ACTIVE DIRECTORY TUSHUNCHASI

Habibjonova Guldofarid Murodjon qizi
Muxammad al – Xorazmiy nomidagi TATU "Kiberxavfsizlik va kriminalistika" kafedrasi stajyor o'qituvchisi
Erkinov Shohjahon Sherali o'g'li
Oripov Asilbek Baxtiyor o'g'li
Saidov Ozodbek Alisher o'g'li
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Mazkur maqolada Active Directory (AD) texnologiyasining nazariy asoslari, arxitekturasi va ishlash prinsiplari ilmiy jihatdan tahlil qilinadi. Active Directory korporativ tarmoqlarda markazlashgan boshqaruv tizimi sifatida foydalanuvchilar, kompyuterlar, guruhlar va boshqa tarmoq resurslarini yagona domen muhitida boshqarishni ta'minlaydi.*

Kalt so'zlar: *Active Directory, domen, Domain Controller, LDAP, Kerberos, autentifikatsiya, avtorizatsiya, Group Policy, replikatsiya, katalog xizmati, axborot xavfsizligi, tarmoq boshqaruvi.*

Zamonaviy axborot-kommunikatsiya texnologiyalari rivojlanishi natijasida korporativ tarmoqlarda foydalanuvchilar, qurilmalar va resurslarni markazlashtirilgan holda boshqarish zarurati yuzaga keldi. Tashkilotlarda yuzlab yoki minglab foydalanuvchilar, serverlar va ishchi stansiyalar mavjud bo'lgani sababli ularni qo'lda boshqarish murakkab va xavfli hisoblanadi. Shu muammolarni hal etish maqsadida Microsoft kompaniyasi tomonidan Active Directory (AD) katalog xizmati ishlab chiqilgan.

Active Directory — bu Windows Server operatsion tizimlarida ishlovchi markazlashtirilgan boshqaruv va autentifikatsiya tizimi bo'lib, u tarmoqdagi barcha obyektlar haqida ma'lumot saqlaydi va ularga kirishni nazorat qiladi.

1.1-rasm. Active Directory

Active Directory ning asosiy mohiyati

Active Directory — bu katalog xizmati (directory service) hisoblanadi.

Katalog xizmati — bu tarmoqdagi obyektlar (foydalanuvchi, kompyuter, printer, server, guruh va boshqalar) haqidagi ma'lumotlarni saqlovchi va ularni boshqaruvchi tizimdir.

AD quyidagi vazifalarni bajaradi:

– Foydalanuvchilarni autentifikatsiya qilish

– Resurslarga ruxsatlarni boshqarish

– Xavfsizlik siyosatini qo'llash

– Domen infratuzilmasini boshqarish

– Markazlashtirilgan nazoratni ta'minlash

Active Directory yordamida administrator butun tarmoqni bitta markazdan boshqarishi mumkin.

Active Directory ning yaratilish tarixi

Active Directory birinchi marta Windows 2000 Server operatsion tizimi bilan taqdim etilgan. Undan oldin Windows NT domen modeli mavjud bo'lgan, lekin u quyidagi kamchiliklarga ega edi:

- Markazlashtirish darajasi past
- Kengaytirilish imkoniyati cheklangan
- Replikatsiya mexanizmi sust
- Xavfsizlik boshqaruvi yetarli emas

Windows 2000 bilan birga Active Directory joriy qilinib, u yanada ishonchli, kengaytiriladigan va xavfsiz tizim sifatida ishlab chiqildi.

Active Directory ning asosiy tushunchalari

Domen (Domain)

Domen — bu Active Directory ning asosiy mantiqiy birligi hisoblanadi. Domen yagona xavfsizlik chegarasi bo'lib, undagi barcha obyektlar yagona siyosat asosida boshqariladi.

Masalan:

```
company.local
university.uz
```

1.2-rasm. Domen

Har bir domen o'z foydalanuvchilari va resurslariga ega bo'ladi.

Domain Controller (DC)

Domain Controller — bu Active Directory ma'lumotlar bazasini saqlovchi va autentifikatsiya jarayonini amalga oshiruvchi serverdir.

DC vazifalari:

– Login va parolni tekshirish

– Kerberos ticket berish

– Siyosatlarni qo'llash

– Replikatsiyani amalga oshirish

Forest (O‘rmon)

Forest — bu bir yoki bir nechta domenlardan tashkil topgan eng yuqori ierarxik tuzilma.

Forest ichida:

– Umumiy sxema (schema)

– Global katalog

– Ishonchli aloqalar (trust relationship) mavjud bo‘ladi.

Tree (Daraxt)

Tree — bu umumiy nom maydoniga ega bo‘lgan domenlar to‘plami.

Masalan:

```
company.local
hr.company.local
it.company.local
```

1.3-rasm. Umumiy maydoniga ega bo‘lgan domenlar to‘plami.

Organizational Unit (OU)

OU — bu domen ichidagi obyektlarni mantiqiy guruhlarga ajratish uchun ishlatiladi.

Masalan:

– HR bo‘limi

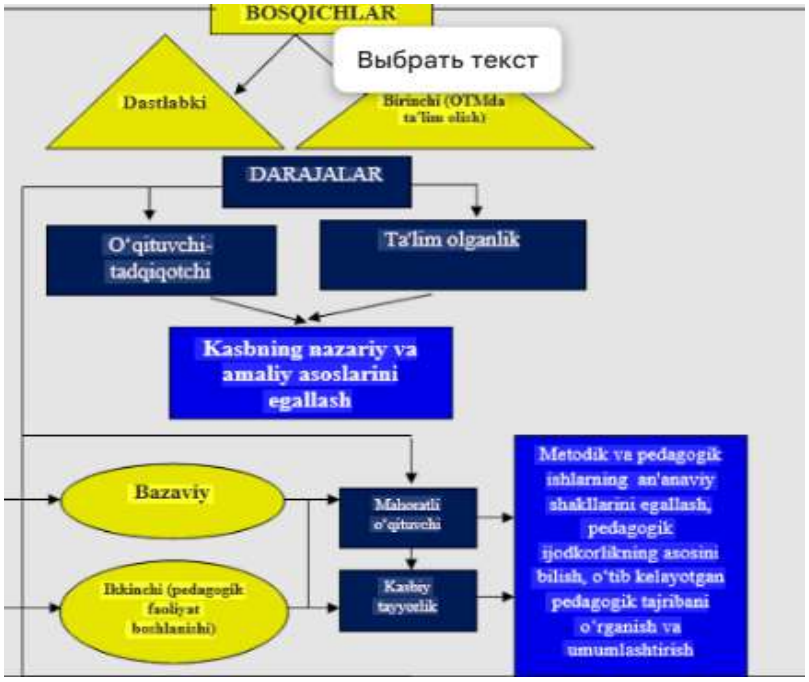
– IT bo‘limi

– Buxgalteriya

OU yordamida:

– Guruh siyosati qo‘llanadi

– Administratorlik vakolatlari taqsimlanadi



1.4-rasm. Organizational Unit

Active Directory ma'lumotlar bazasi

Active Directory ma'lumotlar bazasi NTDS.dit faylida saqlanadi.

U quyidagilarni o'z ichiga oladi:

– Foydalanuvchilar

– Parol hashlar

– Guruhlar

– Kompyuterlar

– Siyosatlar

Ma'lumotlar LDAP protokoli orqali boshqariladi.

Active Directory ishlash prinsipi

Active Directory asosan Kerberos autentifikatsiya protokoli asosida ishlaydi.

Autentifikatsiya bosqichlari:

1. Foydalanuvchi login va parol kiritadi
2. DC foydalanuvchini tekshiradi
3. TGT (Ticket Granting Ticket) beradi
4. Foydalanuvchi resursga kirish uchun xizmat ticketi oladi

Bu jarayon xavfsiz va shifrlangan tarzda amalga oshiriladi.

Active Directory da autentifikatsiya va avtorizatsiya

Autentifikatsiya-Foydalanuvchining kimligini tasdiqlash.

Avtorizatsiya-Foydalanuvchining qaysi resurslarga kirish huquqi borligini aniqlash.

Bu ikki jarayon AD xavfsizligining asosini tashkil qiladi.

Active Directory ning afzalliklari

– Markazlashtirilgan boshqaruv

– Yuqori xavfsizlik

– Kengaytirilish imkoniyati

– Replikatsiya mexanizmi

– Guruh siyosati orqali nazorat

– Single Sign-On (SSO)

Active Directory va xavfsizlik. AD korporativ tarmoqning yuragi hisoblanadi. Agar AD buzilsa:

– Butun domen nazorati yo'qoladi

– Foydalanuvchilar boshqaruvi izdan chiqadi

– Maxfiy ma'lumotlar xavf ostida qoladi

Shu sababli AD xavfsizligi alohida e'tibor talab qiladi.

Active Directory va zamonaviy infratuzilma

Bugungi kunda AD:

– Bulut infratuzilmasi bilan integratsiya qilinadi

– Azure Active Directory bilan ishlaydi

– Hybrid muhitlarda qo'llaniladi

– Zero Trust modeliga moslashtiriladi

Active Directory ning tashkilotdagi roli

Korporativ tashkilotlarda AD quyidagilarni ta'minlaydi:

– Xodimlarni boshqarish

– Kirish nazorati

– Axborot xavfsizligi

– Siyosatlarni markazlashtirish

– Audit va monitoring

Active Directory zamonaviy korporativ tarmoqlarda markaziy boshqaruv va xavfsizlik tizimi hisoblanadi. U foydalanuvchilarni autentifikatsiya qilish, resurslarga kirishni boshqarish va xavfsizlik siyosatlarini qo'llashda muhim rol o'ynaydi.

AD ning to'g'ri konfiguratsiyasi va doimiy monitoringi tashkilot axborot xavfsizligini ta'minlashning asosiy omillaridan biridir.

XULOSA

Active Directory zamonaviy korporativ axborot tizimlarining ajralmas qismi bo'lib, u markazlashgan boshqaruv, xavfsizlik va identifikatsiya jarayonlarini ta'minlovchi asosiy platforma hisoblanadi. Uning asosiy vazifasi tarmoq obyektlarini yagona tuzilma asosida boshqarish va foydalanuvchilarga belgilangan ruxsatlar asosida resurslardan foydalanish imkonini yaratishdan iborat.

Tahlillar shuni ko'rsatadiki, Active Directory ning samaradorligi uning arxitekturaviy to'g'ri loyihalanishi va xavfsizlik mexanizmlarining to'liq joriy etilishiga bog'liq. Kerberos asosidagi autentifikatsiya, LDAP orqali ma'lumot almashinuvi va Group Policy yordamida markazlashgan boshqaruv tizimning yaxlitligini ta'minlaydi. Biroq noto'g'ri sozlash yoki zaif xavfsizlik siyosati tizimni turli tahdidlarga nisbatan himoyasiz qoldirishi mumkin.

Shu bois, Active Directory ni boshqarishda texnik, tashkiliy va xavfsizlik choralarini uyg'un holda qo'llash muhim ahamiyatga ega. Bu esa korporativ tarmoqlarning barqarorligi va axborot xavfsizligini ta'minlashda muhim omil hisoblanadi.

ADABIYOTLAR RO'YXATI:

7. Microsoft Corporation. Active Directory Domain Services Overview. Microsoft Learn, 2023.

8. Microsoft Corporation. Windows Server Active Directory Documentation. Microsoft Docs, 2023.

9. Alperovitch D. The Defender's Dilemma: Identifying and Responding to Advanced Persistent Threats. McAfee White Paper, 2011.

10. Hutchins E., Cloppert M., Amin R. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2011.

11. MITRE Corporation. MITRE ATT&CK Framework Documentation. MITRE, 2023.

12. Russell R., Kent K. Directory Services and Active Directory Security. SANS Institute Reading Room, 2020.

13. Metcalf S. Active Directory Security: Attacks & Defense. Trimarc Security, 2022.

14. Schroeder M., Salter J. Kerberos: An Authentication Service for Computer Networks. IEEE Communications Magazine, 1994.

15. Tankard C. Advanced Persistent Threats and How to Monitor and Deter Them. Network Security Journal, 2011.

16. Skoudis E., Liston T. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall, 2005.

17. O'Gorman G., McDonald G. Ransomware: A Growing Menace. Symantec Security Response, 2012.

18. Grimes R. Hacking the Hacker: Learn from the Experts Who Take Down Hackers. Wiley Publishing, 2017.

19. Kim D., Solomon M. Fundamentals of Information Systems Security. Jones & Bartlett Learning, 2018.