Windows Server 2022 funkciói

Ez a leírás a Windows Server 2022 néhány új funkcióját ismerteti. A Windows Server 2022 a Windows Server 2019 erős alapjaira épül, és számos újítást hoz három kulcstémában: biztonság, Azure hibrid integráció és felügyelet, valamint alkalmazásplatform. Ezenkívül a Windows Server 2022 Datacenter: Azure Edition segít a felhő előnyeinek kihasználásában a virtuális gépek naprakészen tartásához, miközben minimalizálja az állásidőt.

Biztonság

A Windows Server 2022 új biztonsági képességei a Windows Server egyéb biztonsági lehetőségeit kombinálják több területen, hogy mélyreható védelmet nyújtsanak a fejlett fenyegetések ellen. A Windows Server 2022 fejlett többrétegű biztonsága átfogó védelmet nyújt, amelyre a kiszolgálóknak manapság szükségük van.

Biztonságos mag szerver

Egy OEM-partner tanúsítvánnyal rendelkező biztonságos magú szerverhardvere további biztonsági védelmet nyújt, amely hasznos a kifinomult támadások ellen. Ez nagyobb biztonságot nyújthat a kritikus adatok kezelése során a leginkább adatérzékeny iparágakban. A Secured-core szerver hardvert, firmware-t és illesztőprogramot használ a Windows Server fejlett biztonsági funkcióinak engedélyezéséhez. E szolgáltatások közül sok elérhető a Windows Secured-core PC-ken , és mostantól a Secured-core szerverhardverrel és a Windows Server 2022-vel is elérhető.

Hardveres bizalom gyökere

A Trusted Platform Module 2.0 (TPM 2.0) biztonságos kriptoprocesszor chipek biztonságos, hardver alapú tárolót biztosítanak az érzékeny kriptográfiai kulcsok és adatok számára, beleértve a rendszerintegritás méréseket is. A TPM 2.0 képes ellenőrizni, hogy a kiszolgálót legitim kóddal indították-e el, és a későbbi kódvégrehajtással megbízható-e. Ezt hardveres bizalmi alapnak nevezik, és olyan szolgáltatások használják, mint a BitLocker meghajtótitkosítás .

Firmware védelem

A firmware magas jogosultságokkal fut, és gyakran láthatatlan a hagyományos vírusirtó megoldások számára, ami a firmware-alapú támadások számának növekedéséhez vezetett. A biztonságos mag szerverprocesszorok támogatják a rendszerindítási folyamatok mérését és ellenőrzését a Dynamic Root of Trust for Measurement (DRTM) technológiával , valamint az illesztőprogramok memóriához való hozzáférésének elkülönítését közvetlen memóriahozzáférés (DMA) védelemmel .

UEFI biztonságos rendszerindítás

Az UEFI biztonságos rendszerindítás egy biztonsági szabvány, amely megvédi szervereit a rosszindulatú rootkitektől. A biztonságos rendszerindítás biztosítja, hogy a szerver csak a hardvergyártó által megbízható firmware-t és szoftvert indítsa el. A kiszolgáló indításakor a firmware ellenőrzi az egyes rendszerindítási összetevők aláírását, beleértve a firmware-illesztőprogramokat és az operációs rendszert. Ha az aláírások érvényesek, a szerver elindul, és a firmware átadja az irányítást az operációs rendszernek.

Virtualizáció alapú biztonság (VBS)

A biztonságos mag kiszolgálók támogatják a virtualizáció alapú biztonságot (VBS) és a hypervisor alapú kódintegritást (HVCI). A VBS hardveres virtualizációs szolgáltatásokat használ a biztonságos memóriaterület létrehozására és elkülönítésére a normál operációs rendszertől, védve ezzel a kriptovaluta-bányászati támadások során használt sebezhetőségek egész osztályával szemben. A VBS lehetővé teszi a Credential Guard használatát is , ahol a felhasználói hitelesítő adatok és titkok egy virtuális tárolóban vannak tárolva, amelyhez az operációs rendszer nem férhet hozzá közvetlenül.

A HVCI a VBS segítségével jelentősen megerősíti a kódintegritási irányelvek betartatását, beleértve a kernel mód integritását is, amely az összes kernelmódú illesztőprogramot és bináris fájlt ellenőrzi egy virtualizált környezetben az indítás előtt, megakadályozva ezzel az aláíratlan illesztőprogramok vagy rendszerfájlok rendszermemóriába való betöltését.

A Kernel Data Protection (KDP) csak olvasható memóriavédelmet biztosít a nem végrehajtható adatokat tartalmazó kernelmemória számára, ha a memórialapokat a Hypervisor védi. A KDP megvédi a Windows Defender System Guard futási környezet kulcsfontosságú struktúráit a manipulációtól.

Biztonságos kapcsolat

Szállítás: A HTTPS és a TLS 1.3 alapértelmezés szerint engedélyezve van a Windows Server 2022 rendszeren

A biztonságos kapcsolatok a mai összekapcsolt rendszerek középpontjában állnak. A Transport Layer Security (TLS) 1.3 az internet leggyakrabban alkalmazott biztonsági protokolljának legújabb verziója, amely titkosítja az adatokat, hogy biztonságos kommunikációs csatornát biztosítson két végpont között. A HTTPS és a TLS 1.3 mostantól alapértelmezés szerint engedélyezve van a Windows Server 2022 rendszeren, védve a kiszolgálóhoz csatlakozó ügyfelek adatait. Megszünteti az elavult kriptográfiai algoritmusokat, növeli a biztonságot a régebbi verziókhoz képest, és célja a kézfogás minél nagyobb részének titkosítása. További információ a támogatott TLS-verziókról és a támogatott titkosítási csomagokról .

Bár a TLS 1.3 a protokollrétegben alapértelmezés szerint engedélyezve van, az alkalmazásoknak és a szolgáltatásoknak is aktívan támogatniuk kell azt. További információért tekintse meg az adott alkalmazások és szolgáltatások dokumentációját. A Microsoft Security blog további részleteket tartalmaz A Transport Layer Security (TLS) következő szintre emelése a TLS 1.3-mal című bejegyzésében .

Biztonságos DNS: Titkosított DNS-névfeloldási kérések DNS-over-HTTPS-sel

A Windows Server 2022 DNS-ügyfele mostantól támogatja a DNS-over-HTTPS-t (DoH), amely a HTTPS-protokoll használatával titkosítja a DNS-lekérdezéseket. Ez segít megőrizni a forgalmát a lehető legprivátabban azáltal, hogy megakadályozza a lehallgatást és a DNS-adatok manipulálását. További információ a DNS-ügyfél DoH használatára való konfigurálásáról .

Szerverüzenetblokk (SMB): SMB AES-256 titkosítás a leginkább biztonságtudatosak számára

A Windows Server mostantól támogatja az AES-256-GCM és az AES-256-CCM kriptográfiai csomagokat az SMB-titkosításhoz. A Windows automatikusan egyezteti ezt a fejlettebb titkosítási módszert, amikor egy másik számítógéphez csatlakozik, amely szintén támogatja, és a csoportházirenden keresztül is előírható. A Windows Server továbbra is támogatja az AES-128 szabványt az alacsonyabb szintű kompatibilitás érdekében. Az AES-128-GMAC aláírás mostantól szintén felgyorsítja az aláírási teljesítményt.

SMB: Kelet-Nyugat SMB titkosítási vezérlők a belső fürtkommunikációhoz

A Windows Server feladatátvételi fürtjei mostantól támogatják a csomóponton belüli tárolási kommunikáció titkosításának és aláírásának részletes vezérlését a fürt megosztott kötetei (CSV) és a tárolóbusz-réteg (SBL) számára. Ez azt jelenti, hogy a Storage Spaces Direct használatakor dönthet úgy, hogy titkosítja vagy aláírja a kelet-nyugati irányú kommunikációt magán a fürtön belül a nagyobb biztonság érdekében.

SMB Direct és RDMA titkosítás

Az SMB Direct és az RDMA nagy sávszélességet és alacsony késleltetésű hálózati struktúrát biztosít olyan munkaterhelésekhez, mint a Storage Spaces Direct, Storage Replica, Hyper-V, Scale-out File Server és SQL Server. Az SMB Direct a Windows Server 2022 rendszerben mostantól támogatja a titkosítást. Korábban az SMB-titkosítás engedélyezése letiltotta a közvetlen adatelhelyezést; ez szándékos volt, de komolyan befolyásolta a teljesítményt. Mostantól az adatok titkosítva vannak az adatok elhelyezése előtt, ami jóval kisebb teljesítménycsökkenést eredményez, miközben AES-128 és AES-256 védett csomagvédelmet ad.

Az SMB-titkosításról, az aláírásgyorsításról, a biztonságos RDMA-ról és a fürttámogatásról az SMB biztonsági fejlesztései oldalon talál további információt .

SMB a QUIC felett

Az SMB over QUIC frissíti az SMB 3.1.1 protokollt a Windows Server 2022 Datacenter: Azure Edition rendszerben és a támogatott Windows-ügyfelekben, hogy a TCP helyett a QUIC protokollt használják. Az SMB over QUIC és a TLS 1.3 használatával a felhasználók és alkalmazások biztonságosan és megbízhatóan hozzáférhetnek az Azure-ban futó szélső fájlkiszolgálók adataihoz. A mobil- és távmunkás felhasználóknak többé nincs szükségük VPN-re, hogy SMB-n keresztül hozzáférjenek fájlszervereikhez, ha Windows rendszert használnak. További információ az SMB over QUIC dokumentációjában található .

Azure hibrid képességei

Növelheti hatékonyságát és agilitását a Windows Server 2022 beépített hibrid képességeivel, amelyek lehetővé teszik az adatközpontok Azure-ba való kiterjesztését minden eddiginél egyszerűbben.

Azure Arc-kompatibilis Windows-kiszolgálók

Az Azure Arc-kompatibilis kiszolgálók a Windows Server 2022 rendszerrel helyszíni és többfelhős Windows-kiszolgálókat hoznak az Azure-ba az Azure Arc segítségével. Ezt a felügyeleti élményt úgy tervezték, hogy összhangban legyen a natív Azure virtuális gépek kezelésével. Ha egy hibrid gép csatlakozik az Azure-hoz, akkor csatlakoztatott géppé válik, és erőforrásként kezeli az Azure-ban. További információ az Azure Arc engedélyezése szerverek dokumentációjában található .

Windows Admin Center

A Windows Felügyeleti Központban a Windows Server 2022 kezelését lehetővé tévő fejlesztések magukban foglalják a fent említett biztonságos magszolgáltatások jelenlegi állapotának jelentését, és adott esetben lehetővé teszik az ügyfelek számára a szolgáltatások engedélyezését. Ezekről és a Windows Felügyeleti Központ számos további fejlesztéséről a Windows Felügyeleti Központ dokumentációjában talál további információt .

Azure Automanage – Hotpatch

Az Azure Automanage részét képező Hotpatch a Windows Server 2022 Datacenter: Azure Edition rendszerben támogatott. A Hotpatching egy új módja a frissítések telepítésének új Windows Server Azure Edition virtuális gépekre (VM-ekre), amelyek

nem igényelnek újraindítást a telepítés után. További információ az Azure Automanage dokumentációjában található .

Alkalmazási platform

Számos platformjavítás létezik a Windows-tárolókhoz, beleértve az alkalmazás-kompatibilitást és a Kubernetes Windows-tárolók élményét. A jelentős fejlesztés a Windows Container képméretének akár 40%-os csökkentése is, ami 30%-kal gyorsabb indítási időt és jobb teljesítményt eredményez.

Mostantól az Azure Active Directorytól függő alkalmazásokat is futtathat csoportos felügyelt szolgáltatások fiókjaival (gMSA) , anélkül, hogy a tartományhoz csatlakozna a tároló gazdagéphez , és a Windows-tárolók mostantól támogatják a Microsoft Distributed Transaction Control (MSDTC) és a Microsoft Message Queuing (MSMQ) funkciót.

Számos további fejlesztés is leegyszerűsíti a Windows Container élményét a Kubernetes használatával. Ezek a fejlesztések magukban foglalják a csomópont-konfigurációhoz szükséges gazdagép-folyamat-tárolók támogatását, az IPv6-ot, valamint a Calico-val való konzisztens hálózati házirend megvalósítását.

A platform fejlesztése mellett a Windows Felügyeleti Központ is frissült, hogy megkönnyítse a .NET-alkalmazások konténerbe helyezését. Miután az alkalmazás egy tárolóban van, az Azure Container Registry-ben tárolhatja, majd üzembe helyezheti más Azure-szolgáltatásokban, beleértve az Azure Kubernetes szolgáltatást is.

Az Intel Ice Lake processzorok támogatásával a Windows Server 2022 támogatja az üzleti szempontból kritikus és nagyszabású alkalmazásokat, például az SQL Servert, amelyek akár 48 TB memóriát és 2048 logikai magot igényelnek, amelyek 64 fizikai foglalaton futnak. A bizalmas számítástechnika az Intel Secured Guard Extension (SGX) segítségével az Intel Ice Lake-en javítja az alkalmazások biztonságát azáltal, hogy védett memóriával elkülöníti az alkalmazásokat egymástól.

Egyéb fontos jellemzők

Beágyazott virtualizáció AMD processzorokhoz

A beágyazott virtualizáció egy olyan szolgáltatás, amely lehetővé teszi a Hyper-V futtatását egy Hyper-V virtuális gépen (VM) belül. A Windows Server 2022 támogatja az AMD processzorokat használó beágyazott virtualizációt, így több hardverválasztékot biztosít az Ön környezetéhez. További információ a beágyazott virtualizációs dokumentációban található .

Microsoft Edge böngésző

A Microsoft Edge része a Windows Server 2022-nek, amely az Internet Explorert váltja fel. A nyílt forráskódú Chromiumra épül, és a Microsoft biztonsága és innovációja támogatja. Használható a Desktop Experience telepítési lehetőségekkel rendelkező szerverrel. További információ a Microsoft Edge Enterprise dokumentációjában található . Vegye figyelembe, hogy a Microsoft Edge a Windows Server többi részétől eltérően a modern életciklust követi támogatási életciklusa során. A részletekért lásd a Microsoft Edge életciklus-dokumentációját .

Hálózati teljesítmény

UDP teljesítménybeli fejlesztések

Az RTP és az egyéni (UDP) streaming- és játékprotokollok növekvő népszerűsége miatt az UDP egyre népszerűbb protokolllá válik, amely egyre nagyobb hálózati forgalmat hordoz. Az UDP-re épülő QUIC protokoll az UDP teljesítményét a TCP-vel egyenrangú szintre hozza. Figyelemre méltó, hogy a Windows Server 2022 tartalmazza az UDP-szegmentálási kiterhelést (USO). Az USO áthelyezi az UDP-csomagok CPU-ról a hálózati adapter speciális hardverére történő küldéséhez szükséges munka nagy részét. Az USO-t kiegészíti az UDP Receive Side Coalescing (UDP RSC), amely egyesíti a csomagokat, és csökkenti az UDP-feldolgozáshoz szükséges CPU-használatot. Emellett több száz fejlesztést hajtottunk végre az UDP adatútvonalon, mind az adásban, mind a vételben. A Windows Server 2022 és a Windows 11 egyaránt rendelkezik ezzel az új képességgel.

TCP teljesítménybeli fejlesztések

A Windows Server 2022 a TCP HyStart++ -t használja a kapcsolat indítása közbeni csomagvesztés csökkentésére (különösen a nagy sebességű hálózatokban), a RACK -et pedig az újraküldési időkorlátok (RTO) csökkentésére. Ezek a szolgáltatások alapértelmezés szerint engedélyezve vannak a szállítási veremben, és simább hálózati adatáramlást biztosítanak jobb teljesítmény mellett nagy sebességnél. A Windows Server 2022 és a Windows 11 egyaránt rendelkezik ezzel az új képességgel.

Hyper-V virtuális kapcsoló fejlesztések

A Hyper-V virtuális kapcsolói a frissített Receive Segment Coalescing (RSC) funkcióval bővültek. Ez lehetővé teszi a hypervisor hálózat számára, hogy egyesítse a csomagokat, és egy nagyobb szegmensként dolgozza fel. A CPU-ciklusok lecsökkennek, és a szegmensek a teljes adatútvonalon összevonva maradnak, amíg a kívánt alkalmazás fel nem dolgozza őket. Ez jobb teljesítményt jelent mind a külső gazdagépről érkező hálózati forgalomban, amelyet egy virtuális hálózati kártya fogad,

mind a virtuális hálózati kártyáról egy másik virtuális hálózati kártyára ugyanazon a gazdagépen.

Tárolás

Tárhely-migrációs szolgáltatás

A Windows Server 2022 Storage Migration Service továbbfejlesztései megkönnyítik a tárhely áttelepítését a Windows Serverre vagy az Azure-ba több forráshelyről. A Storage Migration Server Orchestrator Windows Server 2022 rendszeren való futtatásakor a következő szolgáltatások érhetők el:

- Helyi felhasználók és csoportok áttelepítése az új kiszolgálóra.
- Áttelepítheti a tárhelyet feladatátvevő fürtökről, áttérhet feladatátvevő fürtökre, és migrálhat az önálló kiszolgálók és a feladatátvevő fürtök között.
- Tárhely migrálása egy Sambát használó Linux-kiszolgálóról.
- Az Azure File Sync használatával egyszerűbben szinkronizálhatja az áttelepített megosztásokat az Azure-ba.
- Migráció új hálózatokra, például az Azure-ra.
- A NetApp CIFS-kiszolgálók migrálása NetApp FAS-tömbökről Windows-kiszolgálókra és -fürtökre.

Állítható tárolási javítási sebesség

A felhasználó által beállítható tárhelyjavítási sebesség a Storage Spaces Direct új funkciója, amely az adatmásolatok javításához (rugalmasság), vagy az aktív munkaterhelések futtatásához (teljesítmény) biztosít erőforrások lefoglalásával az adatok újraszinkronizálási folyamatát. Ez javítja a rendelkezésre állást, és lehetővé teszi a fürtök rugalmasabb és hatékonyabb kiszolgálását.

Gyorsabb javítás és újraszinkronizálás

A tárhely javítása és újraszinkronizálása olyan események után, mint például a csomópontok újraindítása és a lemezhibák, most kétszer gyorsabb. A javítások időbeli eltérése kisebb, így biztosabb lehet abban, hogy mennyi ideig tart a javítás, ami az adatkövetés részletesebbé tételével valósult meg. Ez csak az áthelyezni kívánt adatokat mozgatja, és csökkenti a felhasznált rendszererőforrásokat és az időt.

Tárolóbusz gyorsítótár tárolóterületekkel az önálló szervereken

A tárolóbusz gyorsítótár már elérhető az önálló szerverekhez. Jelentősen javíthatja az olvasási és írási teljesítményt, miközben megőrzi a tárolás hatékonyságát és alacsonyan tartja a működési költségeket. A Storage Spaces Direct megvalósításához

hasonlóan ez a funkció a gyorsabb adathordozókat (például NVMe vagy SSD) lassabb adathordozókkal (például HDD-vel) köti össze rétegek létrehozásához. A gyorsabb médiaréteg egy része a gyorsítótár számára van fenntartva. További információért lásd: Tárolóbusz-gyorsítótár engedélyezése tárolóterületekkel önálló kiszolgálókon .

ReFS fájlszintű pillanatképek

A Microsoft Resilient File System (ReFS) most már tartalmazza a fájlok pillanatfelvételének lehetőségét egy gyors metaadat-művelet segítségével. A pillanatképek abban különböznek a ReFS blokkklónozástól , hogy a klónok írhatók, míg a pillanatképek csak olvashatók. Ez a funkció különösen hasznos VHD/VHDX-fájlokkal rendelkező virtuális gépek biztonsági mentési forgatókönyveiben. A ReFS pillanatképek egyedülállóak abban, hogy a fájl méretétől függetlenül állandó időt vesznek igénybe. A pillanatképek támogatása elérhető a ReFSUtilban vagy API-ként.

SMB tömörítés

Az SMB továbbfejlesztése a Windows Server 2022 és a Windows 11 rendszerben lehetővé teszi a felhasználók vagy alkalmazások számára, hogy tömörítsék a fájlokat a hálózaton történő átvitel során. A felhasználóknak többé nem kell manuálisan tömöríteni a fájlokat a lassabb vagy zsúfoltabb hálózatokon való sokkal gyorsabb átvitel érdekében. A részletekért lásd: SMB tömörítés .