INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

ZAMONAVIY ILM-FAN VA INNOVATSIYALAR NAZARIYASI

ILMIY-AMALIY KONFERENSIYA

2025

Google Scholar doi zenodo OpenAIRE

« ZAMONAVIY ILM-FAN VA INNOVATSIYALAR NAZARIYASI » NOMLI ILMIY, MASOFAVIY, ONLAYN KONFERENSIYASI TO‘PLAMI

2-JILD 6-SON

Konferensiya to’plami va tezislar quyidagi xalqaro ilmiy bazalarda indexlanadi

www.innoworld.net

O‘ZBEKISTON-2025

Tel:+99833 5668868 | Telegram: @Anvarbek_PhD

Active Directory Domain Services (AD DS) arxitekturasi va zamonaviy boshqaruv usullari

Nazirkulov Jamoldin Davlatjon o‘g‘li
Farg‘ona davlat texnika universiteti o‘qituvchisi
Mansurova Ozodaxon Maxamatjon qizi
Farg‘ona davlat texnika universiteti 4-bosqich talabasi
e-mail: omansurova84@gmail.com

Annotatsiya: Ushbu maqolada Active Directory Domain Services (AD DS) tizimining asosiy arxitekturasi, uning komponentlari va zamonaviy boshqaruv tamoyillari yoritiladi. AD DS korporativ tarmoqlarda identifikatsiya, autentifikatsiya va resurslarga kirishni markazlashgan tarzda boshqarish imkonini beruvchi muhim xizmatdir. Maqolada domenlar tuzilmasi, katalog xizmatlarining ishlash mexanizmlari, Group Policy orqali boshqaruv, shuningdek, xavfsizlikni mustahkamlashga qaratilgan yangi yondashuvlar haqida batafsil ma’lumot beriladi.

Kalit so‘zlar: Active Directory, AD DS, domen, katalog xizmatlari, Group Policy, autentifikatsiya, tarmoq boshqaruvi, xavfsizlik.

Аннотация: В статье рассматривается архитектура и ключевые функции Active Directory Domain Services (AD DS), а также современные подходы к управлению корпоративными сетями на основе каталожных служб. AD DS обеспечивает централизованное управление учетными записями пользователей, проверкой подлинности и доступом к сетевым ресурсам. В работе раскрываются структура доменов, принципы функционирования каталогов, использование групповых политик и актуальные методы усиления безопасности инфраструктуры.

Ключевые слова: Active Directory, AD DS, домен, каталожные службы, групповая политика, аутентификация, управление сетью, безопасность.

Abstract: This article explores the architecture and core functionalities of Active Directory Domain Services (AD DS), focusing on its role in centralized identity and access management within enterprise networks. AD DS enables secure authentication, authorization, and the unified administration of network resources. The paper provides an overview of domain structures, directory service operations, Group Policy-based management methods, and modern approaches to enhancing infrastructure security.

Keywords: Active Directory, AD DS, domain, directory services, Group Policy, authentication, network administration, security.

Kirish. Katta hajmdagi korporativ tarmoqlar rivojlanishi bilan foydalanuvchilar, qurilmalar va resurslar o‘rtasidagi o‘zaro aloqalarni yagona

markazdan boshqarish zarurati kuchaydi. Ana shunday ehtiyojlarni qondirishda Active Directory Domain Services (AD DS) tizimi muhim o‘rin tutadi. AD DS - bu Microsoft tomonidan ishlab chiqilgan katalog xizmatlari majmuasi bo‘lib, u tashkilot infratuzilmasida identifikatsiya, autentifikatsiya va avtorizatsiya jarayonlarini tartibga solishga xizmat qiladi. Ushbu tizim nafaqat domenlar tuzilmasini yaratish, balki foydalanuvchilar, guruhlar, kompyuterlar va boshqa tarmoq obyektlarini yagona katalogda boshqarish imkonini beradi.

Bugungi kunda zamonaviy tashkilotlarda axborot xavfsizligi talablarining ortib borishi, tarmoqlar murakkablashuvi va masofaviy xizmatlardan keng foydalanish AD DS boshqaruvini yanada takomillashtirishni talab qilmoqda. Shuning uchun AD DS arxitekturasi, uning asosiy komponentlari va boshqaruv mexanizmlarini chuqur o‘rganish korporativ IT tizimlarining barqaror ishlashini ta’minlashda muhim ahamiyat kasb etadi. Mazkur maqola AD DSning asosiy tamoyillari, Group Policy imkoniyatlari, xavfsizlik choralarini kuchaytirish usullari hamda ushbu xizmatni samarali boshqarishga oid zamonaviy yondashuvlarni tahlil qiladi.

Active Directory Domain Services (AD DS) korporativ tarmoqlarni boshqarishda eng ishonchli va ko‘p funksiyali katalog xizmatlaridan biri hisoblanadi. Uning arxitekturasi ierarxik tuzilishga asoslanib, barcha tarmoq obyektlarini yagona boshqaruv nuqtasi ostida jamlaydi. Domen, o‘rmon, tashkilot bo‘linmalari kabi qatlamlar yordamida AD DS yirik infratuzilmaning tartibli, moslashuvchan va kengaytiriladigan ko‘rinishda bo‘lishini ta’minlaydi. Har bir komponent o‘z vazifasiga ega bo‘lib, bu tizimning ham xavfsizlik, ham boshqaruv nuqtai nazaridan yuqori samaradorlikka erishishiga xizmat qiladi.

AD DSning eng asosiy elementlaridan biri bu - **domen**. Domen ichida barcha foydalanuvchilar va kompyuterlar yagona siyosat asosida boshqariladi. Domenlar o‘zaro ishonch munosabatlari orqali bog‘lanib, katta korporatsiyalar uchun murakkab infratuzilma yaratishga imkon beradi. Domenlarni boshqaruvchi domain controller (DC) serverlari esa katalogdagi barcha o‘zgarishlarni sinxronlash orqali barqaror ishlashni ta’minlaydi. DClarning ko‘pligi va ularning replikatsiya mexanizmlari tizimni ishonchli qiladi.

Active Directory infratuzilmasining yana bir muhim qismi bu - **Organizational Units (OU)**. OUlar virtual bo‘linmalar bo‘lib, ular foydalanuvchilar yoki qurilmalarni mantiqan guruhlash, ularni alohida boshqaruv ostiga olish imkonini beradi. Ushbu mexanizm yordamida yirik tashkilotning bo‘limlari - masalan, buxgalteriya, kadrlar bo‘limi yoki IT bo‘limi - uchun alohida siyosatlar o‘rnatish osonlashadi. Natijada, AD DS moslashuvchan, decentralizatsiyalashgan boshqaruvni qo‘llab-quvvatlaydi.

Tel:+99833 5668868 | Telegram: @Anvarbek_PhD

AD DSni samarali boshqarishda **Group Policy** alohida ahamiyat kasb etadi. Group Policy yordamida kompyuterlar va foydalanuvchi muhitiga tegishli minglab parametrlar markazlashgan holda boshqariladi. Masalan, xavfsizlik siyosatlari, dastur o‘rnatish qoidalari, tarmoq konfiguratsiyalari yoki ishchi stoldagi sozlamalar barchasi GPO orqali boshqariladi. Bu esa administratorlarga tarmoqdagi barcha qurilmalarni yagona siyosat asosida tartibga solishga yordam beradi.

AD DSning zamonaviy boshqaruvi nafaqat standart vositalarga, balki avtomatlashtirilgan yechimlarga ham tayangan. PowerShell bu borada eng qulay vositalardan biri bo‘lib, u yordamida foydalanuvchilarni yaratish, GPOlarni boshqarish, replikatsiyani tekshirish yoki diagnostika qilish kabi jarayonlar tez va aniq bajariladi. Avtomatlashtirish yirik tarmoqlarda inson xatosi ehtimolini kamaytiradi va tizimning boshqaruv samaradorligini sezilarli oshiradi.

Kiberxavfsizlik talablari kuchayib borayotgan bugungi davrda AD DSni himoyalash masalasi eng ustuvor yo‘nalishlardan sanaladi. Kerberos autentifikatsiyasi, ikki bosqichli ruxsatlash, audit loglari orqali monitoring qilish va ro‘yxatga olinmagan qurilmalarni bloklash kabi choralar AD DS xavfsizligini mustahkamlaydi. Domen kontrollerlarini ajratilgan tarmoq segmentlarida saqlash va ularni yirik korporatsiyalarda Zero Trust yondashuvi orqali himoyalash ham zamonaviy talablar qatoriga kiradi.

AD DSning rivojlanishida bulut texnologiyalari ham asosiy o‘rinni egallay boshladi. Mahalliy infratuzilmani Microsoft Azure bilan bog‘lash orqali hibrid arxitektura yaratish, Azure AD Connect yordamida sinxronlash, masofaviy foydalanuvchilarni boshqarish kabi imkoniyatlar tashkilotlar uchun yangi qulayliklar yaratmoqda. Bulut bilan integratsiya AD DSning an’anaviy imkoniyatlarini kengaytirib, uni yanada moslashuvchan va global infratuzilmalar uchun tayyor holga keltiradi.

AD DSning samarali ishlashi va rivojlanishi uchun replikatsiya, ma’lumotlarni zaxiralash va tiklash mexanizmlari ham muhim ahamiyatga ega. Har bir domain controller (DC) muntazam ravishda katalogdagi o‘zgarishlarni boshqa DClar bilan sinxronlaydi, bu esa tarmoqdagi barcha foydalanuvchilar va qurilmalar uchun barqaror va moslashtirilgan muhitni ta’minlaydi. Shu bilan birga, malumotlarning avtomatik zaxiralari va nuqtai nazardan tiklash imkoniyati (disaster recovery) AD DSning yuqori ishonchliligini kafolatlaydi. Yirik korporatsiyalar uchun bu juda muhim bo‘lib, tizimning ishlamay qolishi va ma’lumot yo‘qotilishi natijasidagi xavfni minimallashtiradi.

Zamonaviy tarmoqlarda AD DSni himoya qilish faqat ichki choralar bilan cheklanmaydi, u kiberxavfsizlikning zamonaviy yondashuvlariga ham

Tel:+99833 5668868 | Telegram: @Anvarbek_PhD

moslashtirilgan bo‘lishi kerak. Masalan, **Conditional Access**, **Privileged Access Management (PAM)** va **Just-In-Time (JIT)** admin ruxsatlari kabi funksiyalar AD DS infratuzilmasini yanada xavfsiz qiladi. Ushbu yondashuvlar orqali administratorlarga faqat zarur vaqt va zarur resurslar uchun kengaytirilgan ruxsatlar beriladi, bu esa noto‘g‘ri ishlov berish yoki kiberhujum natijasida zarar ko‘rish xavfini kamaytiradi.

Shuningdek, AD DSni monitoring qilish va diagnostika qilishni avtomatlashtirishning dolzarbligi oshmoqda. Microsoft Sentinel yoki boshqa **SIEM (Security Information and Event Management)** tizimlari bilan integratsiya AD DS faoliyatini real vaqt rejimida kuzatish va xavf-xatarlarni aniqlash imkonini beradi. Masalan, foydalanuvchi hisoblarida g‘ayrioddiy faoliyat, parol o‘zgartirish urinishlari yoki domain controllerlarda shubhali trafikni avtomatik aniqlash va ogohlantirishlar yaratish mumkin. Bu esa korporativ tarmoqlarni kiberxavfsizlik tahdidlaridan himoya qilishda muhim rol o‘ynaydi.

Bugungi kunda AD DSning rivojlanishi bulut integratsiyasi bilan chambarchas bog‘liq. Hibrid infratuzilma orqali mahalliy Active Directory va Azure Active Directory (Azure AD)ni birlashtirish korporatsiyalarga ko‘plab qulayliklar yaratadi. Masofaviy foydalanuvchilarni boshqarish, avtomatik sinxronizatsiya, bulutdagi ilovalarga yagona identifikatsiya bilan kirish (Single Sign-On, SSO) va mobil qurilmalarni boshqarish imkoniyatlari tashkilotlarni global tarmoqlarga moslashtiradi. Shu bilan birga, hibrid yondashuv xavfsizlik, monitoring va siyosatlarni yagona nuqtadan boshqarish imkonini beradi.

AD DSning so‘nggi yillarda rivojlanayotgan yana bir yo‘nalishi bu - **Zero Trust arxitekturasi** bilan integratsiyalashuvdir. Zero Trust modeli asosida, tarmoq ichidagi barcha kirishlar avtomatik ravishda tekshiriladi va har bir foydalanuvchi hamda qurilma har doim identifikatsiya qilinadi. Shu tarzda, hatto ichki tarmoqdagi resurslar ham himoyalanadi va ruxsatsiz kirishlarning oldi olinadi. AD DS bu modelni qo‘llab-quvvatlash uchun Conditional Access, MFA (Multi-Factor Authentication) va Continuous Monitoring funksiyalarini kengaytirilgan holda taqdim etadi.

Yana bir dolzarb yo‘nalish - AD DS va AI (sun’iy intellekt) yordami bilan xavfsizlik va boshqaruvni optimallashtirishdir. Masalan, foydalanuvchi xatti-harakatlarini o‘rganish va tahdidlarni aniqlash uchun AI algoritmlari ishlatiladi. Bu tizim avtomatik ogohlantirishlar berishi, shubhali harakatlarni bloklashi va hatto ruxsatlarni vaqtinchalik cheklashi mumkin. Shu bilan birga, AI yordamida katalogdagi ortiqcha yoki keraksiz foydalanuvchi hisoblarini aniqlash va tozalash jarayoni avtomatlashtiriladi, bu esa boshqaruv samaradorligini oshiradi.

Tel:+99833 5668868 | Telegram: @Anvarbek_PhD

Shu bilan birga, AD DSni kengaytirish va modernizatsiya qilish jarayonida turli auditorlar va siyosatlarni boshqarish qobiliyati ham muhim ahamiyatga ega. Masalan, ma'lumotlar maxfiyligi talablariga javob berish uchun foydalanuvchi guruhlarini mantiqan ajratish, audit loglarini saqlash va nazorat qilish AD DS orqali amalga oshiriladi. Tashkilotlar GDPR, HIPAA yoki boshqa mahalliy va xalqaro standartlarga mos kelishi uchun katalog xizmatlarida ma'lumotlar xavfsizligini ta'minlash zarur.

Xulosa. Active Directory Domain Services (AD DS) korporativ tarmoqlarni markazlashgan tartibda boshqarish, foydalanuvchilarni identifikatsiya qilish va resurslarga xavfsiz kirishni ta'minlashda eng ishonchli texnologiyalardan biridir. Uning domen, OU, Group Policy kabi arxitektura elementlari yirik infratuzilmalarda tizimli va tartibli boshqaruvni shakllantiradi. Zamonaviy talablarga mos ravishda PowerShell orqali avtomatlashtirish, xavfsizlik siyosatlarini kuchaytirish va bulut xizmatlari bilan integratsiya AD DSning samaradorligini yanada oshiradi. Umuman olganda, AD DSni to‘g‘ri loyihalash va boshqarish tashkilotning axborot tizimlari barqarorligi hamda xavfsizligini ta'minlashning asosiy omillaridan biri hisoblanadi.

Foydalanilgan adabiyotlar:

1. Yo‘ldoshev, A., & Ahmedov, R. Kompyuter tarmoqlari va tizimlarini boshqarish. Toshkent: TATU nashriyoti, 2021.

2. Minasi, J. Mastering Windows Server 2019. Wiley Publishing, 2020.

3. Karimov, Sh. “Windows Server asoslari va tarmoq boshqaruvi texnologiyalari.” Axborot tizimlari va texnologiyalari jurnali, 2022.

4. Stanek, W. Active Directory Administration Cookbook. O’Reilly Media, 2019.

5. TATU O‘quv qo‘llanmasi. Operatsion tizimlar va tarmoq xizmatlari. Toshkent, 2020.

6. Microsoft Corporation. Active Directory Domain Services Overview. Microsoft Docs, 2022.

7. Bovet, S., & Burton, T. Understanding Active Directory: Architecture and Management. TechPress, 2021.

Tel:+99833 5668868 | Telegram: @Anvarbek_PhD