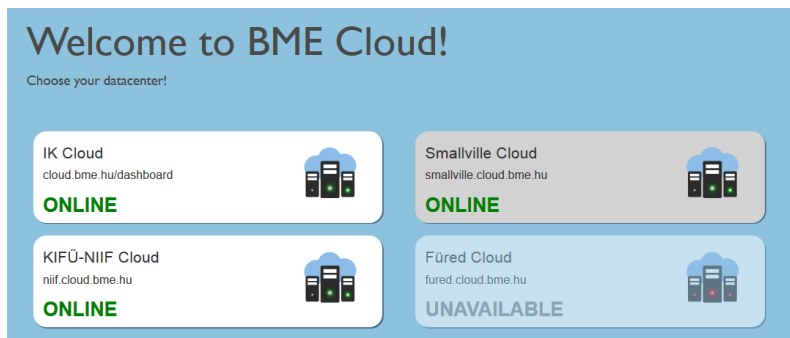


# VIK felhő

(felhasználói összefoglaló)

A VIK oktatói és hallgatói 2018. szeptemberétől virtuális számítógépes infrastruktúrát használhatnak oktatási feladataik ellátásához. A rendszer fizikailag a VIK által felújított egyetemi szuperszámítógépen fut. A szolgáltatást az IIT és az IK közös fejlesztéseként létrehozott CIRCLE felhőmenedzser biztosítja. A rendszer elérése a <https://cloud.bme.hu> választóoldalon keresztül történik. Innen jelenleg 3 adatközpont érhető el:



Az „IK Cloud” az IIT és az IK közös infrastruktúráján több éve üzemelő felhő. A „Smallville Cloud” az egyetemi szupergép (Superman) bővítésével létrehozott felhő. A „KIFÜ-NIIF Cloud” a KIFÜ-NIIF együttműködésben kialakított felhő. Ez utóbbi két erőforrást úgy méreteztük, hogy egyenként ~300 átlagos méretű (1-2 VCPU, 2-4GB RAM, 40GB diszk) virtuális gépet ki tudjanak szolgálni.

A rendszer alapvetően IaaS (Infrastructure as a Service) szolgáltatást valósít meg. Az általános jellegű felhasználói igények kiszolgálása érdekében alapbeállítású operációs rendszereket is felkínál, ezek azonban testre szabhatók majd sablonok formájában elmenthetők. Ezeket a sablonokat az oktató hallgatókhoz vagy hallgatói csoporthoz rendelheti, így azokat a hallgatók példányosíthatják.

A gépek alapesetben mind az egyetemi hálózatról, mind a publikus internetről elérhetőek távoli bejelentkezéssel. Mivel oktatási környezetünkben jelenleg az erőforrásokkal való takarékoskodásra a felhasználók nincsenek ösztönözve, így a rendszer a felhasználói aktivitástól és a géphez rendelt lejáratú időtől függően törli, vagy tartja meg az elindított gépeket.

E lejáratú idő valójában egy életciklust határoz meg. A „labor” életciklus pl. azt jelenti, hogy a gép az indítást követően két óra múlva alvó állapotba kerül. Ebből az állapotból egy héten belül bármikor felébredszthető, és újból 2 óráig üzemel. Egy hét elteltével a gép törlődik, ha az életciklusát nem újítják meg. A megújítások száma nem korlátozott, azaz egy aktív felhasználó ily módon a végtelenségig tudja használni a gépet. Másik tipikus életciklus az ún. „projekt” életciklus, ami egy hónapos folyamatos futást és hat hónapos törlési periódust definiál. Ezt tipikusan szakdolgozat készítéshez, diplomatervezéshez, önálló laborhoz ajánljuk.

Megfelelő jogosultságokkal a rendszerben összetett hálózati struktúra (pl. virtuális klaszter) is kialakítható. A jogosultságok ill. extra erőforrások igénylését űrlap segíti. Az igényeket az üzemeltetés kapja meg és hagyja jóvá, vagy utasítja el.

A rendszer használatával kapcsolatos kérdéseket, kéréseket a [cloud@ik.bme.hu](mailto:cloud@ik.bme.hu) címen fogadjuk.

# VIK felhő

(felhasználói útmutató)

V.1.2

## Tartalom

Bevezetés.....	2
Belépés a rendszerbe .....	2
Virtuális gépek kezelése .....	3
Virtuális gép elérése .....	3
Virtuális gép életciklusa.....	4
Erőforrások módosítása .....	5
Konzol hozzáférés.....	5
Hozzáférések (jogosultságok) szabályozása .....	5
Hálózatok kezelése .....	6
<i>Tevékenységek</i> ellenőrzése .....	7
<i>Sablonok, kialakításának főbb szempontjai</i> .....	7
Memória igény .....	7
vCPU igény.....	8
Diszk terület igény .....	8
Dedikált IP címek .....	8
Ütemezett fix idejű erőforrás allokáció.....	8

2018. szeptember

## Bevezetés

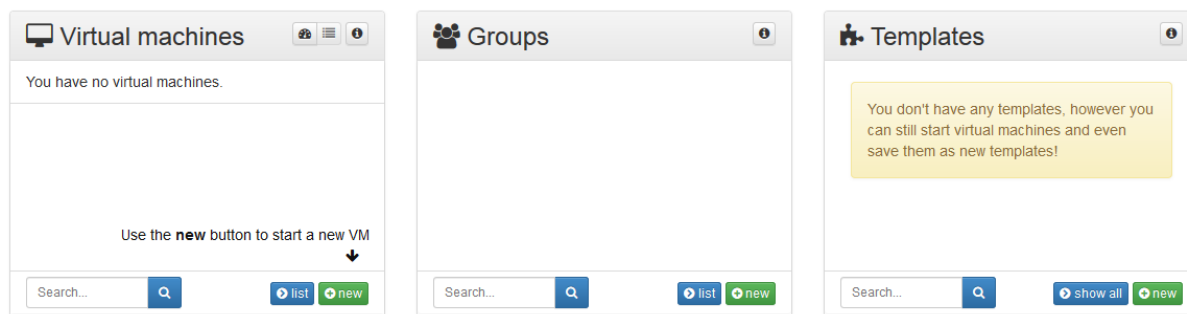
2018. szeptemberétől a VIK oktatói és hallgatói virtuális számítógépes infrastruktúrát használhatnak oktatási feladataik ellátásához. A műszaki megoldást az IIT és az IK közös fejlesztéseként létrehozott CIRCLE felhőmenedzser biztosítja, amely már az egyetemi szupergépen is elérhető. A gép 2012-ben a nagy számítási kapacitást igénylő kutatási feladatok ellátásához lett beszerezve, mint központi infrastruktúra (<https://supermna.eik.bme.hu>), melyet a VIK saját költségén memóriával és háttértárral bővített. A rendszer 30 teljesen azonos felépítésű számítási csomópontból álló gépben most összesen közel 3 TB RAM és 360 fizikai mag van. A háttértár kapacitása közel 160TB. Az eredeti funkciók megtartása mellett (nagy számításigényű kutatási feladatok futtatása), a gép szeptembertől felhő szolgáltatást is biztosít a VIK oktatói és kutatói részére.

A rendszer elérése a <https://cloud.bme.hu> választóoldalon keresztül történik, ahonnan jelenleg 3 adatközpont érhető el. Ezek közül a „Smallville Cloud” az egyetemi szupergép (Superman) bővítésével létrehozott felhő.

Alábbiakban röviden, példákkal illusztrálva összefoglaljuk a CIRCLE rendszer kezelői felületének legfontosabb elemeit. A gyakorlati használatot angol/magyar nyelven elérhető help (<https://smallville.cloud.bme.hu/info/help>) és a felületen megjelenő tooltip ablakok segítik. (A kezdőképernyők nyelve bejelentkezésig a böngésző beállításától, bejelentkezés után az adott felhasználó által megadott preferenciától függ. A továbbiakban az angol nyelven megjelenő felületet mutatjuk be, zárójelben megadva a magyar nyelvű felületen megjelenített szöveget is.)

## Belépés a rendszerbe

A megfelelő adatközpontba (pl: smallville) az egyetemi címtáras azonosítóval lehet belépni a *login with SSO (SSO bejelentkezés)* felíratra kattintva. Sikeres azonosítás után oktatói státusszal rendelkezők három ablakba rendezve látnak információkat (az elrendezés a képfelbontástól függ):



A **Virtual machines** (Virtuális gépek) ablakban a felhasználó a saját virtuális gépeit láthatja, ill. a *new* (új) gombbal itt lehet létrehozni új gépet az elérhető sablonokból. Alapesetben az oktatók csak néhány alapgép (linux+windows változatok) sablonjait látják, a hallgatók pedig csak az oktatók által engedélyezett sablonokat. (Lehetőség van ISO lemezkép feltöltésére is, de ehhez extra jogosultságra és a rendszer mélyebb ismeretére van szükség).

A **Groups** (Csoportok) ablakban az oktató által létrehozott csoportok láthatók. Egy csoporthoz kétféle módon lehet felhasználókat rendelni:

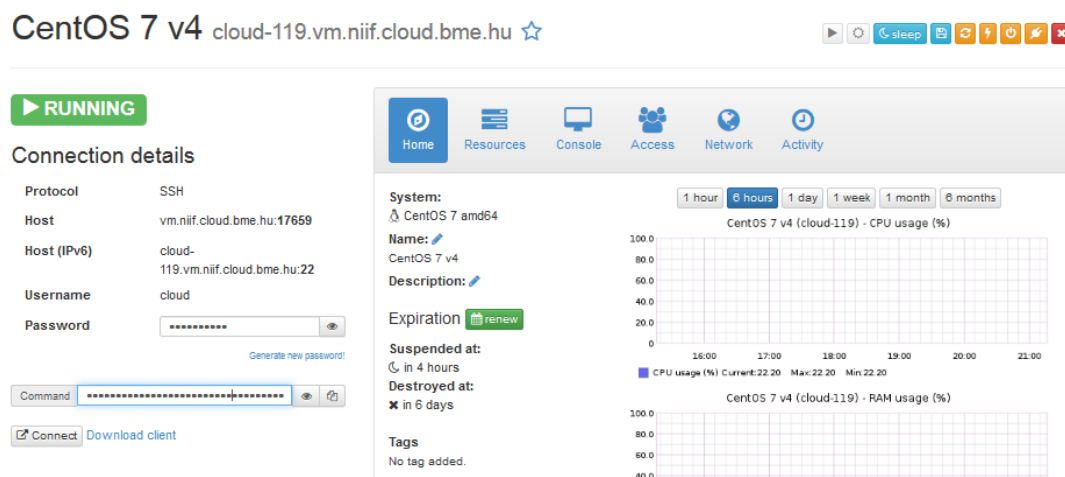
- Neptun kódok vagy eduID azonosítók felsorolásával,
- kurzusazonosítóval (pl. BMEV8IAA03).

Ez utóbbi esetben a kurzust felvevő összes hallgató a csoport tagja lesz. (Sajnos a címtárban még szeptember 7-én sem voltak elérhetőek az őszi kurzusok...)

A **Tempates** (Sablonok) ablakban az oktató által létrehozott sablonok láthatók és kezelhetők. A sablonok kezelésével kapcsolatban a legfontosabb tevékenység a jogosultságok megadása. Három jogosultsági szint létezik (Owner/Tulajdonos, Operator/Operátor, User/Felhasználó), melyek jelentése részletesen olvasható a hozzárendelést lehetővé tevő oldalon.

## Virtuális gépek kezelése

Sikeres gépindítás után, illetve egy már létező gépet kiválasztva a *Virtual machines* (Virtuális gépek) ablakból, az alábbihoz hasonló képernyőképet kapunk:



Ezen az oldalon az adott gép legfontosabb tulajdonságai, valamint a hozzáférés paraméterei láthatók összefoglalva. A *Resources* (Erőforrások), *Console* (Konzol), *Access* (Hozzáférés), *Network* (Hálózat) és *Activity* (Tevékenységek) füleken pedig további részletek jelennek meg, ill. ezekben adhatók meg a gép különféle speciális paraméterei.

A gép működése a felső sorban megjelenő nyomógombok segítségével vezérelhető. Balról jobbra



haladva a következő műveletek hajthatók végre: indítás, ébresztés, mentés, altatás, újraindítás, alaphelyzetbe állítás (reset), leállítás, kikapcsolás és törlés. Az újraindítás, reset, leállítás, kikapcsolás műveletek alapvetően a parancs végrehajtásának módjában térnek el egymástól. Az újraindítás gomb egy Ctrl-Alt-Del kombinációval, a reset gomb a tápellátás ki- és bekapcsolásával, a leállítás pedig egy normál leállítással egyenértékű. A kikapcsolás a tápellátás megszüntetésének felel meg.

## Virtuális gép elérése

A *Console* (Konzol) fül a gép virtuális monitorjának elérésére szolgál, de ez biztonsági okokból csak az oktatók számára engedélyezett. A gépek preferált elérési módja valamilyen hálózati protokoll, ami az alkalmazott operációs rendszertől függ. Tipikusan SSH vagy RDP.

Az alapsablonokból példányosított gépek egyetlen hálózati interfésszel rendelkeznek, ami belső hálózathoz kapcsolódik. A publikus internet felől a gépben futó hálózati szolgáltatások ún. NAT (Network Address Translation) segítségével érhetők el. Az adott operációs rendszerre jellemző, távoli

elérést biztosító protokollok (ssh, rdp) szokásos portjait a rendszer a gép indításakor automatikusan átfordítja egy külső portra.

Ennek részletei láthatók a *Coonection deatils (Kapcsolat részletei)* címsor alatt. A bemutatott példában az elérési protokoll SSH, amihez tartozó szolgáltatás a belső hálózaton a szokásos 22-es porton érhető el. A szűk IPv4-es címtartomány miatt minden virtuális gép kívülről azonos IPv4-es címen érhető el (vm.smallville.cloud.bme.hu, ill. vm.niif.cloud.bme.hu), így nem csak a címet kell változtatni, hanem a portot is. Esetünkben tehát a gép kívülről IPv4 protokoll felett a 17659-es porton, míg IPv6 protokoll felett a szokásos 22-es porton érhető el.

**Connection details**

Protocol	SSH
Host	vm.niif.cloud.bme.hu:17659
Host (IPv6)	cloud-119.vm.niif.cloud.bme.hu:22
Username	cloud
Password	<input type="password"/> <span>Generate new password!</span>
Command	<input type="text"/> <span>Connect</span> <span>Download client</span>

Minden gépen automatikusan keletkezik egy cloud nevű felhasználó, akinek a generált jelszava szintén a *Coonection deatils (Kapcsolat részletei)* címsor alatt látható. Itt látható egy komplett parancssor is (Command/Parancs), amit Unix/Linux parancssorként végrehajtva a gépbe azonnal be tudunk lépni.

Windows alapú helyi gépet használva a távoli virtuális gép RDP protokollal a távoli asztal alkalmazással, SSH protokollal pedig valamilyen ssh klienssel (pl. putty) érhető el. Gyakori használat esetén célszerű egy egyszerű kliens programot is installálni a Windows rendszerű helyi gépre (*Download client/Kliens letöltése* linkre kattintva). A telepítés után a távoli géphez való kapcsolódás a *Connect (Csatlakozás)* gombra történő kattintással azonnal megtörténik. (Lelopja a megfelelő jelszót a képernyőről és megfelelő paraméterekkel elindítja az elérési protokollnak megfelelő programot (távoli asztal vagy putty).

## Virtuális gép életciklusa

Fontos jellemzője egy gépnek a lejárata, ami valójában egy életciklust határoz meg. Oktatási környezetünkben jelenleg az erőforrásokkal való takarékoskodásra a felhasználót nem ösztönzi anyagi érdek, így a rendszer a felhasználói aktivitástól függően törli, vagy tartja meg az elindított gépeket.

Minden elindított géphez két lejárati időpont rendelődik automatikusan: *Suspension (Felfüggesztési)* és *Destroy (Megsemmisítési)* időpont, amelyek time-out jelleggel kerülnek megadásra. Az előbbi elteltével a gép automatikusan alvó állapotba kerül, az utóbbi lejáratakor pedig törlődik. Mindkét time-out tetszőleges alkalommal újraindítható a *renew (megújítás)*

gomb megnyomásával. Az időpontok lejárataáról figyelmeztető üzenetek kerülnek kiküldésre mind on-line módon, mind e-mailben. Maga az életciklus a gép sablonjából öröklődik, azaz a sablonhoz rendelt beállítás jut érvényre a példányosításkor, ami később megfelelő jogosultságokkal felülbíráható. Szükség esetén lejárati idők változtatása külön űrlapon kérhető az üzemeltetéstől. A kérést az üzemeltetés mérlegeli. Szükség esetén felveszi a hallgató konzulensével a kapcsolatot. Jelenleg négy előre definiált életciklust alkalmazunk:

- Rövid labor (2 óra, 1 hét)

**Expiration** 

**Suspended at:**  
🕒 in 4 hours

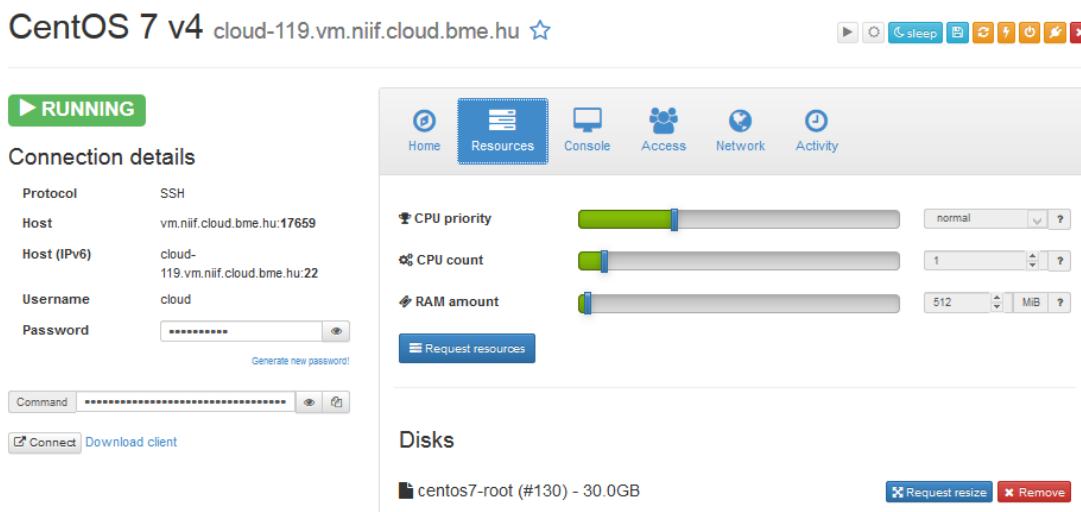
**Destroyed at:**  
✖ in 6 days

- Hosszú labor (5 óra 1 hét)
- Projekt (1 hónap, 1 év)
- Szerver (1 év, 10 év)

Ahol az első idő az altatási, a második a törlési time-out.

## Erőforrások módosítása

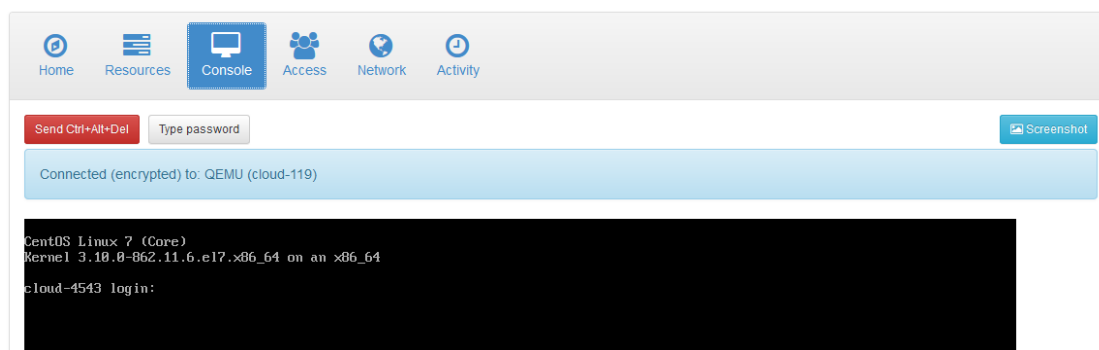
Előfordulhat, hogy egy adott géphez rendelt erőforrások nem elegendőek egy adott feladathoz. Az erőforrások módosítására a *Resources (Erőforrások)* fülön van lehetőség:



A módosításhoz természetesen jogosultságra van szükség. Jogosultság hiányában az életciklus változtatáshoz hasonló módon igény jelezhető az üzemeltetés felé.

## Konzol hozzáférés

A *Console (Konzol)* fül a gép virtuális monitorjának elérésére szolgál, ami biztonsági okokból csak az oktatók számára engedélyezett. Azoknak, akiknek a konzol hozzáférés nem lehetséges, azok képernyőképeket készíthetnek a *Snapshot (Képernyőkép)* gomb segítségével.



## Hozzáférések (jogosultságok) szabályozása

Az *Access (Hozzáférés)* fülön a virtuális gép menedzseri funkcióinak másokkal történő megosztása, illetve a tulajdon átruházása válik lehetővé. Három jogosultsági szint létezik (Owner/Tulajdonos, Operator/Operátor, User/Felhasználó):

**Owner (Tulajdonos)** számára minden művelet megengedett.

**Operator (Operátor)** felhasználókat adhat/törölhet és egyszerűbb attribútumokat változtathat (név, port stb.).

**User (Felhasználó)** láthatja a gép paramétereinek részleteit (pl. jelszó).

The screenshot displays the VIK cloud management interface. On the left, the 'Connection details' panel shows the VM status as 'RUNNING'. It lists the Protocol (SSH), Host (vm.niif.cloud.bme.hu:17659), Host (IPv6) (cloud-119.vm.niif.cloud.bme.hu:22), Username (cloud), and Password (masked). There is a 'Generate new password!' link and a 'Connect (download client)' button. The main panel shows the 'Owner' section with the current owner 'Imre Szeberényi (B6AFNQ)' and a 'Transfer ownership...' link. Below this is the 'Permissions' section, which includes a table with columns 'Who' and 'What'. The table lists 'Imre Szeberényi (B6AFNQ)' as the owner and 'user' as the permission level. There is a 'Save' button and a detailed explanation of the permissions for User, Operator, and Owner levels.

## Hálózatok kezelése

Az alapsablonokból példányosított gépek egy hálózati interfésszel rendelkeznek, ami belső hálózathoz (VM-NET) kapcsolódik. A „Network” fülön újabb interfészek és tűzfalszabályok adhatók a géphez.

The screenshot displays the VIK cloud management interface for a CentOS 7 v4 virtual machine. The top bar shows the VM name 'CentOS 7 v4' and its host 'cloud-119.vm.niif.cloud.bme.hu'. The left panel shows the 'Connection details' with the same information as the previous screenshot. The main panel shows the 'Network' tab, which displays the 'Interfaces' section. It lists the 'VM-NET' interface with its IP addresses (IPv4: 10.34.0.97, IPv6: 2001:738:0:531:734:0:97:0) and DNS name (cloud-119.vm.niif.cloud.bme.hu). There is a 'remove' button next to the VM-NET interface. The 'Port access' section shows the VM's IP address and a '22/tcp' port rule. There is an 'add interface' button and a 'Download client' button.

Az egyes interfészek különböző virtuális hálózathoz köthetők, mely művelet elvégzéséhez az adott virtuális hálózathoz hozzáférési engedély kell. Jelenleg normál felhasználó saját VLAN-t nem tud létrehozni, de a rendszer következő verziójában erre is lesz lehetőség.

Szintén a *Network (Hálózat)* fülön megjelenő felületen keresztül lehet kezelni az úgynevezett menedzselt hálózati interfészek tűzfalszabályait. Egy web szerver installálásakor pl. ki kell nyitni a virtuális gép 80-as és a 443-as portját. NAT-olt hálózat esetén a megadott portokhoz a rendszer kívülről elérhető portokat is rendel. Fontos azonban megjegyezni, hogy amennyiben virtuális gépben futó rendszer is futtat tűzfalat, úgy annak kezelését (port nyitás) az operációs rendszerben adott eszközzel (pl. ufw) kell elvégezni. A képen látható példában a 80-as port a 9108-on, a 443-as port pedig a 13260-as porton érhető el a vm.niif.bme.hu címen. IPv6-os protokollal csak portnyitás történik, mivel ilyenkor NAT-ra nincs szükség.

Port access

IPv4 IPv6

vm.niif.cloud.bme.hu:17659	→	22/tcp	x
vm.niif.cloud.bme.hu:9108	→	80/tcp	x
vm.niif.cloud.bme.hu:13260	→	443/tcp	x

+ → / tcp Add

## Tevékenységek ellenőrzése

Az *Activiy (Tevékenységek)* a fülön ellenőrizhető a gép története illetve géppel menedzseri szempontból végrehajtott műveletek státusza.

**SUSPENDED**

Connection details

Protocol: SSH

Host: vm.niif.cloud.bme.hu:17659

Host (IPv6): cloud-119.vm.niif.cloud.bme.hu:22

Username: cloud

Password:

Generate new password!

Command:

Connect (download client)

Activity

- Sleep** just now, admin (username: admin)
  - Suspend virtual machine – just now
  - Shutdown network – just now
- (2x) Console access**, admin (username: admin)
- Open tcp/443 on cloud-119** 3 hours ago, admin (username: admin)
- Open tcp/80 on cloud-119** 3 hours ago, admin (username: admin)
- Remove unmanaged - cluster interface** 3 hours ago, admin (username: admin)
  - Detach network – 3 hours ago
- Add unmanaged - cluster interface** 3 hours ago, admin (username: admin)
  - Restart networking – 3 hours ago
  - Change ip – 3 hours ago
  - Attach network – 3 hours ago
- Remove managed - PUB interface** 3 hours ago, admin (username: admin)
  - Detach network – 3 hours ago
- Add managed - PUB interface** 4 hours ago, admin (username: admin)
  - Detach networking – 4 hours ago

## Sablonok, kialakításának főbb szempontjai

A különböző oktatási feladatok igen eltérő erőforrás-igényeket támaszthatnak. Az alábbiakban összefoglaljuk a hallgatói használatra szánt sablonokkal kapcsolatos főbb megfontolásokat, tervezési lépéseket.

### Memória igény

Az erőforrások szempontjából szinte a legkritikusabb kérdés, ezért különösen fontos, hogy a lehető legtakarékosabban foglaljunk memóriát, kiváltképp olyan esetben, ha prognosztizálható, hogy sok példányban fog futni a gép. Az egyidejűleg futó példányok számát egy jól megválasztott lejárat idő segít korlátozni. Ha pl. egy 2 órás labortárgy kurzusai egymás után vannak az órarendben, célszerű 2 órára beállítani a futási időt (rövid labor). Így a rákövetkező kurzus indulásakor már többnyire alvó állapotba kerülnek a megelőző kurzus gépei.



Azt is érdemes mérlegelni, hogy az MS Windows rendszerek jóval több erőforrást igényelnek, mint a LINUX rendszerek.

### vCPU igény

Értékét a feladattól függően érdemes megválasztani. Néhány ( $\leq 4$ ) vCPU igénylése indokolt lehet, de csak akkor érdemes 1-nél többet igényelni, ha az adott rendszer valóban ki tudja azt használni.

### Diszk terület igény

Alapvetően gépenként 20-50GB igényre számítunk. A jelenleg használt tárhely kapacitása 16TB. Ez a méret a copy-on-write tárolási technika miatt jelentősen túlfoglalható. Tudni kell azonban, hogy a sablonok a tényleges méretet foglalják. Jelenleg a sablonokra nincs életciklus modell, ezért a sablonok készítésére jogosult felhasználóktól azt kérjük, hogy feleslegesen ne tároljanak sablonokat.

### Diszk I/O és hálózati igény

A diszk I/O-t alapvetően a fizikai gép adottságai korlátozzák. A Smallville gépben egy átlagosnál kicsit jobb teljesítményű diszk alrendszer van. SSD jelenleg nincs. Értelemszerűen a virtuális gépek I/O igénye a diszk alrendszer felé nagyjából összegződik. Tapasztalatunk az, hogy a Windows rendszerek, különösen a Windows 10 induláskor erőteljesen használja a diszket. Ezért célszerű a sablon beállításánál fontolóra venni az I/O igényes szervizek kikapcsolását, a szükségtelen alkalmazások leállítását (pl. Windows Update, indexelés, vírus ellenőrzés, Delivery Optimization).

Hálózati forgalom tekintetében is érdemes a sablonok, illetve alkalmazások igényét felülvizsgálni. E téren azonban eddig nem ütköztünk jelentősebb korlátokba.

### Dedikált IP címek

Indokolt esetben lehetőség van dedikált külső IPv4 címek igénylésére pl. valamilyen publikus szolgáltatás (web szerver) kialakításához. IPv4-es címből azonban alig több, mint 100 cím áll rendelkezésünkre.

### Ütemezett fix idejű erőforrás allokáció

Jelenleg a rendszer nem támogatja, hogy előre megadott időre garantált mennyiségű szabad erőforrás automatikusan lefoglalható legyen. Indokolt esetben (pl. vizsga idejére), ezt jelenleg csak kézi módszerekkel tudjuk biztosítani.