPv6 címek terjesztésének bekapcsolása:

ipv6 unicast-routing

ipv6 dhcp pool GYOR\_A\_v6

address prefix 2001:DB8:CAFE:10::/64

dns-server 2001:DB8:CAFE:40::B

domain-name butor.loc

exit

intetface g0/1.10

ipv6 address 2001:DB8:CAFE:10::1/64

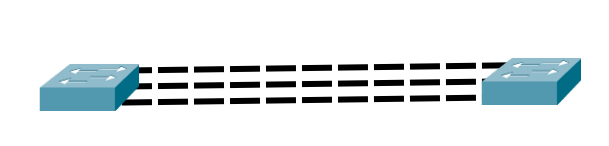
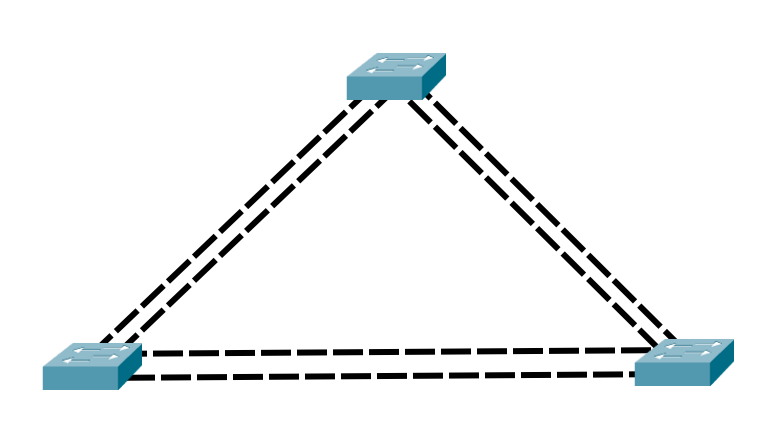
ipv6 address fe80::10 link-local

ipv6 dhcp server GYOR\_A\_v6

ipv6 nd managed-config-flag

# Etherchannel

Az EtherChannel előnyei

A legtöbb konfigurációs feladat elvégezhető az EtherChannel (portcsatorna) interfészen, így nincs szükség a portok egyedi kezelésére, ezzel biztosítható azok következetes beállítása. Az EtherChannel a meglévő switchportokat használja, így nincs szükség gyorsabb és jóval drágább összeköttetésre a nagyobb sávszélesség eléréséhez. Ugyanahhoz az EtherChannel-hez tartozó portok között terheléselosztás valósul meg. Hardvertől függően egy vagy több terheléselosztási mód is alkalmazható. These methods include source MAC and destination MAC load balancing, or source IP and destination IP load balancing, across the physical links. Az EtherChannel-be rendezett portcsoport egyetlen logikai kapcsolatként működik. Ha két switch között több EtherChannel köteg is van, akkor az STP blokkolhat közülük néhányat a hurkok kialakulásának elkerülése érdekében. Ha az STP blokkol egy redundáns kapcsolatot, akkor zárolja az egész EtherChannel-t, vagyis letiltja az összes hozzá tartozó portot. Amikor csak egy EtherChannel kapcsolat létezik, akkor az összes benne levő fizikai port aktív marad, mivel az STP csak egy (logikai) kapcsolatot lát. Az EtherChannel redundanciát biztosít, mert a teljes összerendezett köteg egy logikai kapcsolatot alkot. Továbbá a csatorna valamely fizikai portjának kiesése nem okoz változást a topológiában. Ezért nem szükséges az STP újraszámítása. Amíg legalább egy fizikai port jelen van, addig az EtherChannel is működőképes marad, de a kiesett portok miatt a teljes átbocsátóképesség lecsökken.  
  
Topológiai kialakítás a hálózatban (2 féle) :

# VPN

A VPN (Virtual Private Network) konfigurációja és implementációja alapvető fontosságú a két szervezet belső hálózatai közötti biztonságos kommunikációhoz. A rendszerterv ebben a fejezetben részletesen bemutatja a VPN konfigurációt, kitérve a biztonsági aspektusokra és az előnyökre.

Konfiguráció Részletei:

A rendszerterv először is részletesen ismerteti a VPN konfigurációjának részleteit mindkét szervezet routerén. A konfiguráció magában foglalja az alábbi lépéseket:

* Access-listek definiálása az engedélyezett IP-címek és portok megadásához.
* ISAKMP (Internet Security Association and Key Management Protocol) politika beállítása a kulcsszerződés és a titkosítási algoritmusok meghatározásához.
* Az ISAKMP kulcsok és az IPsec transformációs készletek konfigurálása az autentikáció és a titkosítás számára.
* A kriptográfiai térképek beállítása az IPsec és ISAKMP konfigurációkhoz.

Biztonsági Aspektusok:

A rendszerterv kiemelten foglalkozik a VPN konfiguráció biztonsági részleteivel. Ezek a következők:

* Titkosítás: Az AES 256-bites titkosítás és az SHA algoritmusok használata adataink védelme érdekében.
* Előosztott kulcsok: Az előosztott kulcsok biztosítják az autentikációt és az adatok titkosítását a VPN kapcsolatokban.
* Access-listek: Az access-listek pontosan meghatározzák, hogy mely IP-címek és portok kommunikálhatnak egymással, ezáltal minimalizálva a támadási felületet.
* IPsec transformációs készlet: Az IPsec transformációs készlet biztosítja az adatok titkosítását és integritásának ellenőrzését az adatátvitel során.

A VPN konfiguráció és implementáció számos előnnyel jár mindkét fél számára

Az egyik ilyen a **biztonság**: A VPN egy biztonságos csatornát biztosít a két belső hálózat közötti kommunikációhoz, minimalizálva a külső fenyegetéseket és a bizalmas adatok illetéktelen hozzáférését. **Költségcsökkentés**, mert a VPN lehetővé teszi a két szervezet számára, hogy közös erőforrásokat használjanak, csökkentve a hálózati infrastruktúra költségeit.

VPN konfiguráció és implementáció megfelelő végrehajtása alapvető fontosságú a szervezetek belső hálózatai közötti biztonságos és hatékony kommunikációhoz. A rendszerterv részletesen dokumentálja a konfigurációt, kiemelve annak biztonsági részleteit és előnyeit.

# ASA

A hálózatban megvalósított konfiguráció részletes áttekintésével megérthetjük a tűzfalak és hálózati eszközök kritikus szerepét a biztonságos és hatékony hálózatok működtetésében. Az ASA (Adaptive Security Appliance) eszközök a Cisco egyik legnépszerűbb termékei, melyeket különösen a hálózati biztonság és az adatforgalom szabályozására használnak. A hálózatban megvalósított konfiguráció alapján az ASA konfigurációját és a hálózati kommunikációt mutatjuk be.

Az ASA konfiguráció alapjai

1. **Alapkialakítás és hozzáférési beállítások:**
   * A hostname beállítás megadja a tűzfal nevét, amely fontos a hálózatban lévő eszközök azonosításához.
   * Az enable password és a username/password beállítások a hozzáférési biztonságot szolgálják, hogy csak jogosult felhasználók férhessenek hozzá a tűzfalhoz.
2. **Interfész konfigurációk:**
   * nameif paranccsal az interfészek neveit állítjuk be (INSIDE, OUTSIDE), amelyek a hálózati architektúra érthetőségét segítik.
   * security-level beállítások különböző biztonsági szinteket jelölnek, ahol magasabb szám nagyobb biztonságot jelent. Az INSIDE interfész általában magasabb biztonsági szintet kap.
   * ip add paranccsal az IP-címeket rendeljük az interfészekhez.
3. **OSPF (Open Shortest Path First) routing:**
   * Az OSPF egy dinamikus útválasztási protokoll, amely segít az útvonalak automatikus kiválasztásában a hálózaton belül, hatékonyságát és skálázhatóságát növelve.
   * A hálózati parancsok (network) az OSPF által figyelt IP-cím tartományokat definiálják.
4. **Statikus útvonalak:**
   * A route paranccsal statikus útvonalat adunk meg, amely alapértelmezett útvonalként szolgál az adatforgalom számára, ha nincsenek egyéb elérhető vagy megfelelő dinamikus útvonalak.
5. **ACL (Access Control List) konfiguráció:**

Az ACL-ek a tűzfalakon keresztül menedzselik, hogy milyen forgalom engedélyezett vagy tiltott az egyes interfészeken. Az ACL-eket különösen fontos helyesen konfigurálni, hogy a hálózati biztonsági politikák érvényesüljenek.

* **ACL definiálása és alkalmazása:**
  + access-list ALLOW\_PING extended permit icmp 130.10.10.16 255.255.255.252 any:

Ez az ACL-sor engedélyezi az ICMP forgalmat (általában ping kérésekhez használt), ami kiindul a 130.10.10.16/30 hálózatról és bármilyen cél felé irányul. Ez a beállítás lehetővé teszi a hálózati eszközök elérhetőségének ellenőrzését és a hálózati diagnosztika végrehajtását.

* + access-group ALLOW\_PING in interface OUTSIDE:

Ez a parancs alkalmazza az ALLOW\_PING ACL-t az OUTSIDE interfészen. Az alkalmazott ACL megadja, hogy az adott szabályok melyik interfészen legyenek érvényesek, így biztosítva, hogy a bejövő forgalmat szabályozzuk az adott interfészen

Előnyök

* **Biztonság:** Az interfészek és felhasználók szigorú beállításaival az ASA biztosítja, hogy csak megbízható forgalom haladhasson át a hálózaton, és csak jogosult személyek férjenek hozzá a kezelőfelülethez.
* **Skálázhatóság és rugalmasság:** Az OSPF használata lehetővé teszi a hálózat gyors adaptációját a változásokhoz, új eszközök integrálását és hibatűrő útvonalak kialakítását.
* **Kontroll és átláthatóság:** A részletes interfész- és biztonsági beállításokkal az IT csapat könnyen monitorozhatja és kezelheti a hálózati tevékenységeket, javítva a hálózati menedzsment hatékonyságát.

Ezek a beállítások és előnyök biztosítják, hogy a vállalati hálózatok biztonságosak, megbízhatóak és jól kezelhetőek maradjanak, ami alapvető a mai gyorsan változó informatikai környezetben.

# Forgalomirányítón megvalósított biztonsági funkciók - Tibor

# Vezeték nélküli hálózat - Tibor

# Windows szerver konfigurálása

## DHCP

A Windows Server 2016-os operációs rendszerre DHCP szolgáltatást telepítettünk. Beállításai alapján a Gyor\_B területnek a 192.168.1.32/27 hálózatszegmensből szolgáltat IP címet. Az alábbi képen jól látható, hogy a Windows10 kliens a 192.168.1.37-es IP címet kapta a megfelelő 192.168.1.33-as átjáró IP címével. Ennek megfelelően a bérlet is megjelent a szerver felügyeleti konzolján.



## Active Directory beállítása

A megfelelő IP cím kiosztása után a klienst a szerveren létrehozott AD-ba léptettük. A kép jobb oldali, szerver képernyőképen jól látszik, hogy fut a DNS szolgáltatás, ami nélkül az AD nem látná el a feladatát, illetve felül látszik, hogy létre lett hozva egy tartomány ***Gyor.Server0*** néven. A kliensen az alapértelmezett Workgroup mukacsoportból kezdeményeztük a gép tartományba léptetését a tartomány pontos nevének megadásával. 

A tartományvezérlő a kérelemre egy olyan felhasználó nevét és jelszavát kéri be, akinek joga van a beléptetést végrehajtani. Ha ezt megkapta egy üdvözlő ablakkal rögzíti a belépés tényét, majd újraindítás után már lehetőség van akár egy az AD-n létrehozott felhasználóval is belépni.



Belépés után - az Iroda szervezeti egység tagjaként - Példa Ottó nevű felhasználónk a számára beállított megosztott meghajtót az egyszerűség kedvéért "*Z: megh*ajtó”-ként felcsatolva sikeresen eléri.



Csoportházirend átgondolt beállításaival az egyes szervezeti egységek, így azok tagjai a felhasználók, hálózaton illetve az egyes végponti gépeken alkalmazott jogai, lehetőségei jól szabályozhatók. Óriási előnye, hogy ennek menedzselését a rendszergazda vagy az erre a feladatra jogosultságokkal ellátott személy, központosított módon láthatja el. A felhasználó számára is előnyökkel járhat. Épületen belül a különböző gépeken belépve, az azonosítása után akár mindig ugyanaz a munkakörnyezet fogadhatja, így növelve a kényelmét és a hatékonyságát.

A szerveren megosztott nyomtatási szolgáltatás is fut. A kliens megtalálta és telepítette is a szerveren található és az AD által terjesztett Canon nyomtatót.

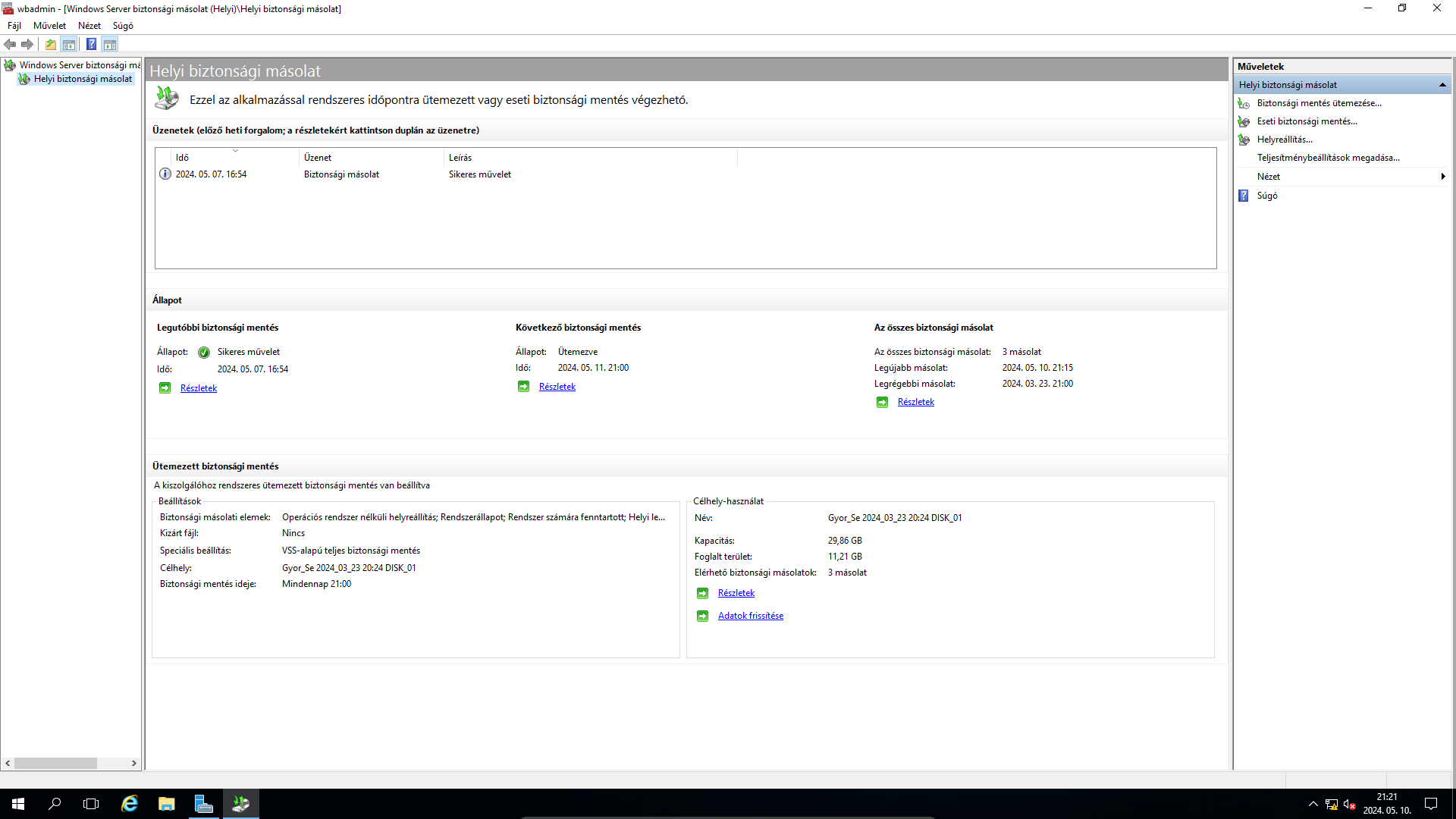


További beállításokkal finomíthatók a felhasználó nyomtatásra vonatkozó jogai.

## Biztonsági mentés

A kiszolgáló biztonsági mentése elengedhetetlen a fontos adatok elvesztésének megakadályozása érdekében. Az időszakos biztonsági mentések konfigurálása lehetővé teszi a rendszer visszaállítását olyan váratlan események előfordulása esetén, mint például a hardverösszetevők meghibásodása, a rendszer helytelen konfigurálása vagy vírusok jelenléte.

A windows Servernek beépített megoldása van erre, amelyet hozzá lehet adni a szolgáltatásokhoz. A mentések automatizálásával és megfelelő ütemezéssel igyekeznünk kell a kár minimalizálására. Rendkívül fontos átgondolnunk a mentések tárolásának módját és helyét és begyakorolni a visszaállítás módját annak sikerességének ellenőrzésével.



# Linux szerver konfigurálása

## Telepítés

A linux szerver a soproni telephelyen üzemel. A telepítés után a Sopron-linux nevet és statikusan beállított IP címet (192.168.0.138/30) kapott. Számos szolgáltatás fut rajta.

DNS, Apache, SSH, FTP, Samba

## DNS

BIND9 DNS szerver szolgáltatás fut rajta. A Windows 10 kliensről tesztelve a butor.loc nevet a Linux feloldja majd sikeres ping válaszokat küld.



## SSH

Egy távoli Windows 10 kliens gépről léptünk be SSH-val. Az azonosítás sikeres volt és a Promptban megjelent a Linux, majd ezután futatható volt akár az MC alkalmazás is.   


## Samba

Az Ubuntu és Windows számítógépek összekapcsolásának egyik legáltalánosabb módja a Samba beállítása fájlkiszolgálóként. Mi is ezt használtuk.



## Apache

Az apache telepítése és aktiválása után – a már működőképes SSH és a Samba segítségével - az alapértelmezett mappába feltöltöttük az egyelőre statikus intranetes információs oldal összetevőit, két HTML fájlt és a hozzájuk tartozó, stílusukat leíró CSS állományt.

A feltöltés után ugyancsak a távoli Windows 10 kliens böngészőjével teszteltünk.[[1]](#footnote-1)

## FTP - Tibor

# Jövőbeni fejlesztések - Krisztián

DMZ létrehozása.

Trello nem sikerült megcsinálni

# Csapatmunka -Krisztián

# Melléklet

Topológia

1. ssh-smb-apache-demo.mp4 [↑](#footnote-ref-1)