ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Alba Regia Műszaki Kar
Természettudományi és Szoftvertechnológiai Intézet

SZAKDOLGOZAT

Felhőalapú Virtualizációs Megoldások: Az Azure Virtual Desktop Infrastruktúra Mint Kód Tervezése és Implementációja

OE-AMK

2024

Hallgató neve: NÉMETH ZSOLT

Hallgató törzskönyvi száma:T001040/FI12904/A-M

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Alba Regia Műszaki Kar
Természettudományi és Szoftvertechnológiai Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Németh Zsolt
Szakdolgozat száma: SZD22011411174916
Törzskönyvi száma: T001040/FI12904/A-M **Neptun kódja:** [redacted]

Szak: mérnökinformatikus
Specializáció: Felhő szolgáltatási technológiák és IT biztonság specializáció

A dolgozat címe: Felhőalapú virtualizációs megoldások: Az Azure Virtual Desktop infrastruktúra mint kód tervezése és implementációja
A dolgozat címe angolul: Cloud-based Virtualization Solutions: Design and Implementation of Azure Virtual Desktop Infrastructure as Code
A feladat részletezése: A hallgató feladata, hogy az infrastruktúra mint kód alkalmazásával valósítson meg egy Azure Virtual Desktop infrastuktúrát magas rendelkezésre állású felhőszolgáltatón keresztül. A hallgató válassza ki és indokolja a megvalósításhoz megfelelő konfigurációs nyelvet és verziókezelő rendszert az IaC szkriptek kezeléséhez. Tervezze meg és implementálja az IaC szkripteket, amelyek segítségével létrehozza az Azure Virtual Desktop infrastruktúrát. Tesztelje az elkészült rendszert, majd mutassa be a továbbfejlesztési lehetőségeket.

Intézményi konzulens neve: Módné Takács Judit

Külső konzulens neve: Varga Gábor
Munkahelye: Hydro Extrusion Hungary Kft.

A kiadott téma elévülési határideje:2026. 07. 10.
Beadási határidő: 2024. 05. 15.

A szakdolgozat: Nem titkos.

Kiadva: Székesfehérvár, 2024. 04. 03. P.H

ÓBUDAI EGYETEM Alba Regia Műszaki Kar Természettudományi és Szoftvertechnológiai Intézet 1. Székesfehérvár

.....
Intézetigazgató

A dolgozatot beadásra alkalmasnak találom: 2024. 05. 15.

.....
belső konzulens

.....
külső konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Alba Regia Műszaki Kar
Természettudományi és Szoftvertechnológiai Intézet

HALLGATÓI NYILATKOZAT

Alulírott hallgató kijelentem, hogy a dolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült dolgozatban található eredményeket az Óbudai Egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Kelt: 2024.04.08

.....

hallgató aláírása

Tartalomjegyzék

1. Bevezetés 1

2. Irodalmi áttekintés 3

2.1 Felhő 3

2.2 Felhő alapú szolgáltatások 4

2.3 Felhő modellek 6

2.3.1 IaaS 6

2.3.2 PaaS 8

2.3.3 SaaS 9

3. Azure Virtual Desktop És Cloud PC 11

3.1 Azure Virtual Desktop 11

3.2 Cloud PC 11

3.3 Cloud PC és AVD 12

4. Megvalósításhoz alkalmas technológiák 13

4.1 Microsoft Azure 13

4.2 IaC technológiák 13

4.2.1 Terraform 14

4.2.2 Azure ARM 16

4.3 Automatizálási eszközök 17

4.3.1 Powershell 17

5. Megvalósításhoz használt technológiák 18

5.1 IaC technológia kiválasztása 18

5.2 Aviatrix 19

5.3 Felhőplatform 20
6. Feladat specifikáció 21
7. Hálózati Áttekintés 23
7.1 Azure hálózati koncepció 23
7.1.1 Virtuális hálózat (VNET) 23
7.1.2 VNET Peering 24
7.1.3 Magas rendelkezésre állás 25
7.2 Hálózati biztonsági csoportok 26
7.3 Útválasztás – Felhasználó által meghatározott útvonalak 26
7.3.1 Internet Ingress Connectivity 27
7.3.2 Internet kilépési kapcsolat 28
7.3.3 DNS –Domain Name Resolution 29
8. HálózatSzegmentálás és Következményei 30
8.1 Tipikus forgalom útvonala 31
8.2 zScaler 32
8.2.1 Public DNS 33
8.2.2 Privát DNS 34
9. Azure virtual desktop kiépítése 35
9.1 Tesztelés 40
10. Automatizálási és továbbfejlesztési lehetőségek 42
11. Összefoglaló 45
12. Summary 46
13. Irodalomjegyzék 47
14. Ábrajegyzék 49

1. BEVEZETÉS

A dolgozat célja egy Azure Virtual Desktop megvalósítása, megtervezése, bemutatása, naprakészen tartása és továbbfejlesztési lehetőségeinek feltárása a kiépítés során. A feladat megvalósításához egy már előre létező publikus felhő platformot fogok használni, ami a Microsoft Azure lesz a későbbiekben. A probléma megoldása során kitérünk az infrastruktúra megvalósításának lehetséges módszereire, és vizsgálni fogjuk a választott technológiák előnyeit és hátrányait. Az implementálás során biztonsági kérdések megválaszolása különböző szervezeti szabályok beállításaival fog történni.

A már elkészült AVD beüzemelése során találkozni fogunk automatizálási, skálázhatósági és elérhetőségi kérdésekkel is, amik megválaszolásra kerülnek az implementálás során. A megvalósítás során kiválasztjuk a megfelelő eszközöket és azokat indokoljuk is.

A Microsoft Azure lényegében egy széleskörű virtualizációt tesz lehetővé világszerte, ahol több száz szolgáltatás közül választhatunk, mint kiegészítő tulajdonságok. Maga a Cloud Computing azt jelenti, hogy az alkalmazások egy távoli kiszolgálón futnak, így nem kell helyi munkaállomásokon futtatnunk az erőigényes szolgáltatásokat és sokkal job skálázhatóságot érhetünk el.

Az infrastruktúra kialakítására nem csak az Azure által előre beépített, biztosított eszközöket fogjuk használni, hanem IaC Infrastructure as Code alapú megvalósítás fog történni. Lényegében az IaC egy olyan absztrakció, ahol nem hardver rendszert építünk fel manuálisan, hanem ezt kódolással érjük el. Az infrastruktúrát nem manuálisan kézzel kell felállítanunk, beállítanunk a felhő platformunkon, hanem automatizálással.

Ennek az automatizációnak a megvalósítására fogjuk használni a Terraformot, illetve Azure ARM-et. Ezeket asz eszközöket fogjuk használni a felhőinfrastruktúránk magjának felállítására.

A Terraform-al a kiépítés és biztonság is automatizálható deklaratív infrastruktúrával és kóddal. Az infrastruktúra és a szabályok kodifikálása, megosztása, verziószámkezelése és végrehajtása az összes infrastruktúrán konzisztens munkafolyamatban történik.

A felhő infrastruktúránkat nem csak létrehozzuk, hanem automatizálási folyamatokat is végre fogunk hajtani rajta, melyhez Powershell-t fogunk használni.

A Powershell egy többplatformos automatizálási és konfigurálási keretrendszer, amely elérhető Linux, Windows, és macOS-en. A Powershell jól működik már meglévő eszközök automatizálására, strukturált adatok módosítására, kezelésére, mint például: JSON, CSV, XML stb. A Powershell még képes REST API-k kezelésére is, legfőképpen rájuk van optimalizálva.

A választott témámban bemutatom, hogyan is biztosítható számunkra egy publikus felhő platformot használó AVD környezet megtervezése, megvalósítása és tesztelése Microsoft Azure platformon. A szakdolgozaton végig haladva részletezni fogom a felhő platformok összehasonlítását és a választott technológia előnyeit és hátrányait.

A témám magába foglalja egy AVD kiépítését. A probléma megoldása alkalmával adaptáltam az alkalmazásokat Microsoft Azure platformhoz. Az infrastruktúra tervezése és a funkciók implementálása számos területet érint a Microsoft Azure platformon melyek: hálózat implementálása a publikus felhő platformra, biztonsági meggondolások, automatizálás és adattárolók használata.

Ezen szempontok lapján értékelem az elkészült AVD koncepcióját és mutatom be a továbbfejlesztési lehetőségeket, amiket alkalmazni fogok a felhő platformon.

2. IRODALMI ÁTTEKINTÉS

A szakirodalom megtekintése és áttekintése során ismertetni fogom a felhőrendszerek fogalmát, működését, előnyeik és hátrányaik áttekintését és méréseit. A felhőtechnológiák csoportosításival is foglalkozni fogunk ebben a fejezetben. Az áttekintés során részletesebben szemléltetni fogom a feladat megvalósításához szükséges felhőtechnológia típusait: publikus, privát, hybrid. A feladat megvalósításához másik fontos technológia a magát a hálózati infrastruktúrát megvalósító automatizáció, a Terraform. Ismertetni fogom a Terraform lényegét, megvalósítását és működésének folyamatát, valamint a felhasznált könyvtárakat.

2.1 Felhő

Egyszerűen fogalmazva, a felhőalapú számítástechnika számítástechnikai szolgáltatások – beleértve a szervereket, tárolóeszközöket, adatbázisokat, hálózatépítést, szoftvereket, elemzéseket és intelligenciát – az interneten (a „felhőn”) [1] keresztül történő szállítását jelenti, hogy gyorsabb innovációt, rugalmas erőforrásokat és méretgazdaságosságot kínáljon. Általában csak azért a felhőszolgáltatásokért fizetünk, amik általunk használva vannak, így csökkenthetjük a működési költségeinket, hatékonyabban üzemeltethetjük felhő infrastruktúránkat, és a nagy skálázhatóságnak köszönhetően jobban tudunk igazodni az üzleti igényeknek, amik napról napra változhatnak.

A felhő definíciója elsőre homályosnak tűnhet, ám lényegében ez egy olyan kifejezés, amely a szerverek leírására szolgál globális szinten, amelyeknek mindegyike különleges egyedi funkcióval van ellátva. A felhő nem egy fizikai jelenség, hanem egy hatalmas hálózat, ami világszerte kiterjed. Ezek a hálózatok össze vannak kapcsolva, és egyetlen rendszerként, ökoszisztémaként működnek. Ezeknek a szervereknek a megtervezésekor, figyelembe vették, hogy adatokat tároljanak és kezeljék ezeket az adatokat, alkalmazásokat futtassanak. A szervereken különböző tartalmakat, mint például videó, webes levelek, különböző szoftvereket vagy pedig közösségi médiát is képesek szállítani. Ahelyett, hogy egy személyi számítógépről férnénk hozzá az adatainkhoz, illetve fájljainkhoz, bármilyen

eszközről el tudjuk érni őket, ha az eszköz rendelkezik internetkapcsolattal, így az információk bárhonnan és bármikor elérhetőek lesznek számunkra.

Alapvetően négy különböző megközelítési módot különböztetünk meg a felhő erőforrások üzembe helyezésére. Találkozhatunk nyilvános felhővel, amely megosztja az erőforrásokat, és a nyilvánosság számára felhasználható szolgáltatásokat kínál az interneten keresztül.

A privát felhő jellemzően egy kimondott helyszínen, egy privát belső hálózaton keresztül kínál szolgáltatásokat, és egy hibrid felhő, amely megosztja a szolgáltatásokat a nyilvános és a magántulajdon között. felhők a céljuktól függően, és egy közösségi felhő, amely csak szervezetek között osztja meg az erőforrásokat, például kormányzati intézményekkel. [2]

2.2 Felhő alapú szolgáltatások

A felhőalapú számítástechnika, számítástechnikai szolgáltatások nyújtását jelenti, beleértve a tárolást, a feldolgozási teljesítményt és az alkalmazásokat az interneten keresztül. Fizikai szerverek vagy számítási infrastruktúra birtoklása és karbantartása helyett az egyének és szervezetek felosztó-kirovó alapon hozzáférhetnek és használhatják a számítási erőforrásokat egy felhőszolgáltatótól.

A számítási felhő legfontosabb jellemzői közé több dolgot is fel lehet sorolni.

Az igény szerinti önkiszolgálás ide tartozik. A felhasználók szükség szerint biztosíthatják és kezelhetik a számítási erőforrásokat a szolgáltató emberi beavatkozása nélkül, emellett széles körű hálózati hozzáférést biztosít. A felhőszolgáltatások számos eszközről, például laptopokról, okostelefonokról és táblagépekről érhetők el az interneten keresztül.

A legfontosabb jellemzők közé tartozik még az erőforrás összevonás. A felhőszolgáltatók egyesítik számítási erőforrásaikat, hogy több ügyfelet szolgáljanak ki, és a különböző fizikai és virtuális erőforrásokat dinamikusan hozzárendeljék és az igényeknek megfelelően hozzárendeljék át.

A felhők előnyei közé tartozik még az, hogy az erőforrások gyorsan növelhetők vagy csökkenthetők a kereslet alapján. A felhasználók csak az általuk használt erőforrásokért fizetnek. A felhőalapú számítástechnikai erőforrásokat mérik, és a felhasználókat használatuk alapján számlázzák ki. Ez a felosztó-kirovó modell költséghatékonyságot és rugalmasságot biztosít.

A felhőalapú számítástechnikai szolgáltatásokat általában három fő modellbe sorolják:

- Infrastruktúra, mint szolgáltatás (IaaS): Virtualizált számítási erőforrásokat biztosít az interneten keresztül. A felhasználók bérelhetnek virtuális gépeket, tárhelyet és hálózatokat.
- Platform as a Service (PaaS): Olyan platformot kínál, amely lehetővé teszi az ügyfelek számára az alkalmazások fejlesztését, futtatását és kezelését anélkül, hogy az infrastruktúra bonyolultságával kellene foglalkozniuk, beleértve a köztes szoftvereket, fejlesztői keretrendszereket és adatbázisokat.
- Szoftver, mint szolgáltatás (SaaS): Szoftveralkalmazásokat szállít az interneten, előfizetéses alapon. A felhasználók webböngészőn keresztül érhetik el a szoftvert anélkül, hogy aggódnának a telepítés, karbantartás vagy frissítések miatt.

A népszerű felhőszolgáltatók közé tartozik az Amazon Web Services (AWS), a Microsoft Azure, a Google Cloud Platform (GCP) és mások. A felhőalapú számítástechnika a vállalkozások és magánszemélyek alapvető technológiájává vált, rugalmasságot, méretezhetőséget és költséghatékonyságot biztosítva a számítási erőforrások kezelésében és felhasználásában.

2.3 Felhő modellek

2.3.1 IaaS

Az Infrastructure as a Service (IaaS) egy felhőalapú számítástechnikai modell, amely virtualizált számítási erőforrásokat biztosít az interneten keresztül [2]. Az IaaS segítségével a felhasználók felosztó-kirovó alapon bérelhetnek és biztosíthatnak virtuális gépeket, tárolókat és hálózati összetevőket, ahelyett, hogy fizikai hardverbe fektetnének és karbantartanák. Ez nagyobb rugalmasságot, méretezhetőséget és költséghatékonyságot tesz lehetővé az egyének és a szervezetek számára.

Az IaaS a virtualizációs technológiára támaszkodik a számítási erőforrások virtuális példányainak létrehozásához. A virtuális gépek (VM-ek) különböző operációs rendszereket és alkalmazásokat futtathatnak ugyanazon a fizikai hardveren. A felhasználók igényeik szerint felfelé vagy lefelé méretezhetik infrastruktúrájukat. Az erőforrások igény szerinti kiépítése rugalmasságot tesz lehetővé a változó munkaterhelések kezelésében.

Az IaaS-szolgáltatók jellemzően önkiszolgáló felületeket vagy API-kat kínálnak, amelyek lehetővé teszik a felhasználók számára az erőforrások biztosítását és kezelését a szolgáltató közvetlen emberi beavatkozása nélkül.

Az IaaS platformokat úgy tervezték, hogy méretezhetőek legyenek, lehetővé téve a felhasználók számára, hogy a változó igényekre reagálva gyorsan és egyszerűen növeljék vagy csökkentsék erőforrásaikat.

A felhasználókat az általuk fogyasztott erőforrásokért számlázási alapon számlázzuk ki. Ez a felosztó-kirovó modell költséghatékonyságot kínál, mivel a felhasználók csak az általuk használt erőforrásokért fizetnek. Az IaaS lehetővé teszi a felhasználók számára a hálózati összetevők vezérlését, lehetővé téve számukra a virtuális hálózatok, tűzfalak és terheléselosztók konfigurálását sajátos követelményeiknek megfelelően.

Az infrastruktúra, mint szolgáltatás általános használati esetei a következők:

- Fejlesztés és tesztelés: Az IaaS-t gyakran használják fejlesztői és tesztelési környezetek létrehozására, lehetővé téve a csapatok számára, hogy szükség szerint gyorsan hozzák létre és eltávolítsák az erőforrásokat.
- Webtárhely: A webhelyek és webes alkalmazások virtuális gépeken való tárolása a felhőben gyakori IaaS-használati eset.
- Adattárolás és biztonsági mentés: Az IaaS platformok méretezhető és megbízható tárolási megoldásokat kínálnak, így alkalmasak adattárolásra, biztonsági mentésre és helyreállításra.
- Katasztrófa utáni helyreállítás: A szervezetek az IaaS segítségével redundáns és földrajzilag elosztott infrastruktúrát hozhatnak létre az üzletmenet folytonosságának biztosítása érdekében katasztrófa esetén.

A népszerű IaaS-szolgáltatók közé tartozik az Amazon Web Services (AWS), a Microsoft Azure, a Google Cloud Platform (GCP) és mások. Ezek a szolgáltatók a virtualizált számítási erőforrások és szolgáltatások széles skáláját kínálják, hogy megfeleljenek a felhasználók különféle igényeinek [3].

2.3.2 PaaS

A Platform as a Service (PaaS) egy felhőalapú számítástechnikai szolgáltatásmodell, amely olyan platformot biztosít, amely lehetővé teszi az ügyfelek számára az alkalmazások fejlesztését, futtatását és kezelését anélkül, hogy a mögöttes infrastruktúra bonyolultságával kellene foglalkozniuk [4]. A PaaS elvonatkoztatja az infrastruktúra-kezelés nagy részét, lehetővé téve a fejlesztők számára, hogy az alkalmazások létrehozására és telepítésére összpontosítsanak.

A PaaS előre elkészített keretrendszereket, könyvtárakat és fejlesztőeszközöket biztosít, amelyek lehetővé teszik a fejlesztők számára, hogy hatékonyabban építsenek alkalmazásokat. Ez magában foglalhatja a különböző programozási nyelvek, adatbázisok és köztes szoftverek támogatását.

A PaaS platformok általában az alkalmazások automatikus telepítését és méretezését kínálják. A fejlesztők minimális manuális beavatkozással telepíthetik kódjukat, a platform pedig szükség szerint kezeli az erőforrások kiépítését és méretezését.

A PaaS-szolgáltatók gyakran kínálnak felügyelt szolgáltatásokat, például adatbázisokat, üzenetküldési sorokat és gyorsítótárat, csökkentve ezzel a fejlesztők működési terheit. Ezeket a szolgáltatásokat a platform karbantartja és frissíti, így a fejlesztők az alkalmazáslogikára összpontosíthatnak.

A PaaS platformokat úgy tervezték, hogy az alkalmazásokat igény szerint automatikusan méretezzék. Ez a méretezhetőség a fejlesztők kézi beavatkozása nélkül érhető el, biztosítva, hogy az alkalmazások képesek legyenek kezelni a változó terheléseket.

A PaaS platformok több felhasználót és alkalmazást támogatnak ugyanazon az infrastruktúrán, elősegítve az erőforrás- és költséghatékonyságot. A PaaS-szolgáltatók gyakran tartalmaznak beépített biztonsági intézkedéseket és megfelelőségi funkciókat az alkalmazások és adatok biztonságának elősegítése érdekében.

Példák a Platform, mint szolgáltatás kínálatára:

- Google App Engine: Teljesen felügyelt szerver nélküli platform, amely lehetővé teszi a fejlesztők számára, hogy az alapul szolgáló infrastruktúra kezelése nélkül építsenek és telepítsenek alkalmazásokat.
- Microsoft Azure App Service: platform webalkalmazások létrehozásához, üzembe helyezéséhez és méretezéséhez. Több programozási nyelvet és keretrendszert támogat.
- Heroku: Az alkalmazások telepítését és kezelését leegyszerűsítő felhőplatform, amely különféle programozási nyelveket támogat.
- AWS Elastic Beanstalk: Könnyen használható szolgáltatás alkalmazások telepítéséhez és méretezéséhez, több nyelv és platform támogatásával.

A PaaS különösen előnyös azoknak a fejlesztőknek, akik a kódírásra és a szolgáltatások kiépítésére szeretnének összpontosítani anélkül, hogy az infrastruktúra-kezelés bonyolultságával kellene foglalkozniuk. Leegyszerűsíti a fejlesztési folyamatot, felgyorsítja a piacra kerülést, és lehetővé teszi az erőforrások hatékonyabb felhasználását.

2.3.3 SaaS

A Software as a Service (SaaS) egy felhőalapú számítástechnikai szolgáltatásmodell, amely szoftveralkalmazásokat szállít az interneten keresztül. Az egyes számítógépekre vagy szerverekre történő szoftver telepítése és karbantartása helyett a felhasználók webböngészőn keresztül érhetik el és használhatják a szoftvert. A SaaS-szolgáltatók tárolják és karbantartják a szoftvert, kezelik a szoftverfrissítéseket és -javításokat, valamint biztosítják az alkalmazás elérhetőségét és biztonságát.

A SaaS-alkalmazások különféle eszközökről, például laptopokról, okostelefonokról és táblagépekről érhetők el az interneten keresztül. A felhasználók bárhonnan hozzáférhetnek a szoftverhez internetkapcsolattal. A SaaS rendszerint előfizetéses alapon érhető el, ahol a felhasználók rendszeres díjat fizetnek a szoftver eléréséért és használatáért. Ez az előfizetési modell gyakran tartalmaz karbantartást, frissítéseket és támogatást.

A SaaS-alkalmazásokat a szolgáltató központilag tárolja és kezeli. Ez a központosított felügyelet szükségtelenné teszi az egyes felhasználóknak vagy szervezeteknek a szoftver helyi telepítését, konfigurálását és karbantartását.

A szolgáltatók kezelik a szoftverfrissítéseket, javításokat és karbantartási feladatokat. A felhasználók mindig hozzáférhetnek a legújabb szolgáltatásokhoz és biztonsági frissítésekhez anélkül, hogy maguknak kellene kezelniük a frissítési folyamatot.

A SaaS platformokat úgy tervezték, hogy több felhasználót vagy szervezetet támogassanak ugyanazon az infrastruktúrán. Az erőforrások hatékony megosztása költségmegtakarítást és méretezhetőséget eredményez.

A SaaS-alkalmazások könnyen méretezhetők, hogy alkalmazkodjanak a felhasználók számában vagy az adatmennyiségben bekövetkező változásokhoz. Az infrastruktúrát a szolgáltató kezeli, így a felhasználók igény szerint növelhetik vagy csökkenthetik a használatukat.

Példák a szoftverre, mint szolgáltatásra:

- Google Workspace: Hatékonysági eszközök sorozata, beleértve a Gmailt, a Google Dokumentumokat, a Táblázatokat és a Diákat, SaaS-ajánlatként.
- Microsoft 365: Tartalmazza a Microsoft Office-alkalmazások, együttműködési eszközök és szolgáltatások, például a Microsoft Teams felhőalapú verzióit.
- Salesforce: Felhőalapú ügyfélkapcsolat-kezelési (CRM) platform, amely számos alkalmazást kínál értékesítéshez, szolgáltatáshoz, marketinghez és egyebekhez.
- Zoom: SaaS-megoldásként szállított videokonferencia- és kommunikációs platform.

A SaaS-t széles körben használják különféle iparágakban és üzleti funkciókban, és olyan előnyöket kínál, mint a költséghatékonyság, a könnyű használat, valamint a szoftveralkalmazások gyors üzembe helyezése és méretezhetősége kiterjedt informatikai infrastruktúra és felügyelet nélkül.

3. AZURE VIRTUAL DESKTOP ÉS CLOUD PC

3.1 Azure Virtual Desktop

Azure Virtual Desktop (AVD) egy Microsoft által nyújtott szolgáltatás, amely lehetővé teszi felhőalapú távoli munkaállomások és alkalmazások biztosítását. Az AVD lehetővé teszi az IT-szervezetek számára, hogy virtuális gépeket futtassanak az Azure-ban, és hogy a felhasználókhoz a hálózaton keresztül elérhetővé tegyék ezeket a munkaállomásokat és alkalmazásokat [5].

Lényegében a távoli munkaállomások lehetővé teszik a felhasználók számára, hogy távolról hozzáférjenek a Windows 10 vagy Windows 11 operációs rendszerű munkaállomásokhoz az Azure-ban. Az AVD lehetővé teszi az alkalmazások virtualizálását és futtatását a felhőben, lehetővé téve a felhasználók számára, hogy bárhol és bármikor hozzáférjenek azokhoz. Az AVD lehetővé teszi a virtuális gépek skálázását és dinamikus kezelését az igényeknek megfelelően.

A Microsoft biztonsági funkciókkal látja el az AVD-t, például többrétegű védelemmel, titkosítással és hitelesítési lehetőségekkel. Integrálható más Microsoft szolgáltatásokkal, például az Azure Active Directory-jal, az Office 365-tel és az Intune-nal.

Az AVD hasznos lehet az IT-szervezetek számára, hogy növeljék a rugalmasságot és a mobilitást, biztosítsák a biztonságot és a felhasználói élményt, valamint egyszerűsítsék az alkalmazások kezelését és frissítését.

3.2 Cloud PC

Egy "cloud PC" vagy "felhőalapú számítógép" egy olyan számítási modell, amelyben a számítógép teljesítése és adattárolása a felhőben, azaz távoli szervereken található. Az ilyen típusú számítógépek lehetővé teszik, hogy a felhasználók távolról hozzáférjenek az alkalmazásokhoz és az adatokhoz bármilyen eszközről, amely internetkapcsolattal rendelkezik. Ezek a számítógépek gyakran virtuális gépekként vagy hálózati alapú számítási szolgáltatásokként működnek, és előnyös lehetnek azoknak, akiknek nagy számítási teljesítményre vagy adattárolásra van szükségük, de nem szeretnének vagy nem tudnak fizikai számítógépeket üzemeltetni.

3.3 Cloud PC és AVD

A Cloud PC (felhőalapú számítógép) és az AVD (Azure Virtual Desktop) két különböző felhőalapú számítási szolgáltatás, amelyek mindkettőt a Microsoft Azure platformon kínálja. Ezek között a következő különbségeket lehet találni. A Cloud PC általában egy teljes virtuális asztali számítógépet kínál, amelyet a felhasználók egyéni munkakörnyezetként használhatnak. Ez magában foglalhatja az operációs rendszert, az alkalmazásokat és az adatokat. A Cloud PC-t általában egyetlen felhasználó használja, és a teljesítmény és az erőforrások némileg statikusak lehetnek.

Az AVD egy rugalmas, skálázható platformot kínál a virtuális asztali számítógépek (VDI) létrehozásához és kezeléséhez, amelyeket több felhasználó is megoszthat. Ez lehetővé teszi az IT-szervezetek számára, hogy központilag kezeljék és biztosítsák a virtuális asztali környezeteket. Skálázhatóbb, és lehetővé teszi több virtuális asztali számítógép (VD) létrehozását és menedzselését, amelyeket több felhasználó is megoszthat. Az AVD lehetővé teszi az erőforrások dinamikus alkalmazkodását a felhasználói igényekhez.

Mindkét szolgáltatást az Azure felhőplatformon keresztül kínálja a Microsoft, de az árak és a licencelési modell kissé eltérhet. Az AVD esetén a licencelési modell lehetővé teszi az Office és más Microsoft szoftverek hozzáférését is bizonyos előfizetések esetén. Mindkét szolgáltatás lehetővé teszi a felhasználók számára, hogy távolról hozzáférjenek a virtuális asztali számítógépekhez, azonban a felhasználási esetektől és az igényektől függően választható a megfelelő szolgáltatás.

4. MEGVALÓSÍTÁSHOZ ALKALMAS TECHNOLÓGIÁK

4.1 Microsoft Azure

A Microsoft Azure-ra gyakran Azure néven hivatkoznak, ez egy teljes körű számítási felhő platform és a Microsoft által biztosított szolgáltatás. Az Azure 2010-ben jelent meg, és az integrált felhőszolgáltatások széles választékát kínálja, ezek a szolgáltatások magukban foglalják az energiaellátást, a tárolást, az adatbázisokat, a gépi tanulást, a hálózatépítést, az elemzést és még sok mást. Lehetővé teszi a szervezetek számára alkalmazások és szolgáltatások létrehozását, üzembe helyezését és kezelését a Microsoft adatközpontjainak világméretű hálózatán keresztül. Az Azure számos operációs rendszert, nyelvet, keretrendszert, adatbázist és eszközt támogat, így sokoldalú és méretezhető megoldás minden méretű vállalkozás számára.

4.2 IaC technológiák

Az Infrastructure as Code (IaC) egy olyan koncepció és gyakorlat a szoftverfejlesztésben és a rendszeradminisztrációban, amely magában foglalja a számítási infrastruktúra gépi olvasható parancsfájl-fájlokon keresztüli kezelését és kiépítését, nem pedig fizikai hardverkonfigurációt vagy interaktív konfigurációs eszközöket. Az IaC célja az infrastruktúra telepítési, konfigurálási és kezelési folyamatának automatizálása, a szoftverfejlesztés elveit az IT infrastruktúra területére hozva [6].

Az IaC deklaratív vagy kötelező megközelítést alkalmaz az infrastruktúra kívánt állapotának meghatározására. Deklaratív megközelítésben megadja, hogyan nézzen ki a végső infrastruktúra, és az IaC eszköz határozza meg, hogyan érje el ezt az állapotot. Egy kötelező megközelítésben lépésről lépésre határozza meg a kívánt állapot elérésének folyamatát.

Az IaC-szkripteket általában verziókezelő rendszerekben (például Gitben) tárolják, így a csapatok nyomon követhetik a változásokat, együttműködhetnek, és szükség esetén visszaléphetnek a korábbi verziókra. A verziókezelés az infrastruktúra-módosítások történetét tartalmazza, megkönnyítve a konfigurációk és a telepítések kezelését az idő múlásával.

Automatizálja az infrastruktúra kiépítését és kezelését, csökkentve a rendszerek felállításához és karbantartásához szükséges manuális erőfeszítést. Az automatizálás elősegíti a következetességet, az ismételhetőséget és a megbízhatóságot az infrastruktúra-telepítések során. Az IAC lehetővé teszi az infrastruktúra egyszerű méretezését a változó munkaterheléshez. A méretezés a konfigurációs fájlok módosításával és újra telepítésével érhető el, az új erőforrások manuális kiépítése helyett.

Az Infrastructure as Code elősegíti a fejlesztési és üzemeltetési csapatok közötti együttműködést. A fejlesztők az alkalmazáskód mellett verziózhatják, megoszthatják és tesztelhetik az infrastruktúra-konfigurációkat, ami hatékonyabb és együttműködőbb munkafolyamatokhoz vezet.

Az IaC-eszközöket gyakran felhő-agnosztikusra tervezték, lehetővé téve ugyanazt a kódbázist különböző felhőszolgáltatóknál vagy akár helyszíni környezetekben. Ez a rugalmasság értékes a többfelhős vagy hibrid felhőalapú stratégiákkal rendelkező szervezetek számára.

A közös infrastruktúra kódként szolgáló eszközök közé tartozik a Terraform, az Ansible, a Puppet, a Chef és a CloudFormation. Ezek az eszközök lehetőséget biztosítanak az infrastruktúra-konfigurációk kódban történő kifejezésére, valamint az erőforrások telepítésének és kezelésének automatizálására.

Összességében az Infrastructure as Code a modern IT és DevOps munkafolyamatok alapvető gyakorlata, amely megkönnyíti az infrastruktúra gyors és megbízható kiépítését az alkalmazások és szolgáltatások támogatásához.

4.2.1 Terraform

A Terraform egy nyílt forráskódú Infrastructure as Code (IaC) eszköz, amelyet a HashiCorp fejlesztett ki. Lehetővé teszi a felhasználók számára az infrastruktúra kódként történő meghatározását, biztosítását és kezelését. A Terraform számos felhőszolgáltatót, helyszíni környezetet és egyéb infrastruktúra-összetevőt támogat, így sokoldalú eszköz az erőforrások konzisztens és automatizált kezeléséhez.

A Terraform deklaratív nyelvet használ az infrastruktúra kívánt állapotának meghatározásához. A felhasználók meghatározzák a kívánt erőforrásokat és konfigurációkat, a Terraform pedig meghatározza, hogyan érheti el ezt az állapotot. A Terraform a felhőszolgáltatók széles körét (pl. AWS, Azure, Google Cloud), valamint számos egyéb infrastruktúra-összetevőt (például adatbázisokat, DNS-t, megfigyelési rendszereket) támogat. Minden támogatott platformot "szolgáltatónak" neveznek, és a Terraform szolgáltatói beépülő modulokat használ az ezekkel a platformokkal való interakcióhoz. A Terraformban az "erőforrás" az infrastruktúra egy része, például egy virtuális gép, tároló vagy hálózati összetevő. A felhasználók a konfigurációs fájljaikban határozzák meg az erőforrásokat, megadva az egyes erőforrások kívánt jellemzőit.

A Terraform nyomon követi az általa kezelt infrastruktúra állapotát. Ez az állapot egy fájlban tárolódik, és rögzíti az egyes erőforrások aktuális állapotát. Ez segít a Terraformnak megérteni, milyen változtatásokat kell végrehajtani, hogy a tényleges infrastruktúra összhangba kerüljön a kívánt konfigurációval.

Mielőtt megváltoztatná az infrastruktúrát, a Terraform végrehajtási tervet készít, amely felvázolja, milyen lépéseket kell tenni a kívánt állapot elérése érdekében. A felhasználók a módosítások alkalmazása előtt áttekinthetik a tervet.

Összességében a Terraform használatával az infrastruktúra hatékonyabban, következetesebben és együttműködve menedzselhető. Lehetővé teszi az infrastruktúra kódjának verziószámát, megkönnyítve a változások időbeli követését. A Terraform széles körben elterjedt a DevOps közösségben, mint eszköz az infrastruktúra felhő-agnosztikus és automatizált módon történő kezelésére.

4.2.2 Azure ARM

Az Azure Resource Manager (ARM) egy eszköz, amit a Microsoft használ, mint IaC megközelítés. Ezzel segíti a Microsoft Azure által biztosított üzembe helyezési és felügyeleti szolgáltatás az Azure-környezet erőforrásainak szervezéséhez és kezeléséhez. Ez az eszköz lehetővé tudja tenni számunkra a felhőben használt erőforrások konzisztens és kiszámítható módon történő üzembe helyezését, frissítését és törlését. Ez a megközelítés a Microsoft által használt IaC eszközökhöz tartozik.[3]

Az Azure-ban lévő erőforrások erőforráscsoportoknak nevezett logikai tárolókba vannak rendezve. Az erőforráscsoportok az erőforrások egyetlen entitásként történő kezelésére és figyelésére szolgálnak.

Az ARM-sablonok deklaratív nyelvet használnak, ami azt jelenti, hogy Ön határozza meg, hogy mit szeretne telepíteni, majd az ARM meghatározza az ehhez szükséges lépéseket. Ez ellentétben áll az imperatív szkriptekkel, amelyek a kívánt állapot eléréséhez szükséges lépések felé irányítják.

A különböző sablonok támogatják a paraméterezést, és ezzel lehetővé teszik azt, hogy az erőforrás-konfigurációkat testre tudjuk szabni a bemeneti paraméterek alapján. Ez megkönnyíti a sablonok újra felhasználását és felhasználását sok helyzetben.

Az ARM integrálódik az Azure RBAC-jával, így szabályozhatja, hogy kik biztosíthatják vagy kezelhetik az erőforrásokat különböző szinteken (előfizetés, erőforráscsoport, erőforrás).

Míg az erőforrásokat programozottan kiépítheti és kezelheti az ARM-sablonok segítségével olyan eszközökön keresztül, mint az Azure CLI vagy a PowerShell. Az Azure Portal segítségével olyan grafikus felületet is létrehozhat és biztosíthat erőforrásokat, amely ARM-sablonokat generál a háttérben.

Az ARM az infrastruktúra automatizálásának és kezelésének kulcsfontosságú összetevője az Azure-ban, szabványosított és méretezhető módot biztosítva az erőforrások biztosítására és kezelésére. Követi az infrastruktúra, mint kód elveit, és támogatja a konzisztens, megismételhető és verziószámú infrastruktúra telepítését.

Míg az erőforrásokat az ARM-sablonok segítségével használhatja és kezelheti olyan eszközökön keresztül, mint a CLI vagy a PowerShell, az Azure Portal segítségével olyan grafikus felületet is létrehozhat és telepíthet erőforrásokat, amely szükség szerint ARM-sablonokat generál.

Az ARM elengedhetetlen az Azurebeli infrastruktúra automatizálásához és kezeléséhez, szabványosított és sokoldalú módot biztosít az erőforrások üzembe helyezésére és kezelésére. Ez összhangban van az Infrastructure as Code elveivel, amely lehetővé teszi a konzisztens, reprodukálható és verzió-vezérelt infrastruktúra-telepítéseket.

4.3 Automatizálási eszközök

4.3.1 Powershell

A PowerShell a Microsoft által kifejlesztett keretrendszer a feladatok automatizálására és az eszközök konfigurálására. A parancssorban lévő Shellből és egy programozási nyelvből áll. A PowerShell célja a Windows alapú operációs rendszerek és alkalmazások adminisztrációjának automatizálása, emellett a Microsoft és harmadik felek különféle technológiáinak kezelésére is használják.

Parancssori felülettel rendelkezik, amely lehetővé teszi a felhasználók számára, hogy parancsok beírásával kapcsolatba lépjenek a rendszerrel. Különféle parancsok, úgynevezett parancsmagok végrehajtását segíti elő, amelyek kicsi, célzott segédprogramok, amelyek meghatározott célokat szolgálnak.

A PowerShell egyik egyedi jellemzője a folyamatvégrehajtás objektumorientált megközelítése. A függvények közötti szövegátvitel helyett a PowerShell strukturált adatokat továbbít. Ez megkönnyíti az adatok következetes kezelését és módosítását.

A PowerShellt általában a feladatok automatizálására és konfigurálására használják. Gyakran használják technológiai környezetekben olyan feladatoknál, mint a rendszerek konfigurálása, szoftverek telepítése.

5. MEGVALÓSÍTÁSHOZ HASZNÁLT TECHNOLÓGIÁK

Magának az infrastruktúrának a kialakításához több IaC, illetve több felhőtechnológiát is választhatunk. Ebben a fejezetben kitérek, hogy miért a bizonyos technológiák lettek választva a feladat végrehajtására.

5.1 IaC technológia kiválasztása

A feladat megvalósításához Terraformot fogunk használni. A Terraform és az Azure Resource Manager (ARM) hasonló célokat szolgálnak az infrastruktúra kódként (IaC) történő engedélyezésével és az erőforrások kiépítésével a felhőben. Vannak azonban különbségek, amelyek az egyiket előnyben részesíthetik a másikkal szemben az egyedi igények alapján. A Terraform több felhőszolgáltatót is támogat, nem csak az Azure-t [7]. Ez a rugalmasság lehetővé teszi a felhasználók számára, hogy egyetlen eszközzel kezeljék az erőforrásokat a különböző felhőkben (AWS, GCP, Azure) és helyszíni környezetekben. Az ARM viszont az Azure-ökoszisztémára jellemző.

A Terraform deklaratív megközelítést követ, ahol Ön meghatározza az infrastruktúra kívánt állapotát, és a Terraform kitalálja, hogyan érheti el azt. Az ARM szigorúbb megközelítést alkalmaz, ahol meghatározza az erőforrások létrehozásának konkrét lépéseit.

A Terraform hatalmas és aktív közösséggel rendelkezik, amely a közösség által támogatott modulok és erőforrások széles skáláját kínálja. Ez megkönnyítheti a különböző infrastruktúra-összetevők kódjának megtalálását és újra felhasználását. Az ARM közössége egyre bővül, de a szélesebb felhasználói bázis miatt kevesebb erőforrással rendelkezik a Terraformhoz képest. A Terraform nyomon követi az infrastruktúra állapotát, ami lehetővé teszi az erőforrások hatékonyabb kezelését, módosítását és megsemmisítését. Az ARM hasonló képességekkel rendelkezik, de további eszközöket igényelhet az összetett állapotkezeléshez.

Az ARM-sablonok natívak az Azure-ban, és egyszerűbbek lehetnek az Azure-központú telepítéseknél. A Terraform, bár sokoldalúbb, kissé meredekebb tanulási görbével rendelkezhet szélesebb hatókörének és több felhőszolgáltató támogatásának köszönhetően.

A Terraform és az ARM is folyamatosan fejlődik, de a Terraform gyakran gyors ütemben vezet be új funkciókat és frissítéseket. Ez a gyakori frissítési ciklus előnyös lehet a legújabb felhőajánlatok naprakészen tartása szempontjából, de kihívásokat jelenthet a stabilitás és a kompatibilitás tekintetében.

Lényegében a Terraform többfelhős támogatása, deklaratív megközelítése és nagyobb ökoszisztémája előnyös választássá teheti a különböző felhőkörnyezetekben rugalmasságot kereső szervezetek számára. Azok számára azonban, akik sokat fektettek az Azureba, és kizárólag erre az ökoszisztémára összpontosítanak, az ARM személyre szabottabb és natív támogatást kínálhat. Végső soron a választás függhet a konkrét igényektől, a meglévő készségkészletektől és attól, hogy a szervezet milyen mértékben szeretné elkerülni a felhőszolgáltatók bezárását.

5.2 Aviatrix

Az Aviatrix egy felhőalapú natív hálózati vállalat. A többi hálózati gyártótól eltérően az Aviatrix szoftverplatform megérti a felhőszolgáltató natív konstrukcióit. Ez lehetővé teszi a natív konstrukciók közvetlen kihasználását és vezérlését a felhőszolgáltató API-jaival, bővítve képességeiket és integrálva azokat szoftverünkbe, hogy kulcsrakész megoldásokat biztosítsanak a szervezetek számára, amelyek felgyorsítják a felhőben való utazást.

Az Aviatrix arra összpontosít, hogy megoldja azokat a gyakori hálózati problémákat, amelyekkel a vállalatok nyilvános felhőútjuk során szembesülnek, miközben olyan közös vezérlősíkot biztosítanak, amely több fiókos/többfelhős automatizálást, fejlett szállítási szolgáltatásokat, biztonsági szolgáltatásokat, hibaelhárítási lehetőségeket és láthatóságot biztosít.

Néhány gyakori vállalati felhasználási esetet:

- Adatközpontból felhőbe (Aviatrix Transit Network megoldás)
- Skálázható tűzfal telepítése a felhőben (tűzfalhálózat)
- Felhőből felhőbe VPN (titkosított társviszony-létesítés felhőben és több felhőben)
- Felhasználótól felhőbe VPN (távoli felhasználói VPN (OpenVPN® alapú SSL VPN megoldás) fejlesztőknek)

- Webhelyről felhőbe VPN (fióktelepről és ügyféloldalról felhőbe)
- Multicloud VPN (Multicloud Peering)

5.3 Felhőplatform

Az Azure több szempontból is kiemelkedik, amelyek erős versenyzővé teszik a felhőplatformok között, de az, hogy határozottan „jobb”, a konkrét igényektől és kontextusoktól függ. Azonban más felhőplatformoknak, például az AWS-nek és a Google Cloud Platformnak (GCP) is megvannak az erősségeik különböző területeken [8]. Az AWS például hosszabb futamidővel rendelkezik a felhőterületen, és számos szolgáltatással rendelkezik. A GCP az adatelemzés és a gépi tanulás terén szerzett szakértelméről ismert.

A „legjobb” felhőplatform kiválasztása gyakran olyan tényezőktől függ, mint a konkrét munkaterhelési követelmények, a meglévő technológiai befektetések, a földrajzi jelenlét, az árképzési modellek és az egyes szolgáltatások vagy integrációk iránti igény. E tényezők értékelése az egyes platformok erősségeihez képest segít a megalapozott döntés meghozatalában.

6. FELADAT SPECIFIKÁCIÓ

Jelen írás célja egy Azure Virtual Desktop tervezése, bemutatása, naprakészen tartása és további fejlesztési lehetőségek feltárása a beüzemelése során. Ennek eléréséhez egy meglévő nyilvános felhőplatformot fogok használni, és a jövőben ez a Microsoft Azure lesz. A probléma megoldása során megbeszéljük az infrastruktúra megvalósításának lehetséges módjait, megvizsgáljuk a választott technológia előnyeit és hátrányait. A megvalósítás során a biztonsági kérdésekre a különböző szervezeti szabályok felállításával kapunk választ.

Az elkészült infrastruktúra üzembe helyezése során automatizálási, skálázhatósági és rendelkezésre állási problémákkal is találkozunk, amelyekre a megvalósítás során kerül sor. A megvalósítás során kiválasztjuk a megfelelő hálózati berendezéseket, hálózati beállításokat, alhálózatokat és biztonsági mentéseket.

A Terraformal deklaratív infrastruktúrán és kódon keresztül automatizálja a konfigurációt és a biztonságot is. Az infrastruktúra és a szabályok kodifikálása, megosztása, verziószáma és érvényre juttatása az összes infrastruktúra konzisztens munkafolyamatában történik.

Nemcsak felhő infrastruktúrát fogunk létrehozni, hanem folyamatokat is automatizálunk rajta, ehhez pedig Powershell-t fogunk használni.

A Powershell egy többplatformos automatizálási és konfigurációs keretrendszer, amely Linuxon, Windowson és macOS-en érhető el. A Powershell kiválóan alkalmas a meglévő eszközök automatizálására, a strukturált adatok, például: JSON, CSV, XML stb. módosítására és kezelésére. A Powershell még a REST API-kat is képes kezelni, és elsősorban ezekre van optimalizálva.

A választott témámban kitérek arra, hogyan biztosítható a hálózati infrastruktúra környezet tervezése, megvalósítása és tesztelése nyilvános felhőplatform segítségével a Microsoft Azure platformon. Ebben a cikkben részletezem a felhőplatformok összehasonlítását, valamint a választott technológiák előnyeit és hátrányait.

A probléma megoldása során az alkalmazást a Microsoft Azure platformra adaptáltam. Az infrastruktúra tervezése és a funkcionalitás megvalósítása számos területet érint a Microsoft Azure platformon, például a hálózati megvalósítást, a biztonsági megfontolásokat, az automatizálást és az adattárolás használatát a nyilvános felhőplatformon.

7. HÁLÓZATI ÁTTEKINTÉS

7.1 Azure hálózati koncepció

7.1.1 Virtuális hálózat (VNET)

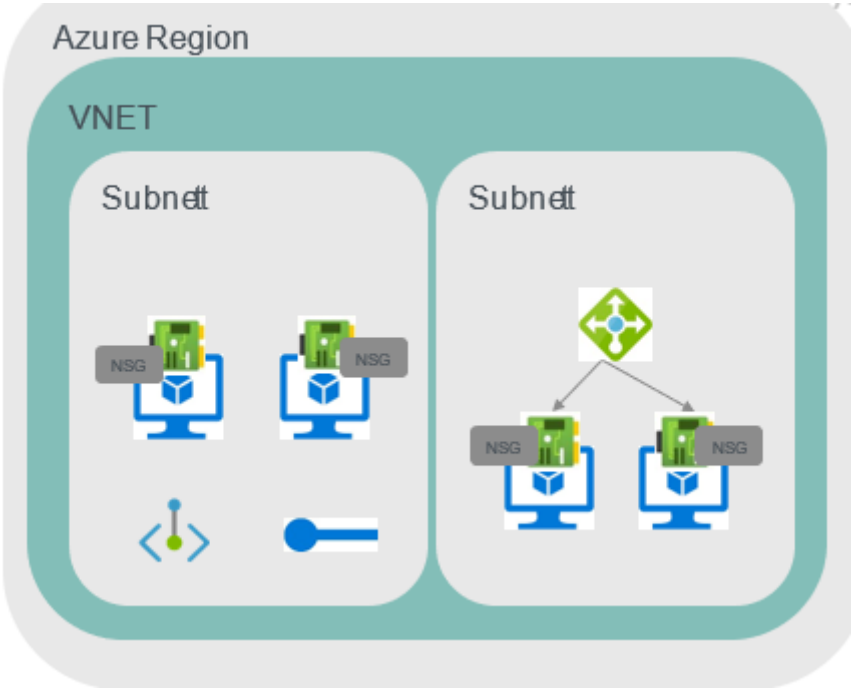
Az Azure több régióból áll. Ezek között a régiók között minden régió VNET-készletet tartalmaz. A VNET egy logikai hálózati rész, amely erőforrásokat tárol hálózati csatlakozási igényekkel (NIC-k, privát/szolgáltatási végpontok stb.).

A VNET egy vagy több IP-előtaggal rendelkezik és egy vagy több alhálózattal rendelkezik előtagokkal a VNET-tartományból. Az alhálózatok nincsenek AZ-okhoz kötve. Alapértelmezés szerint teljes kapcsolat van a VNET erőforrásai között, korlátozva a hálózati biztonsági csoportokkal.

Hydro elnevezés: <BA név>-<IT/OT>-<ENV>-

<szám>-<Régió>-VNET-<szám>,

például. ALME-OT-PRD-01-WEU-VNET-02



7.1. ábra Virtuális hálózat (Saját forrás)

7.1.2 VNET Peering

Két VNET-et ugyan abban a régióban vagy régiók között fogjuk csatlakoztatni. Ezek Azure gerinchálózatot „Azure Backbone network”. Ez egyetlen hálózatként jelenik meg a csatlakozáshoz, de külön erőforrásként fog kezelődni számunkra. Ennek a módszernek nagy előnye a nagy áteresztőképesség.

Különösen fontos kérdések, és veszélyek amire figyelni kell:

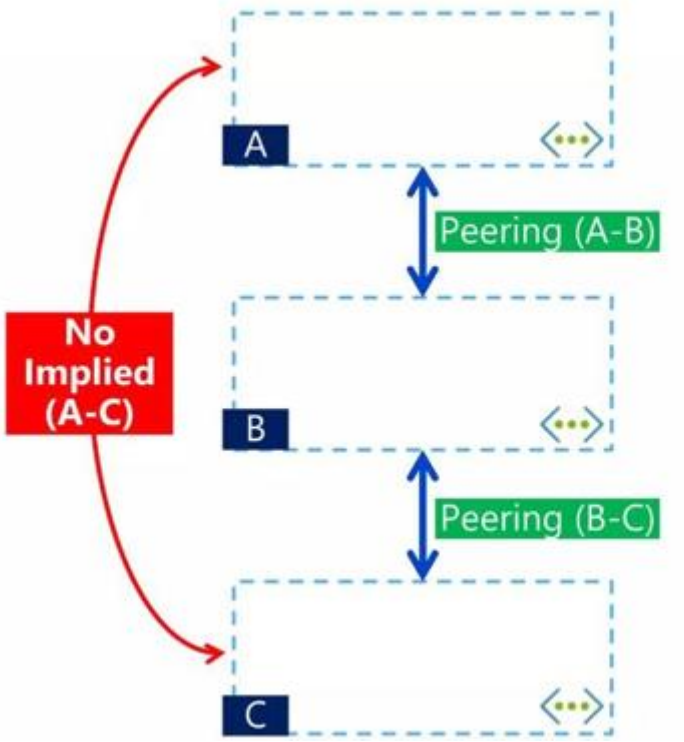
• A VNET peering „társviszony-létesítés” 2 virtuális hálózat között zajlik, és közöttük nem fog megvalósulni tranzitív kapcsolat.

• Az IP-címterek nem fedhetik át egymást.

• A VNET-közi forgalom nincs titkosítva.

• Minden VNET továbbra is rendelkezik saját DNS-beállítással.

• Alapértelmezés szerint: 10 peering „társviszony-létesítés” VNET-enként.



7.2. ábra VNET Peering (Saját forrás)

A virtuális hálózati (VNet) társviszony-létesítés egy olyan mechanizmus, amelyet a számítási felhőben használnak két virtuális hálózat összekapcsolására ugyanazon felhőszolgáltató környezetében, lehetővé téve számukra, hogy úgy kommunikáljanak egymással, mintha ugyanannak a hálózatnak lennének. Íme a VNet társviszony-létesítés bontása:

Virtuális hálózatok összekapcsolása: A virtuális hálózatok társviszony-létesítése lehetővé teszi közvetlen, privát kapcsolat létrehozását két virtuális hálózat között ugyanazon a régión belül vagy ugyanazon felhőszolgáltatón belül [9].

Privát kommunikáció: A társítást követően a virtuális hálózatok privát IP-címek használatával kommunikálhatnak egymással, mintha ugyanannak a hálózatnak lennének. Ez a kommunikáció biztonságosan történik a felhőszolgáltató gerinchálózatán belül, elkerülve a nyilvános internetnek való kitettséget.

Tranzitív kapcsolat: A VNet társviszony-létesítés lehetővé teszi a tranzitív kapcsolatot, ami azt jelenti, hogy ha az A VNet B VNettel, a B VNet pedig C VNettel van társítva, akkor az A és C virtuális hálózatok közvetetten kommunikálhatnak az A és B, valamint a B és C közötti peer kapcsolaton keresztül.

Forgalomfolyamat: A társított virtuális hálózatok közötti forgalom nem hagyja el a felhőszolgáltató hálózati gerincét, ami alacsony késleltetésű és nagy sávszélességű kommunikációt eredményez.

7.1.3 Magas rendelkezésre állás

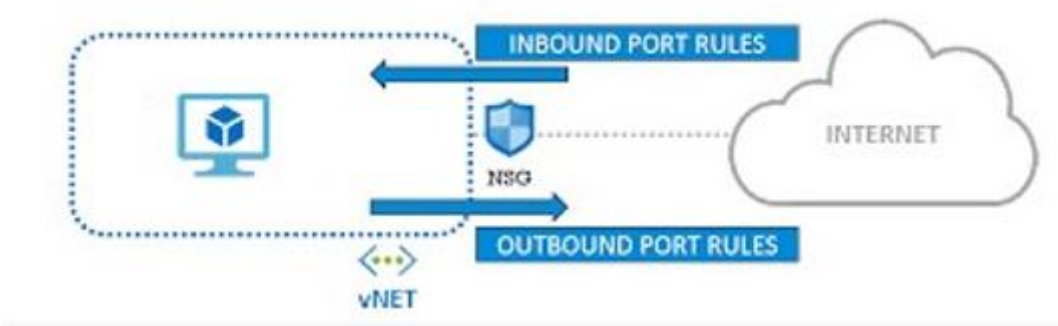
Az Azure régiókból áll és ezek az egyes régiókban több DC, elérhetőségi zóna található. Az rendelkezésre állási zónák rendelkezésre állási készletekkel rendelkeznek (külön tűzrekeszek). Az elérhetőségi készletek mindegyike hibatartományokkal rendelkezik (ugyanaz az áramforrás/hálózati kapcsoló).

Sok Azure-szolgáltatás alapértelmezés szerint régióközi vagy AZ közötti HA-val rendelkezik (például tárhely). A hálózati koncepciók ezt a rendelkezésre állási modellt követik, a legtöbb felhőalapú hálózati komponens AZ-redundáns, vagy AZ-redundáns változatai vannak. Amikor regionális szinten telepítünk valamit, az egyetlen AZ-hoz megy.

7.2 Hálózati biztonsági csoportok

Alapvető hálózati konstrukció, amely forgalomszűrést biztosít a munkaterhelésekhez, nem látható a biztonsági csapat, illetve haladó hálózati megoldások sem láthatók.

A virtuális gép hálózatához van hozzákapcsolva a biztonsági csoport és vezérli, engedélyezi a kimenő és bejövő forgalmat a hálózatunkhoz. Különböző prioritásokat használ, amelyeket tízesével inkrementál.



7.3. ábra Biztonsági csoportok (Saját forrás)

7.3 Útválasztás – Felhasználó által meghatározott útvonalak

Minden alhálózathoz tartozni fog egy útválasztó tábla, ami, ha nincsen társítva az alhálózathoz, akkor a rendszer alapértelmezett útvonalait használja (0/0 az internet felé, hozzáférés a társított VNET-ekhez), a rendszerútvonalakat felülírják az UDR-ek.

Amikor egy csomag elhagyja a felületet, eléri az alhálózathoz tartozó útválasztási táblát.

• Cél előtag: IP-cím vagy szolgáltatáscímke (Microsoft Services, az IP-k gyűjteményét jelenti)

• Next-hop opciók: Internet, Virtuális készülék, Nincs, Virtuális hálózat (helyi), Virtuális hálózati átjáró

A következő ugrás egy társított VNET-re irányítható (ellentétben az AWS-sel) – a forgalom tűzfalra továbbítására szolgál.

7.3.1 Internet Ingress Connectivity

Egy olyan Traffic Manager, ami DNS-alapú terheléselosztást biztosít az Azure-régiók között, amely hasznos a régiók közötti DR-t igénylő külső alkalmazásokhoz [10].

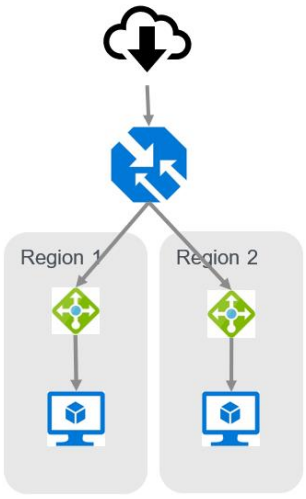
A regionális terheléselosztók vagy alkalmazásátjárók előtt áll.

• CDN (Azure Front Door)

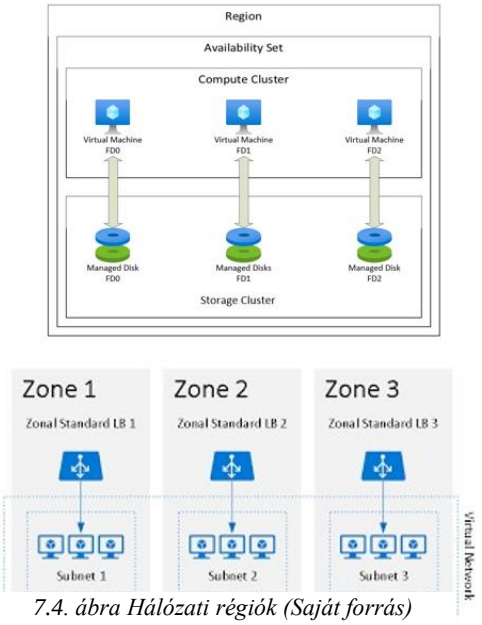
• Tartalmi gyorsítótárat biztosít a felhasználókhoz közeli külső alkalmazások számára a felhasználói élmény javítása érdekében

Olyan külső terheléselosztó, ami, alkalmazás elérhetőséget biztosít a 80/443-as porton kívüli forgalom számára. Nem ad láthatóságot a biztonsági csapatnak, nem végez forgalomszűrést, a forgalmat tűzfallal kell ellátni. Egy vagy több előtérbeli IP-címmel és egy, vagy több háttérkészlettel rendelkezik a munkaterhelésekhez A munkaterheléseket állapotellenőrzésekkel ellenőrzik (ellenőrizzük a mérőszámokat, ha a példányok nem érhetők el). Külső alkalmazásátjárók, ami külső alkalmazások elérhetőségét biztosítja a HTTP/HTTPS forgalom számára.

WAF funkcionalitást és fejlett HTTP/HTTPS útválasztási funkciókat biztosít nyilvános IP a példányon.



7.5 ábra Internet Ingress Connectivity (Saját forrás)



7.4. ábra Hálózati régiók (Saját forrás)

7.3.2 Internet kilépési kapcsolat

A központi tűzfalra mutató útvonal, egy UDR, amely az alapértelmezett útvonalat (0.0.0.0/0) egy központi tűzfal IP-címére irányítja, amely internet-hozzáférést biztosít. Vállalati környezetben ez a preferált internet-hozzáférési mód, ami lényegében egy NAT-átjáró.

Adott alhálózatokhoz csatolt felügyelt szolgáltatás, VNET-enként NAT-átjáró szükséges, és legalább egy nyilvános IP-cím szükséges. Ez egy külső terhelosztó és használatához szükséges beállítanunk kimenő szabályokat az internet-hozzáféréshez.

A virtuális gépen nyilvános IP címet fogunk használni, mert a nyilvános IP közvetlen internet-hozzáférést biztosít, ha az alapértelmezett útvonal az internetre mutat az alhálózatban.

Alapértelmezés szerint minden virtuális gép közvetlen hozzáférést kap az internethez, ha az alhálózat útválasztási táblájában van egy internetre mutató alapértelmezett útvonal (0.0.0.0/0), de ez az alapértelmezett hozzáférés korlátozott, és nem szabad használni, nyugdíjba kerül.

A privát végpont egy hálózati kártya az alhálózatban IP-címmel, amely az Azure-szolgáltatásokat vagy a mögöttes szolgáltatásokat nyújtja a terheléselosztó egy másik VNET-jében vagy egy másik előfizetésben privát úton közvetlenül elérhető.

Előnye az, hogy a forgalom soha nem éri el az internetet. Ez a preferált módszer az Azure-szolgáltatások elérésére mivel, biztosítja a legjobb késleltetést és átviteli sebességet az Azure-szolgáltatások számára.

A DNS-t úgy kell beállítani, hogy a privátra mutasson és a végpont a privát IP-címe a szolgáltatáshoz. Előnye az, hogy On-premről is elérhető, illetve támogatja az NSG-ket a hozzáférés korlázotása érdekében.

A szolgáltatási végpontok közvetlen útvonalakat adnak hozzá az Azure-szolgáltatásokhoz nyilvános IP-címekkel, az alhálózat útválasztási táblázatokhoz (nem látható az Útválasztási táblázatban)

Egyes Azure-szolgáltatások esetében ez a „privát” csatlakozási mód és a forgalom az Azure-hálózaton marad. Mivel az internet felé hoz létre útvonalakat erősen ajánlott használata az Azure-on belül, ahol csak lehetséges

Nem használható a forgalom on-prem vagy egyéb szolgáltatások felé történő irányítására

VNET-ek között

A szolgáltatásvégpont-házirendek felhasználhatók a forgalom további biztonságosabbá tételére a tárolási szolgáltatás végpontjai között. Különböző alhálózatokhoz hozzá lehet fűzni.

7.3.3 DNS –Domain Name Resolution

Az Azure DNS privát (belső erőforrások) és nyilvános (internet) névfeloldást biztosít. Nyilvános zónák tárolhatók az Azure-ban a külső erőforrásokhoz, illetve Privát zónák tárolhatók az Azure-ban a belső erőforrásokhoz [11]. Minden VNET-nél lehetőség van DNS-kiszolgálók beállítására, alapértelmezés szerint az Azure nyilvános feloldója használatos.

Az erőforrásoknak DNS-kiszolgálóként a 168.63.129.16-ra kell mutatniuk a DNS-feloldó IP-címét. Ha egyéni DNS-kiszolgálók vannak beállítva a VNET-hez, a kérések továbbításra kerülnek. Privát DNS-zónák csatolhatók a VNET-ekhez a privát névfeloldáshoz, illetve Privát DNS-zónák lekérdezhetők a helyszínről a Private Resolvers segítségével

Ha hálózat biztoságának megőrzése érdekében különböző hálózatbiztonsági bevált gyakorlatok szükséges használnunk. DDoS védelmet használjunk a külső erőforrásokon és NSG-ket használjunk olyan erőforrásokon, amelyek korlátozzák a bejövő forgalmat, ha lehetséges (nm engedjük meg sehonnan)

Ne használjunk nyilvános IP-címeket közvetlenül az erőforrásokon, győződjön meg arról, hogy a forgalom átmegy a tűzfalon. Biztosítsuk az internetes kimenő forgalom láthatóságát proxy használatával (pl. proxy virtuális gép, tűzfal, zScaler). Amikor csak lehetséges, használjunk privát végpontokat vagy szolgáltatásvégpontokat az Azure-szolgáltatások eléréséhez, és ne használjuk az internetet.

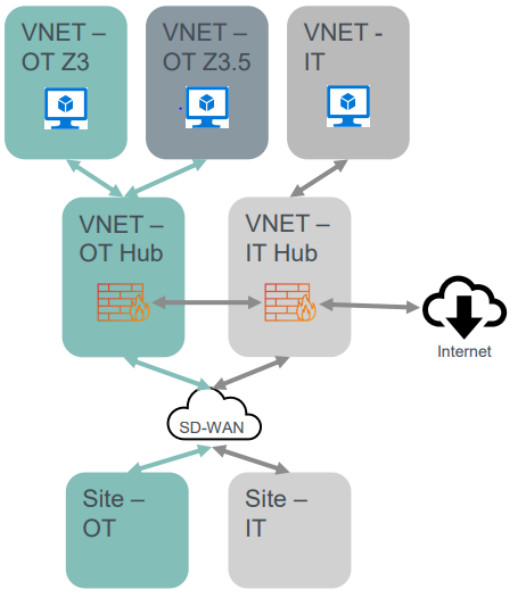
8. HÁLÓZATSZEGMENTÁLÁS ÉS KÖVETKEZMÉNYEI

A felhőben található minden zóna rendelkezik VNET-tárhelykészlettel az adott zóna munkaterhelésére, ami a zónát vezérli. A különböző zónákat tűzfalak védik a felhőben. Ezek dedikált hub VNET-ek-ben találhatóak meg.

Internet-hozzáférés csak a felhőben lévő IT tűzfalakon keresztül lehetséges. A különböző zónák az SD-WAN-on keresztül on-prem-re bővíthetők. Az útválasztás beállítása megakadályozza a kommunikációt az OT Z3.0-ról a felhőben IT munkaterheléseken keresztül.

Minden hálózati erőforrás egy erőforráscsoportban az OT számára (VNET-ek, RTB-k, NAT (átjárók stb.): ALME-OT-PRD-01-Network.

Egy IT erőforráscsoport: ALME-IT-PRD-01-NETWORK.



8.1. ábra Hálózati szegmentáció (Saját forrás)

8.1 Tipikus forgalom útvonala

A Purdue modellnek megfelelően csak az OT zóna 3.0 és zóna 3.5 kommunikálhatnak, vagy a 3.5 zóna és az IT kommunikálhatnak. Ugyanazon zónán belüli kommunikációhoz nem szükséges tűzfalnyílás (több VNET egy biztonsági zónában). A zónák közötti kommunikációhoz az OT és szükség esetén az IT tűzfalat kell nyitni.

Az On-Prem forgalom a forrástól függően eltérő utakon haladhat és a célhely és a különböző tűzfalak érintettek:

• OT Z3.0 a Site OT-hez: Közvetlenül az OT tűzfalon és az SD-WAN-on keresztül a helyszíni OT zónához.

• OT Z3.5 az IT-helyre: OT tűzfalon, IT-tűzfalon, SD-WAN-on keresztül a helyszín IT-zónájához.

• IT a helyszíni IT-hez: Közvetlenül az IT tűzfalon és az SD-WAN-on keresztül a helyszíni IT zónába.

A következő generációs, zScalerrel rendelkező PC-k esetében ez az útvonal más lesz.

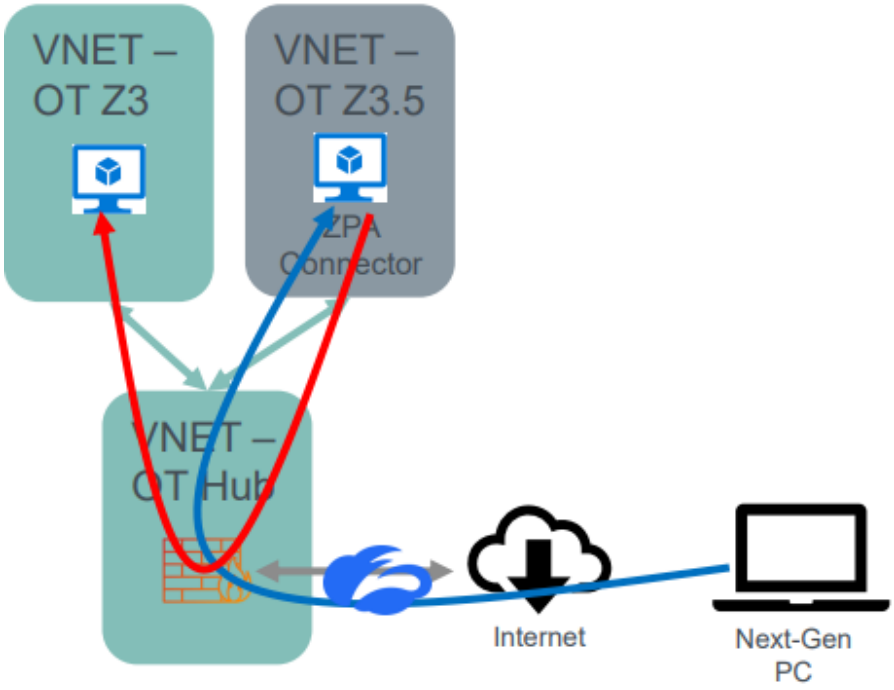
Az internetes kilépést IT-n keresztül a felhőben kell központosítani, így a tűzfalakat és a zScaler-t is. A Z3.0 felől érkező forgalom a Z3.5-ben lévő proxyn halad át a következő internet kilépési ponthoz. Amikor a forgalom a zScaleren halad át, MITM-et hajt végreHTTPS-forgalom esetén annak vizsgálatához az alkalmazásnak rendelkeznie kell a zScaler tanusítványával. Az informatikai tűzfal bizonyos forgalom esetén megkerülheti a zScalert ám ehhez forrás IP-rögzítést kell alkalmaznunk. Az internetes bejutást igénylő alkalmazásoknak az IT biztonsági zónájában kell lenniük a frontend rész eléréséhez (terheléselosztó/hátramenet). A háttérrendszer lehet IT biztonsági zónában vagy OT DMZ (Z3.5) zónában is.

Az internetről történő belépési pontnak egy alkalmazásnak kell lennie. Az átjáró WAF engedélyezve, de bizonyos esetekben még mindig van terheléselosztónk és nyilvános IP-címek a virtuális gépeken. A WAF vagy tűzfal biztonsági láthatóságot ad a forgalomnak.

8.2 zScaler

Minden következő generációs számítógépen telepítve van a zScaler kliens, amely továbbítja a belső forgalmat a zScaler Private Access (ZPA) felé és a külső forgalom a zScaler Internet Access (ZIA) között. A belső felhőforgalomhoz a ZPA virtuális gépeket a felhőben telepítjük az IT biztonsági zónájábanm illetve néhány OT biztonsági zónában.

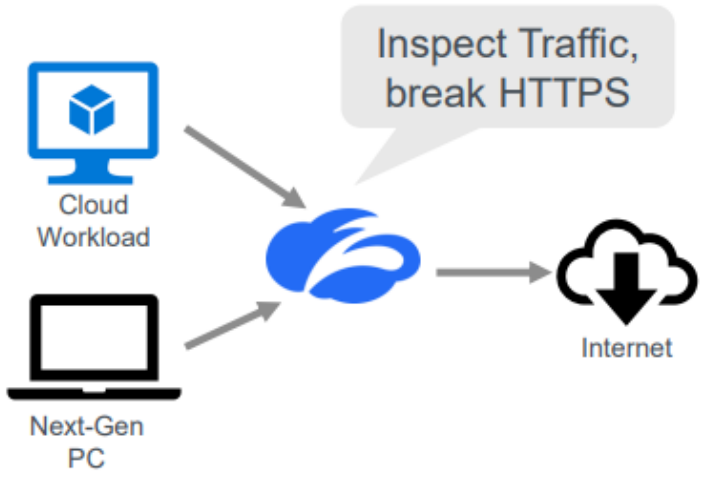
A forgalmat a Next-Gen PC-ről indítjuk, és a zScaler ellenőrzi és ha a házirend lehetővé teszi a továbbítást a legközelebbi ZPA App Connector munkaterheléshez. Amikor a forgalom elhagyja a ZPA-csatlakozót, normál kelet-nyugati forgalom lesz a felhőben.



8.2 ábra zScaler (Saját forrás)

Amikor kilépünk az internetre a következő generációs számítógépről, irodáról vagy a felhőből akkor a zScaler Internet Accessen keresztül fogunk csatlakozni. A zScaler Internet Access (ZIA) ellenőrzi az összes forgalmat, és engedélyezi vagy megtagadja azt, a biztonság meggondolások által meghatározott szabályok és irányelvek alapján. Ha a HTTPS-munkamenetek megszakadtak, az erőforrásoknak meg kell bízniuk a zScaler gyökér bizonyítványában.

Jelenleg csak a 80-as és 443-as porton engedélyezett a felhőben, de ezfokozatosan kerül enegedélyezésre minden forgalom számára. Úgy működik, hogy az összes külső DNS-lekérdezést zScaler IP-címekre oldjuk fel.



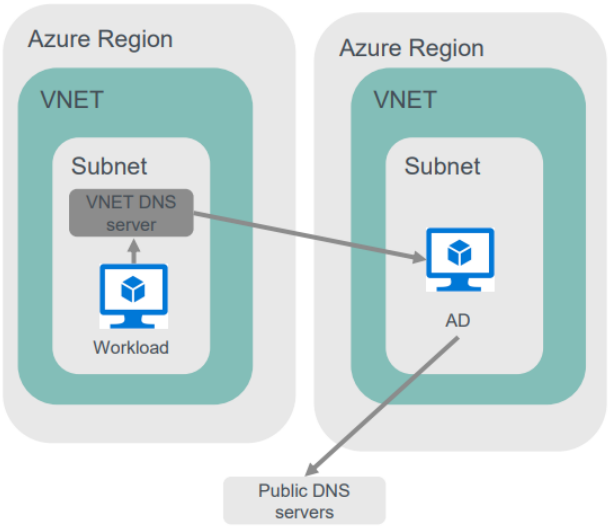
8.3 ábra zScaler 2. ábra (Saját forrás)

8.2.1 Public DNS

A DNS-t mindig az alapértelmezett 168.63.129.16 IP-címre kell beállítani a munkaterheléseken. Minden VNET-en egyénileg konfigurálva kell lennie a Hydro DNS-kiszolgálóknak (DNS-kiszolgálók NHY vagy GLOBAL.TO) A nyilvános DNS-feloldás azokon az AD DNS-kiszolgálókon történik, ahol a kéréseket kérik, és továbbítás szükséges. A nyilvános DSN-zónák csak külső terheléseket tartalmazhatnak.

Az On-Prem munkaterhelések kivéve a következő generációs PC-t, a DNS a Hydro DNS-kiszolgálókra van beállítva és a nyilvános DNS-feloldás az AD DNS-kiszolgálókon történik.

A következő generációs PC-ken más a helyzet. A DNS-t a zScaler oldja fel belső és külső terhelésekhez is, szerver IP 1.0.0.1. Nyilvános munkaterhelés esetén a DNS feloldása a tényleges IP-címre történik.



8.4 DNS (Saját forrás)

8.2.2 Privát DNS

A DNS-t mindig az alapértelmezett 168.63.129.16 IP-címre kell beállítani a munkaterheléseknek. Minden VNET-nek rendelkeznie kell a Hydro DNS-kiszolgálókkal egyéni DNS-ként konfigurálva (szerverek NHY vagy GLOBAL.TO). A VNET-ek privát DNS-zónával rendelkezhetnek a privát felhőalapú erőforrásokhoz. Ha nincs privát zóna csatolva, a privát kéréseket továbbítja az AD szervereknek, amelyek vagy a felhő privát zónáiba továbbítanak, vagy Infoblox/egyéb AD nem felhő eszközhöz.

A belső felhőalapú munkaterheléseket hozzá kell adni az Azure privát DNS-zónáihoz (pl. alme.hydro.com)

On-Prem munkaterhelések-nél (kivéve a következő generációs PC-t) a DNS a Hydro DNS-kiszolgálókra van beállítva, illetve, a privát DNS-feloldás az AD DNS-kiszolgálók használatával történik

Következő generációs PC-nél a DNS-t a zScaler oldja fel belső és külső terhelésekhez is, szerver IP 1.0.0.1. Privát munkaterhelések esetén a DNS egy zScaler-specifikus IP-címre van feloldva, a forgalom viszont zScaler virtuális gépeken keresztül továbbítva van beállítva a felhőben.

9. AZURE VIRTUAL DESKTOP KIÉPÍTÉSE

Azure Virtual Desktop (AVD) segítségével az Azure felhőben távoli munkaállomásokat hozhatunk létre és kezelhetünk. A Terraform egy kiváló eszköz az infrastruktúra kezelésére, ideértve az AVD környezetek létrehozását is. A Terraform segítségével leírhatod az AVD infrastruktúrát és erőforrásokat, és ezután a Terraform parancsokkal automatizálhatod a környezet kiépítését és kezelését [12].

Ez a Terraform konfiguráció egy alapvető AVD környezetet hoz létre, amely magában foglal egy virtuális hálózatot, egy Subnetet, egy virtuális gépet és egy hálózati interfészt. Természetesen ezt a konfigurációt tovább lehet bővíteni az AVD-hoz szükséges további erőforrások hozzáadásával és konfigurálásával.

Fontos megjegyezni, hogy az AVD telepítése Terraform segítségével további konfigurációs elemeket is igényelhet, például a Host Pool-okat, az alkalmazásokat, a felhasználók hozzáférési jogait stb. Ezenkívül az AVD beállításához szükséged lesz az Azure AD-re és az AVD-hoz kapcsolódó további szolgáltatásokra, mint például a diagnosztikai beállításokra is.

```
# Create AVD Workspace
resource "azurerm_virtual_desktop_workspace" "avd_wksp" {
  name = "${var.hostpool_name}-WS"
  location = var.location
  resource_group_name = var.resource_group
  friendly_name = var.hostpool-friendly-name != null ? var.hostpool-friendly-name : "${var.hostpool_name}-WS"

  lifecycle {
    ignore_changes = [ tags ]
  }
}

resource "azurerm_availability_set" "avd_availabilityset" {
  name = "avail-${var.hostpool_name}"
  location = var.location
  resource_group_name = var.resource_group
   lifecycle {
    ignore_changes = [ tags ]
  }
}
```

9.1 ábra Workspace kialakítása (Saját forrás)

Az Azure Virtual Desktop (AVD) munkaterület (Workspace) az AVD szolgáltatás központi eleme, amely lehetővé teszi a felhasználók számára a távoli asztali géphez és alkalmazásokhoz való hozzáférést az Azure-ban. A munkaterület számos komponenst foglal magában, például a felhasználókhoz tartozó Host Pool-okat, az alkalmazásokat és az engedélyezéseket. Ezt az infrastruktúrát Terraformmal is lehet kezelni, hogy automatizálni lehessen a munkaterület létrehozását és kezelését.

```
# Create AVD host pool
resource "azurerm_virtual_desktop_host_pool" "avd_hostpool" {
  resource_group_name      = var.resource_group
  name                     = var.hostpool_name
  location                 = var.location
  start_vm_on_connect      = true
  custom_rdp_properties    = var.host-pool-rdp-settings
  type                     = var.hostpool-type #"Pooled"
  maximum_sessions_allowed = var.sessions_allowed_perhost
  load_balancer_type       = var.load-balancer-type


   lifecycle {
    ignore_changes = [ tags ]
  }
}
```

9.2 ábra Hostpool létrehozása (Saját forrás)

Az Azure Virtual Desktop (AVD) Host Pool egy olyan gyűjtemény, amelyben a virtuális gépek találhatók, amelyek az ügyfeleknek távoli asztali hozzáférést biztosítanak. Ezek a gépek lehetnek például Windows 10-es operációs rendszerek futtatására szolgáló munkaállomások vagy Windows Serverek szerveralkalmazásokhoz.

A Host Pool létrehozásához Terraformmal az azurerm_virtual_desktop_host_pool erőforrást használhatjuk az Azure Terraform provideren keresztül.

Ez a Terraform konfiguráció létrehoz egy AVD host pool-t, amihez hozzárendeli a felhasználókat az alkalmazáscsoportokhoz. A Host Pool-t egy Azure Resource Group-ban és azon belül egy megadott elhelyezkedésen hozza létre. Ezenkívül azonosítja a munkaterületet (workspace_id), amelyhez a host pool tartozik.

Fontos megjegyezni, hogy az AVD Host Pool létrehozásához szükségünk lesz egy előre konfigurált munkaterületre (azurerm_virtual_desktop_workspace), amelyben létrehozhatjuk a Host Pool-t. Az AVD beállítása Terraformmal további konfigurációs elemeket igényelhet, például hálózati konfigurációkat.

```
# Session Host Create
resource "azurerm_windows_virtual_machine" "newhost" {
  depends_on = [ azurerm_network_interface.nic ]
  admin_password        = random_password.vm_password.result
  admin_username        = var.vm_adminname
  license_type          = "Windows_Client"
  location              = var.location
  availability_set_id   = azurerm_availability_set.avd_availabilityset.id
  name                  = "${var.VMName_prefix}${count.index}"
  network_interface_ids = ["${element(azurerm_network_interface.nic.*.id, count.index)}"]
  count                 = var.host_count
  resource_group_name   = var.resource_group
  size                  = var.host_vm_size
  secure_boot_enabled   = true
  vtpm_enabled          = true

  tags = {
    Kyndryl_Managed_Service_Tier = "AVD"
```

9.3 ábra Session Host létrehozása (Saját forrás)

Az "AVD groups" kifejezés általában az Azure Virtual Desktop (AVD) használói csoportokra utal, amelyeket az AVD-ben használnak a felhasználók szervezésére és kezelésére. Ezek a csoportok lehetővé teszik az adminisztrátorok számára, hogy különböző felhasználói jogosultságokat és beállításokat rendeljenek a felhasználók csoportjaihoz.

Az AVD csoportokat általában a felhasználók kezelésére és azonos jogok hozzárendelésére használják, például a hozzáférési jogok beállítására az alkalmazásokhoz, a felhasználói profilkonfigurációkra és a munkaterületek rendezésére.

Ez a Terraform konfiguráció létrehoz egy AVD alkalmazáscsoportot az Azure-ban, és hozzárendeli azt a megadott host pool-hoz és workspace-hez. A többi csoportot és azok konfigurációit hasonlóan lehet definiálni Terraformmal. Fontos, hogy az AVD csoportok létrehozásához szükség lesz a megfelelő hozzáférési jogokra az Azure-ban.

```
# Role Assignment - Resource group
resource "azurerm_role_assignment" "VM_User_Login_permission" {
  scope = var.resource_group_id
  role_definition_name = "Virtual Machine User Login"
  principal_id = azuread_group.AADGroup_RDSUser.id
  depends_on    = [ azuread_group.AADGroup_RDSUser ]
}
```

9.4 ábra Jogosultság állítás (Saját forrás)

Az "AD join extension" az "Azure AD Join" kiterjesztése, ami lehetővé teszi a Windows 10-es vagy Windows 11-es operációs rendszerű eszközök csatlakozását az Azure Active Directory-hoz (Azure AD) [13]. Az Azure AD Join funkció lehetővé teszi az eszközöknek az Azure AD-ba történő integrálását, így a felhasználók egyszerűen és biztonságosan tudnak bejelentkezni az eszközökre a felhőalapú azonosítási rendszer használatával.

Az Azure Virtual Desktop (AVD) környezetben az AD Join extension használható annak érdekében, hogy a távoli munkaállomások, például a virtuális gépek, csatlakozzanak az Azure AD-hoz. Ez lehetővé teszi a felhasználók számára, hogy egyszerűen és biztonságosan jelentkezzenek be az AVD virtuális gépekre az Azure AD hitelesítő adatainak felhasználásával.

Az AD Join extension konfigurálása az AVD környezetben általában az Azure AD integrációs beállítások részeként történik. Ez magában foglalhatja az Azure AD Join opció bekapcsolását a virtuális gépeken, valamint az Azure AD-ba való csatlakozást támogató csoportirányítási beállításokat.

Fontos megjegyezni, hogy az AD Join extension használata előfeltétele az Azure AD konfigurálásának és az Azure Virtual Desktop beállításának.

```
# AD Join Extension
resource "azurerm_virtual_machine_extension" "ad_join" {
  depends_on = [ azurerm_virtual_machine_extension.registersessionhost ]
  name                 = "joindomain"
  count                = var.ad_join ? var.host_count : 0
  virtual_machine_id   = element(azurerm_windows_virtual_machine.newhost.*.id, count.index)
  publisher            = "Microsoft.Compute"
  type                 = "JsonADDomainExtension"
  type_handler_version = "1.3"

  settings = jsonencode({
    "name"="nhy.hydro.com"
    "ouPath"= var.isTest ? "OU=WEU,OU=EIT_Test,OU=AVD,OU=Clients,OU=Cloud,OU=SP11,OU=SP,DC=nhy,DC=hydro,DC=com"
    "user"=var.domainAdminUsername
    "restart"="true"
    "options"="3"
    "NumberOfRetries"="4"
  })
```

9.5 ábra AD join extension (Saját forrás)

A "Workspace DAG associate" (Munkaterület DAG asszociáció) kifejezés alapvetően a munkaterület és a Deployment Accelerator (DAG) közötti kapcsolatra utalhat az Azure Virtual Desktop (AVD) környezetben.

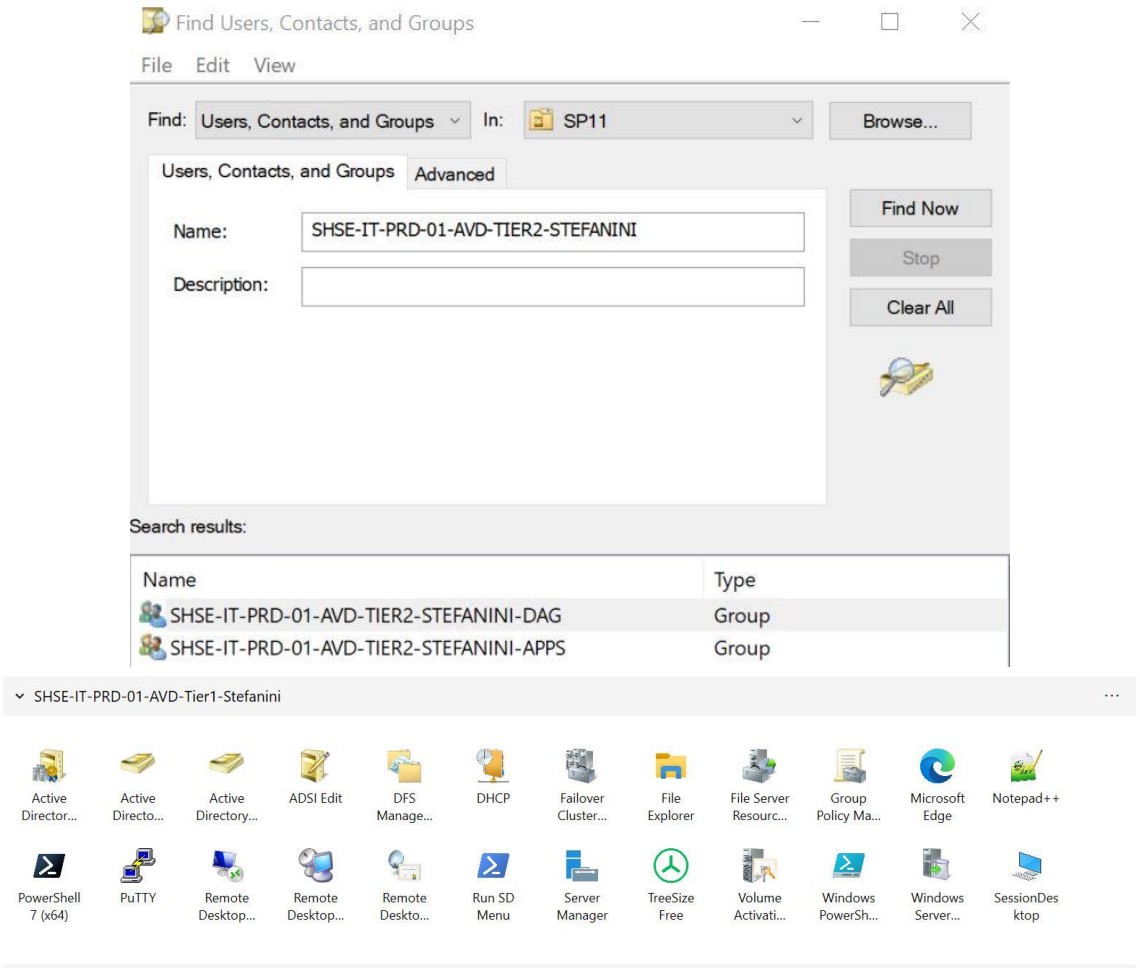
Az AVD Deployment Accelerator (DAG) általában egy eszköz és dokumentációs sorozat, amely segíti az AVD környezet gyors telepítését és konfigurálását. A DAG általában tartalmazza a legjobb gyakorlatokat, útmutatókat és eszközöket az AVD telepítéséhez és konfigurálásához.

```
# Create AVD DAG
resource "azurerm_virtual_desktop_application_group" "avd_dag" {
  depends_on = [ azurerm_virtual_desktop_host_pool.avd_hostpool ]
  resource_group_name           = var.resource_group
  host_pool_id                  = azurerm_virtual_desktop_host_pool.avd_hostpool.id
  location                      = var.location
  type                          = "Desktop"
  name                          = "${var.hostpool_name}-DAG"
  friendly_name = var.dag-friendly-name
  default_desktop_display_name = var.dag-friendly-name
```

9.6 ábra AVD DAG létrehozása (Saját forrás)

9.1 Tesztelés

Az elkészült AVD eléréséhez remote desktop felületet fogunk használni, ahol a megfelelő jogosultságokkal rendelkező felhasználó már elérheti a kívánt avd hostpool-t a felhasználó csoportokba való helyezése után. Ezeket a jogosultságokat AD-ban tudjuk kiadni a bizonyos felhasználói csoportoknak, ezeket a csoportokat az avd léttrehozásánál fogjuk bekonfigurálni terraform segítségével. A felhasználók hozzáadása később is megtörténhet. Az AVD-ken különböző programokat és applikációkat tud a felhasználó használni.



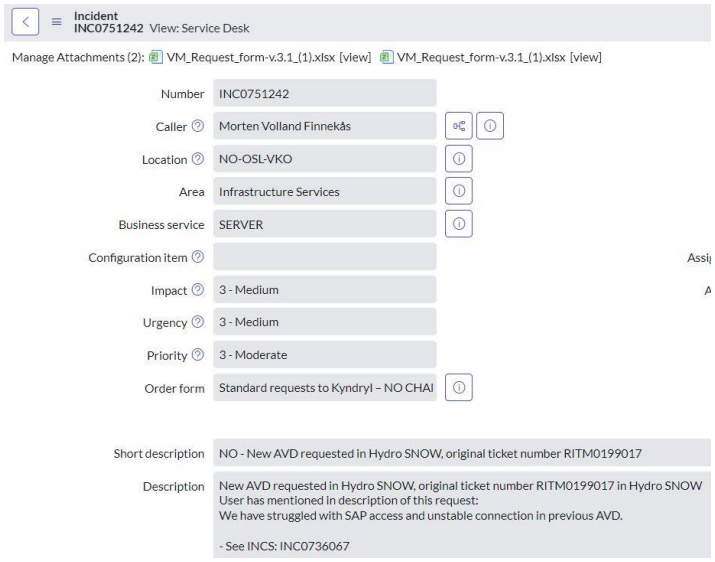
9.7 ábra Remote desktop (Saját forrás)

A felhasználó maga nem tudja változtatni a használható applikációkat, mivel nincs ehhez felhasználói joguk. Ilyen szintű változtatásokra mint az alkalmazás hozzáadása magasabb

jogosultság kell. Az kéréseket a változtatások iránr a felhasználók ServiceNow felületen keresztül tudják továbbítani a platform felügyeletért felelős kollégáknak.

ServiceNow egy felhőalapú platform, amelyet az IT-szolgáltatások automatizálására és menedzselésére használnak [14]. Főként az ITSM (IT Service Management), az ITOM (IT Operations Management) és az ITBM (IT Business Management) területeken használják, de további területeken is alkalmazzák, mint például az ügyfélszolgálat.

ServiceNow segíthet az IT-szervezetnek az IT-szolgáltatások hatékonyabb és átláthatóbb kezelésében, valamint az üzleti folyamatok és igények jobb kiszolgálásában.



9.8 ábra Servicenow (Saját forrás)

10.AUTOMATIZÁLÁSI ÉS TOVÁBBFEJLESZTÉSI LEHETŐSÉGEK

A PowerShell használata az Azure-ban számos előnnyel jár a feladatok kezeléséhez és automatizálásához az Azure felhőkörnyezetben. A PowerShell a Microsoft által támogatott natív eszköz, amely zökkenőmentesen integrálható az Azure-szolgáltatásokkal. A kifejezetten Azure-kezelési feladatokhoz tervezett parancsmagok átfogó készletét biztosítja. A PowerShell lehetővé teszi az ismétlődő vagy összetett feladatok automatizálását. A szkriptekkel hatékonyabban telepítheti, konfigurálhatja és kezelheti az Azure-erőforrásokat, csökkentve a kézi erőfeszítéseket és az emberi hibákat. A PowerShell-szkriptek használhatók az Azure-erőforrások kódként történő meghatározására, megkönnyítve az infrastruktúra kódként (IaC) elveit. Ez a megközelítés lehetővé teszi a verziószámítást, az egyszerűbb együttműködést és a következetes telepítést.

```
param
(
    [Parameter(Mandatory = $true, HelpMessage = "Name of subscription")]
    [string]$SubscriptionName,

    [Parameter(Mandatory = $true, HelpMessage = "Resourcegroup where to deploy the virtual machine")]
    [string]$ResourceGroup,

    [Parameter(Mandatory = $True, HelpMessage = "Please Enter VM short name")]
    [ValidateLength(3, 9)]
    [string]$ShortName,

    [Parameter(Mandatory = $False, HelpMessage = "Please Enter 2 digit serialnumber")]
    [string]$Serverserial="01",

    [Parameter(Mandatory = $False, HelpMessage = "Does it Part of Operational Technology?")]
    [bool]$DoesPartOfOT = $false,

    [Parameter(Mandatory = $False, HelpMessage = "Please enter Location")]
    [ValidateSet("westeurope","brazilsouth","southcentralus")]
    [string]$ServiceLocation = "westeurope",

    [Parameter(Mandatory = $False, HelpMessage = "Please enter Subnet name")]
    [string]$SubnetName,

    [Parameter(Mandatory = $False, HelpMessage = "Please enter VNET Name")]
    [string]$VNETName,

    [Parameter(Mandatory = $True, HelpMessage = "Please enter Business Area")]
    [string]$businessArea,
```

10.1 ábra Virtuális gép létrehozása (Saját forrás)

A szkript bejelentkeztet minket az Azure-fiók a Connect-AzAccount használatával. Erőforráscsoportot hoz létre a New-AzResourceGroup segítségével, valamint, beállítja a virtuális gép konfigurációját a New-AzVMConfig használatával.

Meghatározza az operációs rendszer részleteit és hitelesítő adatait a Set-AzVMOperatingSystem segítségével, illetve megadja a Set-AzVMSourceImage-gel használandó virtuális gép-lemezképet.

Végül létrehozza a virtuális gépet a New-AzVM használatával.

```
#Configure backup.
#Determine Backup policies
Write-Output -InputObject "Determine Backup policies"

if ($OSAndFileBackupPolicy) {
    $OSAndFileBackupPolicy = $OSAndFileBackupPolicy
    Write-Output -InputObject "OS Policy is: $OSAndFileBackupPolicy"
}
else {
    if ($Environment -eq "PRD") {
        $OSAndFileBackupPolicy = "Hydro-PRD"
        Write-Output -InputObject "OS Policy is: $OSAndFileBackupPolicy"
    }
    elseif ($Environment -eq "TST") {
        $OSAndFileBackupPolicy = "Hydro-TST"
        Write-Output -InputObject "OS Policy is: $OSAndFileBackupPolicy"
    }
    elseif ($Environment -eq "POC") {
        $OSAndFileBackupPolicy = "Hydro-POC"
        Write-Output -InputObject "OS Policy is: $OSAndFileBackupPolicy"
    }
    elseif ($Environment -eq "DEV") {
        $OSAndFileBackupPolicy = "Hydro-POC"
        Write-Output -InputObject "OS Policy is: $OSAndFileBackupPolicy"
    }
    elseif ($Environment -eq "DRS") {
        $OSAndFileBackupPolicy = "Hydro-POC"
        Write-Output -InputObject "OS Policy is: $OSAndFileBackupPolicy"
    }
}
```

10.2 Virtuális gép 2 (Saját forrás)

A PowerShell használatával különféle beállításokat konfigurálhatunk egy AVD-hez Azure-ban. Mint a virtuális gép mérete, az operációs rendszerünk azt is, hogy hol helyezkedjenek el az erőforrásaink és felhasználóink jogosultságait is tudjuk állítani.

```
#Connect To Azure
#. .\NGC-Connect-Azure.ps1
. .\NGC-ConnectAzureIdentity.ps1
# HFMcode validation
$validHFM = validate-HFMcode $HFMcode
if ($validHFM) {
    Write-Output -InputObject "The given HFM code $HFMcode is correct"
}
else {
    Write-Output -InputObject "The given HFM code $HFMcode is NOT correct"
    exit
}
#
#Setting up context
$SetContext = Set-AzContext -Subscription $SubscriptionName
Write-Output -InputObject $SetContext

#Creating RG

$ResourceGroupName = $($SubscriptionName) + '-' + $($ShortName).toupper() # + '-' + $($Environment)

$RGNameValidation = Get-AzResourceGroup -name $ResourceGroupName -ErrorAction SilentlyContinue

if (-not $RGNameValidation){
    Write-Output -InputObject "Creating Resource Group accordingly"
    Write-Output -InputObject "Designated Resourcegroupname: $ResourceGroupName"

    $ResourceGroupToBeSet = New-AzResourceGroup `
```

10.3 ábra Erőforráscsoport létrehozása (Saját forrás)

Míg az automatizálást a GBS fejlesztette ki a Terraform és az Aviatrix platform felhasználásával, végül szándékunkban áll megnyitni a konfigurációt a BA-felhasználók számára, lehetővé téve a hálózati telepítés integrálását az alkalmazási folyamatokba, így lehetővé válik í gyorsabb alkalmazás közzététel az AM fejlesztők számára.

Ezt az a tény teszi lehetővé, hogy automatizálásunk a szabványos tapadást kényszeríti ki.

A cél az, hogy olyan felületet hozzunk létre, ahol a fejlesztők hálózati erőforrásokat kérhetnek, amelyek automatikusan telepítésre kerülnek azután.

Szükséges jóváhagyások esetén a fejlesztőknek nem kell aggódniuk a hálózat miatt, csak a követelmények meghatározása után kell működnie.

11.ÖSSZEFOGLALÓ

A felhőtechnológiák továbbra is gyorsan fejlődnek, és jelentős átalakulásokat hajtanak végre az iparágakban. Sok szervezet alkalmazza a többfelhős megközelítéseket, több felhőszolgáltató szolgáltatásait (például AWS, Azure, Google Cloud) kihasználva, hogy elkerülje a szállítói bezárkózást, és élvezze a változatos kínálat előnyeit.

A hibrid felhőmegoldások, amelyek a helyszíni infrastruktúrát nyilvános és privát felhőkkel kombinálják, továbbra is népszerűek a rugalmasság, a megfelelőség és az adatszuverenitás miatt.

A szélső számítástechnika folyamatosan növekszik, lehetővé téve az adatfeldolgozást a forráshoz (eszközökhöz vagy érzékelőkhöz) közelebb. Ez a tendencia elengedhetetlen a valós idejű elemzéshez, a csökkentett késleltetéshez és a sávszélesség optimalizálásához.

Az Internet of Things (IoT) megoldások a felhőtechnológiákat hasznosítják az adatok aggregálásához, feldolgozásához és kezeléséhez, ösztönözve az innovációkat a különböző iparágakban, beleértve az intelligens városokat, az egészségügyet, a gyártást és a mezőgazdaságot.

Szakdolgozatomban bemutattam az általam választott felhőplatformot, ezen belül az Azure virtuális desktop tervezését és annak fontosabb lépéseinek implementálását. Ezen felül ismertettem az kód, mint infrastruktúra alapú infrastruktúra létrehozást, valamint a dolgozat elkészítéséhez használt technológiákat. Bemutattam továbbá a felhőplatformhoz használt automatizációs technológiákat és azok használatát.

A felhőszolgáltatások iránt nagy igény mutatkozik, amely egyre csak növekszik. Az egyre növekvő ügyfélszám miatt a felhőtechnológiák használata elengedhetetlenné válik. Dolgozatom e szempontból fontos, mivel betekintést és bevezetést ír le a felhőtechnológiák alkalmazásához.

12.SUMMARY

Cloud technologies continue to rapidly evolve and transform industries. Many organizations are adopting multi-cloud approaches, leveraging the services of multiple cloud providers (such as AWS, Azure, Google Cloud) to avoid vendor lock-in and enjoy the benefits of diverse offerings.

Hybrid cloud solutions that combine on-premise infrastructure with public and private cloud remain popular for flexibility, compliance and data sovereignty.

Edge computing is constantly growing, enabling data processing closer to the source (devices or sensors). This trend is essential for real-time analytics, reduced latency, and bandwidth optimization.

Internet of Things (IoT) solutions leverage cloud technologies to aggregate, process and manage data, driving innovations in various industries, including smart cities, healthcare, manufacturing and agriculture.

In my thesis, I presented the cloud platform I chose, including the design of the Azure virtual desktop and the implementation of its most important steps. In addition, I explained the creation of infrastructure based on code as infrastructure, as well as the technologies used to prepare the thesis. I also presented the automation technologies used for the cloud platform and their use.

There is a great demand for cloud services, which is only growing. Due to the growing number of customers, the use of cloud technologies becomes essential. My thesis is important from this point of view, as it describes an insight and introduction to the application of cloud technologies.

13.IRODALOMJEGYZÉK

[1] „Microsoft What is cloud computing"

Microsoft, [Online]. Available: https://azure.microsoft.com/en-us/resources/clou computing dictionary/what-is-cloud-computing.

[2] „Felhő alapú szolgáltatások ismertetése"

[Online]. Available: https://sysman.hu/felho-alapu-szolgaltatasok/

[3] „AWS vs Azure vs Google Cloud: Top Cloud Services Compared"

[Online]. Available: https://www.channelinsider.com/cloud-computing/aws-vs-azure-vs-google-cloud/

[4] „Programozási technikák"

[Online]. Available: https://bizuplab.com/hu/technologies

[5] Mi az azure virtual desktop.

[Online] Available: https://learn.microsoft.com/hu-hu/azure/virtual-desktop/overview

[6] „Cisco What is infrastructure as code "

[Online]. Available: https://www.cisco.com/c/en/us/solutions/cloud/what-is-iac.html

[7] „Infrastruktúra, mint kód"

[Online]. Available: https://learn.microsoft.com/hu-hu/dotnet/architecture/cloud-native/infrastructure-as-code

[8] „Aviatrix overview"

[Online]. Available: https://learn.microsoft.com/hu-hu/dotnet/architecture/cloud-native/infrastructure-as-code

[9] „Választás a virtuális hálózatok közötti társviszony-létesítés és a VPN-átjárók között " [Online]. Available: https://learn.microsoft.com/hu-hu/azure/architecture/reference-architectures/hybrid-networking/vnet-peering

[10] „Aviatrix overview"

[Online]. Available: https://aviatrix.com/learn-center/cloud-security/egress-and-ingress/

[11] „What is Azure DNS"

[Online]. Available: https://learn.microsoft.com/en-us/azure/dns/dns-overview

[12] „Deploy Azure Virtual Desktop with Terraform"

[Online]. Available: https://johanvanneuville.com/avd/deploy-azure-virtual-desktop-with-terraform/

[13] „How to add Azure Virtual desktop Session Host to Azure AD Join"

[Online]. Available: https://www.anoopcnair.com/azure-virtual-desktop-session-host-to-azure-ad/

[14] „What is Servicenow"

[Online]. Available: https://flyform.com/insights/articles/what-is-servicenow

14.ÁBRAJEGYZÉK

7.1. ábra Virtuális Hálózat (Saját forrás) 23
7.2. ábra VNET Peering (Saját forrás) 24
7.3. ábra Biztonsági csoportok (Saját forrás) 26
7.4. ábra Hálózati régiók (Saját forrás) 27
7.5. ábra Internet Ingress Connectivity (Saját forrás) 27
8.1. ábra Hálózati szegmentáció (Saját forrás) 30
8.2. ábra zScaler (Saját forrás) 32
8.3. ábra zScaler 2. ábra (Saját forrás) 33
8.4. ábra DNS (Saját forrás) 34
9.1 ábra Workspace kialakítása (Saját forrás) 35
9.2 ábra Hostpool létrehozása (Saját forrás) 36
9.3 ábra Session Host létrehozása (Saját forrás) 37
9.4 ábra Jogosultság állítás (Saját forrás) 38
9.5 ábra AD join extension (Saját forrás) 39
9.6 ábra AVD DAG létrehozása (Saját forrás) 39
9.7 ábra Remote desktop (Saját forrás) 40
9.8 ábra Servicenow (Saját forrás) 41
10.1 ábra Virtuális gép létrehozása (Saját forrás) 42
10.2 ábra Virtuális gép 2 (Saját forrás) 43
10.3 ábra Erőforráscsoport létrehozása (Saját forrás) 44