

AZURE FELHŐ HASZNÁLATI ÚTMUTATÓ OCCOPUSHOZ

Herr Attila
2016. NOVEMBER
VERZIÓ: 1.0

Tartalomjegyzék

Röviden	2
1. lépés – Azure regisztráció	3
1.1 Microsoft-fiók.....	3
2. lépés - Autentikáció.....	5
2.1 Előfizetési azonosító.....	5
2.2 Azure Active Directory webalkalmazás azonosító.....	6
2.2.1 Webalkalmazás készítése	6
2.2.2 Azonosítók, kulcsok megtalálása	7
2.3 Azure Active Directory webalkalmazás kulcs.....	10
2.4 Azure Active Directory webalkalmazás tenant azonosító (OAuth 2.0 endpoint id) .	11
3. lépés – Jogosultság kezelés	12
4. lépés – VM előkészítése	17
4.1 Network security group	17
4.1.1 SSH kapcsolatot engedélyező tűzfal szabály	18
4.2 Storage account.....	18
4.3 VNET.....	19
5. lépés – VM erőforrás információk kigyűjtése.....	21
5.1 Storage Account név.....	21
5.2 Storage Account kulcs	22
5.3 VNET ID	23
5.4 VNET subnet neve.....	23
5.5 VNET lokációja.....	24
5.6 Network security group ID	24
6. lépés – VM létrehozáshoz szükséges adatok.....	25
6.1 Kötelező mezők:	25
6.2 Opcionális mezők:	25
7. Irodalomjegyzék.....	26

Röviden

Ez a dokumentum egy használati útmutatót tartalmaz a Microsoft Azure felhőrendszer Occopus eszközzel való használatához. Amennyiben még nem telepítetted az Occopus-t, először látogass el a weboldalára (<http://occopus.jpds.sztaki.hu/>) további segítségért.

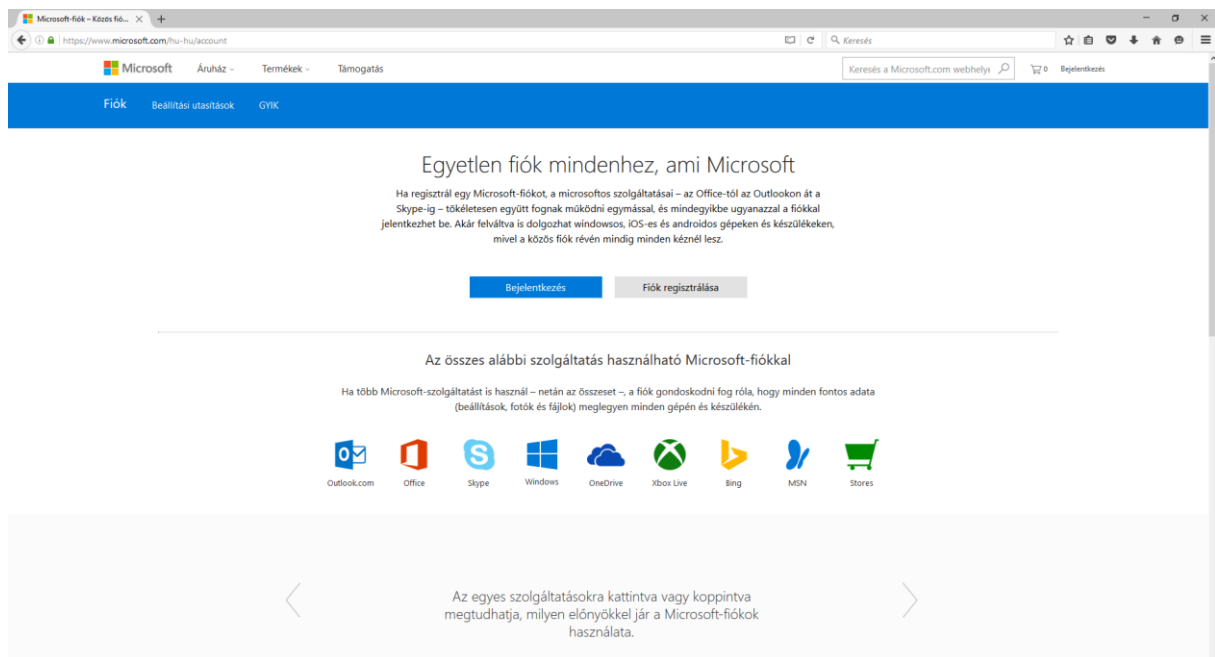
Kérlek, figyelmesen kövesd végig az alábbi lépéseket!

1. lépés – Azure regisztráció

Abban az esetben, ha már rendelkezel Azure előfizetéssel kihagyhatod, ugord át ezt a fejezetet és folytasd az lépés - Autentikáció résznél.

1.1 Microsoft-fiók

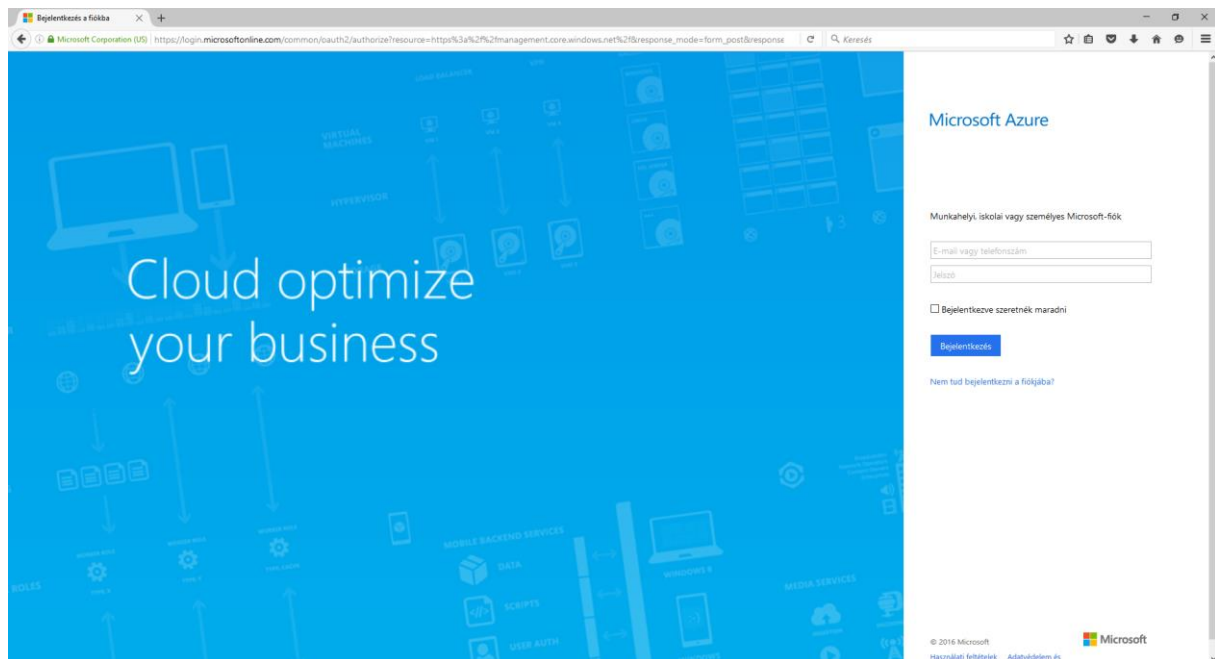
A Microsoft Azure használatához szükség van egy munkahelyi, iskolai vagy személyes Microsoft-fiókra. Személyes Microsoft fiókot ezen a linken tudsz létrehozni <https://www.microsoft.com/hu-hu/account> a *Fiók regisztrálása* gombra rákattintva.



1. Ábra - Microsoft fiók regisztráció

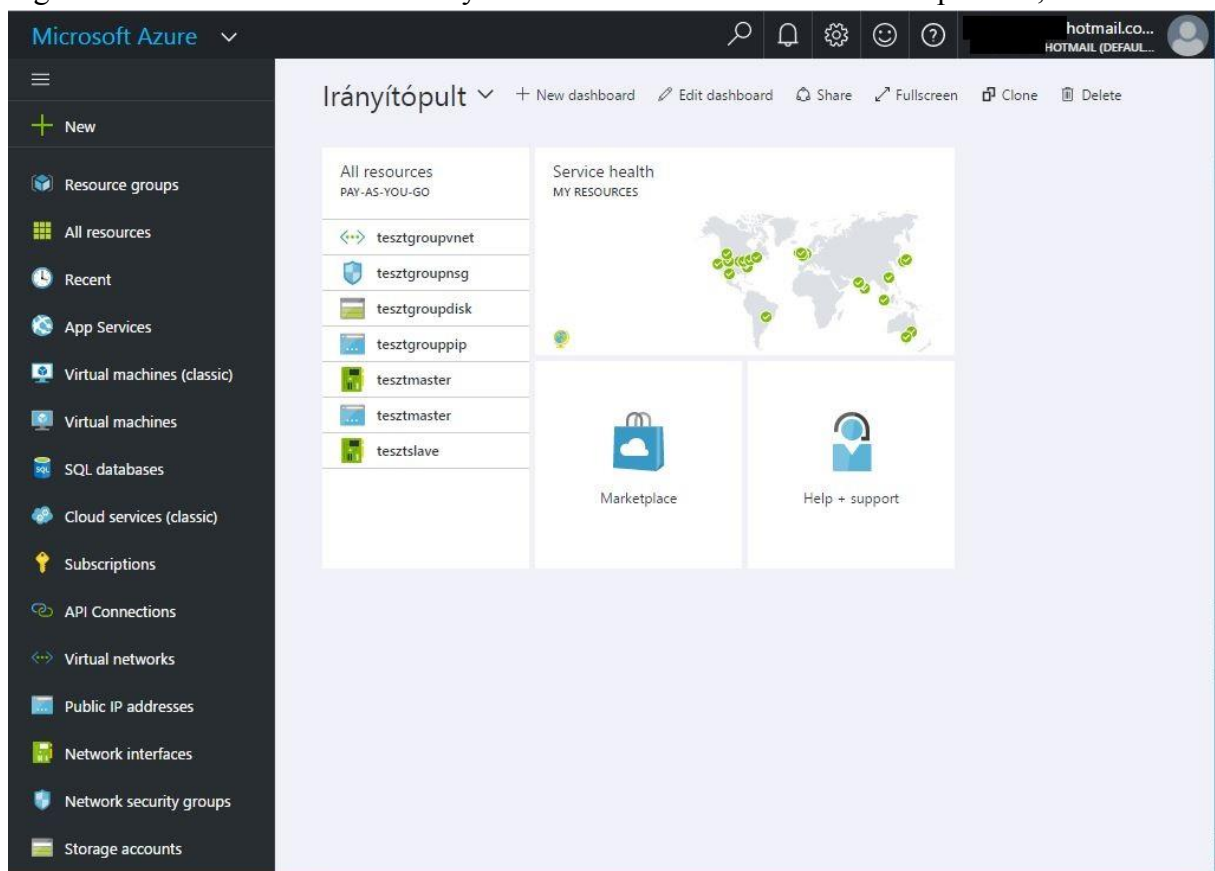
Az ábrához hasonló weboldalt kell látnod.

Sikeres regisztrációt követően a <https://azure.microsoft.com/hu-hu/free/> címet beírva a böngészőbe a zöld *Kezdetben ingyenes* gombra kattintva, átirányít minket a bejelentkezés oldalra, itt értelemszerűen jelentkezz be a Microsoft fiókodhoz tartozó e-mail cím jelszó párossal.

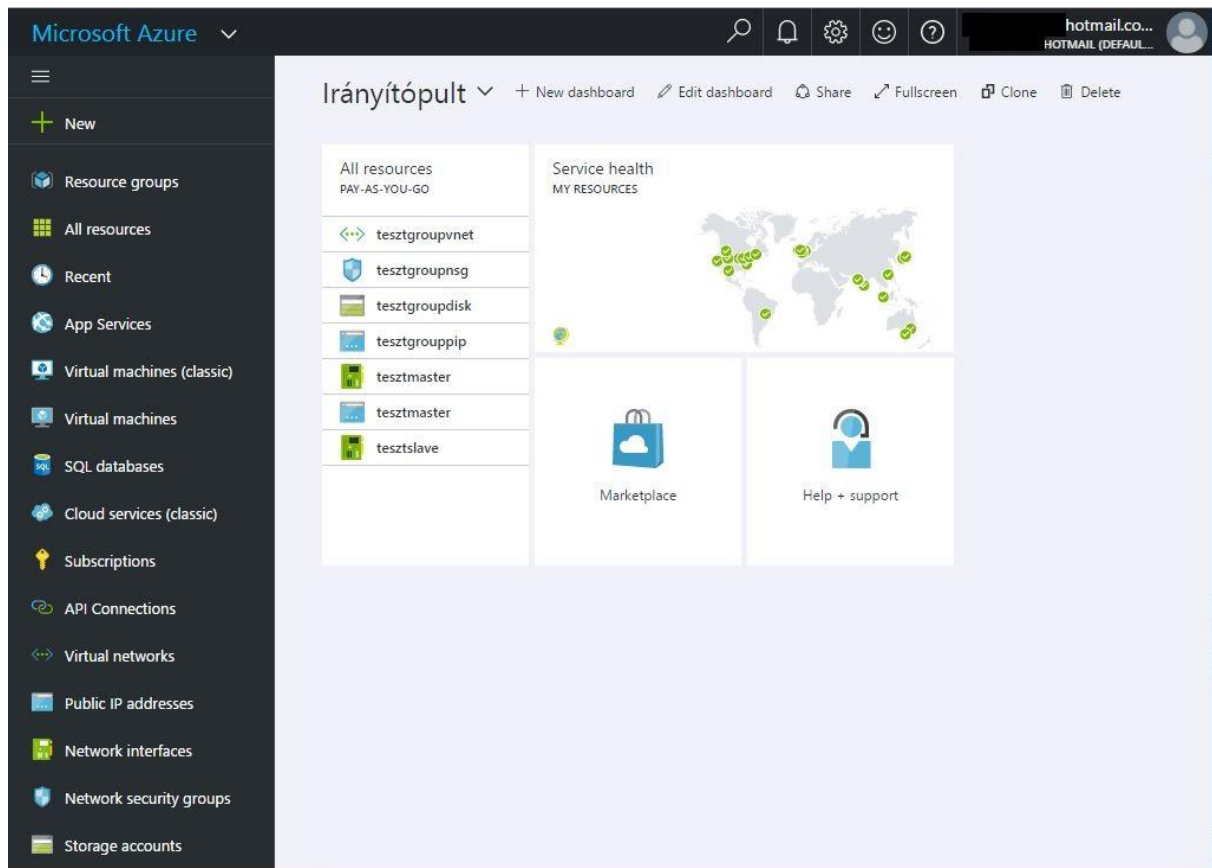


2. Ábra –Azure bejelentkezés

Az ábrához hasonló weboldalt kell látnod. Bejelentkezés után egy Azure regisztrációs oldal fogad, ahol szükséged lesz az általános személyes információkon kívül a telefonszám és bankkártya adatok megadására. Értelemszerűen kövesd az ott található lépéseket, a sikeres regisztrációt követően átirányít az Microsoft Azure portálra, ahol a



3. Ábra található oldalt kell látnod.



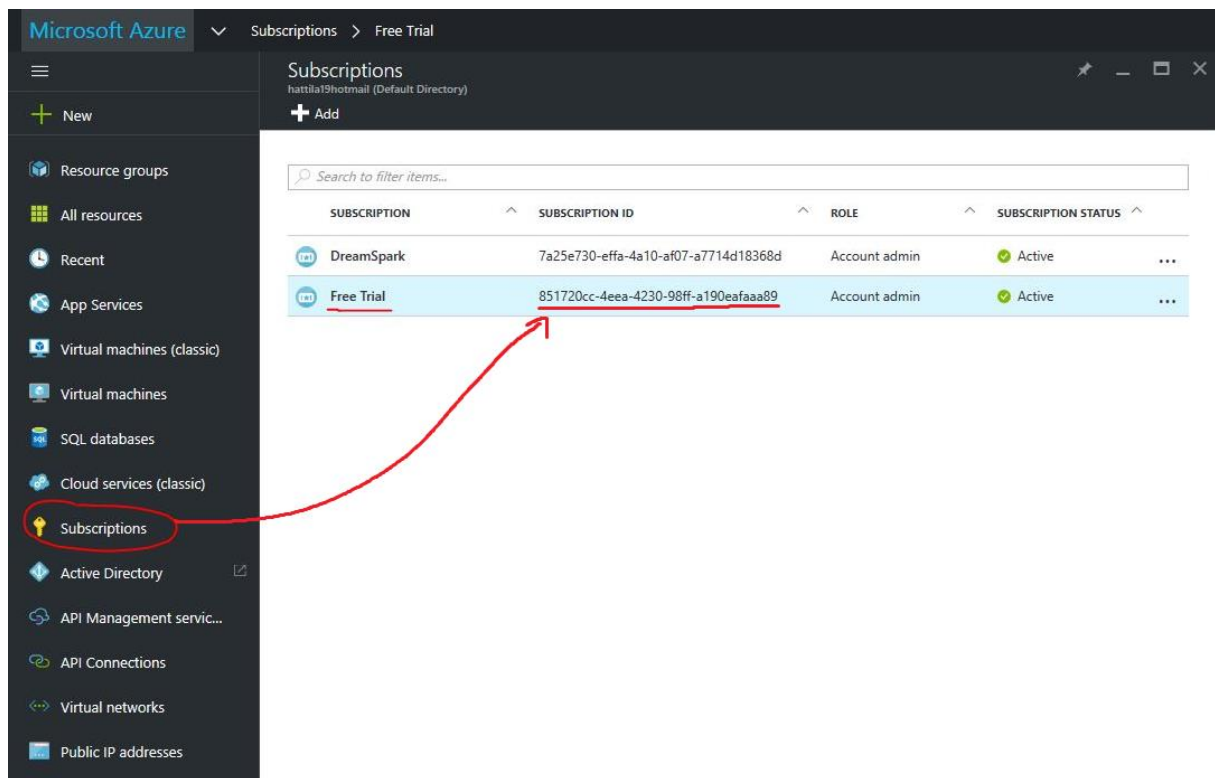
3. Ábra - Azure portál

2. lépés - Autentikáció

Az útmutató során, **vastagon szedett szavak** segítenek a **yaml** fájlokban lévő **kulcsok** azonosításában. Menj a <https://portal.azure.com/> weboldalra, itt érhetjük el a Microsoft Azure felhőrendszerét. Az autentikációhoz, virtuális gépek létrehozásához, menedzseléséhez szükség lesz több azonosítóra, kulcsra is. Amennyiben nincs, először egy webalkalmazást kell létrehozni az Azure Active Directory-ban, majd ehhez jogosultságot kell rendelni. Autentikációhoz szükséges adatok a következő alfejezetekben találhatók.

2.1 Előfizetési azonosító

Az előfizetési azonosítónk a **Subscription ID**, mely megtalálásában a 4. Ábra segít.



4. Ábra - Subscription ID

Először kattints a *Subscriptions* menüpontra, ezután megjelennek az előfizetéseid, a SUBSCRIPTION ID oszlopban láthatod az azonosítót.

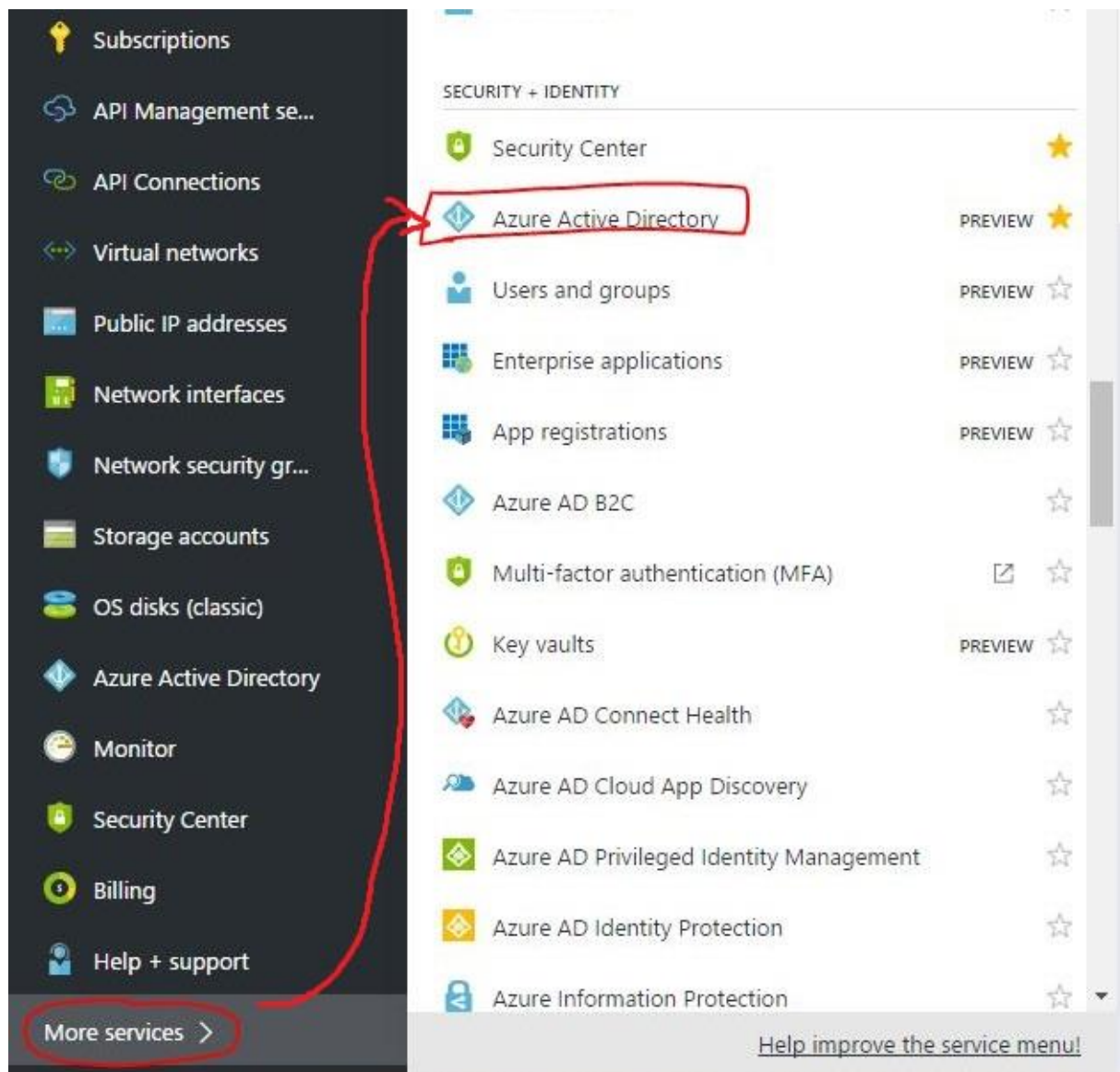
2.2 Azure Active Directory webalkalmazás azonosító

A node leíró fájlban található **Application ID**, a webalkalmazás *Client ID*-ja.

2.2.1 Webalkalmazás készítése

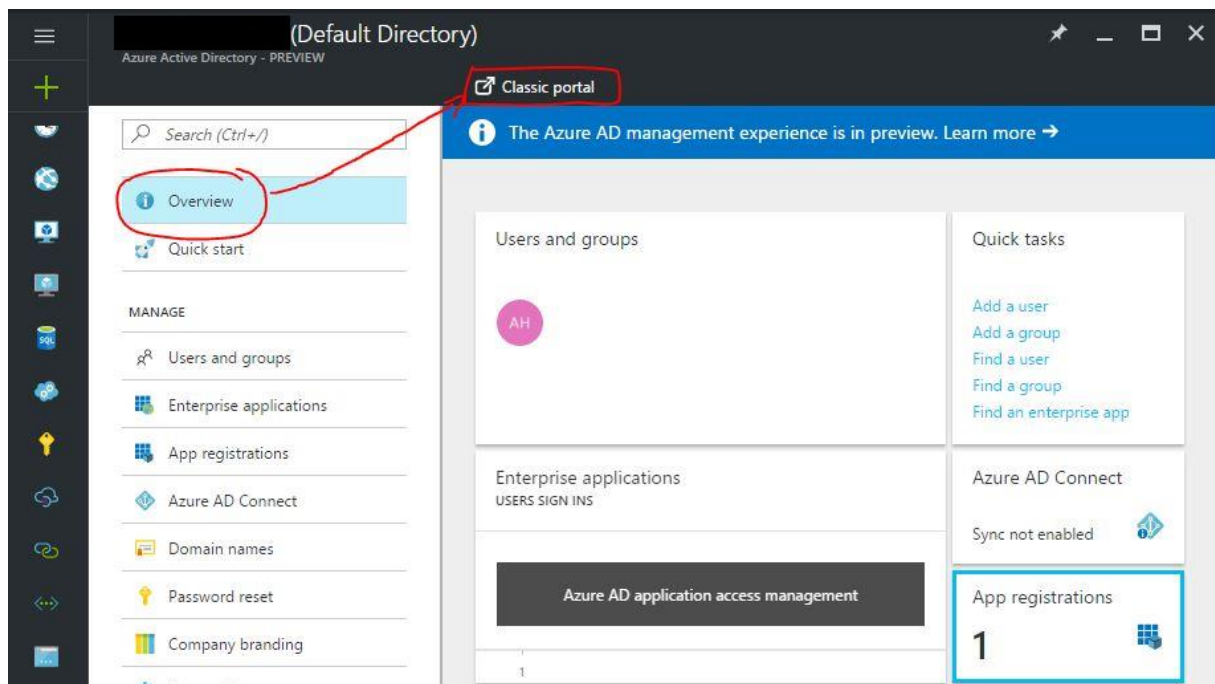
Ezt a lépést mindenképp végezd el, ha még nincs webalkalmazásod. Ennek létrehozásához további segítséget itt találsz: <https://azure.microsoft.com/hu-hu/documentation/articles/resource-group-create-service-principal-portal/>.

2.2.2 Azonosítók, kulcsok megtalálása



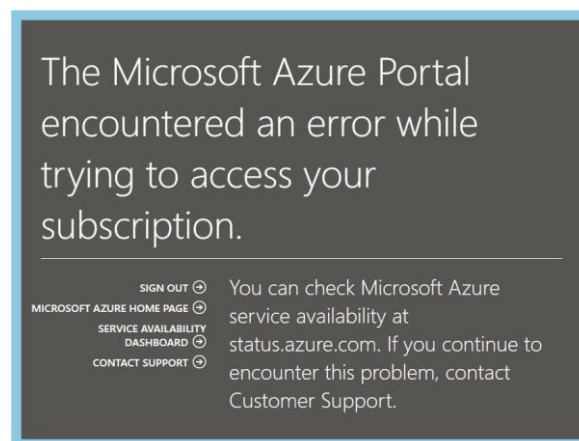
5. Ábra - Azure Active Directory menüpont

Először kattints az Azure Active Directory menüpontra, ha ez nincs a kedvencek között, akkor az 5. Ábraán látható *More Services* gomb megnyomásával, megjelenő listában a *Security + identity* csoportban találod meg.



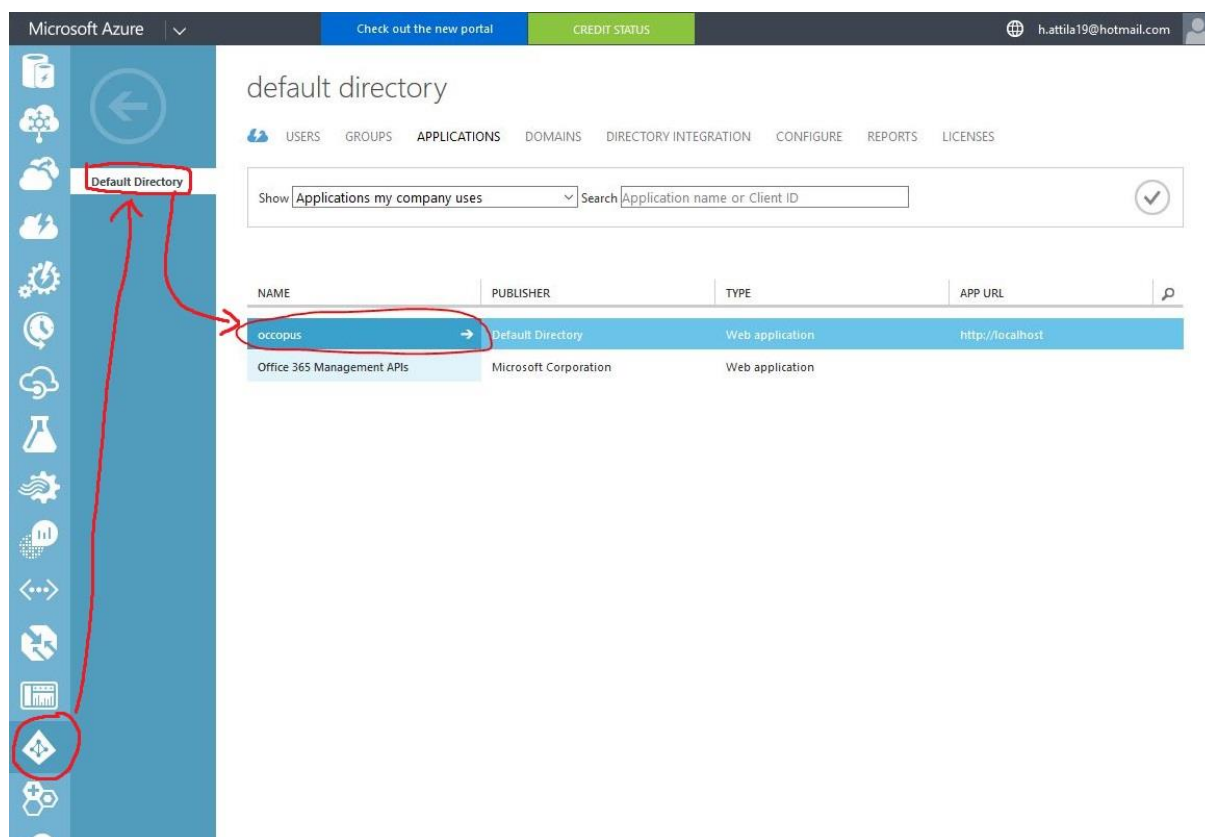
6. Ábra - Active Directory Classic portal gomb

Ezután az Azure Active Directory ablakban az *Overview* gombra kattints, majd a *Classic portal* gomb megnyomásával egy újabb oldalra irányít át minket az Azure.



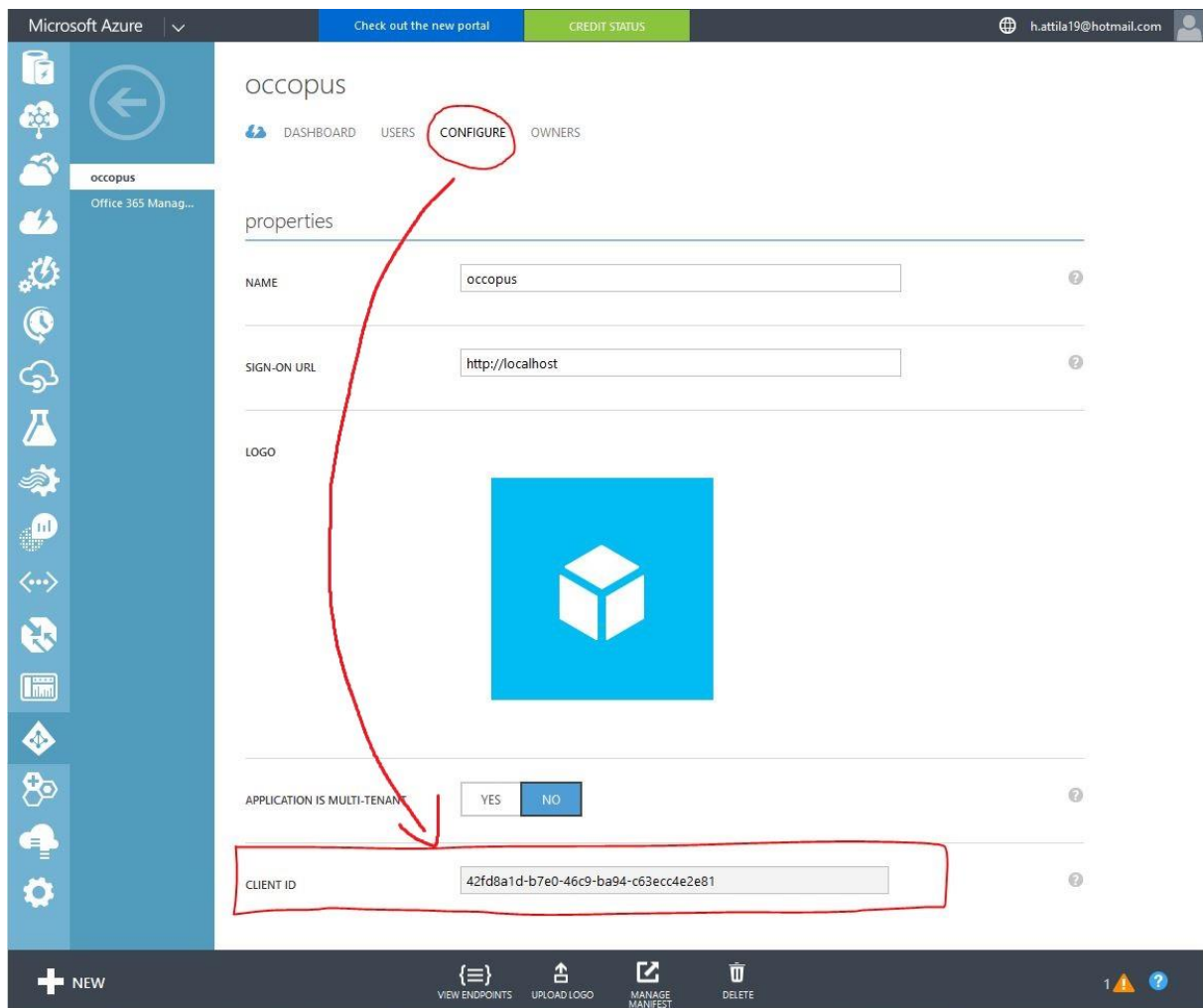
7. Ábra - Azure Active Directory átirányítás hiba

Abban az esetben, ha ez az oldal a 7. Ábraán látható hibát dobja, akkor a nyissunk egy új inkognitó ablakot a böngésző segítségével és menjünk a <https://manage.windowsazure.com> oldalra. Itt jelentkezünk be az Azure-hoz használt azonosítónkkal.



8. Ábra - Azure Active Directory webalkalmazás kiválasztása

Ezek után válasszuk ki az előzőekben létrehozott webalkalmazásunkat a *Default Directory*, *Applications* ablakban, a 8. Ábraán látható módon.

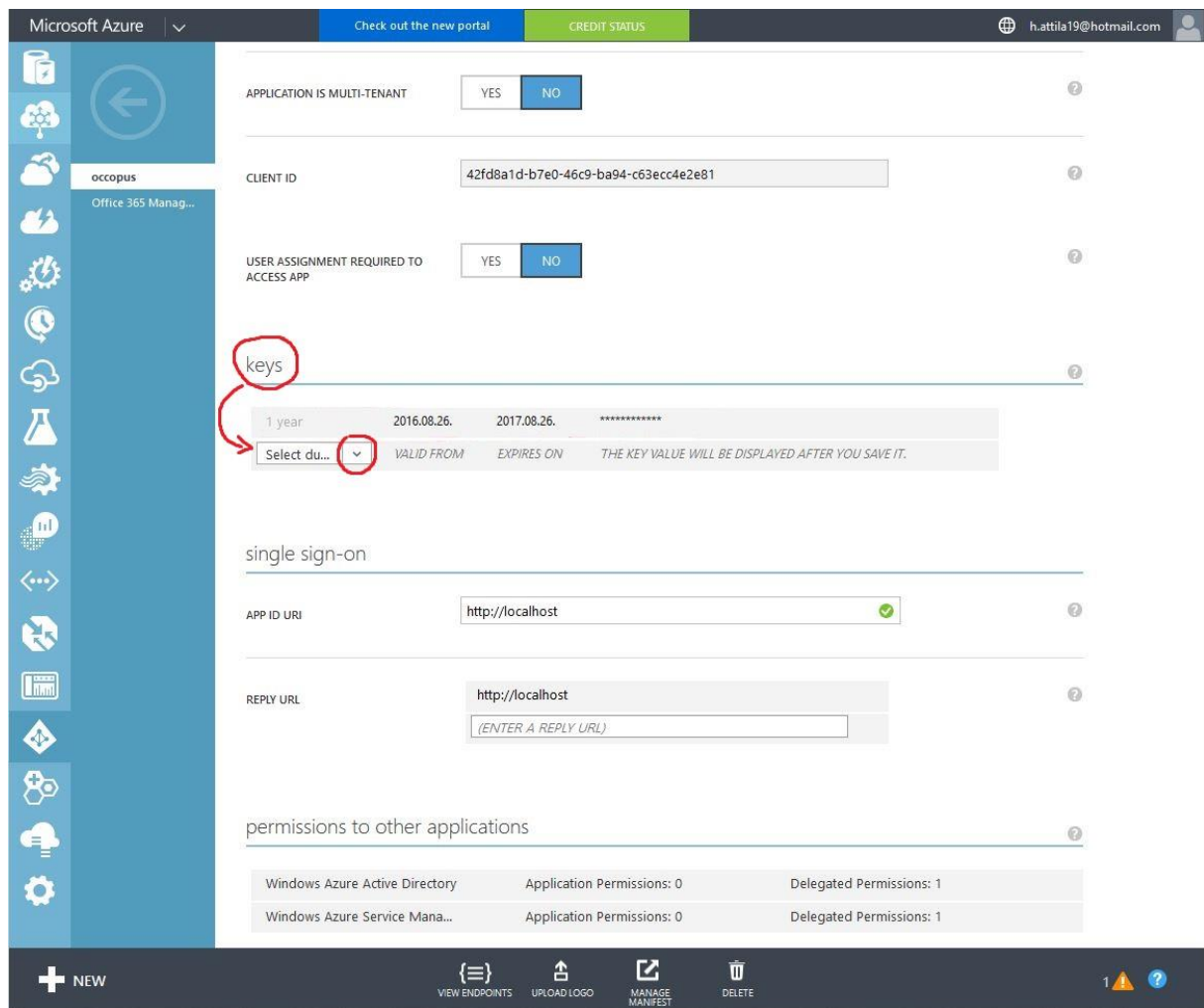


9. Ábra - Webalkalmazás Client ID

A webalkalmazás ablakban kattintsunk a *Configure* fülre, majd görgessünk lejjebb a *Client ID*-hez (lásd: 9. Ábra). Az előbb említett azonosító értékét kell beírunk a node leíró fájlban lévő **Application ID** mezőhöz.

2.3 Azure Active Directory webalkalmazás kulcs

FIGYELEM! A kulcsot csak egyszer tudod megnézni, ezért erősen ajánlott egy fájlba kimenteni, hogy a későbbiekben meglegyen.



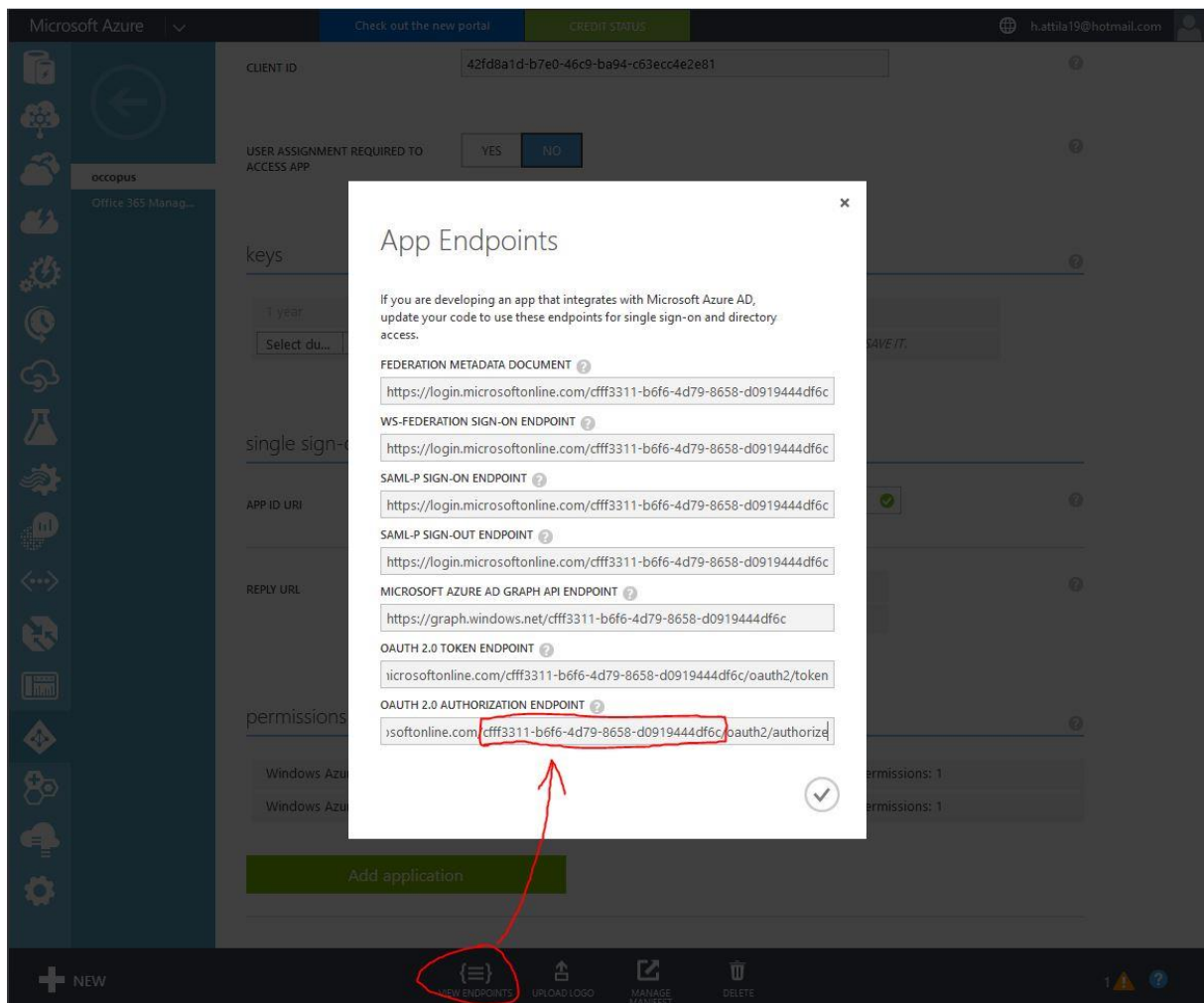
10. Ábra - Webalkalmazás kulcs

A kulcsot ugyancsak a *Configure* fül alatt a *Keys* résznél hozhatod létre. Válaszd ki a kulcs *lejárati idejét* a legördülő menü segítségével, majd kattints az alsó fekete menüsoron megjelenő *Save* gombra, ekkor a kulcs létrejön és láthatóvá válik. Ekkor másold ki a kulcsot és mentsd el egy szöveges fájlba.

A kulcsot az **Application Secret** mezőbe kell beírni.

2.4 Azure Active Directory webalkalmazás tenant azonosító (OAuth 2.0 endpoint id)

Még mindig a *Configure* ablakban vagyunk, az oldal alján, fekete menüsoron található *View endpoints* gombra kattints rá, ekkor megjelennek az *App Endpoints* ablak.

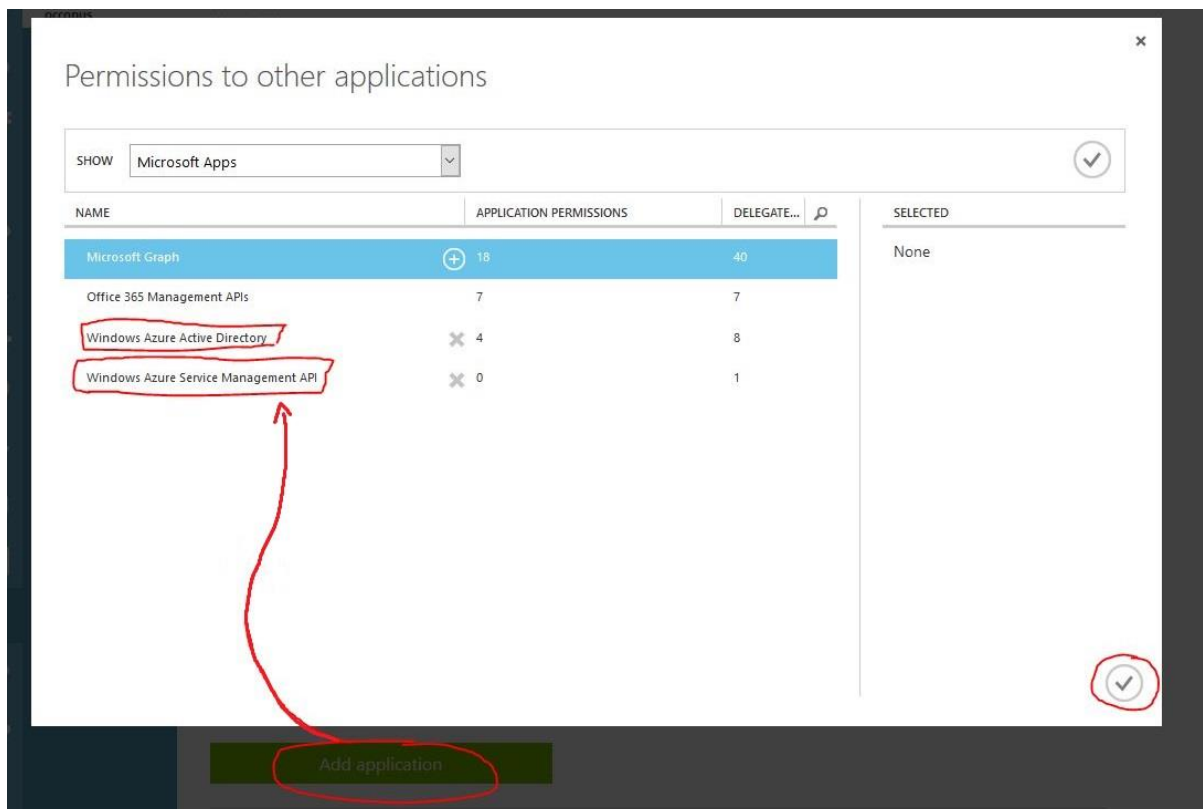


11. Ábra - Webalkalmazás tenant ID

A legelső *Oauth 2.0 authorization endpoint* alatt található URL-ben a 11. Ábraán kijelölt rész a **tenant ID**.

3. lépés – Jogosultság kezelés

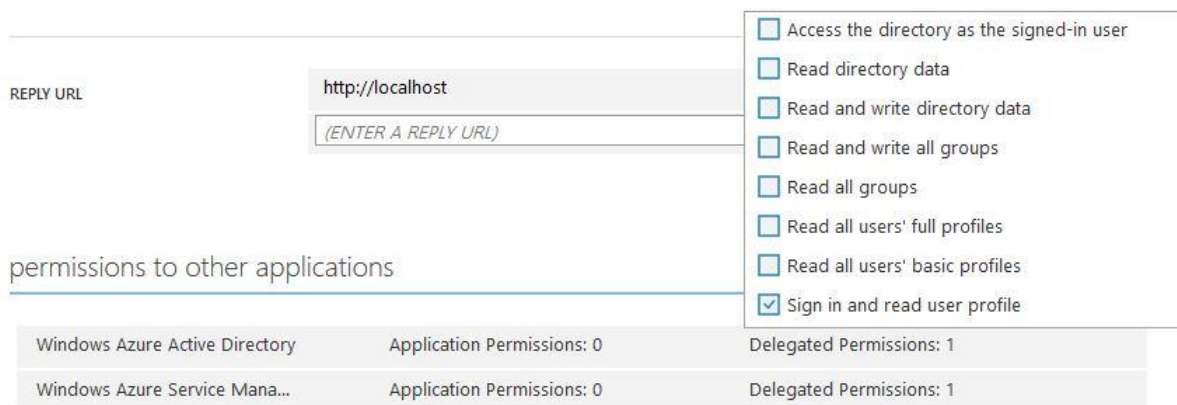
Ebben a lépésben jogosultságot kell hozzárendelni a webalkalmazásunkhoz, azért, hogy később hozzá tudjuk adni az előfizetésünkhöz az alkalmazásunkat. Ezt a *Configure* oldal alján találjuk meg a *permissions to other applications* résznél az *Add application* zöld gombra kattintva tudod megtenni (lásd: 12. Ábra).



12. Ábra - Webalkalmazás jogosultság hozzáadás

Itt add hozzá a *Windows Azure Active Directory* és *Windows Azure Service Management API* alkalmazásokat.

Fontos, hogy legalább a 13. Ábra és a 14. Ábra látható alábbi két jogosultság hozzá legyen rendelve:



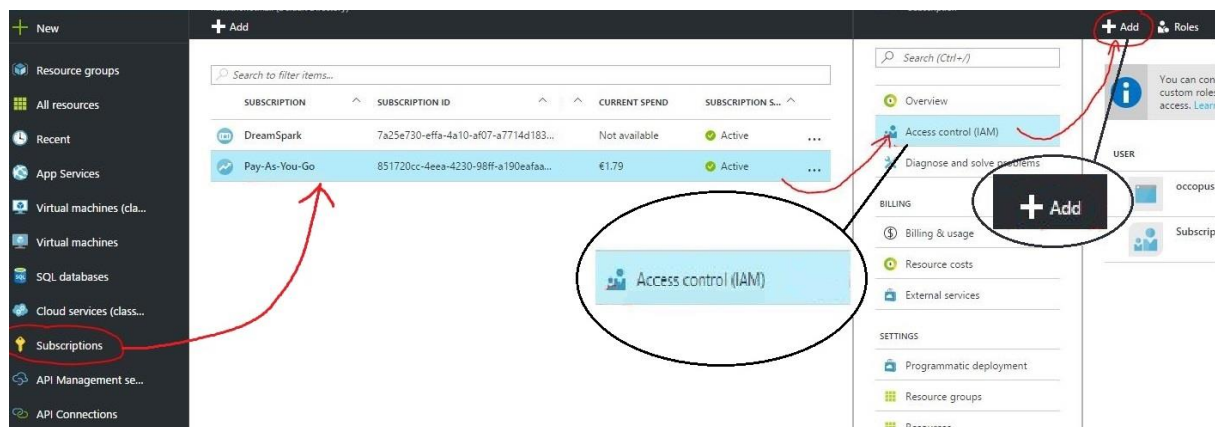
13. Ábra - Webalkalmazás Delegated Permission 1/2



14. Ábra - Webalkalmazás Delegated Permission 2/2

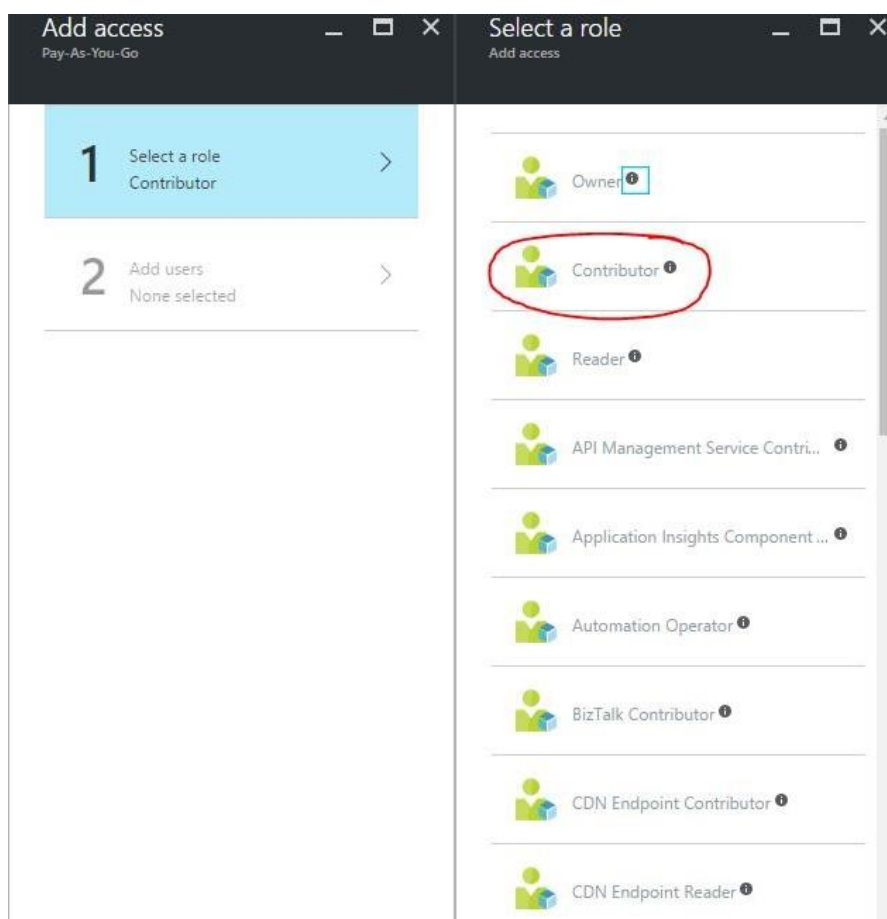
Az ábrákon található jogosultságokat pipáld ki, majd az alsó fekete menüsoron *Save* gombbal mentsd el.

Ha ezek megvannak, térjünk vissza a <https://portal.azure.com/> oldalra. Itt még egy feladatunk lesz. Az elkészített és beállított webalkalmazásunkhoz *Contributor* jogot adni, ami ahhoz szükséges, hogy erőforrás csoportokat tudjunk olvasni, létrehozni, törölni és a benne lévő erőforrásokat menedzselni tudjuk az Occopus eszközzel.



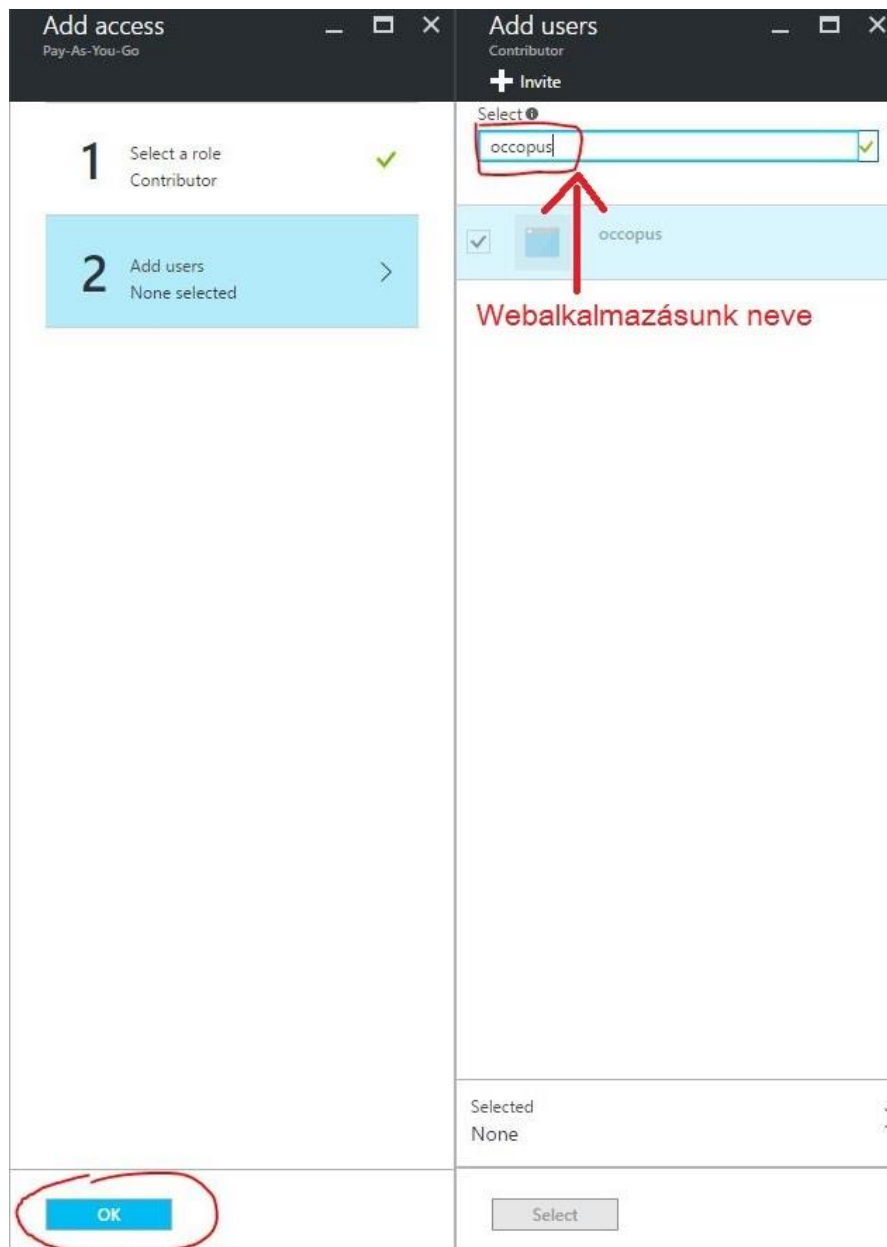
15. Ábra - Előfizetés hozzáférés kezelése

Előfizetésedhez egy új hozzáférést kell hozzáadnod a 15. Ábra látható módon. Először válaszd ki a *Subscription* menüpontot, majd az *előfizetésedet*, amihez hozzá szeretnéd rendelni az Occopus-t. Ezután kattints az *Access control (IAM)* elemre majd az *Add* gombra.



16. Ábra - Előfizetés hozzáférés, szerepkör kiválasztás

Ekkor megjelenik a 16. Ábra látható menü, itt válaszd ki a *Contributor* szerepkört.



17. Ábra - Előfizetés hozzáférés, felhasználó kiválasztás

Majd adjuk hozzá az előző fejezetben létrehozott webalkalmazásunkat. *Select textboxban* keress rá ennek a nevére, válaszd ki és kattints az *OK* gombra (lásd: 17. Ábra). A jogosultság hozzáadása után áttérhetünk a virtuális infrastruktúránk létrehozásának előkészítésének.

Megjegyzés: abban az esetben, ha nem tudod kiválasztani az alkalmazásod, akkor térj vissza az Azure Active Directory webalkalmazás azonosító fejezethez és ellenőrizd, hogy mindent megfelelően készítettél-e el.

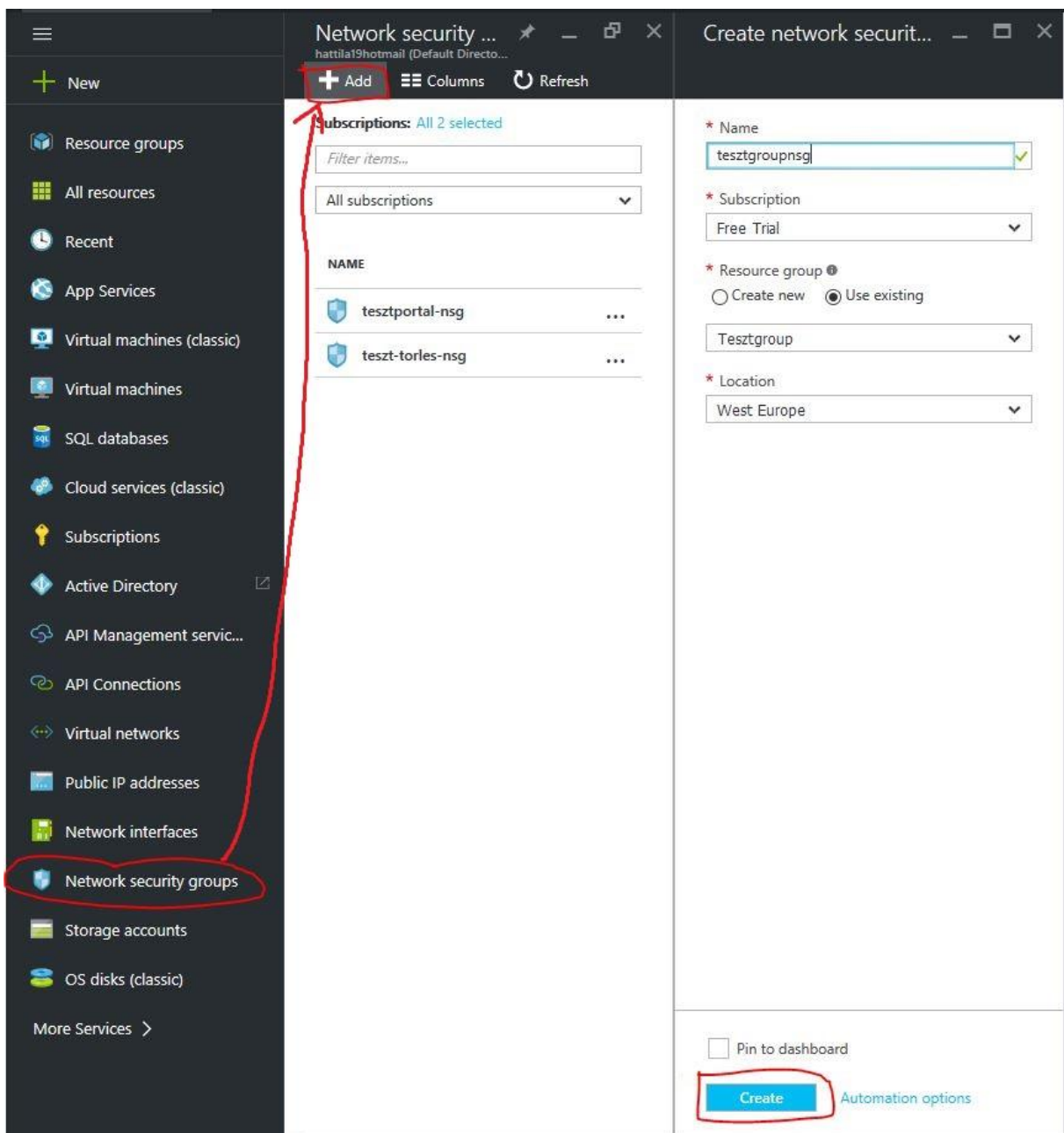
4. lépés – VM előkészítése

Azure-ban a virtuális gépeket erőforrás csoportokban (resource group) hozhatunk létre. Ezért első lépésként amennyiben nincs még ilyened, akkor a *Resource groups* menüpont majd az *Add* gombra kattintva készíts egyet.

Egy virtuális géphez erőforrások szükségesek, ezeket a következők sorrendben hozzuk létre:

4.1 Network security group

Ebben az alfejezetben hozhatunk létre tűzfalszabályokat, amit vagy hálózati kártyákhoz külön-külön vagy egy virtuális alhálózathoz rendelhetünk hozzá.

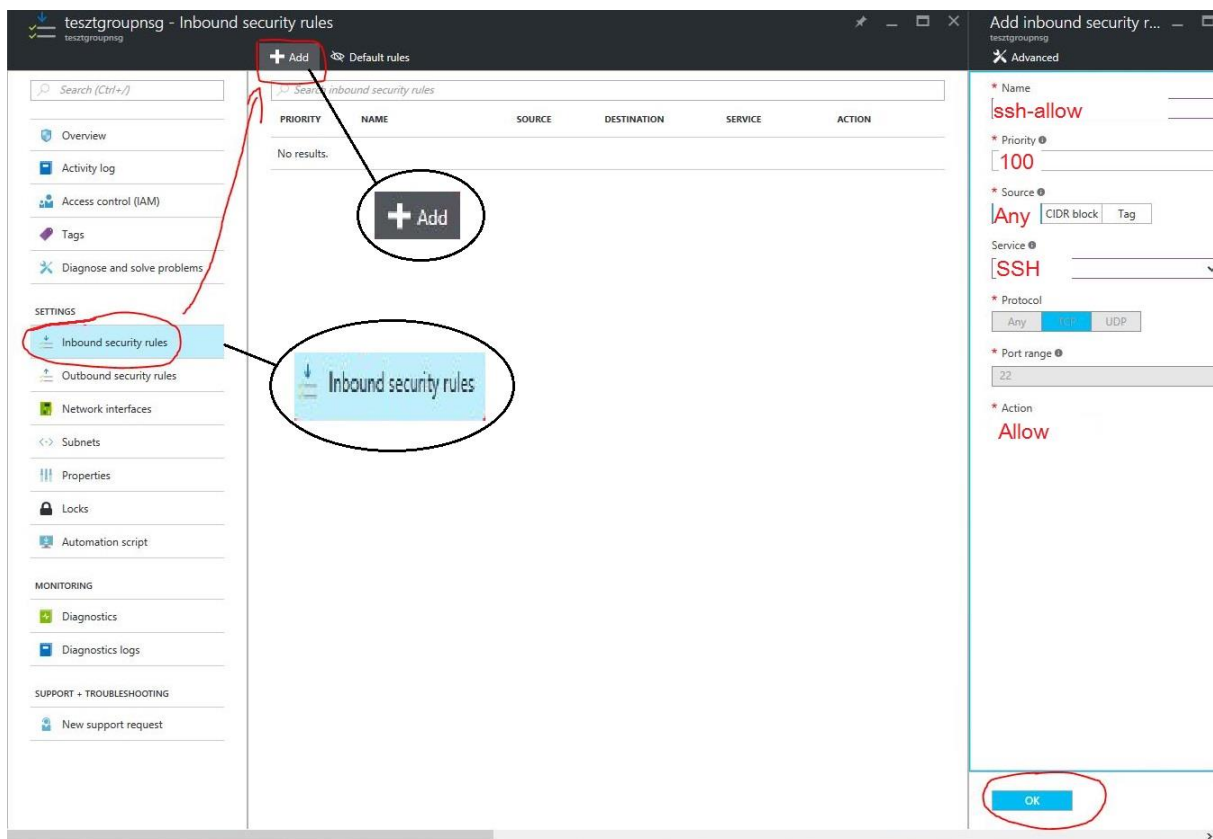


18. Ábra - Network Security Group készítés

A 18. Ábra segítségével válaszd ki a *Network security groups* pontot, majd *Add* gomb, ezután adj *nevet* az erőforrásnak és válaszd ki melyik *előfizetésedhez* és azon belül melyik *Resource group*-ba szeretnéd létrehozni, a *Location* résznél pedig célszerű az *Resource group*-al azonosat kiválasztani. Létrehozni az alsó *Create* gomb megnyomásával tudod.

4.1.1 SSH kapcsolatot engedélyező tűzfal szabály

Ez egy példa szabály, ami célszerű felvenni ahhoz, hogy be tudjunk lépni a virtuális gépünkbe.

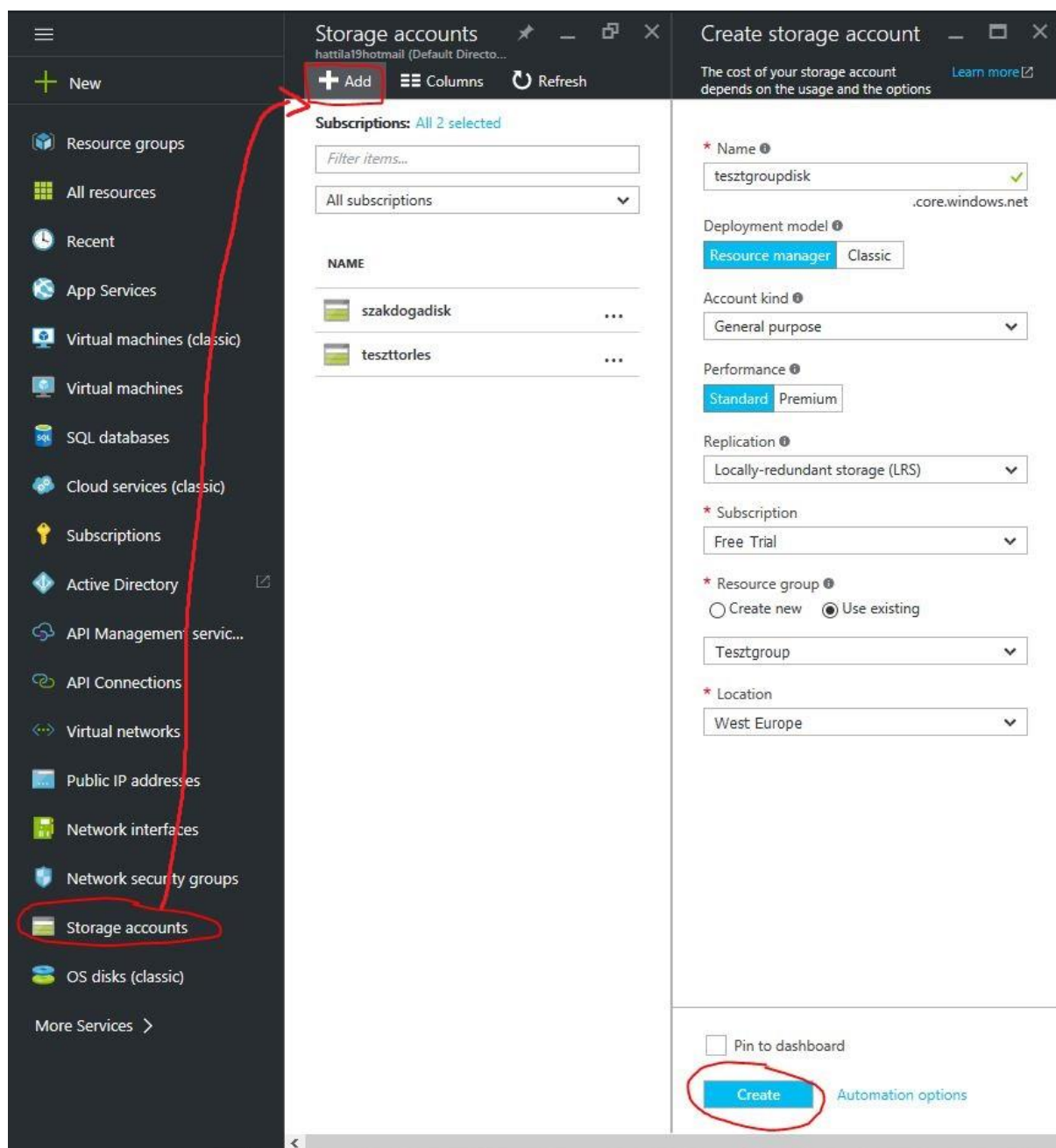


19. Ábra - SSH tűzfal szabály

Az előbb létrehozott *Network security group* ablakában a *Settings* menüpont alatt az *Inbound security rules* elemre kattints rá, majd nyomd meg az *Add* gombot. A megjelenő ablakban lévő mezőket a 19. Ábra látható módon töltsd ki.

4.2 Storage account

A virtuális gépekhez kötelezően hozzá kell rendelni egy *storage account* erőforrást, ezért hozz létre egyet.

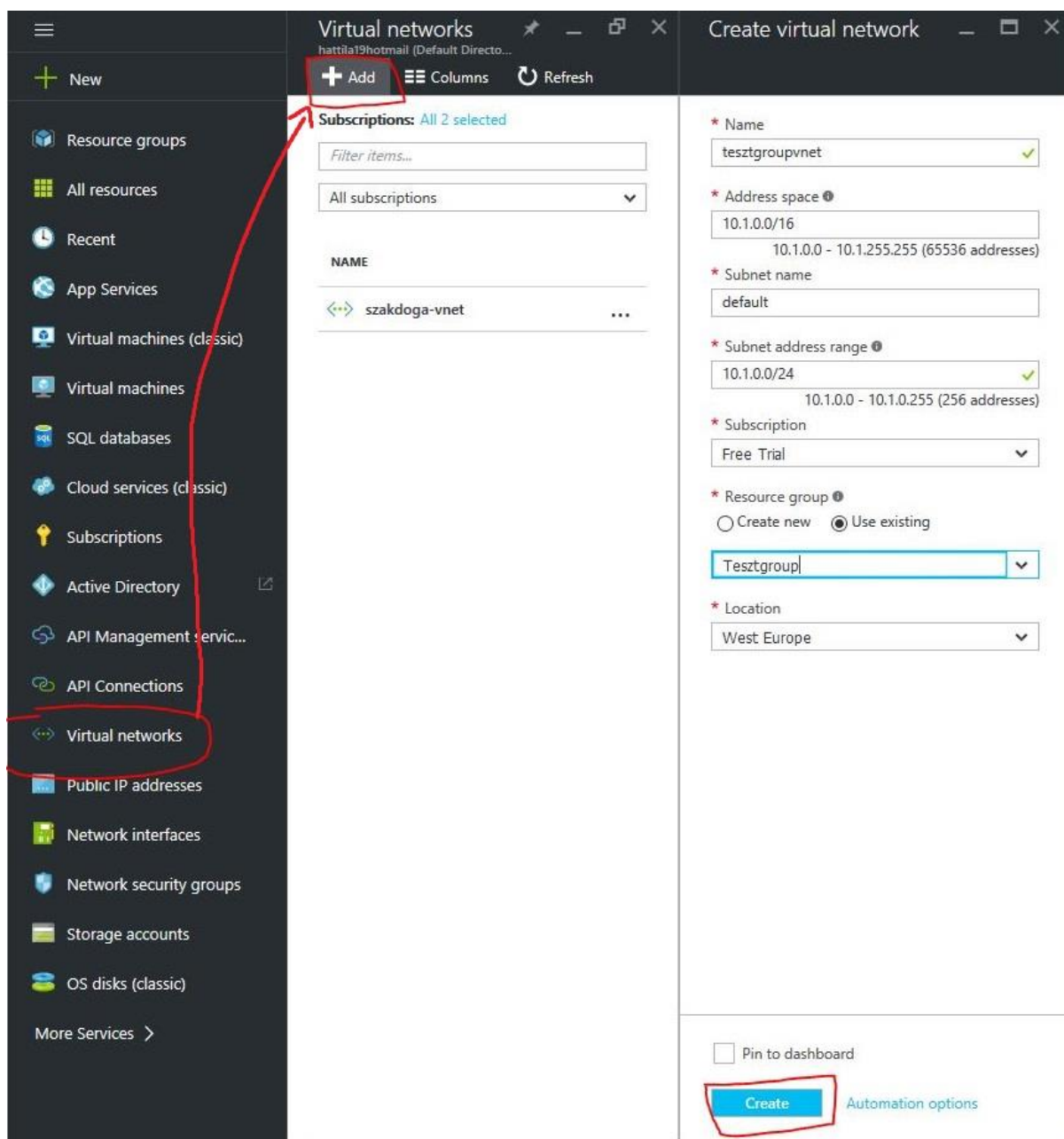


20. Ábra - Storage account készítés

Ezt a *Storage accounts* menüpont, majd *Add* gombra kattintva tudod megtenni. A megjelenő ablakban töltsd ki az 20. Ábra segítségével. A név lehet más is, célszerű beszédes nevet adni.

4.3 VNET

Virtuális hálózat, amihez a hálózati kártyá(ka)t hozzárendeljük. Hozz létre egyet a 21. Ábra segítségével.



21. Ábra - Virtuális hálózat készítés

Virtual network menüpontot válaszd ki, majd *Add* gombot nyomd meg. Ezután az ábra segítségével töltsd ki az adatokat. A név lehet más is, célszerű beszédes nevet adni. Ha ezeket elkészítettük, le tudjuk ellenőrizni az erőforrás csoportok menüpont alatt a végeredményt.

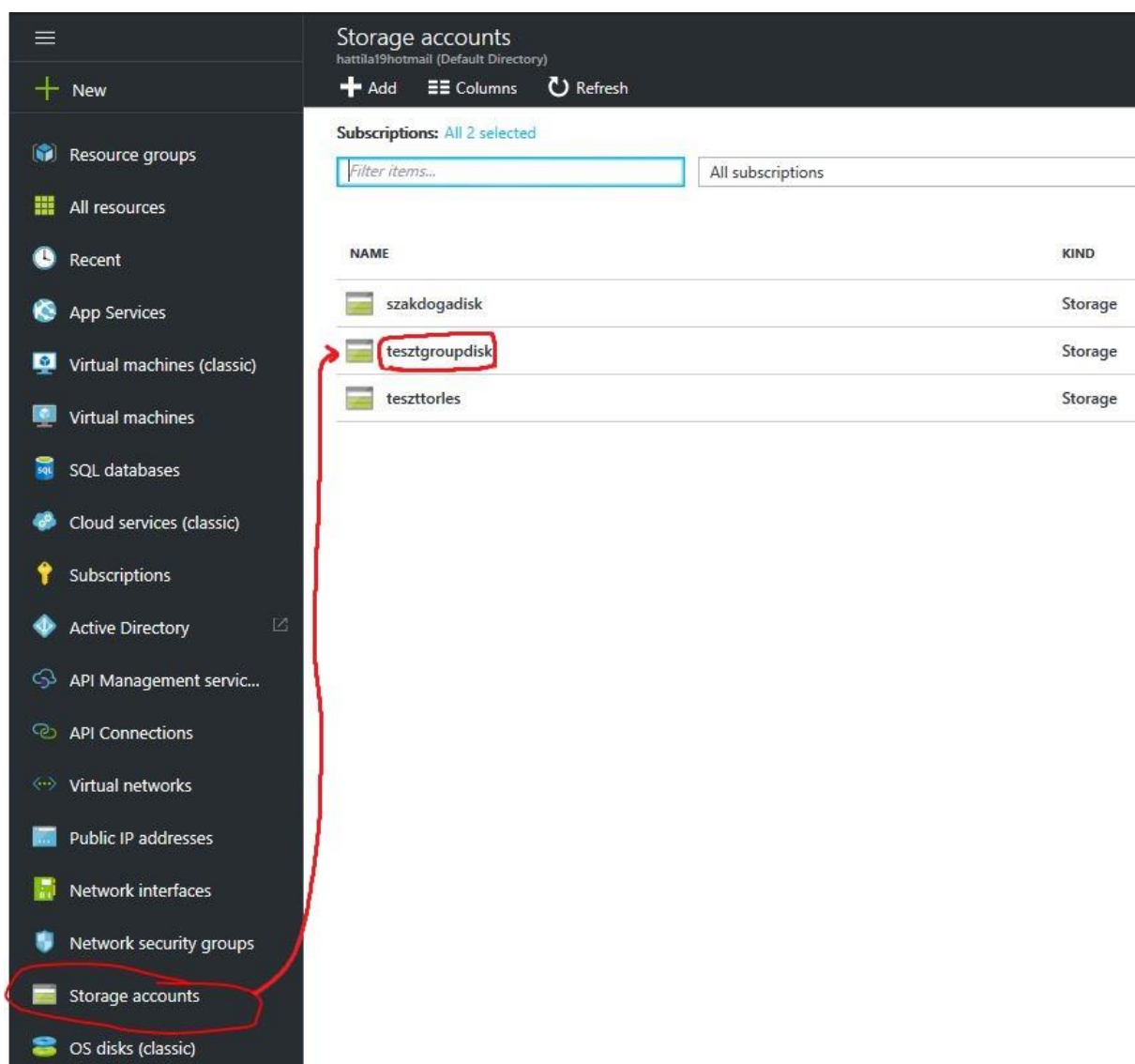
5. lépés – VM erőforrás információk kigyűjtése

Szükségünk lesz az előbb létrehozott erőforrások azonosítójára, pontosabban a

- Storage Account nevére,
- kulcsára,
- VNET ID,
- VNET subnet nevére,
- VNET lokációjára,
- Network Security Group ID.

Ezek megtalálását a következő fejezetekben mutatom be.

5.1 Storage Account név

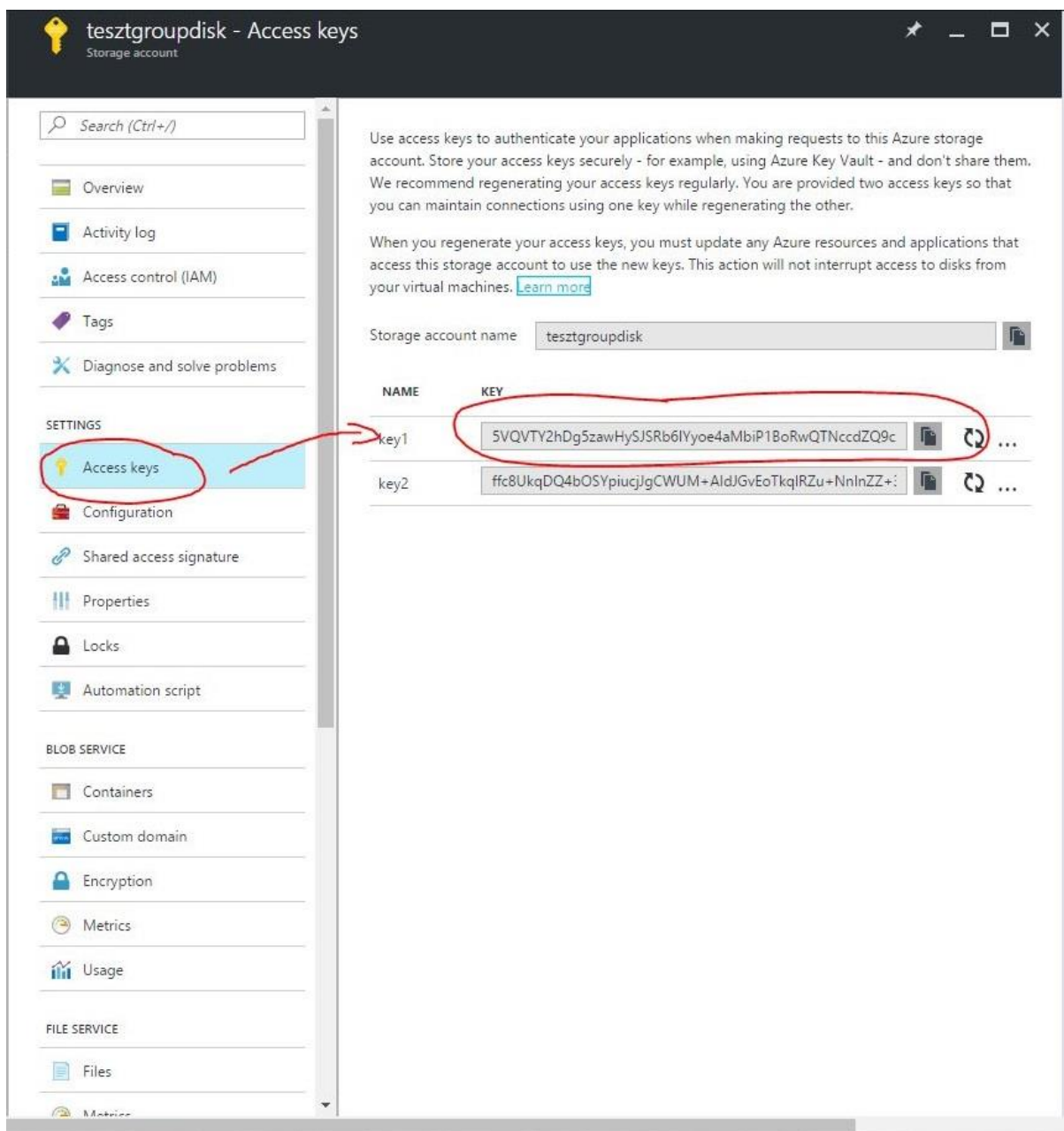


22. Ábra - Storage account név

Ha elfelejtettük az előző fejezetben létrehozott storage account nevét, akkor a *Storage accounts* menüpont alatt a *Name* oszlopban megtaláljuk (lásd: 22. Ábra).

5.2 Storage Account kulcs

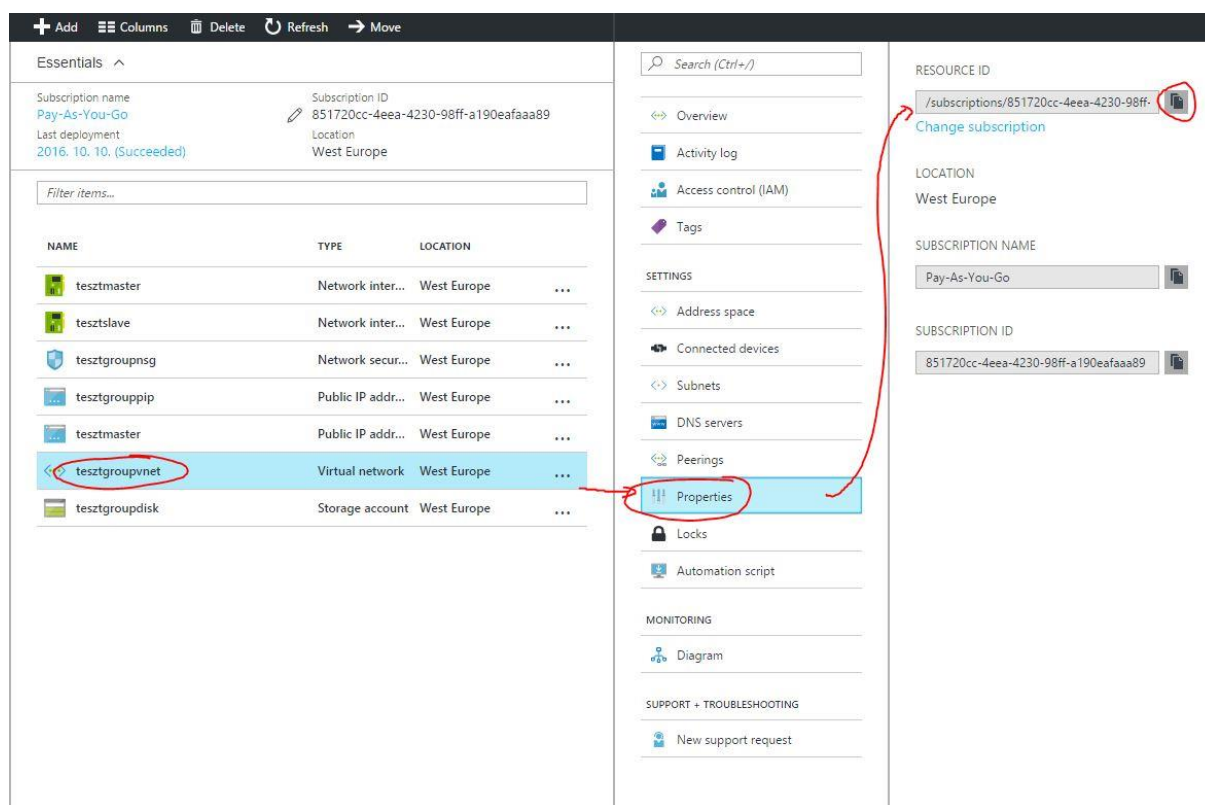
A kulcs azért szükséges, hogy az Occopus hozzáférhessen az *Storage account*-on belüli további erőforrásokhoz (blob-okhoz, konténerekhez).



23. Ábra - Storage account kulcs

A 23. Ábra segítségével az előzőekben létrehozott storage account ablakában a *Settings* almenüben az *Access keys* elemre kattints rá. Ezután a *key1* nevű kulcsot másold ki, a mellette lévő másoló gombbal egyből a vágólapra másolhatod.

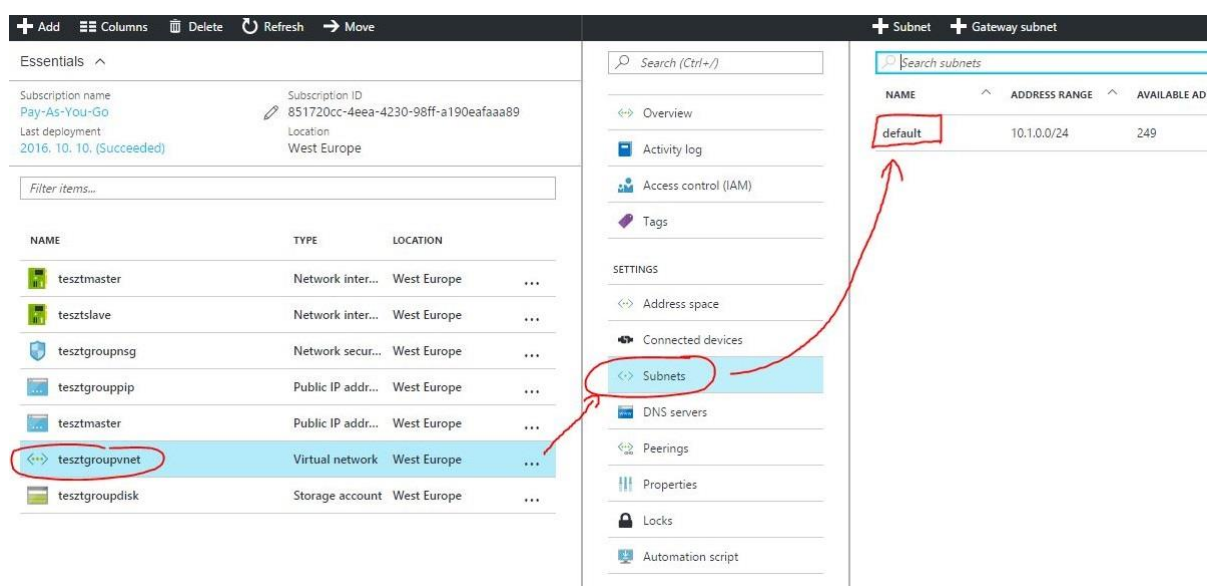
5.3 VNET ID



24. Ábra - VNET ID

A 24. Ábraán látható módon, kattints az általad létrehozott *Resource groups*-on belül a VNET alfejezetben létrehozott VNET nevére, majd a *Properties* menüpontra. Ott találod a *resource id*-t, amit a mellette lévő gomb megnyomásával a vágólapra másolhatod.

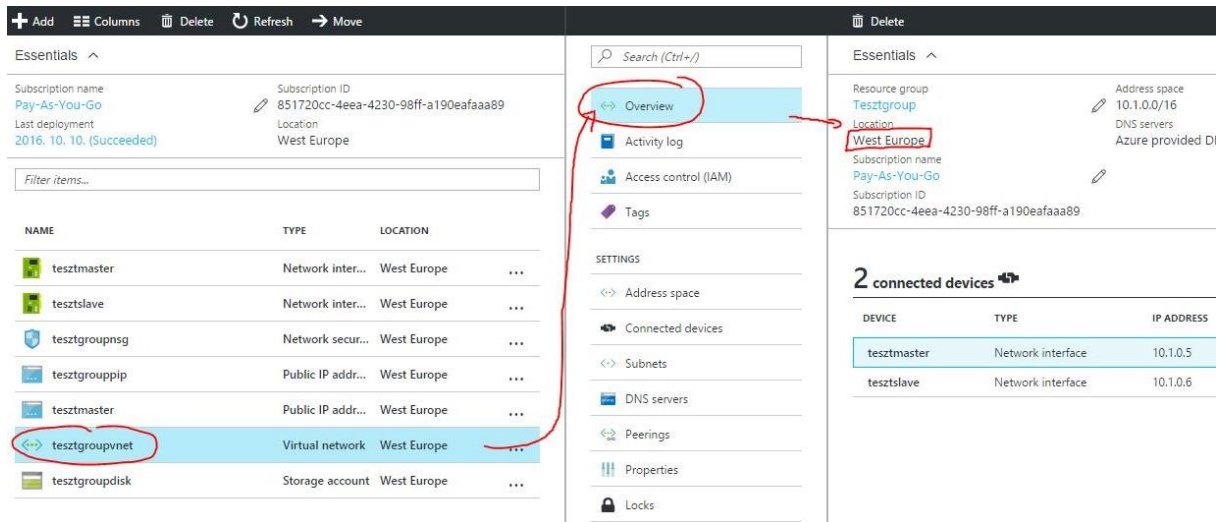
5.4 VNET subnet neve



25. Ábra - VNET subnet név

A 25. Ábra segítségével kattints az általad létrehozott *Resource groups*-on belül belül a VNET alfejezetben létrehozott VNET nevére, majd a *Subnets* menüpontra. Ott találod a subnet nevét.

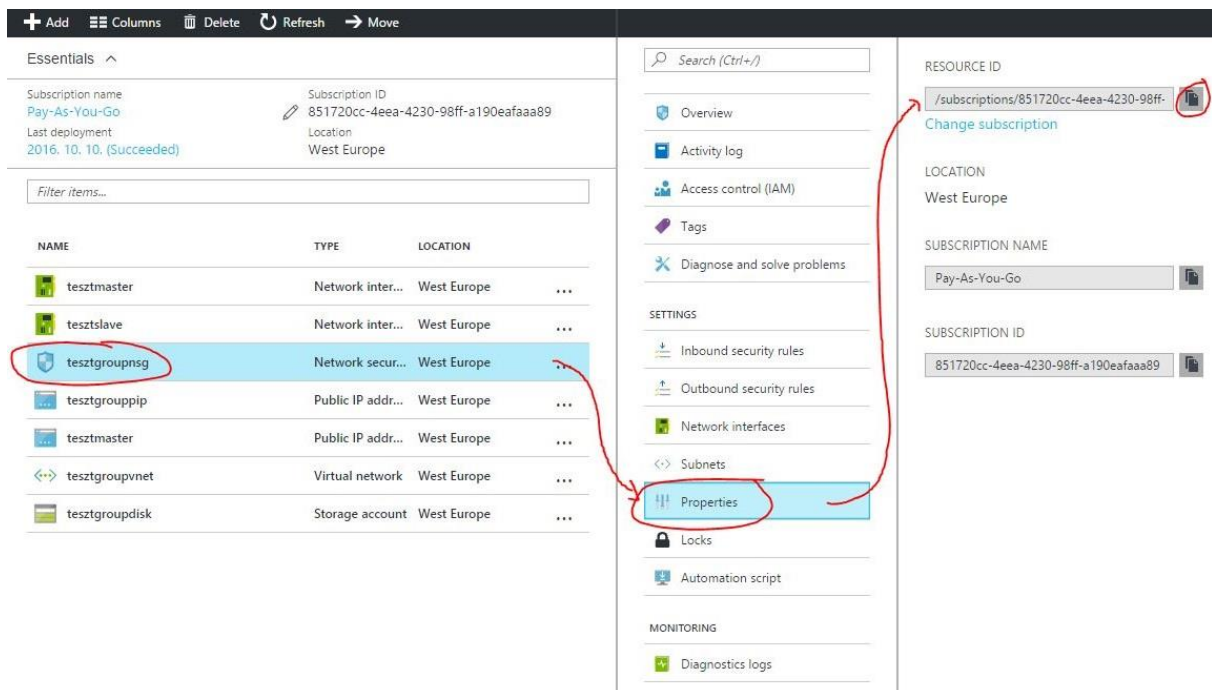
5.5 VNET lokációja



26. Ábra - VNET lokáció

Kattints az általad létrehozott *Resource groups*-on belül belül a VNET alfejezetben létrehozott VNET nevére, majd az *Overview* menüpontra (lásd: 26. Ábra). A *Location* értéke, a lokáció.

5.6 Network security group ID



27. Ábra - Network security group ID

Menj az általad létrehozott *Resource groups*-on belül a Network security group alfejezetben létrehozott Network security group nevére, majd kattints a *Properties* menüpontra a 27. Ábra

láthatóan. Ott találod a *resource id*-t, amit a mellette lévő gomb megnyomásával a vágólapra másolhatod.

6. lépés – VM létrehozáshoz szükséges adatok

Az 5. lépésben kigyűjtött adatokon kívül még az idézőjelek között lévő értékeket is kell megadnunk a `node_definitions.yaml` fájlban, idézőjel nélkül!

6.1 Kötelező mezők:

Az 5. lépésen kigyűjtött adatokon kívül a következők:

- VM lokáció - **vm_location** : „westeurope”
- VM mérete - **vm_size** : „Standard_A1”
VM méretekről további információk itt: <https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-sizes/>
- OS publikáló - **publisher** : „Canonical”
További információk a Linux VM képfájlokról: <https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-linux-cli-ps-findimage/>
- OS neve - **offer** : „UbuntuServer”
- OS típusa - **sku** : „16.04.0-LTS”
- OS verziója - **version** : „latest”
- OS felhasználónév - **username** : „adminka”
- OS jelszó - **password** : „Ez1konnyujelszo”
Kontextualizációhoz Cloud-init: a `cloud-init.txt` fájlban lévő adat.
Cloud-init-et csak UbuntuServer és CoreOS operációs rendszer esetén használható.
További információk itt: <https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-linux-using-cloud-init/>

6.2 Opcionális mezők:

Publikus IP cím igénye - **public_ip_needed** : „True or False” (ha a mező nincs megadva, akkor False)

További információk a statikus kontra dinamikus IP címről itt:

<https://azure.microsoft.com/en-us/documentation/articles/virtual-network-ip-addresses-overview-arm/>

Publikus DNS név - **public_dns_name** : „occpusteszt” (ha a mező nincs megadva, akkor nem lesz DNS név a publikus IP címhez hozzárendelve)

Megtartsa-e a VM-hez tartozó `osdisk.vhd` fájlt VM törléskor - **keep_vhd_on_destroy** : „True or False” (ha nincs a mező megadva, akkor letörli az `osdisk.vhd` fájlt)

7. Irodalomjegyzék

- [1] Use portal to create Active Directory application and service principal that can access resources, <https://azure.microsoft.com/hu-hu/documentation/articles/resource-group-create-service-principal-portal/>,
utoljára megtekintve: 2016. 10. 23.
- [2] Sizes for virtual machines in Azure, <https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-sizes/>,
utoljára megtekintve: 2016. 10. 23.
- [3] Select Linux VM images with the Azure CLI, <https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-linux-cli-ps-findimage/>,
utoljára megtekintve: 2016. 10. 23.
- [4] Using cloud-init to customize a Linux VM during creation,
<https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-linux-using-cloud-init/>,
utoljára megtekintve: 2016. 10. 23.
- [5] IP addresses in Azure, <https://azure.microsoft.com/en-us/documentation/articles/virtual-network-ip-addresses-overview-arm/>,
utoljára megtekintve: 2016. 10. 23.