ACTIVE DIRECTORY ISHLASH PRINSIPI

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

Annotatsiya: Ushbu maqolada *Active Directory* tizimining ishlash prinsipi, uning autentifikatsiya va avtorizatsiya mexanizmlari hamda tarmoq infratuzilmasidagi o'rni batafsil tahlil qilinadi. Active Directory markazlashtirilgan katalog xizmati sifatida foydalanuvchilar, kompyuterlar va boshqa resurslar haqidagi ma'lumotlarni saqlaydi hamda boshqaradi.

Kalt so'zlar: Active Directory, autentifikatsiya, avtorizatsiya, Kerberos, LDAP, domen nazoratchisi, replikatsiya, Group Policy, xavfsizlik siyosati, tarmoq boshqaruvi.

Active Directory (AD) — bu Microsoft Windows Server operatsion tizimlarida ishlovchi markazlashgan katalog xizmati bo'lib, u tarmoqdagi barcha obyektlar haqidagi ma'lumotlarni yagona ierarxik ma'lumotlar bazasida saqlaydi va boshqaradi. Active Directory yordamida foydalanuvchilar, kompyuterlar, serverlar, printerlar, guruhlar, siyosatlar va boshqa resurslar markazlashgan holda nazorat qilinadi.

AD ning asosiy maqsadi — korporativ tarmoqlarda xavfsizlikni ta'minlash, boshqaruvni soddalashtirish va resurslardan samarali foydalanishni tashkil etishdir.

Active Directory quyidagi asosiy vazifalarni bajaradi:

- Foydalanuvchilarni autentifikatsiya qilish
- Resurslarga kirishni avtorizatsiya qilish
- Xavfsizlik siyosatini markazlashgan boshqarish
- Tarmoq obyektlarini ierarxik tuzilma asosida tashkil etish
- Domenlar o'rtasida ishonch (trust) munosabatlarini yaratish

Active Directory ishlashining umumiy mexanizmi

Active Directory ishlash prinsipi "mijoz–server" arxitekturasi asosida tashkil etilgan. Tarmoqdagi foydalanuvchi kompyuteri (client) domen nazoratchisi (Domain Controller) bilan doimiy aloqa o'rnatadi.

Jarayon quyidagicha ishlaydi:

1. Foydalanuvchi domen tizimiga kirishga harakat qiladi.
2. So'rov Domain Controller ga yuboriladi.
3. Domen nazoratchisi foydalanuvchini tekshiradi.
4. Autentifikatsiya muvaffaqiyatli bo'lsa, foydalanuvchiga ruxsat beriladi.
5. Group Policy siyosatlari qo'llanadi.
6. Foydalanuvchi tarmoq resurslariga kirish imkoniyatiga ega bo'ladi.

Bu jarayon markazlashgan boshqaruvni ta’minlaydi va xavfsizlikni kuchaytiradi.

Active Directory ma’lumotlar bazasi va obyekt modeli

Active Directory maxsus ma’lumotlar bazasida ishlaydi. Ushbu baza NTDS.dit faylida saqlanadi. Baza ichida barcha obyektlar saqlanadi.

AD da quyidagi obyekt turlari mavjud:

- User (foydalanuvchi)
- Computer (kompyuter)
- Group (guruh)
- Printer
- Shared Folder
- Organizational Unit (OU)

Har bir obyekt atributlarga ega bo‘ladi. Masalan, foydalanuvchi obyektida:

- Login nomi
- Parol
- Elektron pochta manzili
- Lavozimi
- Telefon raqami kabi atributlar mavjud.

Active Directory sxemasi (Schema) esa obyektlar va atributlarning tuzilishini belgilaydi. Schema butun forest bo‘yicha yagona hisoblanadi.

Autentifikatsiya jarayoni (Kerberos asosida)

Active Directory asosan Kerberos protokoli orqali autentifikatsiya amalga oshiradi.

Autentifikatsiya bosqichlari:

1. Foydalanuvchi login va parolni kiritadi.
2. Kompyuter Kerberos Authentication Server ga murojaat qiladi.
3. Agar ma’lumotlar to‘g‘ri bo‘lsa, foydalanuvchiga Ticket Granting Ticket (TGT) beriladi.
4. Foydalanuvchi TGT yordamida xizmat ko‘rsatuvchi serverlardan Service Ticket oladi.
5. Resursga kirish ta’minlanadi.

Bu tizim parolni ochiq holda tarmoq orqali yubormaslik imkonini beradi va yuqori darajadagi xavfsizlikni ta’minlaydi. Autentifikatsiyadan keyin avtorizatsiya jarayoni boshlanadi.

Ruxsatlar:

- Read (o‘qish)
- Write (yozish)
- Modify (o‘zgartirish)
- Full Control (to‘liq boshqaruv)

Access Control List (ACL) orqali belgilanadi.

Har bir obyekt xavfsizlik identifikatori (SID) ga ega bo‘ladi. SID yordamida tizim foydalanuvchini aniqlaydi.

1.1-rasm. Active Directory ishlash prinsipi

Group Policy ishlash mexanizmi

Group Policy (GPO) — markazlashgan boshqaruv vositasi bo‘lib, foydalanuvchi va kompyuter sozlamalarini nazorat qiladi.

GPO ikki qismdan iborat:

- Computer Configuration
- User Configuration

Group Policy quyidagi tartibda qo‘llanadi:

1. Local Policy
2. Site Policy
3. Domain Policy
4. OU Policy

Bu LSDOU ketma-ketligi deb ataladi.

Group Policy yordamida:

- Parol siyosati
- Hisob bloklanish siyosati
- USB qurilmalarni bloklash
- Firewall sozlamalari
- Dastur o‘rnatish siyosati boshqariladi.

Replikatsiya mexanizmi

Agar tashkilotda bir nechta Domain Controller mavjud bo‘lsa, ular o‘zaro ma’lumot almashadi. Bu jarayon replikatsiya deyiladi.

Replikatsiya xususiyatlari:

- Multi-master model
- Avtomatik sinxronlash
- O‘zgarishlarni kuzatish

– Saytlar orasida jadval asosida ishlash

Bu tizim ishonchlilikni oshiradi va tizim ishdan chiqsa ham ishlashni davom ettiradi.

DNS va LDAP bilan ishlash

Active Directory ishlashi uchun DNS muhim rol o‘ynaydi. Domen nomlari va xizmatlarni topish DNS orqali amalga oshiriladi.

LDAP (Lightweight Directory Access Protocol) esa katalog ma’lumotlariga murojaat qilish protokoli hisoblanadi. Kerberos, DNS va LDAP birgalikda AD ning to‘liq ishlashini ta’minlaydi.

Active Directory ning xavfsizlik modeli

Active Directory xavfsizlik modeli quyidagilarga asoslanadi:

– Kerberos autentifikatsiyasi
– SID identifikatori
– Access token mexanizmi
– Trust relationship
– Audit va monitoring

Foydalanuvchi tizimga kirganda, unga access token yaratiladi. Ushbu token ichida:

– SID
– Guruhlar SID
– Ruxsatlar saqlanadi.

Active Directory ishlashining afzalliklari

Active Directory quyidagi ustunliklarga ega:

– Markazlashgan boshqaruv
– Yuqori xavfsizlik
– Kengaytiriladigan arxitektura
– Ishonchli replikatsiya
– Avtomatlashtirilgan siyosat boshqaruvi

Katta tashkilotlarda minglab foydalanuvchilarni samarali boshqarish imkonini beradi. Active Directory ishlash prinsipi markazlashgan katalog xizmati, Kerberos autentifikatsiyasi, ierarxik tuzilma, replikatsiya mexanizmi va Group Policy boshqaruv tizimiga asoslangan. U korporativ tarmoqlarda xavfsizlikni ta’minlash, resurslardan samarali foydalanish va boshqaruvni soddalashtirishda muhim ahamiyat kasb etadi.

XULOSA

Xulosa qilib aytganda, Active Directory ishlash prinsipi markazlashtirilgan boshqaruv va xavfsizlik mexanizmlariga asoslanadi. Foydalanuvchi tizimga kirishda uning shaxsi Kerberos protokoli orqali tekshiriladi va tasdiqlanadi. LDAP esa katalog ma’lumotlariga murojaat qilish va ularni boshqarish imkonini beradi. Domen nazoratchilari o‘rtasidagi replikatsiya mexanizmi ma’lumotlarning yaxlitligi va uzluksiz ishlashini ta’minlaydi.

ADABIYOTLAR RO‘YXATI

1. Active Directory. – O‘Reilly Media, 2006.

2. Mastering Active Directory. – Packt Publishing, 2016.
3. Microsoft Corporation. Windows Server Active Directory Documentation.
4. Microsoft Learn. Active Directory Authentication and Authorization Guide.
5. Active Directory Domain Services 2008 How-To. – Packt Publishing, 2009.