Vállalati digitalizáció a felhőben a Microsoft Azure használatával

Microsoft Azure ALLWIN Trust driven development

Tartalom

01
Bevezetés

A mai adatvezérelt világunkban a biztonságos felhőalapú rendszerek minden vállalkozás megkerülhetetlen alappillérévé váltak. A digitális transzformáció az egyik legideálisabb eszköz a vállalat fejlesztésére és növekedésére. Szerencsére ezt az átállást nem kell a vezetőknek és menedzsereknek segítség nélkül megoldaniuk, ugyanis már számos piacvezető vállalat kínál transzparens, rugalmas és testre szabható megoldást a fejlődni kívánó cégek számára.

Ebben az e-book-ban megmutatjuk, hogy a Microsoft felhőmegoldásai hogyan járulnak hozzá a vállalati digitalizációhoz és a piaci pozíció megtartásához. A következő oldalakon olyan témaköröket fejtegetünk, mint a vállalati digitalizáció üzleti előnyei, vagy olyan gyakran feltett kérdéseket, mint a skálázhatóság, a kiberbiztonság, az automatizáció és a rendelkezésre állás.

02

Mi a felhőszolgáltatás és mi a Microsoft Azure?

02

A Microsoft Azure léptéke

Mit nyújt ezen kívül a Microsoft?

IaaS, PaaS, SaaS
Ügyfélút a felhő felé

A felhőszolgáltatás azt jelenti, hogy a vállalatnak nincs szüksége sem saját infrastruktúra kialakítására (adattárolás,hálózat, erőforrások, szoftverek), sem pedig az infrastruktúrát üzemeltető IT csapatra, mert ezt a felhőszolgáltató biztosítja. Így jelentős megtakarítás érhető el, és az egyes bérelt erőforrások is rugalmasan kezelhetőek.

A Microsoft Azure léptéke

A Microsoft Azure globális infrastruktúrája több mint 200 adatközpontból áll, amelyeket egy összefüggő hálózat köt össze, magas rendelkezésre állást, skálázhatóságot biztosítva. A Microsoft ügyfelei könnyen kiválaszthatják, hogy mely régióban kívánják üzemeltetni az alkalmazásaikat, amelyre lehetőség van egyszerre több régióban is.

Ha valaki kíváncsi a Microsoft Azure globális hálózatára, a következő oldalon egy nagyon látványos formában meg is tekintheti: https://infrastructuremap.microsoft.com/explore

Mit nyújt ezen kívül a Microsoft?

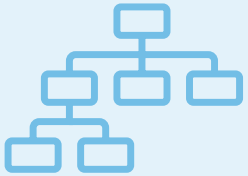
A Microsoft Magyarország meg tudja azt valósítani, hogy tetszőleges telephelyhez kialakított hálózathoz olyan szolgáltatásokat ad hozzá, amelyeket saját telephelyen vagy nem gazdaságos fenntartani, vagy a megfelelő szakemberek, esetleg speciális tudás hiánya miatt ezek létrehozása nem lehetséges.

A felhőszolgáltatás szinte az összes vállalat mindennapi életének szerves részét képezi, csak sokan nem veszik észre, hogy ők ezt a megoldást már alkalmazzák. Ilyen például az, amikor egy flotta szolgáltatótól gépjárművet vesznek igénybe. Ilyenkor a vállalatnak nem egy autóra van szüksége, hanem egy megoldásra, amivel különböző helyre eljuthatnak egy-egy üzemeltetett szolgáltatást igénybe véve. Ez az a probléma, amire a felhő választ ad.

IaaS, PaaS, SaaS - Ügyfélút a felhő felé

1. Infrastructure as a Service:

Ebben az esetben szervereket, adattárházakat és különböző hálózati megoldásokat is bérelhetnek a vállalatok az Azure-től, de minden mást, mint például a szoftvert - annak fejlesztését és karbantartását - a saját IT csapatnak kell kezelnie.



2. Platform as a Service:

Ilyenkor a vállalatok egy lépéssel az infrastruktúra fölé lépnek, amikor már az operációs rendszereket és az egyéb middleware megoldásokat egy külső szolgáltató menedzseli.

3. Software as a Service:

Ez a teljes felhőalapú működést testesíti meg, amikor már a szoftver karbantartását is leveszi egy külső szolgáltató az ügyfelek válláról.

IaaS, PaaS, SaaS - Ügyfélút a felhő felé

Amikor egy ügyfél elindul a felhő felé, akkor általában egy már meglévő infrastruktúrát szándékozik átemelni a felhőbe. A szervereket, a tárhelyeket és a hálózati eszközöket egy az egyben le lehet képezni a Microsoft felhő szolgáltatásának segítségével.

Innentől kezdve elindulhat egy biztonságos, üzemeltetett közreműködés, azoknak a feladatoknak a kiszervezésével, amelyeket a vállalat eddig extra szolgáltatásként vett igénybe néhány szerver fenntartása miatt. Ilyen például a klimatizálás, a tervszerű karbantartás, a biztonsági szolgálat, vagy probléma esetén a kiszálló szolgáltatás.

Ezután következik a kérdés, hogy hogyan lehetne ez még egyszerűbb és olcsóbb?

Következő lépésként a szolgáltató egy kész adatbázist biztosít az ügyfél számára, amihez kap egy felhasználónevet és jelszót.

Ilyenkor az, hogy ez a háttérben hogyan van kezelve, mentve, frissítve és biztonságossá téve, már a szolgáltató felelőssége, viszont az ügyfélnek még mindig el kell végeznie a szoftver frissítésével, patchelésével és mentésével járó feladatokat.

A legtöbb vállalat ezután is keresi az ennél jobb, olcsóbb és kényelmesebb megoldásokat, amikor nekik már a szoftverfejlesztéssel sem kell foglalkozniuk.

Az utolsó lépés a teljes felhőalapú működés felé, amikor az ügyfél például levelező rendszert szeretne alkalmazni anélkül, hogy bármilyen technológiai kérdéssel kelljen foglalkoznia. Ekkor jutnak el a cégek a Microsoft Exchange Online szolgáltatásáig, ami a legtipikusabb képviselője a szoftver szolgáltatásoknak. Itt már egy kész szoftvert kapnak, amit csak használniuk kell igényeik szerint.

A Software as a Service megoldásokról ezeken kívül az is elmondható, hogy egy főre visszaosztva ezek kerülnek a legkevesebbe. Ráadásul még tovább lehet optimalizálni őket úgy, hogy a megrendelő ugyanazt a minőségű szolgáltatást kapja, csak olcsóbban.

03

Microsoft Azure technológiai előnyök

03

Az Azure üzleti és technológiai előnyei között mindenképpen **meg kell említenünk a skálázhatóságot, a rendelkezésre állást és a kiberbiztonságot is,** amelyekről részletesebben is írni fogunk még ebben az e-bookban.

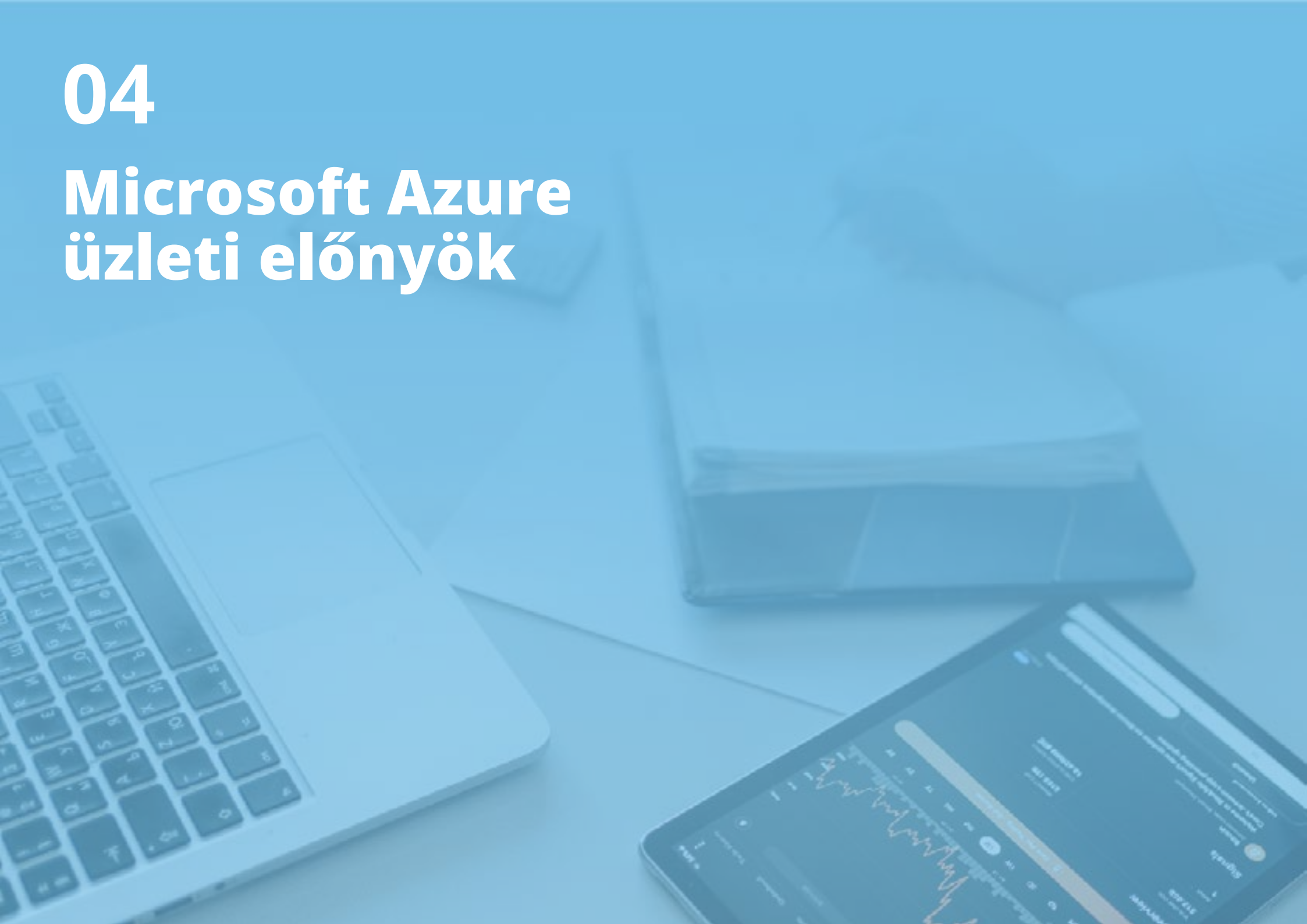
Ezen felül a **rendszer gyors és megbízható, ráadásul támogatja az automatizációt is,** ami rengeteg stresszt és felelősséget levesz az ügyfelek válláról.

Ezek mellett az egyik legfontosabb előnye, hogy **az Azure termékek egymással összekapcsolhatók,** így egy olyan gördülékenyen működő ökoszisztémát kaphatnak a vállalatok, ami az ő, és az ügyfeleik igényeit is teljes mértékben kielégítik. Egy App Service esetében, ha egy cég a webalkalmazása alá egy adatbázist szeretne elhelyezni, akkor egyszerűen igénybe kell vennie az Azure SQL szolgáltatását, majd a kettőt össze kell kötni egymással. De ugyanígy logolás céljával könnyedén integrálható a Log Analytics vagy az App Insights megoldás is bármilyen rendszerbe.

Továbbá **a Microsoft folyamatos frissítéseket biztosít a termékeire,** így a cégek biztosak lehetnek abban, hogy mindig a legkorszerűbb technológiákat és a legújabb verziókat alkalmazzák mindennapos működésük során.

04

Microsoft Azure üzleti előnyök



04

A pandémia hatására lassabbá, drágábbá és bonyolultabbá vált a hardver eszközök beszerzése. Ennek hatására megnőtt annak az ideje, amíg egy ötlet eljut a megvalósításig. **Az Azure-nak köszönhetően elképesztően fel lehet gyorsítani ezt a folyamatot, ráadásul a munkamenet is leegyszerűsödik.**

Amennyiben később kiderül, hogy valami mégsem a tervek szerint megy, és valamilyen megvásárolt termékre nincs szükség, akkor egyszerűen az Azure-ban azt ki lehet kapcsolni. Ezáltal nem marad a polcon semmilyen termék kihasználatlanul. **Az új életszituációkhoz és piaci helyzethez mérten ki lehet találni egy új architektúrát, amihez a szükséges elemeket percek alatt be lehet kapcsolni a rendszerben.**

Ráadásul arról sem szabad megfeledkezni, hogy **egy bérelt infrastruktúra vagy SaaS megoldás alkalmazása esetén az ötlet megszületésénél nem kell 5-6 évre előre gondolkodni a háttér technológia szintjén.**

Továbbá a megszerzett tőkének a nagy részét nem kell hardver beszerzésre költeni. Ebben az esetben azon sem kell gondolkodni, hogy ha 2 év múlva csökken a megrendelések száma, akkor mit lehet csinálni a fölösleges kapacitással, vagy ha duplázódik, akkor hogyan fogjuk kiszolgálni azt. Az Azure használatával a forgótőke megmarad, és valóban csak annyit kell fizetni a használatáért, amennyit a vállalat el is használt. **Közmű jelleggel működik, amennyi a fogyasztás, annyi a fizetendő díj is.** Ezáltal a termelt bevétel és az IT költség arányos marad egymáshoz képest.

Ez még a szoftverfejlesztési időszak alatt is igaz. Sok esetben a fejlesztési környezet használata ingyenes vagy alacsony költségvetésű az Azure használatával, majd az éles környezetet kell csak felskálázni a keresletnek megfelelően.

05

Költség kalkulátor

05

Az Azure rendelkezik egy olyan költség kalkulátorral, amivel a vállalatok kiszámolhatják, hogy a Microsofttól igénybe vett eszközök vagy szolgáltatások a kívánt rendszerrel mekkora havi vagy éves költséget jelentenének. A cégek kiválaszthatják, hogy euróban, dollárban vagy más valutában szeretnének fizetni a szolgálatásokért (ez függ az előfizető országától és régiójától), és azt is, hogy az üzemeltetést melyik kontinens központjába szeretnék igényelni.

Ezentúl arra is van lehetőség, hogy hosszabb távú elköteleződés esetén még tovább csökkenjenek az ezzel járó kiadások. Ezzel a megoldással akár 30-70%-os megtakarítás is elérhető egyes erőforrások esetében.

06
Skálázhatóság

06

Automatizált skálázás

A skálázás iránya: horizontális és vertikális

A Microsoft Teams skálázásának példája

Horizontális skálázás

Vertikális skálázás

Mi alapján dönti el az Azure, hogy szükség van-e skálázásra?

Támogatja az open source megoldásokat a Microsoft?

A skálázhatóság a felhőszolgáltatások egyik legnagyobb előnye. De mit is jelent az, hogy skálázható egy rendszer?

Az, hogy egy rendszer skálázható, azt jelenti, hogy a felhasznált erőforrások növelésével a nagyobb terhelést is ki tudja szolgálni ugyanolyan optimálisan és gyorsan, mint a kisebb terhelést.

Automatizált skálázás

Egy rendszert manuálisan és automatikusan is lehet skálázni. Az automatikus skálázás bizonyos metrikák alapján történik. Ez lehet például a szükséges CPU, memória kapacitás, vagy a HTTP kérések száma is.

Automatizált skálázás során, amennyiben a rendszer növekedést érzékel a nyomon követett mérőszámban, a beállított minimum és maximum paraméterek között mozogva optimalizálja az erőforrásokat. Ezáltal a rendszer egyforma minőségben tudja kiszolgálni az ügyfeleket, függetlenül a terhelés mértékétől.

A skálázás iránya - horizontális és vertikális

Az, hogy egy vállalatnak melyik megoldást kell alkalmaznia, attól függ, hogy mi a célja a skálázásnak.

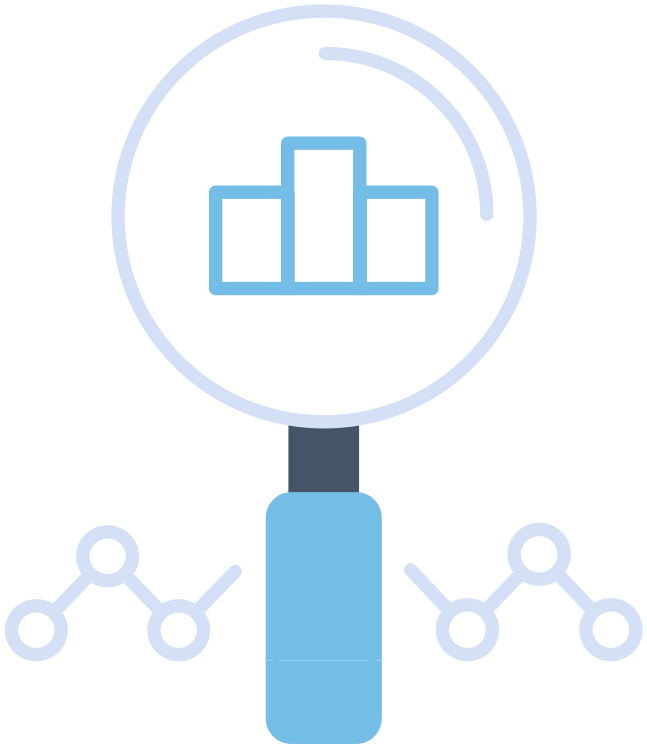
Horizontális az a skálázás,

amikor több azonos méretű erőforrásokkal rendelkező példány kerül elindításra egyszerre, annak érdekében, hogy ezek biztosítani tudják a megfelelő kapacitást.

Vertikális az a skálázás,

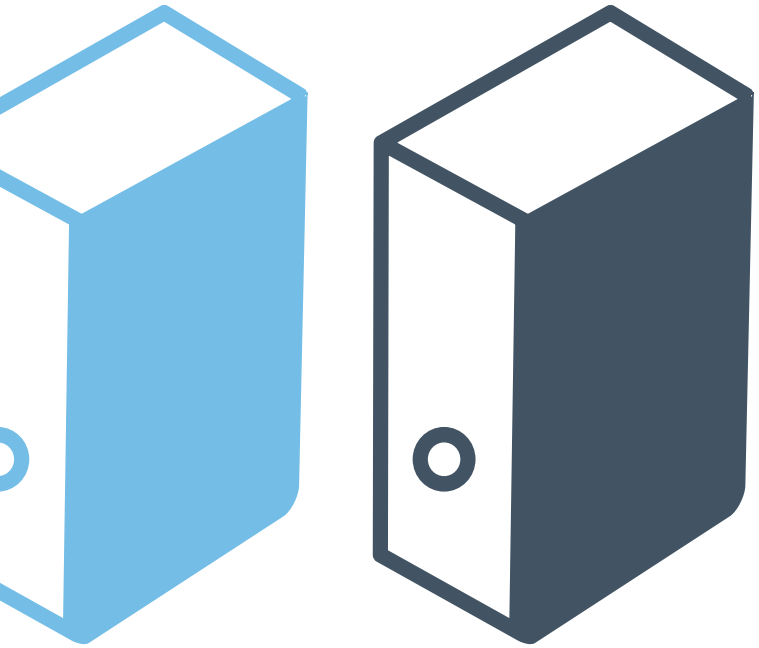
amikor több azonos méretű erőforrásokkal rendelkező példányok indulnak el a megadott léptékben. Beállítástól függően jelentheti azt hogy egyesével növeljük a példányok számát, de lehetőség van arra is,hogy egyszerre több is induljon.

A Microsoft Teams skálázásának példája



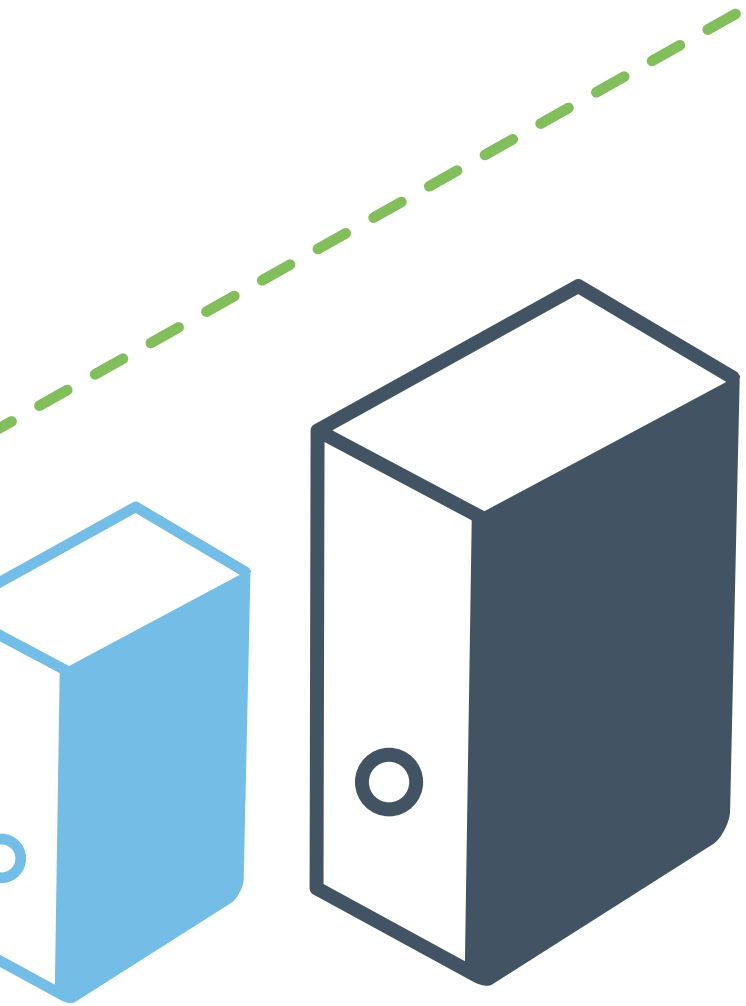
A pandémia hatására jelentősen megnőtt a kereslet a Microsoft Teams iránt, amelynek eredményeként a vállalatóriásnak is skáláznia kellett az erőforrásait. Kezdetben pillanatok alatt óriási terhelés érte a rendszert, melyet sikerült orvosolniuk úgy, hogy **24 óra alatt a hetvenszeresére skálázták a rendszer kapacitását.** Viszont még ez is kevésnek bizonyult, ugyanis az ügyfelek olyan dolgokat tapasztaltak, amely ügyfélélmény szintjén nem képviselte a vállalat értékeit. Emiatt a következő időszakban még tízszeresre bővítették a teljesítményt. **Így néhány nap leforgása alatt hétszázszorosára méretezték át a rendszert úgy, hogy az közben végig működött.**

Horizontális skálázás



A horizontális skálázás nagy előnye, hogy gyorsan megtörténik az új példány elindítása, legyen szó akár egy virtuális gépről, akár egy Azure App Service rendszerről. Az App Service mellett VM Scale Set és AKS Node Pool esetén is kiváló választás a horizontális skálázás.

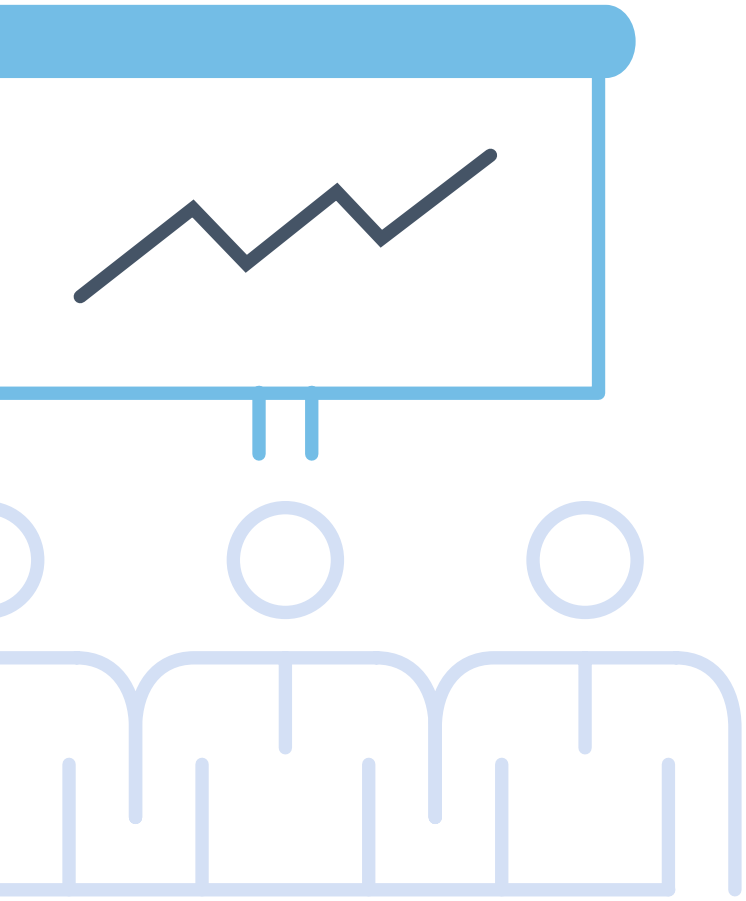
Vertikális skálázás



Példának itt is az Azure App Service-t és a VM Scale Set-et lehet említeni. Nagy különbség a horizontális és a vertikális skálázás között, hogy az utóbbi esetében nem lehet automatikusan skálázni, illetve szolgáltatás kiesés nélkül nem lehet ezt a módszert alkalmazni. Ennek az oka az, hogy ilyenkor pont az a szerver változik, amin az alkalmazás fut.

A vertikális skálázást akkor érdemes használni, amikor például a vállalat tudja, hogy az erőforrásait nem fogja felhasználni a munkaórákon kívül, esténként vagy hétvégénként. Ilyenkor a rendszert le lehet skálázni ideiglenesen, majd felskálázni, amikor eljön az ideje. Ezt batchekkel és scriptekkel lehet automatizálni.

Mi alapján dönti el az Azure, hogy szükség van-e skálázásra?



Függetlenül attól, hogy horizontális vagy vertikális skálázásról van szó, azt, hogy szükség van-e rá, különböző metrikákra alkalmazott szabályokkal dönthetjük el. Ez lehet akár egy vagy több metrika is, például a CPU kihasználtsága, a memória vagy a HTTP kérések száma.

Ennek a megközelítésnek a célja, hogy az ügyfél valóban annyit fizessen, amennyit használ, így költséghatékonyan tarthatja fenn az infrastruktúráját.

Támogatja az open source megoldásokat a Microsoft?

A Microsoft-nál futó környezetek jelentős része használ open source megoldásokat. Ezen kívül a virtuális gépek körülbelül fele open source rendszeren alapszik, amelyek tökéletesen integrálódnak ebbe a környezetbe a Microsoft felhőjében található compute erőforrásokat használva. Gyakorlatilag már az összes nagy támogatott Linux disztribúció elérhető az eszköztárukban.

Ennek a magyarázata az, hogy a Microsoft igyekszik egy olyan környezetet teremteni az ügyfeleknek, ahol ők dönthetik el, hogy mi az, ami legjobban kiszolgálja az igényeiket. A Microsoft ehhez biztosít egy kiszámítható és megbízható platformot.

Valójában a Microsoft felhőjében rengeteg gyártó megoldása elérhető. A cég nem szeretné a saját termékeinek használatára kötelezni az ügyfeleket, ezért a piactéren keresztül a legtöbb elismert nemzetközi márka terméke az ügyfelek rendelkezésére áll. **Bár mindenre adott egy natív megoldás az Azure-ban is, nincs kizárva annak a lehetősége, hogy más alternatívát alkalmazzanak a felhasználók.** Viszont más szolgáltató termékének használata esetén nem a Microsoft biztosítja a technikai támogatást, hanem maga a gyártó.

07
Biztonság

07

- Biztonság a Microsoft-nál
- Felelősség és biztonság
- Szerverbiztonság *(példákkal)*
- Architektúra biztonságos költöztetése a felhőbe
- Katasztrófahelyzetek megoldása
- Feltörések elleni védekezés
- Hogyan védekezik a Microsoft az ehhez hasonló veszélyek ellen?
- E-mail csatolmányok ellenőrzése
- Az IT demokratizálása

Sokan a biztonság kérdéskörét hozzák fel ellenérvnek a felhőszolgáltatások ellen, pedig éppen ez az a szempont, ami miatt előnyösebb lehet ezt választani, mint egy lokális, telephelyi üzemeltetést.

Biztonság a Microsoft-nál

A Microsoft a cég jövőjét a felhőre tette fel. Ha az ügyfelek bizalma meginog ebben a tekintetben, az komoly kockázatot jelent a vállalat számára, ezért a biztonság náluk az egyik legkiemeltebb terület. Éves szinten 1 milliárd dollárt költenek kizárólag a biztonsági fejlesztésekre és a biztonságos környezet fenntartására. Pontosan emiatt az adatközpontok katonai biztonsági szintű épületek, többszörözött energia betáplálással, hűtéssel és internetkapcsolattal.

Az elmúlt időszakban megsokszorozódtak azok a tevékenységek, melyek végeredménye az, hogy az ügyfeleknek kiemelt figyelmet kell fordítaniuk arra, hogy ne kompromittálódjon a környezetük, ami anyagi, erkölcsi és egyéb problémákat okozhat számukra. Emiatt a közeljövőben egy külön szolgáltatási területként fogja a Microsoft megjeleníteni a biztonságot.

Ez azt jelenti, hogy a jelenleg elérhető megoldások mellett, mint például Azure és az Office 365, megjelenik a biztonság is, mint egy különálló üzletág.

A túlterheléses támadások elkerülésében például az Azure DDoS Protection megoldása segít. DDoS támadás esetén a HTTP kérések számának növelésével próbálják meg túlterhelni a rendszert, azonban, ha az automatikus skálázás alapjaként a HTTP kérések metrikája van beállítva, a rendszer nagyon hamar elérheti a beállított maximum szerverszámot. Ezt pedig az ügyfélnek fizetnie kellene, ugyanis minden fogyasztás alapon számítódik. Így a biztonság megfelelő beállításával és finomhangolásával is lehet költséget csökkenteni.

Felelősség és biztonság

Nem mehetünk el a biztonság kérdésköre mellett a felelősség említése nélkül sem. A Microsoft minden olyan eszközt az ügyfelek rendelkezésére bocsát, melyekkel biztonságossá tehetik a rendszerüket. Viszont az, hogy ebből egy biztonságos környezetet épít-e az ügyfél vagy a partnere, az már nem a Microsoft felelőssége. Amikor egy port nyitva marad, vagy amikor valaki nem gondoskodik arról, hogy bekapcsoljon egy tűzfalat, akkor bár felhőben üzemelteti a cég a rendszerét, de mégis kiteszi a támadás veszélyének.

Szerencsére a Microsoft partnereknek, mint például az ALLWIN is, lehetőségük van arra, hogy konzultációt kérjenek a Microsoft szakértőitől miután megterveznek egy rendszert. A Microsoft partnerek közvetlen kapcsolatban vannak a cég képviselőivel, akikhez bátran fordulhatnak kérdésekkel, kérésekkel, proof of concept-tel vagy más teszt környezeti kérésekkel, hogy együtt leellenőrizzék, hogy az megfelel-e minden modern elvárásnak.

Szerverbiztonság

A szerverek biztonságáról úgy érdemes beszélnünk, hogy hogyan segít ebben az Azure portál, amin keresztül egy vállalat a környezetét üzemelteti.

A portálon keresztül folyamatosan monitorozza a rendszert a felügyeleti réteg, ami eredményként ad egy 0-tól 100-ig terjedő pontszámot - Secure Score-t, ami megmondja, hogy az infrastruktúra mennyire biztonságos. Itt egyedi határok meghúzására is van lehetőség, például, ha eléri a 70-et a cég rendszere, akkor az biztonságosnak tekinthető.

A felület javaslatokat ad arra, hogy hogyan lehetne ezt a biztonsági pontszámot növelni.

Néhány példa a javaslatokra:

- Túl sok rendszergazdai jogosultsággal rendelkező felhasználó van a rendszerben.

- Van olyan rendszergazda, akinél nincs bekapcsolva a többtényezős hitelesítés.

- Van olyan virtuális gép, ahol nyitva vanaz RDP port.

- Van olyan virtuális gép, aminek nincsen titkosítva a drive-ja.

Amennyiben az ügyfél követi ezeket a javaslatokat, az eredmény egy sokkal biztonságosabb környezet lesz.

Szerverbiztonság

Ezen kívül arra is lehetőség van, hogy a különböző patcheknek, frissítéseknek a telepítése központosítva legyen. Ennek értelmében a patch management az Azure-re van bízva, így mindent el fog intézni ezzel kapcsolatban.

Itt még azt is érdemes megemlíteni, hogy vannak olyan szerver verziók ma a piacon, amelyeket bizonyos üzleti vagy technológiai okok miatt kénytelenek használni az ügyfelek, azonban ezeknek lejárt már az élettartama. Ezek úgynevezett end of support fázisban vannak. Ez egy jól kalkulálható időtartam, hiszen amikor kijön egy új verzió, a 0. pillanattól már látható, hogy meddig lesznek frissítések a rendszerhez, valamint meddig lesznek biztonsági frissítések, és ez mikor áll meg.

Ha valakinek ilyen szervere van, akkor a Microsoft lehetőséget ad arra, hogy ha ez a szerver Azure-ban van üzemeltetve, akkor a szerver árában benne van az is, hogy a vállalat továbbra is kapni fogja ezeket a biztonsági frissítéseket. Ezeket a frissítéseket a különböző Azure termékeknél és szolgáltatásoknál tudod ellenőrizni. Amennyiben ezeket valaki egy telephelyen szeretné biztonságosan üzemeltetni, nagyon nehéz ezt biztosítani úgy, hogy az a megfelelő védelmi szinten működjön, miközben egy éles környezet fut rajta.

Ennek értelmében a Microsoft egy olyan vállalást tett az Azure felhasználók felé, hogy évekkel megnyújtja a biztonsági frissítések szállítását.

Erről az oldalról indulva pontos leírást találhatsz arról, hogy bizonyos termékek esetén még mennyi idő áll rendelkezésre arra, hogy egy régebbi rendszeren futó megoldás korszerűsítésre kerüljön.

Architektúra biztonságos költöztetése a felhőbe

Ehhez a gondolkodáshoz és a jövőbeli stratégia kialakításához érdemes külsős Microsoft szakértő céget bevonni, ugyanis soha nincs úgy, hogy egy adatbázis csak önmagában áll. Általában az mindig kapcsolódik valami más eszközhöz, például egy ügyviteli rendszerhez, ezért az egész architektúrát egyben érdemes elemezni. Mindig komplexen, komplett architektúrában kell gondolkodni, és erre mindenképpen érdemes egy felhőszolgáltatásban jártas tanácsadó cég tanácsát kérni, mint például az ALLWIN.

Katasztrófahelyzetek megoldása

Tegyük fel, hogy van egy telephelyi környezet, ahol a szerverek üzemelnek. Elmegy az áram, elönti a víz az alagsort, ahol a szerverek üzemelnek stb. Ilyen esetben hogyan lehet biztosítani az üzleti folytonosságot?

Erre az esetre találta ki a Microsoft az Automated Site Recovery megoldásukat, amikor egy jelképes rendelkezésre állási díjért folyamatosan biztosítanak egy tartalék telephelyet tartalék szerverekkel, amelyek szinkronban vannak az élesekkel. **Így, ha a telephelyen valami probléma történik, akkor ezek át tudják venni a kiesett szerverek szerepét anélkül, hogy néhány percnél több ideig állna fenn a szolgáltatás kiesése.**

Magyarországon szerencsére viszonylag ritkák a természeti katasztrófák, viszont már az észak-amerikai kontinens mellett Európában is egyre gyakoribbá válnak a hurrikánok vagy az árvizek. Emiatt legalább koncepció szintjén érdemes egy katasztrófaelhárítási tervvel rendelkezni, amihez a Microsoft-nál szolgáltatás szinten is minden adott.

Nagyon sok több telephellyel rendelkező cégnek van katasztrófaelhárítási terve, de a tapasztalat azt mutatja, hogy ezek sosem voltak kipróbálva, letesztelve. Ha odasétálnánk egy szerverszobába és lekapcsolnánk a főkapcsolót, vajon hány helyen indulnának be a megfelelő mechanizmusok úgy, hogy pár percnél nagyobb kiesést az ne eredményezzen?

Emiatt ezeket a terveket érdemes felülvizsgálni, aktualizálni és tesztelni. A felhő technológia ebben is segít, hiszen olcsón adja az ehhez szükséges szolgáltatásokat.

Feltörések elleni védekezés

2019-ben a NASA-tól adatok szivárogtak ki, ugyanis valaki egy fali aljzatban bedugva felejtett egy gyufásdoboz méretűés körülbelül $30 értékű Raspberry Pi készüléket. Ezen keresztül jutottak be a hackerek a NASA rendszerébe, ahol azért óriási összegeket költenek a biztonságra.

Minden vállalat biztos abban, hogy éjszaka, amíg nincs senki a telephelyen, addig semmi nem marad bedugva a fali aljzatban? Megfelelő beléptető rendszert alkalmaznak, amiből kiderül, hogy ki és mikor járt bent a szerverszobában? Vajon mit nehezebb meghackelni: egy több ezer szervert tartalmazó adatközpontot, ahol gyakorlatilag azt sem tudja az ügyfél, hogy hol található a gépe, vagy egy telephelyet, ahol minden megtalálható?

Hogyan védekezik a Microsoft az ehhez hasonló veszélyek ellen?

Az egyik legfontosabb biztonsági funkció a mesterséges intelligencia alapú arcfelismerő rendszer, amelyek folyamatosan monitorozzák a teret, ahol ezek a rendszerek futnak. Amennyiben egy munkavállaló olyan területre keveredik az adatközponton belül, ahová már nem lenne jogosultsága belépni, abban a pillanatban, amikor ezt a rendszer regisztrálja, az illető már nem alkalmazottja a vállalatnak. Továbbá adathordozó nem kerülhet ki a cég területéről, kizárólag ledarált állapotban. Azt is érdemes megemlíteni, hogy a területre bevezető út úgy lett kialakítva, hogy autóval ne lehessen belehajtani az épületbe.

A Microsoft-nál nincs olyan, hogy egy port, amit valaki nem használ, aktív marad és arról nem kap senki sem egy biztonsági értesítést.

Megdöbbentő lehet, de egy ilyen léptékű adatközpontot kizárólag néhány alkalmazott üzemeltet, ugyanis olyan nagy mértékben automatizált a rendszer, hogy minimálisan van csak szükség emberi beavatkozásra. Ráadásul azt is tudjuk, hogy a legtöbb problémát a nem megfelelő operátori beavatkozás okozza, emiatt ez a megközelítés csak még inkább csökkenti a biztonsági veszélyek kialakulásának lehetőségét.

Meg kell említeni azt is, hogy a Microsoft is használ alvállalkozókat, akiknek a listája publikusan elérhető. A lista átnézése után bármely ügyfél megteheti azt, hogy ha neki egy alvállalkozó a versenytársa, akkor csak erre a tényre hivatkozva felmondhatja a szerződését a Microsoft-tal mindenféle következmény nélkül, akkor is, ha hűségnyilatkozatot tett.

E-mail csatolmányok ellenőrzése

Amikor valaki egy levelet kap Office 365-ben, a melléklet viselkedéselemzésen megy keresztül, amennyiben a vállalat a megfelelő licensszel rendelkezik. Ilyenkor a rendszer felhúz egy virtuális környezetet, amit Detonation Chamber-nek neveznek, és ott lefuttatja a csatolmányt, majd elemzi a viselkedését. Nyúl valamihez a registry-ben? Próbál kommunikálni bizonyos szerverekkel? Fent van a küldő IP címe a listán, ahol azokat tárolják, ahonnan valamilyen támadást vezérelnek?

De az alap e-mail ellenőrzési funkciók közé tartozik a Microsoft-nál a spam szűrés és a vírusírtás, amelynek a felhasználónkénti havi költsége kevesebb, mint egy kávé ára a sarki közértben.

Az IT demokratizálása

A Microsoft vállalása és egyben szlogenje az, hogy demokratizálják az IT-t. Ezt úgy váltották valóra, hogy egy nagy multinacionális vállalat is ugyanannyit fog fizetni felhasználónkként ugyanazokért a szolgáltatásokért, mint egy két fős könyvelő cég. Azáltal, hogy felhőalapú megoldásokat biztosítanak, annyira le tudták csökkenteni a költségeket, hogy a kisméretű vállalkozások számára is elérhetővé váltak ezek a magas színvonalú eszközök.

08

Magas rendelkezésre állás

Az eddig felsorolt biztonsági tényezőket egészíti ki még az is, hogy a **Microsoft havi rendelkezésre állási mutatókkal operál, aminek az értéke 99,5%.** Az Azure Admin Center-ben a felhasználók folyamatosan és egyszerűen követhetik az általuk igénybe vett szolgáltatások állapotát, hiszen a cég nem egyedi problémaként kezeli az esetleges fennakadásokat, hanem vállalati szinten értesíti az összes ügyfelet, ha egy-egy kiesés éppen őket is érinti.

A Microsoft pénzügyi garanciát vállal az SLA-ra (Service-Level Agreement), ami a szolgáltatásokban van, emiatt transzparensen látható, ha egy kiesés érinti az ügyfelet.

Azt itt érdemes tisztázni, hogy 100%-os rendelkezésre állással egy szolgáltató sem tud üzemelni. Nem az a kérdés, hogy lesz-e incidens, mert biztos, hogy lesz, hanem az a kérdés, hogy hogyan reagál rá a szolgáltató, mennyire transzparensen kommunikál, és ad-e bármilyen visszatérítést abból a díjból, amit beszedett az adott szolgáltatásért.

Lokális és globális redundancia

Az Azure-ban a legalacsonyabb biztonsági szint szerint is minden disc legalább három példányban tárolódik egy adatközponton belül. Ha valaki a Microsoft rendszerét használja és adatot tárol, akkor abból minimum három példány készül, hogy kiesés esetén ne történjen adatvesztés. Ezt nevezzük lokális redundanciának.

Ezen kívül arra is van lehetőség, hogy külön rack-ben legyenek elhelyezve ezek a példányok külön árammal, klímával és adatkapcsolattal. Továbbá az is megoldható, hogy a példányok külön update domain-be kerüljenek. **A Microsoft-nál sosem történik olyan, hogy minden egyes másolat alatt egyszerre frissítsék a virtualizációs réteget,** ugyanis látják, hogy a gépek ugyanazért felelősek, így egyszerre csak egy fog állni, amíg a rendszer újraindul alatta.

Ha valaki még ennél is magasabb adatbiztonságra törekszik a folyamatos rendelkezésre állás mellett, akkor akár földrajzilag több elkülönített adatközpontban is elhelyezhetők a másolatok. Sőt, akár még egy read only példány létrehozása is lehetséges egy másik lokáción.

Emiatt nem fordulhat elő ezekkel a megoldásokkal, hogy egy zsarolóvírus titkosítja az összes elérhető másolatot. Valamint ezáltal minimalizálható a szolgáltatáskiesések aránya is, hiszen nagyon kicsi annak a valószínűsége, hogy több adatközpontban egyszerre megy el az áram, vagy történik egy globális természeti katasztrófa, ami minden szervert érint.

09

Esettanulmányok

09

- Intranet megoldás
- Globális webportál megoldás
- Egészségügyi megoldás

Az elméleti rész után nézzünk néhány valós gyakorlati példát arra, amikor az Azure felhő szolgáltatásait alkalmaztuk ügyfeleinknél.

Intranet megoldás

Itt a feladatunk az volt, hogy fejlesszünk egy intranet megoldást egy nemzetközi nagyvállalat számára, amelyet több mint 4000 alkalmazott tud igénybe venni több nyelven, más-más időzónákban. Ebben az esetben már adott volt, hogy az alkalmazottak felhasználói adatait Azure-ban kezelik. Itt meg kellett valósítani egy AD authentikációt, illetve IP cím szűréseket, amit még kiegészítettünk az Application Gateway megfelelő konfigurációjával. A gyorsaság fenntartása miatt, és azért, hogy a sok kérés ne okozzon fennakadást, az Azure CDN (Content Delivery Network) megoldását használtuk, ami cache-eli a tartalmakat.

Ezeken felül egy olyan autentikációt is megvalósítottunk, hogy amikor a tartalmak a CDN-ben frissülnek, akkor maga a rendszer is autentikál a szerver felé, hogy ne juthasson be olyan kérés az intranet üzemeltetésébe, ami nem ellenőrzött.

Erőforrásként az Azure App Service-eket használtuk, amelyeknél automatikus horizontális skálázást alkalmaztunk. Ennek az egyik időpontja a reggeli órákra került beállításra, amikor a munkavállalók megérkeznek az irodába, elolvassák a hírleveleket és elkezdik a napi feladataikat, ami megnövekedett kapacitást igényel.

Annak érdekében, hogy a frissítések, javítások és upgrade-k esetében ne történjen kiesés az alkalmazásban, az Azure DevOps-ot használtuk. Továbbá egy CI/CD pipeline segítségével valósítottuk meg, hogy az új frissítések ne okozzanak fennakadást.

Globális webportál megoldás

Ennél a globális multinacionális vállalatnál az Azure Kubernetes Service-t (AKS) használtuk az Azure CDN és DevOps mellett. A vállalat, illetve leányvállalatai számára webportált fejlesztettünk. Arra törekedtünk, hogy egy magas rendelkezésre állással és kiemelkedő biztonsággal rendelkező rendszert adjunk át ügyfelünk részére.

Ebben az esetben az AKS biztosította a magas rendelkezésre állást, ugyanis egy adott szolgáltatásból a segítségével több példányt futtattunk.

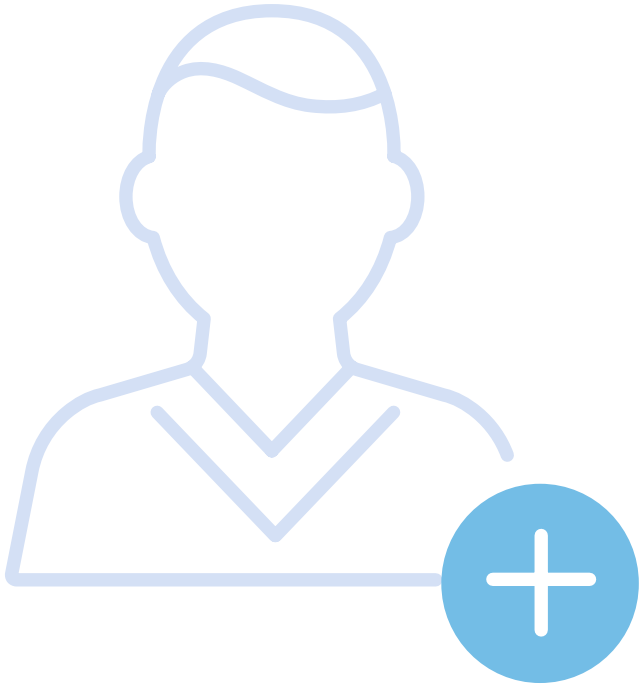
A projekt érdekessége, hogy Windows Node Pool-t alkalmaztunk, ami nagy előnye az Azure szolgáltatásnak, ugyanis más szolgáltatók nem támogatják annyira a Windows Node Pool-okat, mint a Microsoft. Azért kellett Windows-os Node Pool-t alkalmazni, mert egy olyan tartalomkezelő (CMS) rendszert használ a vállalat, ami jelenleg csak Windows-on képes futni.

A CDN használata szintén a magas rendelkezésre állásban nyújtott támogatást. Ügyfelünknél szinte csak statikus weboldalakat kellett kiszolgálni, ahol elkészítik a tartalmat, azt kipublikálják, és az bizonyos ideig változatlan marad. A rendszer körülbelül 99%-a ilyen statikus tartalmakból áll, így a CDN miatt még ha bármi probléma történik a Kubernetes-szel, a webportál a látogatók igényeit ki tudják szolgálni.

A DevOps használatánál is igyekeztünk egy olyan megoldást összeállítani a deployment során, ami biztosítja azt, hogy szolgáltatás kiesés nélkül tudjunk telepíteni vagy rollbackelni.

Ami a biztonságot illeti, ügyfelünknél magában a cluster-ben üzemeltettük a tűzfalat, aminek költségoptimalizálási okai voltak, de így is gyakorlatilag ugyanazt a biztonsági szintet tudtuk biztosítani, mint az App Gateway.

Egészségügyi megoldás



Ebben az esetben egy külföldi egészségügyi partnerünk számára fejlesztettünk egy olyan megoldást az Azure Kubernetes használatával, ami költséghatékony üzemeltetést, rugalmas konfigurációt és horizontális skálázási lehetőségeket tett lehetővé. Itt több szolgáltatás fut ugyanazokon a VM Scale Set-eken. Ezzel tudtuk azt biztosítani, hogy nem kell minden szolgáltatás számára App Service-t vásárolni, ami költségcsökkentést eredményezett partnerünknek.

Az AKS előnye ezen kívül, hogy különböző környezetekbe ki tudtuk telepíteni a rendszert, mivel az szétválasztásra került a konfigurációtól. Ezalatt érthetjük a különböző érzékeny adatok tárolását is, amit a Kubernetes szintén támogat, hiszen beépített megoldást garantál arra, hogy például az SQL szerverhez tartozó connection string-et el tudjuk tárolni biztonságos módon.

További előnye a Kubernetes-nek, az úgynevezett self-healing funkció, ami azt jelenti, hogy ha elérhetetlenné válik egy komponenspéldány, akkor a rendszer azonnal indít egy újat.

Partnerünknél a horizontális skálázást két szinten oldottuk meg, hiszen maga az alkalmazás példány is skálázható horizontálisan Kubernetes-en belül. Ezen felül az Azure lehetővé teszi azt is, hogy magát a Pool-ban levő VM-ek számát skálázzuk automatizáltan, ha azoknak elfogytak a rendelkezésre álló erőforrásaik.

10
Konklúzió

Összességében elmondhatjuk, hogy a Microsoft Azure egy olyan felhő-megoldás, ami támogatja a vállalatokat és vállalkozókat a fejlődésben és digitalizációban azáltal, hogy skálázható, biztonságos, és magas rendelkezésre állással rendelkező technológiát kínál számukra elérhető áron.

Az e-bookban láthattuk, hogy a Microsoft hatalmas erőfeszítéseket tesz azért, hogy ügyfeleik adatait és alkalmazásait biztonságosan tárolja, akár a Föld több pontján is. Emellett az Azure használatával rugalmasan változtathatóak az alkalmazások és az infrastruktúrák az adott piaci körülményekhez igazodva, így a vállalat valóban csak annyit fog fizetni a szolgáltatásokért, amennyit fel is használt. Ezáltal nem lesz több kihasználatlan hardware, ami több forgótőkét biztosít a fejlesztés és üzemeltetés számára.

Amennyiben egy cég úgy dönt, hogy jelenlegi lokális infrastruktúráját át szeretné költöztetni a felhőbe, érdemes egy szakértő partner tanácsát és segítségét igénybe vennie. Ennek oka az, hogy egy adatbázis sosem áll egymagában, ezért mindig komplett rendszerként kell azt vizsgálni a hozzá kapcsolódó eszközök figyelembevételével. Ez a legtöbb esetben komplex megoldást is igényel, amihez rendszerszemlélet és kiadós tervezés szükséges.

11

Az ALLWIN-ről

ALLWIN
Trust driven development

Az ALLWIN egy 2007-ben alapított budapesti központtal rendelkező vállalat. Csapatunk többek között egyedi .NET szoftverfejlesztéssel foglalkozik. Olyan élvonalbeli technológiákkal segítjük a partnereink fejlődését, amelyek lefedik a szoftverfejlesztési szolgáltatások teljes életciklusát. Munkánk során mindvégig arra törekszünk, hogy eredményeinkkel és a közös munka során transzparens kommunikációnkkal ügyfeleink üzleti sikereit számokban is mérhetővé tegyük.