WINDOWS OT NI VIRTUAL PLATFORMADA SOZLASH BOSQICHLARI: DRAYVERLAR, TARMOQ VA XAVFSIZLIK CHORALARI.

Umarov Bekzod Azizovich
Farg‘ona davlat unversiteti Amaliy matematika va informatika kafedrasi katta o’qituvchisi p.f.b.d (PhD)
baumarov@mail.ru
Xomidova Mohichexra Axrorjon qizi
Farg’ona Davlat Unversiteti talabasi
mohiyusufova4@gmail.com
https://doi.org/10.5281/zenodo.15687163

ARTICLE INFO

Qabul qilindi: 10-Iyun 2025 yil
Ma’qullandi: 14-Iyun 2025 yil
Nashr qilindi: 18-Iyun 2025 yil

KEY WORDS

Virtualizatsiya, Windows OT, foydalanuvchi muhiti, optimallashtirish, tizim samaradorligi, foydalanuvchi tajribasi, xavfsizlik, resurslarni boshqarish.

ABSTRACT

Windows operatsion tizimini virtual platformada sozlashning muhim bosqichlari tizimni samarali va xavfsiz ishlashini ta'minlash uchun muhimdir. Ushbu maqolada Windows OTni virtual muhitda sozlash jarayonining asosiy bosqichlari, jumladan drayverlar, tarmoq konfiguratsiyasi va xavfsizlik choralari haqida so‘z yuritiladi. Virtualizatsiya, drayverlarning mosligini tekshirish, tarmoq aloqalarining sozlanishi va xavfsizlikka oid choralar tizimning ishlash samaradorligini oshiradi. Virtual platformada Windows tizimini muvaffaqiyatli ishlatish uchun to‘g‘ri konfiguratsiyalarni amalga oshirish zarur.

Hozirgi kunda texnologiyalar juda tez rivojlanmoqda, bu esa kompyuter tizimlarining ishlashiga katta ta'sir ko'rsatmoqda. Virtualizatsiya texnologiyalari, ayniqsa, operatsion tizimlarni virtual platformalarda sozlash va boshqarish jarayonini yanada samarali va qulay qilmoqda. Virtual muhitda Windows operatsion tizimini ishlatish esa, tizim resurslaridan samarali foydalanish va xavfsizlikni ta'minlashni bir vaqtning o'zida amalga oshirish imkoniyatini beradi. Virtualizatsiya orqali bir nechta virtual mashinalar yaratish, ularni turli maqsadlar uchun ishlatish, va bu jarayonni to‘g‘ri sozlash operatsion tizimning samaradorligini oshiradi. Shu bilan birga, Windows operatsion tizimining virtualizatsiyada ishlashining o'ziga xos xususiyatlari bor, jumladan, drayverlar, tarmoq va xavfsizlikni sozlash masalalari.

Windows operatsion tizimi o'zining keng tarqalganligi va ko'p turdagi dasturlarni qo'llab-quvvatlash imkoniyati bilan mashhur. Virtualizatsiya esa bu tizimni bir nechta foydalanuvchilarga bir vaqtning o'zida ishlatish va samarali boshqarish imkoniyatini yaratadi. Windows OT ning virtualizatsiyada ishlashini amalga oshirishda ko‘p o'zgarishlar va sozlashlarni talab etadi. Bular orasida eng muhimlaridan biri – virtual platformada to‘g‘ri drayverlarni tanlash va sozlashdir. Drayverlar tizimning to‘g‘ri ishlashini ta'minlaydi, shu bilan birga, virtualizatsiya jarayonida ularning mosligi va samaradorligi alohida ahamiyatga ega. Drayverlarning mos kelmasligi tizimning sekinlashishiga yoki hatto ishlamasligiga olib kelishi mumkin. Shu sababli, Windows OT ni virtual platformada sozlashda drayverlar masalasiga e'tibor berish zarur.

Virtualizatsiya muhitida tarmoq sozlamalarini to‘g‘ri amalga oshirish ham muhim ahamiyatga ega. Windows operatsion tizimining virtual platformada ishlashida tarmoqni sozlash nafaqat resurslarni samarali taqsimlash, balki xavfsizlikni ta'minlash uchun ham zarur. Virtualizatsiya muhitida tarmoqni sozlash ko‘plab masalalarni hal qiladi, jumladan, virtual mashinalar orasida to‘g‘ri aloqani ta'minlash, tarmoq orqali ma'lumot uzatishning tezligini oshirish va tarmoq xavfsizligini ta'minlash. Virtualizatsiya jarayonida tarmoq aloqalarini optimallashtirish, foydalanuvchilar uchun yaxshilangan tarmoq muhitini yaratishga yordam beradi. Windows OT ni virtual platformada sozlashda xavfsizlikni ta'minlash eng muhim omillardan biridir. Xavfsizlik choralari virtualizatsiya muhiti uchun alohida ahamiyatga ega, chunki virtual mashinalar o'rtasida izolyatsiya mavjud bo‘lishi kerak. Xavfsizlikni ta'minlash uchun virtualizatsiyada ma'lumotlarni shifrlash, parollarni boshqarish tizimlari va xavfsizlik protokollarini qo‘llash zarur. Tarmoq xavfsizligini ta'minlash ham muhimdir, chunki virtual muhitda ma'lumotlar osonlik bilan tarmoq orqali uzatiladi. Buning uchun virtualizatsiya texnologiyalari ko'plab xavfsizlik choralarini o'z ichiga oladi, masalan, virtual LAN (VLAN) yordamida tarmoqni izolyatsiya qilish va xavfsizlikni yaxshilash.

Shu bilan birga, Windows operatsion tizimining virtual platformada sozlanishi o‘ziga xos xususiyatlarga ega bo‘lib, virtualizatsiya texnologiyalarining rivojlanishi bilan yana-da samarali va xavfsiz bo‘lishi mumkin. Windows OTni virtual platformada sozlashda har bir bosqichda amalga oshirilishi kerak bo‘lgan konfiguratsiyalarni to‘g‘ri bajarish tizimning ishlash samaradorligini oshiradi va xavfsizlikni ta'minlaydi. Virtual mashinalarning to‘g‘ri ishlashi uchun kerakli drayverlar va tarmoq aloqalari o‘rnatilishi, shuningdek, tizimni xavfsiz sozlash zarur. Virtualizatsiya texnologiyalari Windows OTning yangi imkoniyatlarini ochib beradi, lekin ularni to‘g‘ri sozlash hamda xavfsizlikni ta'minlash uchun to‘g‘ri yondoshuvlar talab etiladi. Windows OTni virtual platformada samarali ishlatish uchun drayverlar, tarmoq va xavfsizlikni sozlashning har biri o‘zining o‘rniga ega. Bu jarayonlar to‘g‘ri amalga oshirilsa, virtualizatsiya muhitida Windows operatsion tizimi samarali va xavfsiz ishlaydi. Shunday qilib, Windows OT ning virtual platformada sozlanishi – bu nafaqat tizimning samaradorligini, balki foydalanuvchi tajribasini yaxshilash uchun ham zarur bo‘lgan jarayon. Shu bilan birga, texnologiyalarning rivojlanishi bilan Windows OTning virtualizatsiya uchun imkoniyatlari doimiy ravishda kengayib boradi, bu esa tizimni boshqarishda yangi imkoniyatlarni yaratadi.

Windows operatsion tizimini virtual platformada sozlash nafaqat tizimning samaradorligini oshirish, balki uni xavfsiz va barqaror ishlashini ta'minlash uchun ham muhimdir. Virtualizatsiya texnologiyalari yordamida Windows OSni virtual mashinalarda ishlatish foydalanuvchilarga bir nechta operatsion tizimlarni bir vaqtning o‘zida ishlatish imkoniyatini yaratadi. Biroq, virtualizatsiya muhiti ko‘p hollarda jismoniy tizimdan farq qiladi, shuning uchun Windows OSni virtual platformada to‘g‘ri sozlash zarur. Ushbu jarayonning muhim bosqichlari orasida drayverlar, tarmoq konfiguratsiyasi va xavfsizlik choralari alohida ahamiyatga ega.

Drayverlarning mosligini ta'minlash

Windows operatsion tizimining virtualizatsiya muhitida ishlashi uchun to‘g‘ri drayverlar muhim ahamiyatga ega. Virtualizatsiya muhiti doimiy ravishda jismoniy tizimdan farq qilgani uchun, drayverlar virtual muhitga mos ravishda o‘rnatilishi kerak. Drayverlar tizimning asosiy komponentlari bo‘lib, har qanday apparat qurilmasi va tizimning o‘zaro ishlashini ta'minlaydi.

Virtualizatsiya muhitida, apparatning virtual versiyasi mavjud bo‘lib, bu drayverlarning mosligini tekshirish zarur.

Windows OSda drayverlarning mosligini tekshirishda avvalo quyidagi muhim omillarni hisobga olish kerak:

1. **Virtualizatsiya uchun drayverlar**: Virtualizatsiya uchun maxsus drayverlar, masalan, VMware, Hyper-V, yoki VirtualBox uchun ishlab chiqilgan drayverlar, Windows tizimining to‘g‘ri ishlashini ta'minlashda muhim ahamiyatga ega. Bu drayverlar virtualizatsiya tizimi bilan ishlash uchun optimallashtirilgan bo‘lib, apparatga kirishni ta'minlaydi.
2. **Birinchi darajali qurilmalar uchun drayverlar**: Masalan, virtualizatsiya muhitida ishlayotgan Windows OSda xotira, protsessor, va tarmoq qurilmalari uchun to‘g‘ri drayverlar talab qilinadi. Bu drayverlar virtual qurilmalar bilan uzviy ishlashini ta'minlaydi.
3. **Xotira va saqlash uchun drayverlar**: Virtualizatsiya muhiti xotira va saqlash resurslarini bo‘lishadi, shuning uchun bular uchun drayverlar to‘g‘ri sozlanishi kerak. Xotira resurslarining samarali boshqarilishi tizimning ishlash tezligini oshiradi va qo‘shimcha yukni kamaytiradi.
4. **Xavfsizlikni ta'minlash uchun drayverlar**: Virtualizatsiya muhitida xavfsizlikni ta'minlashda antivirus va firewall drayverlari muhim rol o‘ynaydi. Bu drayverlar tizimni tashqi tahdidlardan himoya qilish uchun zarur.

Drayverlar muammolarini hal qilishda, Windows OS tizimi uchun yangi drayverlarni ishlab chiqarish va yangilash doimiy ravishda amalga oshirilishi kerak. Shuningdek, Windowsning yangi versiyasiga mos ravishda eski drayverlarni yangilash tizimning samarali ishlashini ta'minlaydi.

Tarmoq konfiguratsiyasi

Windows OSni virtual platformada sozlashda tarmoq aloqalarini to‘g‘ri sozlash tizimning barqaror va xavfsiz ishlashini ta'minlash uchun zarur. Virtualizatsiya muhitida tarmoq aloqalarini sozlashda bir nechta muhim nuqtalar mavjud. Bu nuqtalar quyidagilarni o‘z ichiga oladi:

1. **Virtual tarmoq yaratish**: Virtualizatsiya muhiti orqali bir nechta virtual tarmoqlarni yaratish mumkin. Bu virtual tarmoqlar, masalan, Virtual LAN (VLAN) orqali izolyatsiya qilinishi va har bir virtual mashina uchun alohida tarmoq interfeysi taqdim etilishi kerak. Bu usul tarmoq xavfsizligini ta'minlashga yordam beradi.
2. **Tarmoq moslamalari**: Windows OSni virtualizatsiya muhitida tarmoqni sozlashda tarmoqni tahlil qilish va moslamalarini to‘g‘ri o‘rnatish zarur. Virtual tarmoq interfeysi va jismoniy tarmoq orasidagi aloqani sozlash uchun, maxsus sozlamalar va tarmoq manzillari o‘rnatilishi kerak.
3. **Qo‘shimcha xavfsizlik protokollari**: Virtualizatsiya muhiti orqali tarmoq xavfsizligini ta'minlashda IPsec, VPN, va boshqa xavfsizlik protokollarini o‘rnatish kerak. Bular virtual mashinalar orasidagi xavfsiz aloqa uchun zarur.
4. **Tarmoq monitoringi**: Tarmoq monitoringi va trafikni tahlil qilish virtualizatsiya muhitida alohida e'tiborni talab qiladi. Windows OSda tarmoq monitoringi orqali trafikni kuzatib borish, tarmoqdagi nosozliklarni aniqlash va tizimning barqarorligini oshirish mumkin.

Tarmoqni sozlashda tizim resurslaridan samarali foydalanish va tarmoq xavfsizligini ta'minlash zarur. Virtualizatsiya muhiti orqali tarmoq aloqalarining izolyatsiyasi va xavfsizlik choralari yanada mustahkamlanadi.

Xavfsizlikni ta'minlash

Windows OTni virtualizatsiya muhitida xavfsizlikni ta'minlash – bu tizimning eng muhim qismlaridan biridir. Virtualizatsiya orqali bir nechta tizimlar bir vaqtning o‘zida ishlayotgan bo‘lsa, xavfsizlikka oid choralarning to‘g‘ri o‘rnatilishi zarur. Windows OSni virtualizatsiya muhitida xavfsiz ishlatish uchun quyidagi xavfsizlik choralarini ko‘rish lozim:

1. **Ma'lumotlarni shifrlash**: Virtualizatsiya muhitida ma'lumotlarni shifrlash usullari, masalan, BitLocker yoki boshqa shifrlash vositalari orqali, ma'lumotlarni xavfsiz saqlash zarur. Bu usul tizimdagi barcha ma'lumotlarni himoya qiladi va zararli dasturlardan himoya qiladi.
2. **Parollarni boshqarish**: Windows OSda parollarni boshqarish tizimni xavfsiz qilish uchun zarur. Parolning murakkabligi va o‘zgartirilishi doimiy ravishda nazorat qilinishi kerak. Bundan tashqari, ikki faktorli autentifikatsiya (2FA) yordamida xavfsizlikni oshirish mumkin.
3. **Firewall va antiviruslarni o‘rnatish**: Virtualizatsiya muhitida Windows OSni himoya qilish uchun firewall va antiviruslarni o‘rnatish zarur. Bu tizimni tashqi va ichki xavflardan himoya qilishga yordam beradi.
4. **Patchlar va yangilanishlar**: Windows OSning yangilanishlarini o‘rnatish tizimning xavfsizligini oshirishga yordam beradi. Virtualizatsiya muhitida tizimning barcha patchlarini doimiy ravishda yangilab borish kerak. Bu, tizimdagi zaifliklarni bartaraf etadi va xavfsizlikni ta'minlaydi.
5. **Izolyatsiya qilish**: Virtualizatsiya muhitida har bir virtual mashina o‘zining alohida xavfsizlik zonasi bilan ishlaydi. Bu virtual mashinalarning o‘zaro izolyatsiyasini ta'minlaydi, shuning uchun bir virtual mashinada yuzaga kelgan xavf boshqa tizimlarga ta'sir qilmaydi.

Xavfsizlikni ta'minlashda tizimning to‘g‘ri sozlanishi va xavf-xatarlarni tahlil qilish muhimdir. Windows OSni virtual platformada xavfsiz ishlashini ta'minlash uchun yuqoridagi choralardan foydalanish zarur.

Windows operatsion tizimini virtual platformada sozlash bugungi kunda ko‘plab kompaniyalar va foydalanuvchilar uchun samarali va xavfsiz ishlashni ta'minlashning muhim qismiga aylanmoqda. Virtualizatsiya texnologiyalari yordamida Windows OSni turli tizimlarda bir vaqtning o‘zida ishlatish va resurslardan samarali foydalanish imkoniyati yaratilmokda. Biroq, virtualizatsiya muhitida Windows OTni to‘g‘ri sozlash uchun bir nechta muhim bosqichlar mavjud bo‘lib, ular orasida drayverlar, tarmoq konfiguratsiyasi va xavfsizlikni ta'minlash alohida ahamiyatga ega. Birinchi navbatda, Windows OSning virtual platformada ishlashi uchun to‘g‘ri drayverlar juda muhimdir. Virtualizatsiya muhiti jismoniy tizimdan farq qiladi, shuning uchun virtual muhit uchun maxsus drayverlar o‘rnatilishi kerak. Bu drayverlar tizimning samarali ishlashini ta'minlashga yordam beradi. Tizimning to‘g‘ri ishlashi uchun virtualizatsiya muhitiga mos drayverlarning mosligi va samaradorligi alohida ahamiyatga ega. Drayverlar, xususan, xotira, protsessor va saqlash qurilmalari uchun to‘g‘ri sozlangan bo‘lishi kerak. Aks holda, tizimning ishlash tezligi pasayadi yoki resurslar noto‘g‘ri taqsimlanishi mumkin. Virtualizatsiya muhiti uchun Windows OS drayverlarining mosligini tekshirish va

yangilab borish muhimdir. Windows OSda drayverlarning yangilanishi tizimni tez va samarali ishlashini ta'minlaydi, shuningdek, virtual muhitda xavfsizlikni oshirishga yordam beradi.

Tarmoqni sozlash ham Windows OTni virtualizatsiya muhitida ishlatishda muhim bosqichdir. Virtual platformada tarmoq aloqalarini to‘g‘ri sozlash tarmoq resurslarining samarali taqsimlanishini ta'minlaydi va foydalanuvchilar orasidagi aloqalarni optimallashtiradi. Virtualizatsiya muhitida tarmoqni sozlashda, avvalo, virtual LAN (VLAN) kabi texnologiyalardan foydalanish zarur. Bu texnologiyalar yordamida tarmoqni izolyatsiya qilish va virtual mashinalar orasidagi xavfsiz aloqani ta'minlash mumkin. Tarmoqni sozlashda, shuningdek, tarmoq manzillari va aloqa protokollarining to‘g‘ri o‘rnatilishi ham muhimdir. Tarmoqning samarali ishlashi uchun Windows OS tizimi uchun maxsus tarmoq drayverlari va sozlamalar kerak bo‘ladi. Windows OS virtual muhitda tarmoq aloqalarini boshqarish va optimallashtirish foydalanuvchilarni tezkor va ishonchli aloqalar bilan ta'minlash imkoniyatini yaratadi. Xavfsizlikni ta'minlash Windows OTni virtualizatsiya muhitida muvaffaqiyatli ishlashning muhim qismlaridan biridir. Virtualizatsiya muhitida xavfsizlikni ta'minlashda bir nechta omillarni hisobga olish zarur. Birinchi navbatda, tizimdagi barcha ma'lumotlar va resurslar himoya qilinishi kerak. Virtualizatsiya muhitida ishlayotgan Windows OS uchun shifrlash vositalari va antivirus dasturlarini o‘rnatish xavfsizlikni ta'minlash uchun zarur. Shuningdek, virtualizatsiya muhiti orqali bir nechta virtual mashinalar ishlashi bilan xavfsizlikka ta'sir etadigan tahdidlar ko‘payishi mumkin. Shu sababli, har bir virtual mashina alohida xavfsizlik zonasi bo‘lib, ularning o‘rtasidagi izolyatsiya to‘g‘ri sozlanishi kerak. Tarmoq xavfsizligini ta'minlash uchun tarmoqning izolyatsiyasi va ma'lumotlarni shifrlash texnologiyalarini qo‘llash zarur.

Windows OSni virtual platformada xavfsiz ishlatish uchun parollarni boshqarish tizimlari, ikki faktorli autentifikatsiya (2FA) va boshqa xavfsizlik choralari qo‘llanilishi kerak. Parolning murakkabligi va o‘z vaqtida yangilanishi tizim xavfsizligini oshirishga yordam beradi. Tizimning to‘g‘ri konfiguratsiyasini amalga oshirish va xavfsizlik protokollarini o‘rnatish Windows OSni virtualizatsiya muhitida xavfsiz ishlashini ta'minlaydi. Xavfsizlikni oshirishda yangilanishlar va patchlar o‘rnatilishi, tizimning zaif tomonlari va xatoliklarini bartaraf etishga yordam beradi. Virtualizatsiya jarayonida Windows OSni sozlashning bir nechta muhim bosqichlari amalga oshirilishi kerak, jumladan, tizim drayverlarini to‘g‘ri sozlash, tarmoq aloqalarini optimallashtirish va xavfsizlikni ta'minlash. Bu jarayonlarni amalga oshirish tizimning samaradorligini oshiradi, foydalanuvchi tajribasini yaxshilaydi va xavfsizlikni ta'minlaydi. Windows OTni virtualizatsiya muhitida ishlatish orqali foydalanuvchilar o‘z ish jarayonlarini yanada tez va samarali amalga oshirish imkoniyatiga ega bo‘ladilar. Shuningdek, virtualizatsiya texnologiyalari yordamida bir nechta tizimni bir vaqtda boshqarish va resurslardan samarali foydalanish imkoniyatini yaratadi. Bundan tashqari, virtualizatsiya texnologiyalari yordamida Windows OSni turli tizimlarda ishlatish kompaniyalar va tashkilotlarga resurslarni samarali boshqarish, xizmatlarni tezda amalga oshirish va tizimlarning barqarorligini ta'minlashda yordam beradi. Virtualizatsiya jarayonida tizimni optimallashtirish va xavfsizlikni ta'minlashning to‘g‘ri usullari tizimning uzoq muddatli ishlashini ta'minlaydi.

Xulosa qilib aytganda, Windows operatsion tizimini virtual platformada to‘g‘ri sozlash jarayoni muhim bosqichlarni o‘z ichiga oladi, jumladan drayverlar, tarmoq va xavfsizlikni ta'minlash. Har bir bosqichni to‘g‘ri bajarish Windows OSning samarali ishlashini ta'minlaydi

va foydalanuvchilar uchun qulay va xavfsiz ish muhiti yaratadi. Virtualizatsiya texnologiyalarining rivojlanishi bilan Windows OSni virtualizatsiya muhitida ishlatish imkoniyatlari yanada kengayadi va tizimlarni boshqarishda yangi imkoniyatlarni yaratadi. Shunday qilib, Windows OTni virtualizatsiya muhitida samarali va xavfsiz ishlatish uchun barcha zaruriy sozlashlar amalga oshirilishi kerak.

Foydalanilgan adabiyotlar:

1. Umarov B. RAQAMLI TEXNOLOGIYALAR VOSITASIDA PEDAGOGLARNING PROFESSIONAL KOMPETENTLIGINI RIVOJLANTIRISH MAZMUNI //Евразийский журнал математической теории и компьютерных наук. – 2023. – Т. 3. – №. 5. – С. 87-93.
2. Azizovich U. B. PRINCIPLES OF FORMING TEACHER COMPETENCE THROUGH INNOVATIVE TECHNOLOGIES. Finland International Scientific Journal of Education //Social Science & Humanities. – 2023. – Т. 11. – №. 5. – С. 823-828.
3. Azizovich U. B. PEDAGOGICAL-PSYCHOLOGICAL PRINCIPLES OF THE FORMATION OF PROFESSIONAL COMPETENCE //Confrencea. – 2023. – Т. 6. – №. 6. – С. 204-212.
4. Azizovich U. B., Zarifjon o’g’li X. N. BULUT TEXNOLOGIYALARINING AFZALLIKLARI VA KAMCHILIKLARI //TA’LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 46-54.
5. Azizovich U. B., Rustamjon o‘g‘li R. Z. MA’LUMOTLARNI SHIRFLASH TENALOGIYALARI VA XAVFSIZLIK STANDARTLARI //TA’LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 105-108.
6. Azizovich U. B. et al. OLAP TIZIMLARINING ASOSIY PRINSIPLARI //TA’LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 81-86.
7. Azizovich U. B. THE DEVELOPMENT OF PROFESSIONAL COMPETENCY OF TEACHERS IN EDUCATIONAL TECHNOLOGY BASED ON DIGITAL TECHNOLOGIES //Eurasian Journal of Mathematical Theory and Computer Sciences. – 2024. – Т. 4. – №. 7. – С. 11-14.
8. Azizovich U. B. et al. MASHINALI O ‘QITISHDA REGRESSIYA ENG KICHIK KVADRATLAR USULINI QO ‘LLASH //INNOVATION IN THE MODERN EDUCATION SYSTEM. – 2024. – Т. 5. – №. 46. – С. 266-270..