



MTA CLOUD

Felhasználói kézikönyv v1.0

MTA Cloud csapat
info@mta.cloud.hu

Tartalom

Bemutató	2
Az MTA Cloud célja	2
Mire jó az MTA Cloud	2
Kinek ajánljuk	3
Használati útmutató	3
Az MTA Cloud-ból elérhető szolgáltatások	3
Virtuális gépek típusai – Operációs rendszerek és Flavor-ok	3
Hálózat	4
Regisztráció menete	4
Belépés	4
Virtuális gép létrehozása	5
Kötelező paraméterek	5
További ajánlott paraméterek	6
Instance elérése és kezelése böngészőből	7
Instance elérése és kezelése külső kapcsolattal	8
Instance elérése SSH kapcsolattal	8
Publikus IP nélküli Instance elérése távolról SSH-val	9
SSH kapcsolat kétkulcsos hitelesítéssel	9
Felhasználó létrehozása Linuxban	10
Open VPN felállítása heat template használatával	10
Hibák, illetve a projekttel kapcsolatos további igények bejelentése	11

Bemutakozás

Az MTA Cloud célja

Az egész világon rohamtempóban terjednek a Cloud szolgáltatások mind akadémiai és egyetemi, mind üzleti környezetben, melynek oka a nagymértékű rugalmasság és skálázhatóság, ami lehetővé teszi, hogy a Cloud technológiát számtalan alkalmazásra és nagyon sokféle kapacitásméret mellett lehet alkalmazni. Ennek az új trendnek és kihívásnak kívánt eleget tenni az MTA is, új Cloud szolgáltatásának felállításával, amely az MTA SZTAKI és az MTA WIGNER FK Adatközpont közös munkája nyomán jött létre. Célunk az volt, hogy a kutatók számára könnyebben és gyorsabban biztosítsuk azokat a számítási és tárolási kapacitásokat, amelyek egy-egy nagyobb kutatási projekt megvalósításához szükségesek. Az MTA Cloud célja a kutatás támogatása (és nem az irodai tevékenységek).

Mire jó az MTA Cloud

A Cloud szolgáltatásokban tipikusan három szintet szoktak megkülönböztetni: infrastruktúra Cloud (IaaS), platform Cloud (PaaS) és szoftver Cloud (SaaS). Az MTA Cloud ezek közül az infrastruktúra Cloud (IaaS) szintet célozza meg, amire a későbbiekben a további szintek is építhetők. Az MTA Cloud, mint IaaS Cloud lehetővé teszi az akadémiai kutatók számára, hogy különböző típusú és méretű infrastruktúrákat alakítsanak ki dinamikusan, az aktuális projektjeik igényei szerint anélkül, hogy a jelenleg szokásos hosszúságú és bonyolult beszerzési eljárásokon kellene keresztülmenniük. Így például az egyszerű desktop gépektől (pl. Windows, Linux, Mac PC-k) a szuperszámítógép teljesítményt nyújtó számítási fürtökig (pl. PBS fürt, LSF fürt) számos különböző típusú és méretű infrastruktúrát építhetnek ki az MTA Cloud-ban, számítási kapacitásuk növelése érdekében.

Az MTA Cloud nagyméretű tárolókapacitást is nyújt a tudományos adatok ideiglenes tárolására, arra az időre, amíg a Cloud-ban kialakított infrastruktúrán futó alkalmazások az adatok feldolgozását végzik. Az adatok biztonságos tárolását a legkorszerűbb OpenStack Cloud alkalmazása biztosítja.

Kinek ajánljuk

Az MTA Cloud-ot azon kutatóknak ajánljuk, akik

- nagy mennyiségű adatot számítógéppel dolgoznak fel vagy szeretnének megosztani
- egy vagy több számítógépen használnak kutatást támogató szoftvereket
- számítógépfürtöt, szerverparkot, adatközpontot, szuperszámítógépet használnak
- számításigényes vagy adat intenzív szimulációkat és/vagy egyéb feldolgozásokat végeznek

Használati útmutató

Az MTA Cloud-ból elérhető szolgáltatások

Az MTA Cloud egy infrastruktúra szolgáltatás, amelynek segítségével virtuális számítási kapacitást tudunk az igénylők, felhasználók számára rendelkezésre bocsájtani. Ezen erőforrásokat hálózatba kötött virtuális gépek formájában tudjuk biztosítani.

Virtuális gépek típusai – Operációs rendszerek és Flavor-ok

Operációs rendszerek:

- **CentOS 7** - CentOS-7-x86_64-GenericCloud-1606-20160705
- **Ubuntu 14.04 server** - ubuntu-14.04.4-server-cloudimg-amd64-20160218-dp
- **Ubuntu 16.04 server** – ubuntu-16.04-server-cloudimg-amd64-20160615-dp

Flavour-ok (igényelhető fizikai géptípusok)

Név	VCPUS	RAM	Disk
m1.small	1	2 GB	20 GB
m1.medium	2	4 GB	40 GB
m1.large	4	8 GB	80 GB
m1.xlarge	8	16 GB	160 GB

Hálózat

A projekt példányai között felállítandó hálózati kapcsolat. Alapértelmezetten választható egy [projektnév]-net nevű hálózat, ami hozzáadható a példányhoz. A Network → Networks fül alatt lehetőség van új hálózatok létrehozására.

Regisztráció menete

A regisztrációt a cloud.mta.hu weboldal [“Csatlakozás az MTA cloudhoz”](#) menüpontja alatt lehet elindítani. **Fontos megjegyezni, hogy az igénylés alapfeltétele az, hogy az igénylő rendelkezzen eduID-val.** A regisztrációs űrlap kitöltésénél kérjük, hogy a „VÁRHATÓ SZOFTVEREK” mezőbe ne csak a futtatni tervezett szoftverek számát, de azok nevét is írják be. A másik fontos pont, hogy az „ÖSSZES IGÉNYELT ERŐFORRÁS” megadásánál kérjük, vegyék figyelembe a fent felsorolt, elérhető flavor-ok típusait, és azok erőforrásainak fényében határozzák meg az igényelt erőforrásokat. Természetesen amennyiben más erőforrásokkal rendelkező flavor-re is szükség lenne az is megoldható, de ez elnyújthatja az igénylés folyamatát.

Belépés

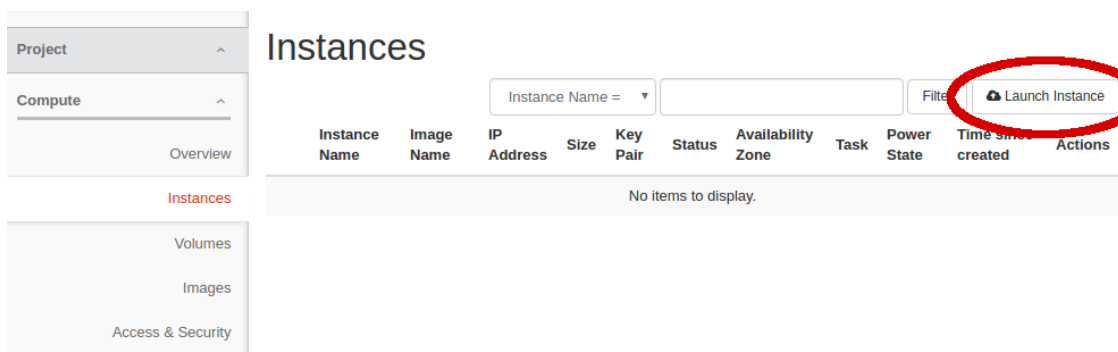
A belépésre az alábbi linken van lehetőség. Attól függően, hogy az MTA Cloud mely szolgáltatója vállalja az Ön projekt igényének kiszolgálását, attól függően az alábbi linkek egyikén keresztül léphet be. Erről a regisztráció folyamán kap tájékoztatást.

- <https://sztaki.cloud.mta.hu>
- <https://wigner.cloud.mta.hu>

A 'Federated Login (eduGAIN)' opcióban a szervezet kiválasztása után van lehetőség a felhasználói név és a jelszó beírására.

Virtuális gép létrehozása

Új virtuális gép létrehozására a Compute → Instances → Launch Instance menüpont alatt van lehetőség.



Az új felugró ablakban kell beállítani a gép paramétereit. A *-al jelöltek kitöltése kötelező.

Ha kívülről importált SSH kulccsal akarja létrehozni az instancet, érdemes azt először külön beimportálni (Compute → Access & Security → Key Pairs → Import Key Pair), majd az instance létrehozásánál már csak hozzáadni a beimportált kulcspárt a helyes működés érdekében.

Kötelező paraméterek

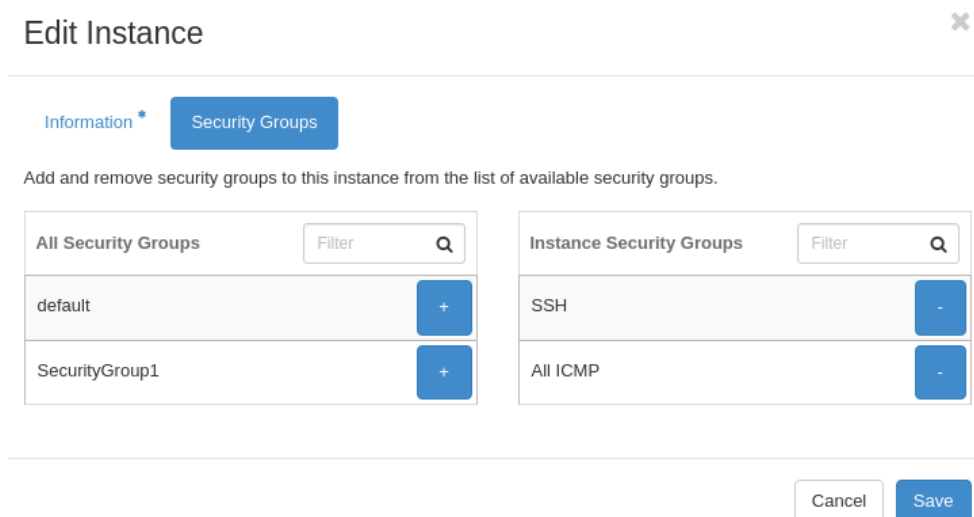
- **Instance Name:** a példány neve
- **Count:** létrehozandó példányok száma a beállított paraméterekkel (alapértelmezetten 1)
- **Flavor:** a példányhoz tartozó erőforrás hozzárendelés (RAM, CPU mag, tárhely). Az általunk meghatározott csomagokból adhatóak hozzá a + nyomógombra kattintva
- **Networks:** a projekt példányai között felállítandó hálózati kapcsolat. Alapértelmezetten választható egy [projektnév]-net nevű hálózat, ami hozzáadható a példányhoz.

További ajánlott paraméterek

- **Key Pair:** a virtuális gép a hozzáadott publikus kulccsal fog legenerálódni, aminek segítségével SSH kapcsolat építhető fel (az adott publikus kulcs privát kulcs párjának birtokában) az OpenStack felületétől függetlenül a virtuális gépünkre. Abban az esetben, ha még nincs feltöltve publikus kulcs a listába, az megtehető a Compute → Access & Security → Key Pairs fül alatt. Kulcs létrehozására két lehetőség van:
 - az általunk generált publikus kulcs kerül feltöltésre a saját gépünkről az „Import Key Pair” gombra kattinva,
 - generálható a Dashboard-on, a „Create Key Pair” gombra kattintva. Itt automatikusan letöltésre kerül a „Download Key Pair” oldalra navigálva a kulcs privát része a kliensgépre, illetve a „Key Pairs” listába bekerül az új generált publikus kulcs.

FONTOS: a „Download Key Pair” oldalon a Download key pair „[KEY_PAIR_NAME]” linkre kattintva újra letöltődik a privát kulcs, ami felülírja az elsőre generált kulcspárt, így érvényét is veszti. Az összes gépen, ami ezalatt a kulcspár alatt generálódott, a beállított SSH kapcsolat meghibásodhat.
- **Security Groups:** különböző tűzfalszintű csoportszabályok adhatóak hozzá a példányhoz. Ezeket akkor kell hozzáadni a virtuális géphez, ha kívülről kell elérni valamilyen szolgáltatását a virtuális gépnek, vagy kommunikációt kell létesíteni vele. Vannak előre definiált, sokszor használatos biztonsági csomagok (pl. SSH elérést biztosító szabály, ami kinyitja a 22-es portot). Az alap csoportszabályok portjai a külvilág felé is nyitva lesznek, ha az adott példányhoz Floating IP-t rendelünk (erről szó esik az „Instance elérése külső kapcsolattal” fejezet alatt). Specifikusabb igény esetén, szabadon létrehozható szabály a Compute → Access & Security → Security Groups fül alatt. A „default” szabályt ajánlott hozzáadni ahhoz a virtuális géphez, aminek látnia kell a külvilágot, illetve a virtuális hálózatban kommunikálnia kell a többi virtuális géppel.

Ha már létrejött az instance, utána is van lehetőség módosítani a hozzáadott security groupokat a létrejött instance Edit Instance → Security Groups menüpontjában.



Edit Instance ✕

Information * **Security Groups**

Add and remove security groups to this instance from the list of available security groups.

All Security Groups	Filter	Q
default		+
SecurityGroup1		+

Instance Security Groups	Filter	Q
SSH		-
All ICMP		-

Cancel Save

A „Launch Instance” gombra kattintva elindítható a definiált példány a választott Image fájlból. A Compute → Instance menüpont alatt láthatóak az eddig létrehozott példányok, amik között látható az újonnan létrehozott példány is.

Instance elérése és kezelése böngészőből

A **Compute** → **Instance** oldalon az Instance névre kattintva négy fülre tagolódik az oldal:

- **Overview:** az kiválasztott Instance adatai vannak kilistázva
- **Console:** itt lehet használni a virtuális gépet böngészős felületről.
- **Action Log:** az OpenStack felületéről menedzselt eljárások listája
- **Logs:** a virtuális gép logja. Abban az esetben, ha nem lehet elérni külső kapcsolattal, vagy konzolos felületről, itt lehetséges értesülni bármiféle hibáról, ami az Instance működéséről szól.

Ubuntu rendszerek esetén az alap felhasználónév *ubuntu* és a jelszó szintén *ubuntu*. Ezt az első belépés után át kell írni. Ha a console nem akarja érzékelni az egér kattintást, akkor érdemes kikattintani a szürke részre és újra bekattintani a console területére.

Instance elérése és kezelése külső kapcsolattal

A kiválasztott virtuális gép (Compute → Instances) sorában, az „Actions” oszlopban a lefelé mutató nyílra kattintva egy lenyíló menü jelenik meg, itt az „Associate Floating IP”-re kell rákattintani. A megjelenő moduláris ablakban az „IP Address” lenyíló menüben kell kiválasztani a már allokált floating IP címet. Ezek után az „Associate” nyomógombra kattintva megtörtént a virtuális gép publikus IP címének hozzárendelése.

Ezt a Compute → Instances oldalon található táblázatban láthatjuk meg az IP Address oszlopban, a „Floating IPs” kiírás alatt. Külső címre a floating IP a következőképpen van leképezve: 10.1.21.X → 193.224.176.X ; inentől kezdve a virtuális gépet a 193.224.176.X címről lehet elérni. (Példa: 10.1.21.80 → 193.224.176.80)

Instance elérése SSH kapcsolattal

A „Virtuális gép létrehozása” fejezet alatt a Key Pair résznél hozzáadott kulcspárt használva lehet először kapcsolatot létesíteni SSH-t használva a virtuális gép között. A virtuális géphez egy külső IP címet kell rendelni, hogy a külvilágból is el lehessen érni, ez a „Instance elérése és kezelése külső kapcsolattal” fejezetben leírtak szerint tehető meg.

A privát kulcsok biztonságos kezelése (sérülés, elvesztés, idegen kézbe kerülés elkerülése) a felhasználó felelőssége! Privát kulcsot megfelelő helyre (~/.ssh/id_rsa fájl) kell rakni, megfelelő (600-as) jogosultsággal:

```
chmod 600 [privat_kulcs_neve]
```

Nix rendszereken a következő parancsot kell kiadni terminálban az SSH kapcsolat felépítéséhez:

```
ssh -i [privát_kulcs_elérési_útja] [felhasználónév]@[virtuális_gép_publikus_címe]
```

```
példa: ssh -i ~/.ssh/id_rsa gipszjakab@148.6.200.80
```

Windows rendszerekben a PuTTY program a legelterjedtebb SSH kapcsolat felépítésére. A beállítások a következők:

Session: Hostname: [virtuális gép IP címe], Port: 22, Connection Type: SSH

Az SSH → Auth menüpont alatt, a Tallózás.. (Browse...) gombra kattintva adható hozzá a kapcsolathoz használatos privát kulcs.

Publikus IP nélküli Instance elérése távolról SSH-val

Minden projekthez 1 publikus IP-t biztosít az MTA Cloud, aminek következménye, hogy több Instance létrehozása esetén nem mindegyik látható közvetlenül a külvilág felől. A megoldás erre a következő:

A publikus IP-vel NEM rendelkező szerveren a következőket kell konfigurálni terminálban (*Nix):

```
sudo nano /etc/ssh/sshd_config → A szerkesztőben ki kell keresni a „PasswordAuthentication yes” vagy a „PasswordAuthentication no” részt. Ezt a sort ki kell törölni és a következővel helyettesíteni: „PasswordAuthentication yes”. Ezt követően el kell menteni és kilépni.
```

Kilépés után a következő parancsot kell kiadni:

```
Ubuntu: sudo service ssh restart
```

```
Centos: sudo service sshd restart
```

Ezek után az elérendő virtuális gépen levő felhasználókkal be lehet ssh-zni a publikus IP-vel rendelkező virtuális gépről (amire természetesen direktbe is lehetséges SSH-zni).

A nagyobb biztonságot és funkcionalitást nyújtó SSH kapcsolat konfigurálása az „SSH kapcsolat kétkulcsos hitelesítéssel” részben olvasható.

SSH kapcsolat kétkulcsos hitelesítéssel

Mindenekelőtt SSH kulcspárt kell generálni a kliensgépen, ennek parancsa:

```
ssh-keygen
```

A bekért alapbeállításokat elfogadva (amihez csak entereket kell nyomni), a következő parancsot kell kiadni ugyanazon gépen a célgép felé, amihez SSH-zni szükséges:

```
cat ~/.ssh/id_rsa.pub | ssh [felhasználó_a_célgépen]@[célgép_címe] "mkdir -p ~/.ssh && cat  
>> ~/.ssh/authorized_keys"
```

Abban az esetben, ha létrehoztuk az összes felhasználóhoz a kétkulcsos hitelesítést, akkor érdemes letiltani az SSH konfigurációs fájljában a jelszavas hitelesítést a virtuális gépeken.

Felhasználó létrehozása Linuxban

Többször szükséges lehet új felhasználót létrehozni egy adott virtuális gépen a jogosultsági szintek, munkafeladatok, vagy éppen csak az SSH elérés céljából. A következő parancsot érdemes kiadni egy felhasználó létrehozásához:

```
sudo useradd -s /bin/bash -m [felhasználónév]  
sudo passwd [felhasználónév]
```

Ezután bekéri a terminál az új felhasználó jelszavát.

Open VPN felállítása heat template használatával

A cloud oldalán Orchestration/Stacks menüpont

Launch Stack

Url kiválasztása: <https://raw.githubusercontent.com/burgosz/heat-templates/master/openvpn.heat>

Megjelenő ablak kitöltése:

- Stack Name: Tetszőleges név
- Password: A jelszava, amit első bejelentkezéskor megadott.
- Public IP: Ez lesz az OpenVPN szervered publikus IP-je. A projekthez allokált floating IP-t kell megadni (Compute/Access & Security/Floating IPs).

- Image: Ubuntu 16.04 LTS for Heat
- Flavor: A Small elég, de ha másra is akarja használni a gépet, értelemszerűen lehet nagyobb is.
- Keypair name: A saját SSH kulcsa.
- Private Network: A projekjéhez allokkált hálózat neve.
- vpn_cidr: Ide egy olyan subnetet kell adni ami nem ütközik a projekje belső hálózatával és célszerű arra is figyelni, hogy annak a kliens gép egyik hálózatával se ütközzön. (A default tipikusan jó).

A Launch gombra kattintva létrejön a virtuális gép, amin fut egy OpenVPN szerver. A stack nevére kattintva az Overview menüben lesz egy OpenVPN client config. Ezzel a konfigurációval tud csatlakozni. Valamint egy ca certificate, ennek a tartalmát be kell másolnod az openvpn config mappájába ca.crt néven. Ezzel a módszerrel felhasználók az cloudon használt felhasználónevével és jelszavukkal tudnak csatlakozni a VPN szerverre, de csak akkor, ha tagjai a projektnek.

Angol tutorial VPN szerver létrehozására: [Openvpn server tutorial](#). Ez a tutorial teljesen megfelelő az MTA Cloud-ra is.

[Hibák, illetve a projekttel kapcsolatos további igények bejelentése](#)

Az MTA Cloud szolgáltatással kapcsolatos kommunikáció és támogatás e-mail formájában történik. A közös e-mail cím: info@cloud.mta.hu. Az erre az e-mail címre bejelentett hibákból, igényekből egy bejelentési űrlap generálódik, melyet az MTA Cloud csapat kijelölt tagja kezel.