

Válasz

Dr. Kő Andrea Professzor Asszony

„Zsarolóvírus-támadások időkritikus felismerése gépi tanulás alkalmazási lehetőségeinek vizsgálatával centralizált fájl tárolási környezetekben”

című PhD értekezéshez írt

opponensi véleményére

Mindenekelőtt szeretném kifejezni őszinte köszönetemet Dr. Kő Andrea Professzor Asszonynak azért a figyelemért és alaposságért, amellyel dolgozatomat elolvasta és értékelte. Részletes és körültekintő opponensi véleménye számomra megtiszteltetés, különösen azért, mert a bíráló nem csupán a dolgozat egyes részleteire, hanem annak koncepciójának, módszertani és szerkezeti kérdéseire is kiterjedt. A megfogalmazott kritikai észrevételeket és javaslatokat köszönettel fogadom, és az érintett kérdések tekintetében a bíráló megállapításaival egyetértek. Külön köszönöm, hogy opponensem több olyan pontra is ráirányította a figyelmet, amelyek a dolgozat egyes állításainak pontosítását, bizonyos összefüggések árnyaltabb bemutatását, illetve a dolgozat szerkezetének és felépítésének továbbfejlesztését lehetővé tették. Meggyőződésem, hogy az észrevételek és javaslatok jelentősen hozzájárultak a dolgozat, és ezáltal a tézisek végső formájának és tartalmának kialakításához. Az opponensi vélemény ugyanakkor nemcsak a jelen dolgozat továbbfejlesztése szempontjából jelentett értékes segítséget számomra, hanem olyan szakmai szempontokat is adott, amelyek további kutatómunkám során is hasznosíthatók lesznek. A dolgozathoz kapcsolódó kérdésekre és észrevételekre az alábbiakban igyekszem tételesen, a dolgozatban bemutatott kutatási eredményekre és módszertani megfontolásokra támaszkodva, legjobb tudásom szerint válaszolni.

1. Milyen módosításokra lenne szükség az ötödik fejezetben ismertetett mérés megismétléséhez, ha az újabb Windows Server verziókat (Windows Server 2022, vagy Windows Server 2025) vennénk figyelembe a Windows Server 2019 helyett?

A dolgozatban a Windows Server 2019 tudatosan referenciarendszerként szerepelt. A mérés célja nem pusztán a két operációs rendszer nyers sebességének összevetése volt, hanem annak vizsgálata, hogy az ARDS fájlkiszolgáló a hozzáadott biztonsági mechanizmusok mellett milyen teljesítményt nyújt egy tipikus Windows-alapú referencia-környezethez képest. Windows Server 2022-re vagy 2025-re történő átálláskor nem lenne helyes egyszerűen csak az operációs rendszert lecserélni, és ugyanazokat a számításokat újra elvégezni. A Windows Server 2019, 2022, 2025 és a SAMBA 4.19.3 alapvetően egyaránt támogatja az SMB 3.1.1-et, ezért a protokoll alapvető verzióváltása nem teszi szükségessé az ARDS fájlkiszolgáló módosítását. Ugyanakkor a Windows Server 2022 és különösen a 2025 új SMB verzió biztonsági funkciói miatt a referencia-környezet pontos konfigurációját már rögzíteni kell. Az ARDS fájlkiszolgáló valamint a Windows referenciakörnyezetek

összehasonlításának módszertani érvényességéhez azonos SMB-dialektus és lehetőség szerint azonos biztonsági szolgáltatási szint mellett kellene elvégezni a mérést. Ahhoz, hogy az új SMB verzió nyújtotta biztonsági funkciókat a mérések során kihasználhassuk szükséges a kliens oldali operációs rendszerek korszerű és aktív frissítésekkel támogatott verzióit használni. Így a korábbi Windows 7 x64 SP1, Windows 10 x64 Pro 21H2 és Ubuntu 22.04.4 LTS verziókat Windows 10 22H2, Windows 11 26H1, Ubuntu 26.04.1 LTS kiadásokra cserélném. A referencia-rendszer kiválasztását ebben az esetben nem kizárólag az operációs rendszer verziója, hanem annak támogatottsága, vállalati alkalmazhatósága, SMB-kompatibilitása és az adott időszakban jellemző KKV-üzemeltetési gyakorlat alapján indokolnám meg. A mérések során a reprodukálhatóság egyik fontos eleme az volt, hogy a hardver- és szoftverkörnyezet dokumentált, a fájlvitelek ismételten történnek, és az eredményeket átlaggal, szórással, illetve a tranziens értékek kiszűrésének segítségével értékeltem, ezért ezt a módszertani struktúrát nem változtatnám meg. Újra kellene azonban definiálni és dokumentálni a kiszolgálók hardveres és szoftveres konfigurációját, az SMB-beállításokat, valamint azokat a biztonsági szolgáltatásokat – például a vírusvédelmet, a VSS-t vagy a BitLockert –, amelyek a mérési eredményeket befolyásolhatják és részletesebb képet adhatnak a teljesítményekről. Véleményem szerint a mérési eljárás többi lényeges eleme változatlanul fenntartható lenne, tehát ugyanazokat a fájlméreteket, fájlműveleteket, az 1 és 10 Gbit/s-os hálózati sávszélességet, a mérési módszertant, valamint referencia-alapú teljesítményindikátort alkalmaznám. Összefoglalva: a mérés megismétléséhez a referencia-rendszert és annak konfigurációját kellene aktualizálni mind kliens, mind pedig kiszolgálói oldalon, az alkalmazott mérési módszertan és a teljesítményindikátor lényegében változtatás nélkül megtartható lenne.

2. Kellene-e módosítani az ARDS fogalmi modellen egy ilyen esetben és ha igen mit?

Az ARDS modell alapvetően nem a teljesítményméréshez használt referenciakörnyezetre épülő megoldásként van definiálva, hanem bizonyos védelmi mechanizmusok (pl.: pillanatfelvételek készítése, adatszivárgás észlelése, fájlműveletek monitorozása, honeypot meghajtók monitorozása, IDS/IPS) implementálását ajánlja az infrastruktúra meghatározott pontjain. A modell tehát koncepcionálisan nem a Windows Server 2019-hez kötött, ezért ez operációsrendszer-független koncepcionális szint. Így másik referencia kiszolgáló esetén az ARDS modell változatlan maradna, csupán új referencia környezettel hasonlítanánk össze az egyik komponensének egy lehetséges implementációját, de a vizsgálat fókusza továbbra is a fájlkiszolgálón alkalmazott védelmi mechanizmusok teljesítményhatásán lenne. Amit viszont pontosítanék, az a fogalmi modell és a konkrét technológiai megvalósítás közötti hangsúlyozott különbségtétel. Lényeges lenne a fogalmi modell definiálásakor kiemelni, hogy az operációs rendszer, a fájlrendszer (OpenZFS), a fájlkiszolgáló komponens (SAMBAs), illetve a konkrét biztonsági megoldások a modell megvalósításának eszközei, nem pedig annak fogalmi alapjai. Összefoglalva: álláspontom szerint önmagában a Windows Server verziójának megváltozása miatt az ARDS fogalmi modelljét nem kellene módosítani. Ennek oka, hogy az ARDS modell lényegi eleme nem maga az alkalmazott operációs rendszer, hanem a központi fájlkiszolgáló védelmi koncepciója, így például a

fájlműveletek monitorozása, a detekció, az adatvédelem és a helyreállítás támogatása. Ez azt jelenti, hogy ha a Windows Server 2019 helyére 2022 vagy 2025 kerülne, akkor a referencia-környezet és a mérési konfiguráció változna, de maga az ARDS architekturális koncepciója változatlanul alkalmazható maradna.

Végül még egyszer köszönöm Professzor Asszony támogató véleményezését és téziseim elfogadását. Kérem tisztelt Professzor Asszonyt, hogy a bírálóiban felvetett kérdésekre, javaslatokra adott válaszaimat, magyarázataimat szíveskedjen elfogadni.

Veszprém, 2026. szeptember 28.



Arányi Gábor

doktorjelölt,

okl. mérnökinformatikus