******

A Kormányzati adatközponti felhőbe illesztés műszaki követelményei

Verzió 7.1  
2017. június 23.

Tartalomjegyzék

[1 Bevezetés 4](#_Toc483294593)

[2 Új kormányzati Felhő (KAK Felhő) 4](#_Toc483294594)

[2.1 KAK Felhő architektúra alapsémája 4](#_Toc483294595)

[2.2 A KAK Felhő környezet üzemeltetésének logikai architektúrája 5](#_Toc483294596)

[2.3 Alapvető irányelvek 6](#_Toc483294597)

[2.3.1 Biztonsági alapelvek 6](#_Toc483294598)

[2.3.2 Támogatott alkalmazói rendszer kialakítási modellek 9](#_Toc483294599)

[2.3.3 Adatközpontok működési módja 12](#_Toc483294600)

[3 KAK Felhő szolgáltatások 13](#_Toc483294601)

[3.1 IaaS szintű ellátási szolgáltatások 13](#_Toc483294602)

[3.1.1 Virtuális szerver szolgáltatás 13](#_Toc483294603)

[3.1.2 Virtuális adatközpont szolgáltatás 14](#_Toc483294604)

[3.1.3 Docker konténer futtatása 14](#_Toc483294605)

[3.2 DBaaS szintű szolgáltatások 15](#_Toc483294606)

[3.3 PaaS szintű ellátási szolgáltatások 15](#_Toc483294607)

[3.3.1 Alkalmazás kiszolgáló szolgáltatás 15](#_Toc483294608)

[3.4 SaaS szintű ellátási szolgáltatások 16](#_Toc483294609)

[3.4.1 Levelezés, csoportmunka szolgáltatás 16](#_Toc483294610)

[3.4.2 Dokumentumkezelő (ECM és BPM) szolgáltatás 17](#_Toc483294611)

[3.4.3 Tartalomkezelő (CMS) szolgáltatás 17](#_Toc483294612)

[3.4.4 E-Learning szolgáltatás 17](#_Toc483294613)

[3.5 Kiegészítő szolgáltatások 18](#_Toc483294614)

[3.5.1 Több privát IP cím 18](#_Toc483294615)

[3.5.2 Fix publikus IP cím 18](#_Toc483294616)

[3.5.3 Tárhely szolgáltatás (IaaS (block device) alapú kiegészítő szolgáltatás) 18](#_Toc483294617)

[3.5.4 Objektumtár szolgáltatás (IaaS alapú kiegészítő szolgáltatás) 18](#_Toc483294618)

[3.5.5 Fájlkiszolgáló (NAS) (IaaS alapú kiegészítő szolgáltatás) 19](#_Toc483294619)

[3.5.6 Terheléselosztás 19](#_Toc483294620)

[3.5.7 SSL terminálás, kliens oldali certificate kezelés 20](#_Toc483294621)

[3.5.8 Naplózási szolgáltatás 20](#_Toc483294622)

[3.5.9 Teljesítmény- és állapotfigyelés szolgáltatás 21](#_Toc483294623)

[3.5.10 Webalkalmazás-tűzfal (WAF) 21](#_Toc483294624)

[3.5.11 Mentés szolgáltatás 22](#_Toc483294625)

[3.5.12 Archiválás szolgáltatás 23](#_Toc483294626)

[3.5.13 Adatbázis kiszolgáló szolgáltatás (DBaaS) 24](#_Toc483294627)

[3.5.14 Adatközponti alap szoftver infrastruktúra szolgáltatások 31](#_Toc483294628)

[3.6 Üzleti szolgáltatásonként a hozzájuk rendelhető kiegészítő szolgáltatások táblázata 32](#_Toc483294629)

[4 Architekturális illeszkedés követelményei 34](#_Toc483294630)

[5 Szakrendszer fejlesztőjének feladata és felelősségei 35](#_Toc483294631)

[5.1 Biztonsági besorolás meghatározása 35](#_Toc483294632)

[5.2 Vírusvédelem 35](#_Toc483294633)

[5.3 Közreműködés az infrastruktúra tervezésében, adatszolgáltatás 35](#_Toc483294634)

[5.4 EWS csatlakozás 36](#_Toc483294635)

[6 A KAK Felhő bővítése 36](#_Toc483294636)

[6.1 WAN 37](#_Toc483294637)

[6.2 LAN 38](#_Toc483294638)

[6.3 Menedzsment hálózat 38](#_Toc483294639)

[6.4 SAN 39](#_Toc483294640)

[6.5 Tároló kapacitás 39](#_Toc483294641)

[6.5.1 SAN alapú tároló kapacitás 39](#_Toc483294642)

[6.5.2 OpenStack tároló kapacitás 39](#_Toc483294643)

[6.6 Számítási kapacitás 41](#_Toc483294644)

[6.7 Adatbázis farmok bővítése DBaaS szolgáltatás esetén 42](#_Toc483294645)

[6.7.1 Microsoft SQL 42](#_Toc483294646)

[6.7.2 Oracle 44](#_Toc483294647)

[6.8 Szükséges licencek 44](#_Toc483294648)

[6.8.1 Felhő automatizálási rendszer licencek 44](#_Toc483294649)

[6.8.2 Virtuális gépek licencei 44](#_Toc483294650)

[6.8.3 Támogató rendszerek licencei 44](#_Toc483294651)

[7 Kormányzati hosting szolgáltatás 45](#_Toc483294652)

[7.1 Szolgáltatás általános ismertetés 45](#_Toc483294653)

[7.2 Fizikai biztonsági környezet jellemzői 45](#_Toc483294654)

[7.3 Szolgáltatások megvalósításának műszaki feltételei 45](#_Toc483294655)

[7.4 Géptermi környezet 46](#_Toc483294656)

[7.4.1 Eszközök elhelyezése 46](#_Toc483294657)

[7.4.2 PDU-k csatlakozása 46](#_Toc483294658)

[7.4.3 Redundáns elektromos energia ellátás 46](#_Toc483294659)

[7.4.4 Klimatizálás 47](#_Toc483294660)

# Bevezetés

Jelen dokumentum tájékoztatást ad az új Kormányzati adatközponti felhő (továbbiakban KAK Felhő) nyújtotta szolgáltatásokról, a KAK Felhőhöz bővítéssel történő illeszkedésről, valamint útmutatót ad a felhő alapú környezetben futtatandó rendszerekkel szembeni elvárások érvényesítéséhez. A dokumentum ezáltal meghatározza azokat a figyelembe vehető közös komponenseket, amelyek használatára szükség van az egyes szakrendszeri fejlesztések esetén, valamint feladatokat állapít meg a beköltözni kívánó szakrendszerek fejlesztői számára. A dokumentum kitér a Kormányzati hosting szolgáltatásra is, mely a Kormányzati Felhő szolgáltatás melletti lehetőség a Kormányzati Adatközpont lehetőségeinek kiaknázására.

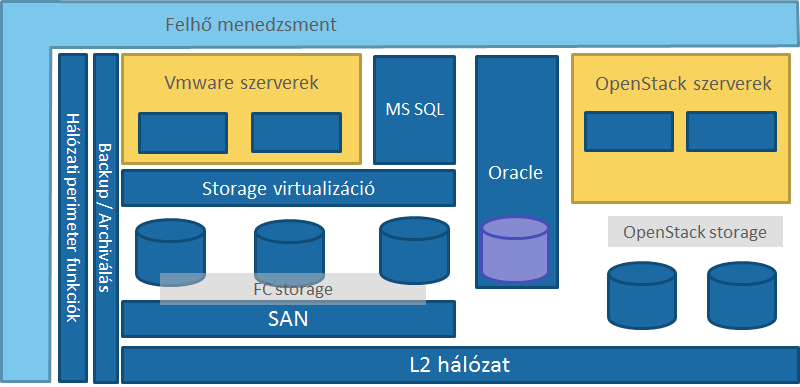
Kormányzati Adatközpontnak (KAK) nevezzük a két új telephelyen létrejövő géptermeket. A géptermek feladata a KAK Felhő befogadása, valamint a felhőbe nem integrálható rendszerek számára hosting-szerű elhelyezés biztosítása. A továbbiakban a két környezet követelményeit tárgyaljuk

# Új kormányzati Felhő (KAK Felhő)

A jövőben fejlesztendő rendszerek futtató környezete az új kormányzati adatközponti felhő, a KAK Felhő. A KAK Felhő egy privát informatikai felhő, mely IaaS, PaaS, SaaS szolgáltatásokat nyújt. A kialakítandó rendszereknek integrálhatóaknak kell lenniük a KAK Felhő által nyújtott szolgáltatásokkal.

## KAK Felhő architektúra alapsémája

A KAK Felhő két telephelyen kerül felépítésre. Egy-egy telephelyen a következő architektúra kerül kialakításra:



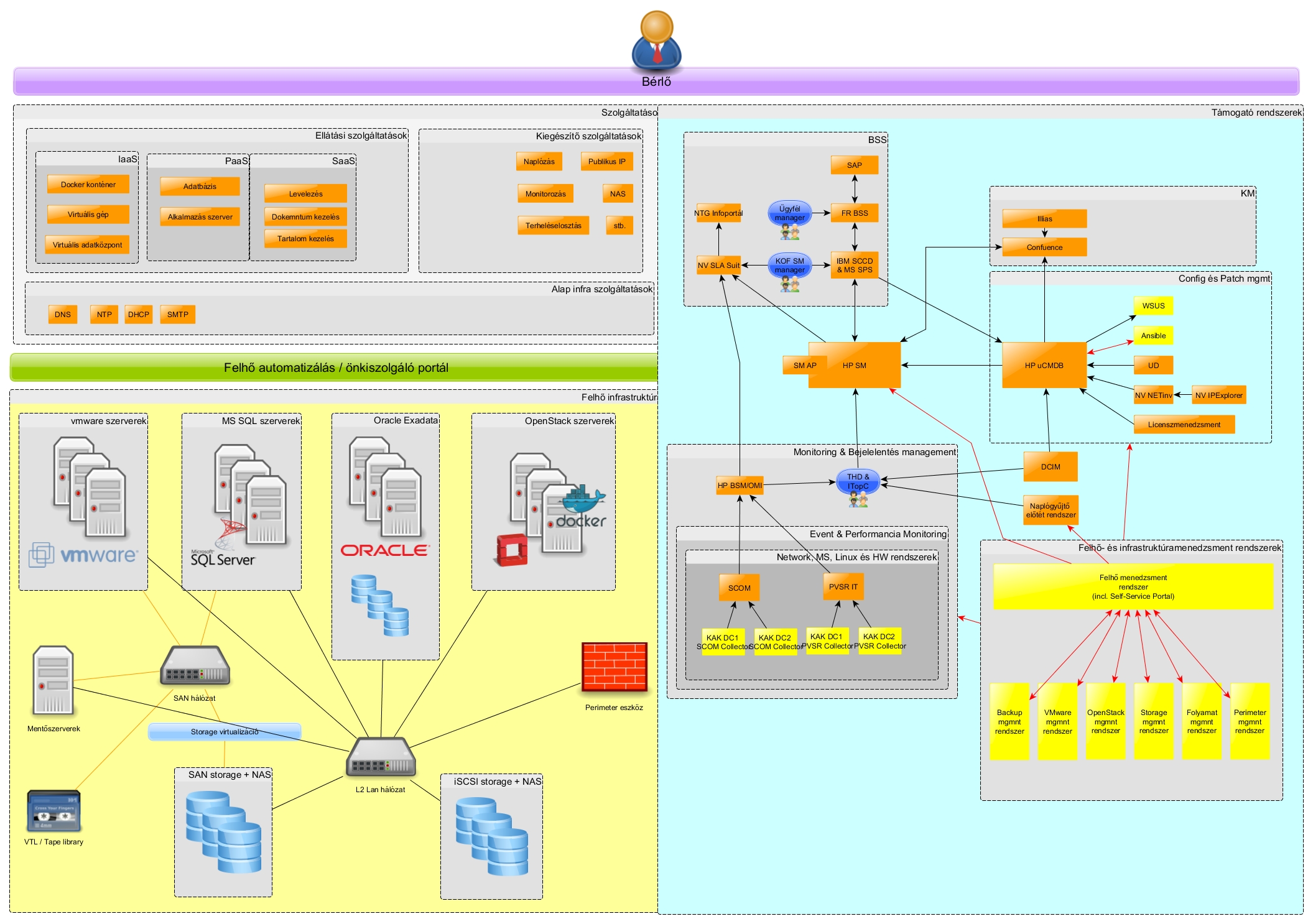
1. ábra KAK Felhő architektúra alapsémája

Az architektúra kialakításánál figyelembe vett alapvetések:

* A KAK Felhő VMware és OpenStack alapú számítási kapacitást tartalmaz.
* A VMware alapú szerverek 16 GBites FC SAN hálózaton keresztül kapcsolódnak a tároló rendszerekhez. A tárolók és a szerverek közé terveztünk egy storage virtualizációs megoldást a későbbi bővítésként bejövő tárolók egyszerű integrálhatósága érdekében. Ennek a pontost használatáról és konfigurációjáról a beszerzett megoldás pontos típusának ismeretében fogunk dönteni.
* Az OpenStack alapú rendszerek Ethernet hálózaton, iSCSI-n érik el a tárolót. Az itt tervezett tároló rendelkezik az OpenStack-ben megkövetelt Cinder driverrel.
* Mind a két tároló rendelkezik natív NAS funkcionalitással.
* A tervezett SAN hálózat a VMware alatti tárolót (vagy tárolókat), a VMware szervereket, valamint a mentéshez használt mentőszervereket, VTL-eket és Tape Library eszközöket köti össze klasszikus, telephelyenként két fabricos felépítésben. A Fabric-ban minden berendezés két külön adatúton érhető el amelyeknek – a legelejét és a legvégét kivéve – nincs közös pontja.
* A különböző elemeket elsősorban a Felhő menedzsment konfigurálja: ez hozza létre a virtuális gépeket, VLAN-okat, perimeter szabályokat, konfigurálja a mentést, stb.
* Microsoft SQL és Oracle DBaaS szolgáltatásokat a felhő nem virtualizáltan, hanem fizikai hardveren biztosítja.

## A KAK Felhő környezet üzemeltetésének logikai architektúrája

A KAK Felhő infrastruktúra és szolgáltatásai az alábbi logikai architektúra szerint lesznek kialakítva:



2. ábra KAK Felhő környezet logikai architektúrája

Az architektúra kialakításánál figyelembe vett alapvetések:

* Az ábra „Felhő infrastruktúra” tömbje tartalmazza a kialakítandó infrastruktúra szolgáltatásokat:
  + „VMware szerverek” és „Openstack szerverek” jelzik a virtualizált erőforrások fizikai hátterét biztosító elemeket
  + Az infrastruktúra menedzsment biztosítja a kapcsolódó fizikai és logikai erőforrások menedzsment funkcióit.
* „Szolgáltatások” blokk jelöli azon bérlők számára kiajánlható ellátási szolgáltatásokat, amelyek a „Felhő automatizálás, Önkiszolgáló portál” által a „Fizikai infrastruktúra” infrastruktúra szolgáltatásaira épülve hozhatóak létre.
* „Felhő automatizálás” jelenti azt a réteget, amelyen keresztül a bérlők számára kiajánlott szolgáltatások létesítése, konfigurációja és a virtuális erőforrások hozzárendelése történik a bérlő szolgáltatás-példányaihoz
  + A szolgáltatás-példányokhoz tartozó virtualizált erőforrások létesítését és konfigurációját az „Felhő infrastruktúra” rétegen keresztül valósítja meg, de a szolgáltatások működése során a „Felhő automatizálás” réteg nem vesz részt a közvetlen kiszolgálásban.
  + Az alkalmazott erőforrások, illetve szolgáltatás példányok konfigurációja során létrejött rendszer-elemeket és kapcsolatokat (példányosításokat) CMDB-ben tároljuk.
  + „Alap infra. szolgáltatások” jelentik azokat az alap szintű szolgáltatásokat, amelyek az adott infrastruktúra, ill. a kiajánlott szolgáltatások működéséhez elengedhetetlenek
    - a különválasztás azt mutatja, hogy az alap infrastruktúra és bérlő számára nyújtott szolgáltatások kapcsán eltérő, és elkülönített módon kell biztosítani a megfelelő támogatást.
* „Bérlő” jelzi az ellátott szervezet összes különféle jellegű szolgáltatáshoz történő kapcsolódását (egyúttal jelzi az összes üzleti, adminisztrátor, felhasználó és eszköz szintű kapcsolódást).
* „Támogató rendszerek” foglalja össze a felhőn kívül a NISZ-nél rendelkezésre álló támogató rendszereket, amelyhez integrációt biztosítani kell (a doboz kifejtése a rendszerfelügyelet és szolgáltatás támogatás alfejezetekben elérhető).

## Alapvető irányelvek

A KAK Felhő fentiekben vázolt architekturális sémájához kapcsolódóan a szolgáltatási modell szervezési irányelvei, törvényi előírások, a szolgáltató és a felettes szerv (BM) működtetést érintő döntései határozzák meg a megoldások kialakítását. Az alfejezet említett irányelveket gyűjti össze, valamint az általános követelmények kiegészítésével lefekteti a KAK Felhő helyi megoldásaival kapcsolatban érvényesítendő biztonsági elvárásokat, ajánlásokat is.

Az alábbiakban összefoglaljuk azok az alapelveket, amelyek a szolgáltatások kialakítását és üzemeltetését szabályozzák.

### Biztonsági alapelvek

A KAK, valamint a felhő alapú működési környezet kialakításához kapcsolódóan „Az állami és önkormányzati szervek elektronikus információbiztonságáról” szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és a 41/2015. (VII. 15.) BM végrehajtási rendeletének (a továbbiakban: Vhr.) figyelembe vétele szükséges, továbbá a 187/2015 (VII.13) Kormányrendelet, mely 2. §-a alapján a Kormány Nemzeti Elektronikus Információbiztonsági Hatóságként (a továbbiakban: hatóság) a Nemzetbiztonsági Szakszolgálatot jelölte ki, illetve a rendelet 6. § (1) c) pontja értelmében a hatóság ellenőrzi az információtechnológiai fejlesztési projektekben az információbiztonsági követelmények teljesülését. A Nemzeti Elektronikus Információbiztonsági Hatóság feladatait 2015. október 1-től a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI) látja el.

A KÖFOP projektek végrehajtása során a projektgazda köteles az NKI-val együttműködni. Az NKI a KÖFOP fejlesztések teljes életciklusát nyomon követi, a tervezés kezdetétől a végrehajtási/megvalósítási szakaszon át egészen a létrehozott megoldás üzembe állításáig. A projektgazda a projekttel összefüggő adatszolgáltatási kötelezettségét az NKI által kiadott hatósági segédlet használatával köteles teljesíteni.

A projektgazda a projekt tervezett biztonsági intézkedéseit magában foglaló megvalósíthatósági tanulmányt, valamint a kitöltött hatósági segédletet megküldi az NKI-nak. A részletes megvalósíthatósági tanulmányban foglalt fejlesztések információbiztonsági követelményeknek történő megfeleléséről az NKI hatósági állásfoglalást bocsát ki, melynek részeként – a projekt ütemezéséhez illeszkedően – meghatározza, hogy a biztonsági intézkedések kialakításával összefüggő dokumentációkat véleményezés céljából az NKI részére milyen határidővel szükséges megküldeni. A projektgazdának az NKI észrevételeit, kifogásait a dokumentációkban alkalmaznia kell, illetve a fejlesztés során kötelezően meg kell valósítani.

Az Ibtv. és a végrehajtásához kapcsolódó előírások jelenleg nem tartalmaznak egyértelmű elvárásokat a felhő megoldásokra, mivel azokban konkrét Elektronikus Információs Rendszerek (a továbbiakban: EIR) számára megfogalmazott követelmények állnak rendelkezésre. A KAK Felhőt kialakításából fakadóan kettős szerepében kell vizsgálni:

* egyrészt a kialakításra kerülő infrastruktúra, mint általános, tetszőleges EIR számára biztosított infrastruktúra szerint;
* másrészt a kialakításra kerülő magas-szintű (SaaS) szolgáltatások miatt, szolgáltatásonként definiált EIR-ként.

Mivel előzetesen nem azonosítható és biztonsági szempontból nem minősíthető a KAK Felhő által kezelendő adatok köre, továbbá az alkalmazási szintű eljárások (a SaaS szolgáltatásokat kivéve) egyértelműen a bérlők (adatgazdák) hatáskörébe esnek, így a felhő nem is minősülhet, nem tekinthető önálló EIR-nek.

A KAK Felhőnek alkalmasnak kell lennie a Vhr.-ben meghatározott (bizalmasság, sértetlenség, rendelkezésre állás szempontjából is) 5-ös biztonsági osztályba sorolt elektronikus információs rendszerek kiszolgálására. Ez nem azt jelenti, hogy ne lehetnének a felhőnek 5-ös szintnél alacsonyabb biztonsági szinten biztosított szolgáltatásai: példaként, ha a felhőben szolgáltatott levelezést csak 3-as szinten sikerül megvalósítani, akkor azt 5-ös rendszerek nem vehetik igénybe, amennyiben ilyen szolgáltatásra van szükségük, akkor saját megoldást kell biztosítaniuk. A NISZ a szolgáltatás katalógusában szereplő elemekről adatot szolgáltat az ügyfeleinek annak érdekében, hogy az EIR megfeleljen a törvényi szabályozásnak.

Az NKI által végrehajtandó audit sikeres teljesítése érdekében a KAK Felhő kialakítását, továbbá a KAK Ibtv. megfelelőségi vizsgálatra történő felkészítését a projekt során fentiek figyelembe vételével végre kell hajtani. A követelményeknek történő teljes körű megfelelés biztosítása mind a NISZ, mind pedig a megvalósításban közreműködő beszállítók részéről folyamatos együttműködést, feladatellátást igényel. Az alábbi védelmi intézkedés csoportok tekintetében ez a következő főbb feladatokat jelenti:

Adminisztratív védelmi intézkedések

A projekt keretében elkészítésre kerül a KAK rendszerszintű informatikai biztonsági szabályozása és szükséges további kapcsolódó eljárásrendjei, valamint a KAK Felhő elvárt, magas szintű, folyamatos működtetéséhez szükséges minden dokumentáció (pl.: műszaki, fejlesztési és üzemeltetési dokumentációk, rendszertervek, rendszerbiztonsági tervek, stb.).

Fizikai védelmi intézkedések

A KAK fizikai- és környezeti védelme – így például az adatközpontok beléptetési rendszere és rendje – a Vhr.-ben meghatározott elveknek és követelményeknek megfelelően kerül kialakításra.

Logikai védelmi intézkedések

A KAK Felhőnek, kiszolgáló környezetének meg kell felelnie a legmagasabb, 5-ös biztonsági besorolású EIR-ekkel szemben támasztott követelményeknek illetve részkritériumoknak is, úgy tekintve, mintha a besorolt EIR egy vagy több rendszereleme működne a KAK-on belül. Ebből következően a KAK egyes rendszerelemeinek a Vhr.-ben előírt, az adott rendszerelemmel kapcsolatban releváns biztonsági követelményeket kell tudnia teljesíteni, érintett komponenseire vonatkozóan jellemzően az alábbi területeket lefedve:

* határvédelmi intézkedések;
* kommunikáció biztonsága;
* szeparációs követelmények teljesítése;
* adattárolás, adatkezelés biztonsága;
* biztonsági funkciók, folyamatok elkülönítése;
* biztonsági mentés, archiválás;
* privilegizált hozzáférések kezelése és felügyelete;
* biztonsági események naplózása, ezek kezelése.

Amennyiben az NKI kezdeményezi, a projektgazda a fejlesztés részeként köteles vállalni, hogy az NKI által kialakításra kerülő, a közigazgatási rendszereket a kibertérből érő támadások azonosítását, ezáltal a szervezeti integritás erősítését támogató korai jelzőrendszerhez való csatlakozás alapvető műszaki feltételeit a fejlesztés keretében megteremti és azt a rendszer teljes életciklusában fenntartja. A központi elemző alrendszerből és a projektgazda védett rendszere meghatározott be és kimeneti hálózati csomópontjain elhelyezett szenzorokból álló jelzőrendszer a bemenő és kimenő forgalmat vizsgálja szignatúra és viselkedés alapú metódusokkal. A projektgazdának meg kell adnia a szenzor műszaki/technikai méretezéséhez szükséges adatokat (pl.: átlagos és csúcs hálózati forgalom) és az NKI útmutatása alapján meg kell teremtenie a szenzor telepítésének infrastrukturális és egyéb feltételeit.

A projekt megvalósítása során – az előzetesen meghatározott ütemterv szerint – beérkezett dokumentációkat az NKI megvizsgálja, illetve összeveti a vonatkozó tervdokumentációkkal. Ha a vizsgálat a tervezett biztonsági intézkedések megvalósításának hiányát tárja fel vagy lényeges kockázatot azonosít, akkor az NKI kezdeményezi a hiányosságok pótlását, illetve a kockázat kezelését. A projektgazda a projekt fejlesztési fázisainak lezárását megelőzően a hiányosságokat pótolni, a lényeges kockázat tárgyában kockázatkezelési intézkedést köteles hozni.

Az utolsó végrehajtási projektszakasz zárása előtt a projekt megvalósítása során beérkezett dokumentációk, valamint a projekt során tervezett biztonsági intézkedések megvalósítását érintő kockázatok függvényében az NKI az Ibtv. 14. § (2) bekezdés alapján részleges vagy teljes megfelelőségi vizsgálat (audit), illetve az Ibtv. 18. § (1) bekezdés alapján sérülékenység vizsgálat lefolytatását rendelheti el.

A korábban felmerült, még nem pótolt hiányosságokat és nem kezelt kockázatokat, valamint az esetlegesen lefolytatott audit illetve sérülékenység vizsgálat során feltárt hiányosságokat és kockázatokat a projekt zárását megelőzően kezelni szükséges. A projekt keretében létrehozott rendszer biztonsági megfelelősége, az NKI által megállapított hiányosságok pótlása, valamint a kockázatkezelési intézkedés meghozatala kapcsán készített szakmai beszámoló NKI általi elfogadása a projekt fejlesztési fázisai lezárásának és az üzembe helyezésnek a feltétele.

### Támogatott alkalmazói rendszer kialakítási modellek

A kialakításra kerülő KAK két telephelyen kerül elhelyezésre, melyet „A” és „B” telephelynek nevezünk.

Alapvetés, hogy az éles alkalmazás környezet az „A” telephelyen, a teszt-, fejlesztői-, oktatási környezetek a „B” telephelyen futnak. Katasztrófa szituáció esetén kizárólag az éles alkalmazás futtatását biztosítjuk, a teszt, fejlesztői és oktatási környezeteket nem, kivéve, ha erre utasítást kapunk, és a megfelelő erőforrások rendelkezésre állnak.

A továbbiakban bemutatásra kerülő négy modell alapvetően a rendelkezésre állás kialakításában tér el. A legnagyobb SLA-t a KAK Felhőre fejlesztett alkalmazások számára lehetséges biztosítani, amely katasztrófa esetén néhány perc alatti automatikus átállást tesz lehetővé. A többi esetben az alkalmazás architektúrájától független, infrastruktúra szintű megoldás kialakítását támogatjuk.

Az alábbiakban sorra vesszük a HA (High Availability, telephelyen belüli egyszeres meghibásodás) illetve az egész „A” telephely kiesése esetén fellépő DR (Disaster Recovery) - katasztrófa elhárítási eseteket. A „B” telephely kiesése az éles „A” telephely működésében nem jelent változást. Természetesem az „B” telephely kiesése során a NISZ értesítést küld az érintett adatgazdák felé, illetve mindent elkövet annak érdekében, hogy a telephely a lehető legkevesebb adatvesztéssel újra elérhető legyen.

A katasztrófa elhárítás során jelentkező különféle igényeket a „B” telephelyen futó teszt, fejlesztői és oktatási környezetek leállításával lehet kielégíteni. Említett környezetek csak az „A” telephely teljes helyreállítása és az eredeti helyzet visszaállítása után, lesznek helyreállíthatók a „B” telephelyen. Teljes telephelyi DR esemény során minden olyan tevékenységet el kell végezni, amely ahhoz szükséges, hogy az SLA-kban foglalt rendelkezésre állást a KAK Felhő biztosítani tudja.

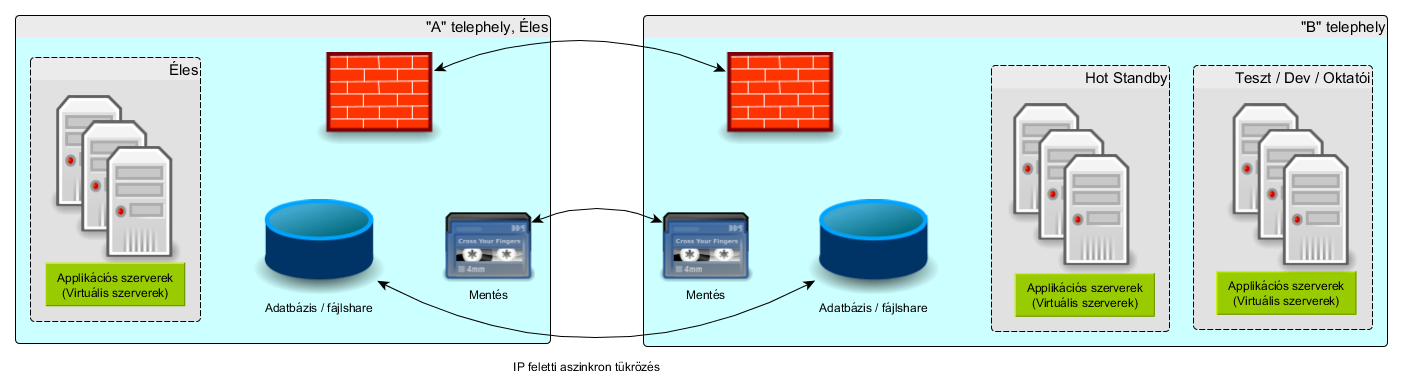
A felhőben az alábbi négy alkalmazás modell támogatott:

#### Felhőre fejlesztett alkalmazások

A felhőre fejlesztett alkalmazásokon azt értjük, hogy az alkalmazás webes felülettel rendelkezik a felhasználók felé, és legalább a következő rétegekből áll:

* Load balancer
* Applikációs szerverek (virtuálisak)
* Perzisztencia réteg (fájl share / adatbázis / object store)
* több site-os kialakítás

Az applikációs szerverek lehetőség szerint állapotmentesen működjenek.



3. ábra Felhőre fejlesztett alkalmazások

HA (High Availability) - magas rendelkezésre állás megoldása:

* A Load balancer-eket a redundáns perimeter eszköz fogja biztosítani, így annak a kiesése nem okoz leállást (legrosszabb esetben a sessionök vesznek el, ezért az éppen bejelentkezett felhasználóknak újra kell authentikálni)
* Egy applikációs szerver kiesése esetén elindul egy új, ha az applikációs szerver tényleg állapotmentes, akkor a kiesése / újraindulása egyáltalán nem érzékelhető felhasználói oldalról. Ha nem sikerül teljesen állapotmentesre, akkor a rajta átmenő sessionök vesznek el, a felhasználókat újra kell authentikálni.
* Perzisztencia réteg: Az adatbázis és a storage rétegben nincs SPOF, egy eszköz kiesése nem okoz a felhasználók számára érzékelhető változást.
* HA esemény esetén gyakorlatilag nincs kiesett idő.

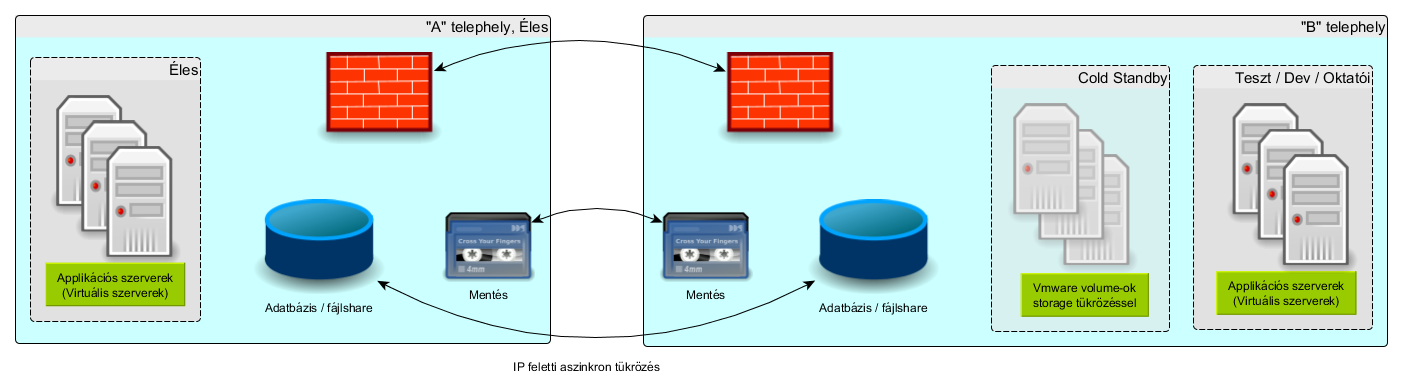
DR (Disaster Recovery) - katasztrófa elhárítási megoldás telephely kiesés esetén:

* A perimeter eszköz site-ot vált, a további kéréseket a „B” site-on futó applikációs szerverek felé továbbítja, melyek a „B” site adatbázisát / fájl szerverét veszik igénybe. A felhasználóknak valószínűleg megszakad a kapcsolata, és újra kell authentikálni / ellenőrizni kell, hogy az utolsó művelet sikeres volt vagy sem. A kiesési idő várhatóan kevesebb, mint 20 perc.

#### „Legacy” nagy rendelkezésre állású rendszerek

A címben foglalt alkalmazások alatt a következőt értjük:

* Jellemzően nem használnak load balancer-t
* Egy vagy több virtuális szerverből állnak
* Az adataikat fájl share-en vagy adatbázisban tárolják
* Magas rendelkezésre állással szükséges futtatni őket.



4. ábra „Legacy” nagy rendelkezésre állású rendszerek

HA (High Availability) - magas rendelkezésre állás telephelyen belüli megoldása:

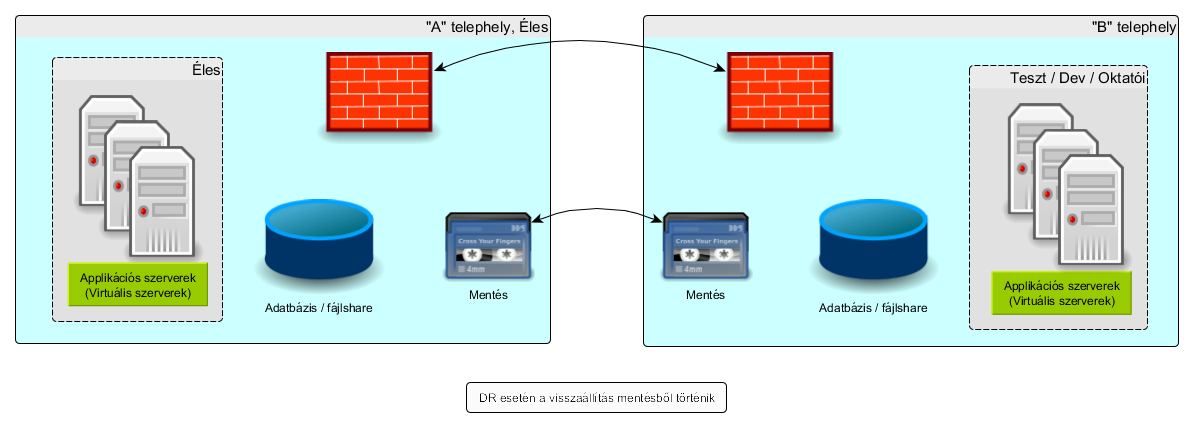
* Virtuális szerverek: egy szerver kiesése esetén elindul egy új. A szerveren átmenő sessionök vesznek el, a felhasználókat újra kell authentikálni. Egy szerver kiesése kevesebb, mint 20 perc kiesést okozhat.
* Perzisztencia réteg: Az adatbázis és a storage rétegben nincs SPOF, egy eszköz kiesése nem okoz a felhasználók számára érzékelhető változást.

DR (Disaster Recovery) - katasztrófa elhárítási megoldás telephely kiesés esetén:

* A „B” site-on a tükrözött volume-okat aktív módba rakjuk, és felismertetjük a Vmware / OpenStack virtualizációs réteggel. A felismertetett gépeket elindítjuk, a szükséges módosításokat (ha vannak) egy automatizmus elvégzi rajtuk.
* A perimeter eszköz eközben site-ot vált, a további kéréseket a „B” site-on futó szerverek felé továbbítja. A felhasználóknak megszakad a kapcsolata, és újra kell authentikálni / ellenőrizni kell, hogy az utolsó művelet sikeres volt vagy sem. A kiesési idő várhatóan több óra, mert több ilyen rendszer is lehet, akik „sorban állnak”, és várnak a virtuális gépek felismertetésére és az elindításukra.

#### Kevésbé kritikus rendszerek

A kevésbé kritikus rendszerek egy telephelyesek. A kevésbé kritikus rendszerek egyébként lehetnek felhőre fejlesztettek és Legacy típusúak is, HA jellegű - az „A” telephelyen belüli magas rendelkezésre állás keretében biztosított - esemény esetén ettől függ a kiesési idő. A mentés, mint minden esetben itt is duplikált a két telephely között, így az „A” telephely teljes megsemmisülése esetén is vissza lehet állítani a szükséges erőforrások biztosítása után a rendszert működőképes állapotba.



5. ábra Kevésbé kritikus rendszerek

HA (High Availability) - magas rendelkezésre állás telephelyen belüli megoldása:

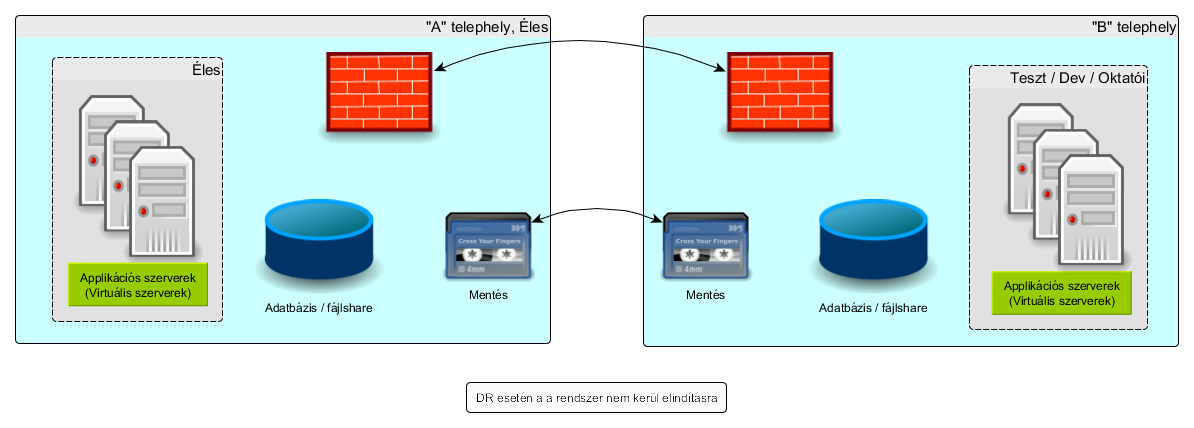
* Virtuális szerverek: egy szerver kiesése esetén elindul egy új. A szerveren átmenő sessionök vesznek el, a felhasználókat újra kell authentikálni. Egy szerver kiesése felhőre fejlesztett rendszer esetén nem okoz kiesést, Legacy típusú rendszernél várhatóan kevesebb, mint 20 perc kieséssel számolhatunk.
* Perzisztencia réteg: Az adatbázis és a storage rétegben nincs SPOF, egy eszköz kiesése nem okoz a felhasználók számára érzékelhető változást.

DR (Disaster Recovery) - katasztrófa elhárítási megoldás telephely kiesés esetén:

* A „B” site-on a visszaállítás mentésből történik, a kiesési idő várhatóan több nap.

#### Nem kritikus rendszerek

A nem kritikus rendszerek egy telephelyesek. A nem kritikus rendszerek egyébként lehetnek felhőre fejlesztettek és Legacy típusúak is, HA esemény esetén ettől függ a kiesési idő. A mentés, mint minden esetben itt is duplikált a két telephely között, így az „A” telephely teljes megsemmisülése esetén is vissza lehet állítani a szükséges erőforrások biztosítása után a rendszert működőképes állapotba.



6. ábra Nemkritikus rendszerek

HA (High Availability) - magas rendelkezésre állás telephelyen belüli megoldása:

* Virtuális szerverek: egy szerver kiesése esetén elindul egy új. A szerveren átmenő sessionök vesznek el, a felhasználókat újra kell authentikálni. Egy szerver kiesése felhőre fejlesztett rendszer esetén nem okoz kiesést, Legacy típusú rendszernél várhatóan kevesebb, mint 20 perc kieséssel számolhatunk.
* Perzisztencia réteg: Az adatbázis és a storage rétegben nincs SPOF, egy eszköz kiesése nem okoz a felhasználók számára érzékelhető változást.

DR (Disaster Recovery) - katasztrófa elhárítási megoldás telephely kiesés esetén:

* DR esetén a nem kritikus rendszerek a normál működés visszaállításáig nem kerülnek elindításra.

### Adatközpontok működési módja

A BM iránymutatásának megfelelően az elsődleges központban az éles rendszerek, a másodlagos központban pedig maximum a teszt- fejlesztői- és oktatói környezet futnak. A két központ között aszinkron replikációt használunk.

Ugyan az adatok tárolását biztosító hardver és szoftver környezet egyszeres meghibásodások (SPOF) ellen védett, de nagy kiterjedésű - egyszerre több komponenst érintő - katasztrófa jellegű meghibásodások esetén, az elsődleges telephelyen önmagában nem biztosítható az adatok teljes körű helyreállítása. A nagyobb léptékű adatvesztés elkerülését biztosítják a rendszeres mentések, de az utolsó mentés óta eltelt időszak módosításai csak a műveletek másodlagos adatközpontba történő replikációjával őrizhetők meg. Az aszinkron replikáció következménye, hogy az adatállományokat vagy azok tárolását biztosító infrastruktúrát érhetik olyan sérülések, amelyek következményeképpen az utolsó jóváhagyott tranzakciók egy része nem jut el a másodlagos adatközpontba. Ekkor a szolgáltatásnak a másodlagos telephelyen történő helyreállítása során - a meghibásodások jellegének és a replikáció késleltetésének függvényében - adatvesztés jelentkezhet.

Ilyen értelemben az adatközpont tároló infrastruktúrája önmagában nem jelent tökéletes védelmet az adatvesztések ellen. Olyan rendszerek esetén, ahol a minimális adatvesztés sem engedhető meg, ott az alkalmazási rendszer architektúrájában, ill. működési logikájában kell kialakítani a megfelelő védelmet (pl. az alkalmazási tranzakciók alternatív csatornán való lokális, ill. távoli párhuzamos rögzítésével).

# KAK Felhő szolgáltatások

A KAK Felhő az alábbi ellátási szolgáltatásokat (IaaS, PaaS, SaaS) és kiegészítő szolgáltatásokat nyújtja:

## IaaS szintű ellátási szolgáltatások

### Virtuális szerver szolgáltatás

**Általános definíció**

A virtuális szerver szolgáltatás keretében definiálásra kerül egy virtuális gép, a gépekhez tartozó minimum és maximum értékek közötti paraméterekkel együtt (vCPU, vRAM, vStorage, operációs rendszer). A gépek különböző zárt virtuális hálózati szegmensekbe (VLAN, VXLAN) szervezhetők, melyek között az adatáramlást – tűzfalon keresztül – szabályok alapján lehet korlátozni. A létrejövő architektúrán üzembe állítható az ügyfél számára a saját infrastruktúrája. Erőforrások későbbi módosítása technológiailag megvalósítható szerződésmódosítás és előzetes jóváhagyást követően.

A virtuális szerver szolgáltatás a virtuális adatközpont szolgáltatás megvalósítással történik, azaz egy tenanthoz tartozó virtuális szerverek erőforrásai egy poolként kezelhetők, szerződésmódosítás nélkül a pool határain belül átkonfigurálhatók.

**Mentés és archiválás**

A felhőben biztosított mentés és archiválás, illetve helyreállítás kialakításának általános szempontjait a 3.5.11 Mentés szolgáltatás és 3.5.12 Archiválás szolgáltatás alfejezetek tartalmazzák. Mivel az archiválás - az utóbb hivatkozott alfejezetben vázoltak szerint – a mentéshez analóg módon valósul meg, az alábbiakban nincs külön részletezve.

Mentéshez az IBM Spectrum Protect terméket használjuk. A virtuális szerverek mentése történhet image alapon illetve amennyiben a virtuális gépen használt operációs rendszer támogatja, agent alapon is.

Az image (vm) alapú mentés a Bérlő számára kizárólag a szolgáltató által támogatott formában vehető igénybe a felhő management felületén keresztül, és ekkor a teljeskörű felügyeletet a szolgáltató biztosítja. Image alapú mentés esetén a Bérlő feladata az adott virtuális gép konzisztens állapotba hozása (pl. suspend). A helyreállításokat a szolgáltató egyedi bejelentések alapján végzi, és az egyes szolgáltatás példányok vonatkozásban független módon hajtja végre.

A VM-ek kapcsán a Bérlő hatáskörében lévő elemekre a NISZ agent alapú támogatást nem biztosít az önkiszolgáló portálon keresztül. Agent alapú mentésnél a virtuális gépeken futó operációs rendszerek alatt lévő Backup-Archív (BA) agent-en keresztül történik a mentés és helyreállítás, a menedzsment felületet a Spectrum Protect biztosítja, a Bérlőnek ezt használva kell a mentését beállítania.

Agent alapú mentés esetén a bérlő szabadon használhatja a Spectrum Protect által kínált integrált eszközöket és folyamatszervezést támogató megoldásokat (mint például a különböző adatbázis- vagy alkalmazás szerverekkel történő integráció).

Agent alapú mentés esetén a Bérlőnek az alábbi jellegű Spectrum Protect által támogatott mentési módszerek állnak a rendelkezésre:

* progresszív inkrementális mentés
* szelektív mentés (egyedi fájlok megadása)
* journal alapú mentés
* integrált adatbázis mentés

IaaS szolgáltatási szint esetén a mentést a Bérlő konfigurálja, konzisztens mentés készítése és komplex helyreállítások végrehajtása minden esetben a Bérlő feladata és felelőssége. Ez abban az esetben is igaz, ha a Bérlő egyébként azokat a virtuális gép image-eket használja, melyeket a NISZ saját, magasabb szintű szolgáltatásaihoz hozott létre.

**Virtuális gép létrehozása**

A virtuális gépek létrehozása a következő módokon képzelhető el:

* A NISZ biztosít különböző alap operációs rendszer template-eket, melyeket a Bérlő a megfelelő csomagok vagy programok telepítésével és a konfigurációs fájlok testre szabásával példányosíthat. Ugyan a NISZ ajánl kereskedelmi operációs rendszereket is, de IaaS szintű szolgáltatás esetén ezek licenc helyes működése a bérlő felelőssége, az IaaS szint feletti licenceket (pédául és nem kizárólag az operációs rendszer, alkalmazás szerver, adatbázis szerver licencek) a Bérlőnek kell biztosítania.[[1]](#footnote-2)
* A NISZ biztosítja a magasabb szintű (SaaS, PaaS) szolgáltatásaihoz használt template-eket a Bérlők számára. Mivel ez továbbra is IaaS szolgáltatást jelent, sem az operációs rendszerre sem az operációs rendszer felett levő rétegekre semmilyen támogatást vagy frissítést nem tartalmaz a szolgáltatás, azt a Bérlőnek magának kell megoldania. A rendszergazdai jogok – ellentétben a Paas, SaaS szolgáltatásokkal – a Bérlőhöz kerülnek. Ezeknek a template-eknek a közlése csak annyiban egyszerűsíti a Bérlő feladatait, hogy nem egyesével kell telepítenie és konfigurálnia a különböző komponenseket az alap template-eket használva – mondjuk egy LAMP környezet létrehozásánál –, hanem azt egyszerre, egy lépésben, előre konfigurálva, készen megkapja.
* A Bérlőnek lehetősége van saját template feltöltésére, mely kizárólag az általa menedzselt tenantban válik elérhetővé.

Virtuális gépet nem lehet tetszőleges méretben létrehozni, hanem figyelembe kell venni a „4 Architekturális illeszkedés követelményei” fejezetben meghatározott korlátokat.

### Virtuális adatközpont szolgáltatás

A virtuális adatközpont szolgáltatás keretében definiálásra kerülnek erőforrás (elsősorban vCPU, vRAM és vStorage) limitek, amiken belül tetszőlegesen létrehozható egy vagy több virtuális gép az ügyfél számára. A gépek különböző zárt virtuális hálózati szegmensekbe (VLAN, VXLAN) szervezhetők, melyek között az adatáramlást – tűzfalon keresztül – szabályok alapján lehet korlátozni. A létrejövő architektúrán üzembe állítható az ügyfél számára a saját infrastruktúrája. Az előre definiált limitek határáig lehetőség van az erőforrások dinamikus használatára. Az általunk tervezett rendszer ezt támogatja mind az adminisztrációs felületen, mind szoftveres API-n keresztül. Az API-n keresztüli támogatottság lehetővé teszi bizonyos feltételek mellett az elasztikus skálázódást, mely horizontális (új virtuális gépek hozzáadásával) lehetőséget ad a változó igények kiszolgálására.

### Docker konténer futtatása

A virtuális szerver szolgáltatáshoz hasonló szolgáltatás, mely esetben a szolgáltatások szeparációját a virtualizálásnál kisebb overheaddel rendelkező konténer technológiával valósítjuk meg. Docker konténer esetében a NISZ üzemeltetés csak a Docker konténeren végez műveleteket (például konténer indítása vagy leállítása), a konténeren belül nem – ezért a konténeren belül használt technológiára nincs megkötés, de a NISZ üzemeltetés nem tud segítséget nyújtani a konténeren belüli hibák elhárításához.

Docker konténereket OpenStack alatt szolgáltatunk, az OpenStack által natívan támogatva (azaz nem virtuális gépen belül futtatott Dockerről beszélünk). Ez azt is jelenti, hogy a 1004/2016. (I. 18.) Korm. határozat által nem nevesített informatikai rendszerek esetén amennyiben Docker felhő szolgáltatást szeretnének igénybe venni, úgy az OpenStack környezet (OpenStack tároló, OpenStack számítási kapacitás) kell bővíteni az igénybe veendő szolgáltatások erőforrás igényeinek megfelelően.

Docker esetén a tenant adminisztrátor saját Docker Registryt állíthat be akár a felhőn kívül, akár azon belül, egy erre a célra bérelt virtuális gépen.

## DBaaS szintű szolgáltatások

DBaaS szolgáltatást infrastruktúra tervezési és biztonságtechnikai okokból Szolgáltató kizárólag csak mint kiegészítő szolgáltatást biztosít. Ennek megfelelően a szolgáltatások leírásai az „3.5.13 Adatbázis kiszolgáló szolgáltatás (DBaaS)” fejezetben találhatóak.

## PaaS szintű ellátási szolgáltatások

A PaaS szintű szolgáltatások esetén (mind az ellátási, mind a kiegészítő szolgáltatásoknál) általánosan elmondható, hogy a NISZ által biztosított szintig az üzemeltetést a NISZ végzi. Ez azt is jelenti többek között, hogy a NISZ rendszeres, előre bejelentett, tervezhető időközönként telepíti a javítócsomagokat (patch) először a dev, teszt, oktatói környezetekben, majd az éles környezetben is. A NISZ csak egy stabil verziójú szoftver kiadást üzemeltet a platform szolgáltatásokban. Amennyiben egy rendszer számára nem megfelelő a NISZ által üzemeltetett verzió, úgy lehetőség van a továbbiakban az adott szolgáltatást ellátó virtuális gépet átminősíteni IaaS szintre, melyet a bérlő maga is üzemeltethet vagy a NISZ Zrt.-vel az IaaS szint feletti részre külön üzemeltetési szerződést köthet. (Ennek egyedi ára várhatóan meghaladja PaaS szinten igénybe vett szolgáltatás árát.)

### Alkalmazás kiszolgáló szolgáltatás

A KAK Felhő által biztosított alkalmazás kiszolgálók: Java (JVM), .NET, Python, és PHP. Az alkalmazásszerver példányok bérlői elhatárolása egységesen VM szinten történik, és a kiszolgálás jellegéből következően a bérlőnek nincs a VM-eken belül operációs rendszer szintű hozzáférése. Így a kapcsolódó egyéb szolgáltatások igénybe vétele (pl. NAS csatolása és a hozzáférések kiosztása) is a szolgáltató támogatásával, illetve a felhőmenedzsment portál felületén vagy bejelentés alapján történhet. Ahogy az alkalmazásszerver végezhet strukturált állományokból való betöltéseket, illetve NAS-ra kimutatásokat tárolhat és publikálhat, ugyanúgy átmeneti állományokat is képezhet objektumtárból letöltött dokumentumok mentéséhez és archiválásához. Ezen állományok kezeléséhez a bérlőnek *nincsen az adott hoszton belül közvetlen kontrollja*, így az adott szerveren a konzisztens konfigurációk és állapotok agent alapú mentését sem végezheti egyedi intézkedések nélkül. (Természetesen a NAS-on könyvtárakat másik, saját hatáskörében lévő IaaS VM szolgáltatáson felcsatolhatja, így közvetlenül is követheti az állapotokat.)

A felhőben biztosított mentés és archiválás, illetve helyreállítás kialakításának általános szempontjait a „3.5.11 Mentés szolgáltatás” és „3.5.12 Archiválás szolgáltatás” alfejezetek tartalmazzák. Mivel az archiválás - az utóbb hivatkozott alfejezetben vázoltak szerint – a mentéshez analóg módon valósul meg, az alábbiakban nincs külön részletezve.

Az alkalmazás szerver PaaS szolgáltatások kapcsán a mentés és archiválás specifikumai az alábbiak:

* mivel az alkalmazásszerver bérlői elhatárolása általában VM szinten történik, az image alapú támogatott mentés a felhőmenedzsment önkiszolgáló felületén keresztül biztosított (a helyreállítás itt is bejelentés alapján történhet)
* a szolgáltató agent alapú mentést alapértelmezés szerint nem végez a VM-ek operációs rendszerén belül
* a bérlő számára lényeges konfigurációs elemek, NAS könyvtárak, illetve egyéb állományok regisztrációja alapján azok agent alapú mentése a bérlő IBM Spectrum Protect tenant hozzáférésével lehetséges.

#### Java (JVM) kiszolgálók (Tomcat és JBoss)

A Java kiszolgáló egy olyan webtárhely szolgáltatás, amely bekonfigurált Tomcat vagy JBoss alkalmazás kiszolgálót tartalmaz. A felhasználó a fájlokat SFTP szolgáltatáson keresztül tudja feltölteni és egy webes felületen keresztül deployolni. A felhasználó shell szintű hozzáférést nem kap, de az alkalmazás kiszolgálóban adminisztrátori jogokkal rendelkezik. A lokálisan tárolt logokat a felhasználó megnézheti / letöltheti.

#### .NET kiszolgáló

A .Net kiszolgáló olyan Microsoft IIS 10 alapú webtárhely szolgáltatás, amely bekonfigurált ASP.NET Framework 4.7, vagy ASP.Net Core 1.0 támogatást tartalmaz.

A felhasználó a fájlokat SFTP szolgáltatáson keresztül tudja feltölteni. A felhasználó shell szintű hozzáférést nem kap. A lokálisan tárolt logokat a felhasználó megnézheti / letöltheti.

#### Python kiszolgáló

A Python kiszolgáló egy olyan Apache webtárhely szolgáltatás, amely bekonfigurált mod\_wsgi modult tartalmaz. A felhasználó a fájlokat SFTP szolgáltatáson keresztül tudja feltölteni és egy webes felületen keresztül deployolni. A felhasználó shell szintű hozzáférést nem kap. A lokálisan tárolt logokat a felhasználó megnézheti / letöltheti.

#### PHP kiszolgáló

A PHP kiszolgáló egy olyan Apache webtárhely szolgáltatás, amely bekonfigurált mod\_php modult tartalmaz. A felhasználó a fájlokat SFTP szolgáltatáson keresztül tudja feltölteni és egy webes felületen keresztül deployolni. A lokálisan tárolt logokat a felhasználó megnézheti / letöltheti.

## SaaS szintű ellátási szolgáltatások

A komplex - infrastruktúra, platform és alkalmazási elemeket is magába foglaló - SaaS szolgáltatások felügyelete egészében és általában, benne a mentés vagy archiválás beállítása is teljes mértékig a szolgáltató hatókörében van. A felhőben biztosított mentés és archiválás, illetve helyreállítás kialakításának általános szempontjait a „3.5.11 Mentés szolgáltatás” és „3.5.12 Archiválás szolgáltatás” alfejezetek tartalmazzák. A SaaS szolgáltatásokhoz kapcsolódó komplex mentési megoldások műszaki paramétereit (RPO, RTO) a szolgáltatási katalógus tartalmazza, a helyreállításokat itt is minden esetben bejelentés alapján biztosítja a NISZ.

### Levelezés, csoportmunka szolgáltatás

Olcsó, könnyen skálázható, modern, web alapú levelező- és csoportmunka szerver-környezet kialakítása a cél, amely megfelelően támogatja a bérlőkezelést. A szolgáltatásként történő igénybevétel és a gyors bevezetés különösen újonnan alakuló, vagy elavult rendszert használó szervezetek számára lehet előnyös. Célunk teljes körűen kiváltani a freemail, gmail és más ingyenes levelezés szolgáltatások kormányzati célú felhasználását.

A kiválasztásra kerülő termék önmagában tartalmazni fog tenant kezelést. Az igényelt postafiók számot és a levelezéshez igényelt tárterület mennyiséget szükséges megadni. A létrejövő, tenanthoz kötött levelezés további kezelését a tenant adminisztrátora a termék natív felületén tudja elvégezni.

A szolgáltatás tartalmazni fog a postafiókokhoz kapcsolódóan spam-szűrést és vírusvédelmet is.

A levelezési szolgáltatás mentése központilag történik, az esetleges visszaállítást Service Desk jegyen keresztül szükséges kérni.

### Dokumentumkezelő (ECM és BPM) szolgáltatás

A Dokumentumkezelő szolgáltatás keretében a NISZ az Alfresco Community Edition verzióját biztosítja. A tenant kezelést nem az Alfresco-n belül kerül megoldásra, hanem minden tenant külön szeparált Alfresco környezetet vagy környezeteket kap. Az Alfresco adminisztrátor jogosultságot megkapja a tenant adminisztrátor, az Alfresco alatt levő operációs rendszerben / adatbázis kezelőben viszont nem kap jogosultságokat.

Az Alfresco ClamAV vírusvédelmi megoldást tartalmaz beépítetten, de ha a bérlő rendelkezik a bérleményén belül egyéb, ICAP protokollt támogató AV megoldással, az is beköthető.

Az Alfresco illetve az alatta levő operációs rendszer rendszeres frissítéséről és mentéséről a NISZ gondoskodik. A mentés visszaállítást külön Service Desk ticketben kell kérni.

### Tartalomkezelő (CMS) szolgáltatás

CMS szolgáltatásként a NISZ Drupal tartalomkezelőt szolgáltat. A tenant kezelést nem a Drupalon belül kerül megoldásra, hanem minden tenant külön szeparált Drupal környezetet vagy környezeteket kap. A Drupal adminisztrátor jogosultságot megkapja a tenant adminisztrátor, a Drupal alatt levő operációs rendszerben / adatbázis kezelőben viszont nem kap jogosultságokat.

A Drupal ClamAV vírusvédelmi megoldást tartalmaz beépítetten.

A Drupal architektúra a következő két verzióban kerül kialakításra:

* 2 alkalmazás és 2 db szerver
* egy szerveres CMS rendszer

Az Drupal illetve az alatta levő operációs rendszer rendszeres frissítéséről és mentéséről a NISZ gondoskodik. A mentés visszaállítást külön Service Desk ticketben kell kérni.

### E-Learning szolgáltatás

E-Learning szolgáltatásként a NISZ a Moodle nyílt forráskódú tanulási platformot szolgáltatja. A tenant kezelést nem a Moodlen belül kerül megoldásra, hanem minden tenant külön szeparált Moodle környezetet vagy környezeteket kap. A Moodle adminisztrátor jogosultságot megkapja a tenant adminisztrátor, a Moodle alatt levő operációs rendszerben / adatbázis kezelőben viszont nem kap jogosultságokat.

A Moodle ClamAV vírusvédelmi megoldást tartalmaz beépítetten.

Az Moodle illetve az alatta levő operációs rendszer rendszeres frissítéséről és mentéséről a NISZ gondoskodik. A mentés visszaállítást külön Service Desk ticketben kell kérni.

## Kiegészítő szolgáltatások

Kiegészítő szolgáltatásnak nevezzük azon szolgáltatásokat, amelyek önállóan nem, csak valamely ellátási szolgáltatás kiegészítéseként lehet igénybe venni. A „3.6 Üzleti szolgáltatásonként a hozzájuk rendelhető kiegészítő szolgáltatások táblázata” fejezet jelöli, hogy az ellátási szolgáltatások mellé milyen típusú kiegészítő szolgáltatás rendelhető.

### Több privát IP cím

Amennyiben valamelyik szolgáltatás szükségessé teszi további privát IP címek felvételét (például VIP cím), úgy a virtuális gépeknek automatikusan kiosztott IP címek mellé a VLAN méretéig további IP címek foglalhatóak.

### Fix publikus IP cím

A kiegészítő szolgáltatás keretében fix külső, publikus IP cím szolgáltatás rendelhető korlátozott mennyiségben. A nyilvános IP címekkel történő gazdálkodás és a címek Ellátott részére történő kiosztása a NISZ feladata. Maga a publikus IP cím a felhő esetén a perimeter eszközön lesz beállítva, mint ami a szolgáltatást publikálja. A hosting környezet esetében pedig az ügyfél valamelyik eszközén (legtöbb esetben tűzfalán) történik a beállítás.

### Tárhely szolgáltatás (IaaS (block device) alapú kiegészítő szolgáltatás)

Block device tárhely szolgáltatás keretében további diszk volume-ok (például vmware alatt vmdk-k) adhatók meglevő virtuális gépekhez. A tárterület bekonfigurálása, csatolása, illetve fájlrendszer létrehozás a tárterület felett annak a feladata, aki az operációs rendszer szintet üzemelteti. Azaz IaaS szolgáltatásnál a bérlő feladata, magasabb szintű szolgáltatásnál a NISZ feladata.

Technikai korlátok miatt egy diszk volume mérete nem haladhatja meg a 2TB-ot. Ennél nagyobb méret esetén több volume-ot kell igényelni, és azokat szükség (guest) operációs rendszer szinten kell összefogni.

### Objektumtár szolgáltatás (IaaS alapú kiegészítő szolgáltatás)

A Felhő általbiztosított OpenStack Object Storage (SWIFT) egy magas rendelkezésre állású, elosztott, konzisztens object/blob tároló. Az objektumok létrehozása, módosítása és kivétele Object Storage API-n keresztül történik, ami Representational State Transfer (REST) web szervizekként került implementálásra. A részletes API dokumentáció itt található:

<https://docs.openstack.org/developer/swift/api/object_api_v1_overview.html>

A multi tenant működés úgy kerül megvalósításra, hogy az objektumok a tenant adminhoz (OpenStack projekthez) rendelt Swift account alatt kerülnek elhelyezésre, dedikált konténerben.

A szolgáltatást **nemcsak OpenStack, hanem egyéb IaaS és általában PaaS környezetből** is igénybe lehet venni.

A platform kialakítása az objektumok (adatok) többszörös tárolási redundanciáján keresztül biztosítja azok magas rendelkezésre állását és hibatűrését, ami egyaránt védelmet nyújt az eszközszintű egyszeres és a kiterjedt (katasztrófa jellegű) meghibásodások ellen. Az objektumtár önmagában nem biztosítja az adatszintű (szándékos vagy vétlen destruktív műveletekből, esetleg alkalmazási hibából eredő) sérülések kapcsán a helyreállítás lehetőségét. Ugyanúgy önmagában nem támogatja a tárolt állapotok bizalmas - törvényességi vagy egyéb szempontoknak megfelelő - megőrzését, ehhez applikáció szintű támogatás (például az objektumok titkosítása) szükséges.

**Objektumtár mentése és archiválása**

Az API alapon elérhető objektumtár szolgáltatásban tárolt adatok mentéséhez és archiválásához szükséges folyamatok (eljárások, scriptek) kidolgozása minden esetben a bérlő feladata, mivel a tárolt adatokról és a hozzáférésekről a szolgáltatónak nincs információja. A szolgáltató biztosítja a mentő és archiváló rendszer eléréshez szükséges API felületek folyamatos működését és azok integrációjához kapcsolódó dokumentációkat. Ez azt jelenti, hogy a NISZ a kiajánlott objektum tárat nem menti, a Bérlőnek kell – jellemzően alkalmazás oldali logikát követve, alkalmazás oldalról megtámogatva – az objektum tárban tárolt menteni szükséges adatokról és metaadatokról konzisztens mentést készítenie.

### Fájlkiszolgáló (NAS) (IaaS alapú kiegészítő szolgáltatás)

A KAK Felhőbe települő alkalmazások számára gyakran szükséges közös, hálózati tárhely. A preferált megoldás ilyenkor az előző pontban említett objektumtár használata, de szükség esetén CIFS és NFSv4 alapú tárhelyet központi NAS (Network Attached Storage) segítségével tudjuk biztosítani.

NAS storage-ból technikai korlátok miatt tenantonként egy darab NFSv4 és egy darab CIFS vehető igénybe, melyek a tenant admin által megadott LDAP-okból vagy AD-kból authentikálnak.

A NAS szolgáltatások kapcsán a mentés és archiválás kialakításának sajátos szempontjai a következők:

* a bérlők számára elérhető NAS kiszolgálók platform és teljes felhő szinten összevont mentése naponta egyszer – külön kérés nélkül – a szolgáltató által ütemezett módon megtörténik
  + a támogatott mentésből való helyreállítás itt is bejelentés alapján történhet
* konzisztens mentések végrehajtása a többi szolgáltatáshoz hasonlóan a bérlő felelőssége, amit célszerűen az alkalmazás helyén ütemezhet az IBM Spectrum Protect agent alapú eszközeinek segítségével (mivel a bérlőnek a NAS kiszoláglóhoz nincs közvetlen hozzáférése, ilyen értelemben az agent alapú kiegészítő opciót is a NAS-t alkalmazó VM vagy PaaS szolgáltatás kapcsán érvényesítheti)

### Terheléselosztás

A szolgáltatás nagyteljesítményű hardveres terheléselosztást biztosít a Felhő határát képező F5 perimeter eszköz segítségével L4 vagy L7 szinten. A terhelés elosztásnál a következő paraméterek állíthatók:

* **Round Robin**  (igény esetén priority group-al kiegészítve) – a belső címeket lista alapján sorban szólítja meg, amely kombinálható prioritás megadásával. Előnye a gyors döntési késleltetés, azonban nem veszi figyelembe a háttér szolgáltatás aktuális terhelését.
* **Ratio alapú**. Lehet **statikus** vagy **dinamikus**. Előbbi során a kapcsolatok súlyozás alapján kerülnek továbbításra. „Dinamikus ratio” esetében a súlyozást befolyásolja a belső rendszer szervereinek aktuális terhelése is, amely alapján a súlyozás folyamatosan változik.
* **Leggyorsabb** – az új kapcsolatokat mindig az a belső cím kapja, amely a folyamatos vizsgálatok alapján aktuálisan a leggyorsabban válaszol.
* Külső illetve belső load balancing
* **Legkevesebb kapcsolat** – az a belső cím kapja az új kapcsolatot, amelyiknél a döntés pillanatában a legkevesebb nyitott kapcsolat van.
* Vizsgált **(Observed)** - az a belső cím kapja az új kapcsolatot, amelyiknél meghatározott intervallumon belül (pl. elmúlt 1 óra, stb.) a legkevesebb Layer 4 kapcsolat volt. Olyan környezetben a legjobb, ahol a belső végpontok teljesítménye folyamatosan ingadozik.
* Predictive
* Least Sessions
* L3 address
* session persisztencia (cookie illetve kliens IP alapú)
* health check (monitor) hozzárendelés (kiszolgálók monitorozása)

A megoldások működhetnek együtt host IP címmel (pl. virtuális szerver node) vagy szoftver példánnyal (member) – ez utóbbi arra vonatkozik, ha egy virtuális szerveren több példány is fut ugyanabból a szoftverből, különböző TCP porton, vagy logikai (alias) IP címen. A terhelés elosztás kalkulációja történhet egyedi tag alapján, vagy a szolgáltatáshoz rendelt összes tag (pool) együttes vizsgálatával.

Fontos, hogy a szoftver környezetnek minden esetben támogatni kell a választott megoldást. A szolgáltató felelősségi határa IaaS esetében a határvédelmi eszközig, SaaS és PaaS szolgáltatás esetén a szolgáltató által üzemeltetett szoftverig terjed. IaaS szolgáltatáson működő belső környezetre vonatkozó hibakeresés a Bérlő feladata.

Az elérhető paraméterek közül a projekt későbbi fázisában kerül meghatározásra, hogy mi kerül kivezetésre az önkiszolgáló portálra, és mi az, ami csak Service Desk ticket segítségével kérhető és egyedileg konfigurált.

### SSL terminálás, kliens oldali certificate kezelés

Az SSL terminálást, azaz az SSL kapcsolatok (mint például a HTTPS kapcsolatok) esetén a komoly számítási kapacitást igénylő titkosítási folyamat központi kezelését F5 perimeter eszköz biztosítja, így az alkalmazás szerverek felé már csak a titkosítás nélküli forgalom kerül elküldésre.

Ennek a szolgáltatásnak egy alesete, amikor a felépített SSL csatornán a kliens (a kezdeményező) is SSL tanúsítvánnyal azonosítja magát annak bizonyítása érdekében, hogy jogosult igénybe venni a szolgáltatást. A kliens lehet, egy Internet felöl érkező ügyfél, de lehet egy szolgáltatást igénybe vevő alkalmazás szerver is. Ilyen esetben megadható, hogy az SSL terminálást végző eszköz ellenőrizze, hogy

* a kapott kliens oldali tanúsítvány érvényes-e (nem járt le, nem vonták vissza),
* az előre beállított aláíró tanúsítvánnyal írták-e alá.

Lehetséges olyan megoldás, amikor az alkalmazás titkosított adatfolyamát nem a perimeter eszköz terminálja, hanem csak átengedi L4 szinten és a titkosítást az alkalmazás oldja fel. Az ilyen esetekben azonban – lévén az alkalmazás VLAN-jában nem csak titkosítatlan adatok forgalmazása történik – a kötelező NKI EWS rendszerhez való csatlakozás a tenant bérlőjének a feladata.

### Naplózási szolgáltatás

A KAK Felhő projektben külön naplógyűjtő és naplóelemző rendszer kerül bevezetésre. A NISZ által üzemeltetett szintig (minimum hypervisor szint, de a szolgáltatás katalógusban szereplő PaaS, SaaS szolgáltatások esetében magasabb szintek is) a naplóállományok gyűjtését és elemzését mindenképpen a NISZ végzi. A NISZ szolgáltatási szintje felett keletkező naplóállományok esetében több lehetőség van:

* A NISZ által nem üzemeltetett szintekre a naplógyűjtést és naplóelemzést, mint kiegészítő szolgáltatást nyújtja a NISZ. Az ehhez való illeszkedés a futtatott rendszer szempontjából fejlesztést igényelhet, hiszen a megfelelő naplóállományokat elő kell tudni állítani, illetve az adott típusú napló formátumot meg kell tanítani a naplóelemzőnek.
* A NISZ által nem üzemeltetett szintekre a naplógyűjtést és naplóelemzést a futtatott rendszer integráltan tartalmazza.

Naplóállományok hozzáférhetősége:

* A kiegészítő szolgáltatásként nyújtott naplógyűjtés esetén a naplóállományokhoz a NISZ folyamatos, online hozzáférést biztosít. Naplóelemzés esetén adott gyakoriságú (heti, havi) és biztonsági eseményhez kötött riportot készít a NISZ a naplóelemzés eredményéről, melyet az Ügyfél/Adatgazda IBF-e számára hozzáférhetővé tesz.
* A NISZ által üzemeltetett szinteken keletkező naplóállományok Service Desk ticket segítségével kikérhetők. A kérés jogosságát a NISZ ellenőrzi, és indokolt esetben a kérést elutasíthatja.
* A PaaS szintű szolgáltatások esetén a naplók korlátos ideig lokálisan is tárolódnak, megtekintésükre és letöltésükre az adott géphez rendelt, tenant oldali adminisztrátor felhasználója jogosult.
* A külön VM-eken biztosított DBaaS szolgáltatások, úgymint: MongoDB, PostgreSQL és MariaDB, naplóállományaihoz a PaaS szintű szolgáltatásokkal analóg módon az adott géphez rendelt, tenant oldali adminisztrátor felhasználó jogosult hozzáférni.
* Az Oracle adatbázis szolgáltatáshoz tartozó tenant szintű naplóállományokhoz az Oracle Enterprise Manager Cloud Controll-on, míg az MS SQL adatbázis szolgáltatás esetében az SQL Server Agent logokhoz Management Studio-n keresztül lehet hozzáférni.
* A perimeter eszköz naplóállományaihoz a kiegészítő szolgáltatásként nyújtott naplógyűjtés esetén a NISZ folyamatos, online hozzáférést biztosít a tenant számára. A javasolt megoldás a perimeter naplózásával kapcsolatban az elemzési szolgáltatás igénybevétele, amely esetén adott gyakoriságú (heti, havi) és biztonsági eseményhez kötött riportot (forgalmi, WAF, stb.) készít a NISZ a naplóelemzés eredményéről és az Ügyfél/Adatgazda IBF-e számára hozzáférhetővé teszi.

### Teljesítmény- és állapotfigyelés szolgáltatás

A tenant által használt gépek pillanatnyi teljesítmény- és állapot adatait (a gép fut-e, mekkora a CPU, memória, I/O terhelés) az önkiszolgáló ügyfélportálon publikáljuk. Ezen felül lehetőség van szolgáltatásként igénybe venni a saját alkalmazások és megoldások monitorozására az OMD (Open Monitoring Distribution) monitorozó szoftvert, melynek központi részét a NISZ üzemelteti.

Az OMD alapja a Nagios/Icinga monitorozó szoftver, melyet kiterjesztettek tenant képes működéssel. Az alkalmazás egy OMD agent által képes felderíteni az OS-ben futó szolgáltatásokat és rendszerállapot mutatókat. Az OMD adott ügyfélhez tartozó felületén az ügyfeleknek kell a saját monitoring pontjaikat adminisztrálni illetve felügyelni, NISZ ilyen szolgáltatást nem nyújt, az OMD központi részére vonatkozó hibabejelentést fogad és abban támogatást nyújt.

Az alkalmazás egy OMD agent által képes felderíteni az OS-ben futó (jellemző, azaz nem mindenre kiterjedő) szolgáltatásokat és rendszerállapot mutatókat.

### Webalkalmazás-tűzfal (WAF)

Az F5 perimeter eszköz beépítve tartalmazza az elterjedtebb általános web-alapú támadások például XSS, SQL Injection) elleni védelmet. A tenant adminisztrátora az önkiszolgáló ügyfélportálról beállíthatja, hogy ezt szeretné használni, vagy „tanuló” móddal felveszi az összes, a szolgáltatás által használt URL-t/HTTP headert, és ezekre szűkíti a perimeter eszköz által átengedett forgalmat, esetleg monitoring módot használ.

A WAF funkció egyéb módon (regexpekkel történő) beállítása Service Desk ticket segítségével, az üzemeltetéssel egyeztetve lehetséges.

A perimeter eszközön keletkező, a tenanthoz tartozó logokhoz való hozzáférést a NISZ a „3.5.8 Naplózási szolgáltatás” fejezetben leírtak szerint biztosítja. Lehetőség van ezen kívül a perimeter eszközön keletkező biztonsági eseményekről rendszeres, automatikus riportot igényelni a NISZ-től.

### Mentés szolgáltatás

A KAK Felhő által biztosított felhő alapú működési környezetben beállítható mentés mind komplett virtuális gép (image szintű mentés), mind agent alapú mentés formájában. A mentés DDT (disc-to-disc-to-tape) formában kerül megvalósításra. Terveink szerint az első szinten használt VTL biztosít annyi erőforrást – virtuális drive-ot és sávszélességet – hogy a bérlők megkötés nélkül legyenek képesek menteni, azaz nem szükséges egyeztetni felhő szinten a rendelkezésre álló mentőablakokról. A mentéseknek a VTL-ről a tape library-ba való ütemezését a NISZ végzi.

A NISZ a Felhőben IBM Spectrum Protect mentőszoftvert használ, mely rendelkezik tenant kezelési képességgel. A mentőszoftverben minden tenanthoz VTL fejek kerülnek dedikálásra. A mentési konfigurációk és a katalógusok elhatárolása szintén a Spectrum Protect-ben történik. Az agent alapú mentést a Spectrum Protect saját kezelő felületén (CLI vagy webes) tudja a tenant adminisztrátora beállítani és ütemezni, valamint itt képes visszaállítást is indítani. Az image alapú mentés ad hoc vagy ütemezett kezdeményezése az önkiszolgáló portál felületéről lehetséges

A mentési szolgáltatás két módon kerül megvalósításra:

* **támogatott mentés**: A bérlő az önkiszolgáló portál felületén megjelöli a mentendő szolgáltatásokat, amivel elfogadja, hogy minden további mentési beállítást a szolgáltató kezel, beleértve az ütemezést, a mentendő információk körét és mentési eljárást is. Ez érvényes a szolgáltató által támogatott felhőszolgáltatásokra (PaaS, DBaaS, SaaS), ahol a mentés működését mindvégig a szolgáltató felügyeli. A szolgáltató által menedzselt mentés agent és image alapon, illetve komplex szolgáltatások esetén ezek kombinációjával is történhet (lévén a szolgáltatónak a virtualizáció szintjén is megvan a hozzáférése).
  + Rendszeres mentés az önkiszolgáló portálon megjelölt példányokról történik, a szolgáltató által megjelölt időablakban. A példány mentésre való előkészítése ezen időszakra a bérlő feladata.
  + Az igény szerinti, ad-hoc mentések kezdeményezése is az önkiszolgáló portálon keresztül történik, és előbbihez hasonlóan a példány előkészítése ekkor is a bérlő feladata.
  + Az önkiszolgáló portálon keresztül kezdeményezett rendszeres és eseti mentések visszaállítása – különös tekintettel az image mentésekre – minden esetben bejelentés alapján történik.
  + A támogatott mentést és helyreállítást a NISZ biztosítja előre definiált RTO és RPO paraméterek mellett a szolgáltatás keretein belül.
* **egyedi mentés**: A kiegészítő mentési szolgáltatás igénybe vételével a bérlő az adott szolgáltatás kapcsán hozzáférést kap az IBM Spectrum Protect megfelelő agent alapú eszközeihez.
  + Az egyedi mentések kapcsán a mentés beállítása és ütemezése, a végrehajtás felügyelete teljes mértékben a bérlő felelőssége.
  + A mentést Spectrum Protect saját kezelő felületén (CLI vagy webes) tudja a bérlő adminisztrátora beállítani és ütemezni, valamint itt képes visszaállítást is indítani.
  + Az egyedi mentések és helyreállítások kapcsán a kívánt RPO és RTO értékeknek megfelelő eljárások beállítása és ütemezése a bérlő felelőssége.

Több felhőszolgáltatást érintő **konzisztens mentési** és **helyreállítási** **eljárás** kialakítása a bérlő feladata. Konkrét felhőszolgáltatás példányok kapcsán a bérlő bejelentés keretében kérheti a szolgáltató hatáskörébe eső mentések (image-k, egyéb) visszaállítását. A helyreállítást a szolgáltató minden esetben egyedi példányokon, és egymástól független eljárás keretében végzi. Ehhez illeszkedhet a bérlő saját egyedi mentéseinek helyreállítása és további konfigurációs lépések, amelyek kapcsán igénybe veheti a Spectrum Protect munkafolyamat szervezési támogatását (szkriptelési lehetőségeit). A bérlő alkalmazási rendszereinek indítása előtt a szoftver- és adat-konzisztencia megteremtése minden esetben a bérlő felelőssége. Ennek érdekében a NISZ az image alapú mentések visszaállítása esetén kikapcsolt virtuális gépeket ad át (az indítási sorrend betartása a Bérlő feladata), illetve az esetleges agent alapú mentések visszatöltésénél csak az adatok fájl szintű visszaállítását végzi el egy ideiglenes könyvtárba, az adatok betöltését például az adatbázisba nem, mert fenn áll a veszélye, hogy az üzleti logika ismerete nélkül a mentésből való visszaállítás során inkonzisztenssé válik a rendszer.

Napi riportok a tenant admin megadott email címére kerülnek kiküldésre, ami tartalmazza a sikeres és sikertelen mentések állapotát.

Egyéb mentési funkció - például dedikált kazettára írás, kazetta kivétele a robotból – nem része a NISZ szolgáltatásának.

### Archiválás szolgáltatás

Kéttípusú archiválási funkciót kínál a KAK Felhő:

* egy-egy kiválasztott mentés hosszú távú megőrzését, és
* API-t ahhoz, hogy az alkalmazások megvalósítsák saját archiválási funkciójukat.

Mindkét típusú archiválás kapcsán az infrastruktúra szintű háttérmegoldást a fent vázolt mentési szolgáltatásokhoz hasonlóan az IBM Spectrum Protect biztosítja.

Szolgáltatás vagy tárolási platform szintű, statikus archiválás

Törvényességi vagy egyéb funkcionális szempontoknak megfelelően szükség lehet teljes szolgáltatások, vagy akár a komplex alkalmazási rendszerek és kapcsolódó adatbázisok együttes állapotának hosszú távú, konzisztens és bizalmas megőrzésére. A bérlők számára a felhő ezt a típusú szintű archiválást az előző alfejezetben részletezett mentés analógiájára, teljes konfigurációk (adatbázis és alkalmazási platformok), adatbázisok vagy egyéb tárterületek teljes körű mentésének hosszú távú megőrzésével biztosítja. A mentés kapcsán részletezett megoldások és a felelősség elhatárolása lényegében az archiválás kapcsán is érvényesek.

Adat vagy objektum szintű, dinamikus archiválás

Tartós üzem következtében az alkalmazási rendszerekben felgyűlhetnek olyan adatok, amelyeket a napi használat során egyáltalán nem vagy csak nagyon ritkán érintenek a feldolgozások, viszont egyaránt terhelik az alkalmazás működését és az adminisztratív (pl. napi mentési) kapacitásokat. Jelentős költségmegtakarítást jelent az ilyen jellegű adatoknak a jóval olcsóbb tárolási eszközökre való mozgatása.

Amennyiben egyáltalán nem használatosak, akkor az adott adatkör valamilyen eszköz szintű elhatárolásával (pl. csak olvasható táblatérbe való leválogatásával) az adott szett az előző archiválási metódus szerint kompakt módon archiválható, és – akár későbbi fázisban - az alkalmazási környezetből eltávolítható (természetesen a törvényi és egyéb funkcionális igények szem előtt tartásával).

Amennyiben egyes passzív adatkörök, objektumok és dokumentumok, vagy komplett tranzakciók adatainak használatára csak ritkán kerül sor, akkor azok időlegesen eltávolíthatók a normál tárolási logikából. Mivel ilyen kisebb és lezárt adatkörök dinamikus ki és visszahelyezésére is szükség lehet, a felhő az alkalmazások ilyen jellegű programozható működését egy archiváló API hívással támogatja.

A dinamikus, adat szintű archiválás esetén az alkalmazásnak magának kell gondoskodnia arról, hogy képes legyen az adatok egy körében csak a meta adatokat / kumulált értékeket élő adatbázisban tartani, és a valós, ritkán használt adatokat a biztosított API-n keresztül lassabb elérésű tárolóra írni. Amennyiben hivatkozás történik ezekre az adatokra, szintén a biztosított API-n keresztül lehet visszaolvasni onnan. A szolgáltatás csak az archiválás technikai feltételeit biztosítja, az archiválás egyéb funkcióit az alkalmazói rendszernek kell biztosítania.

A bérlő egyéb szolgáltatásaitól függetlenül, a felhő az archivált adatok elérését egységesen a legmagasabb szintű, az 1. modellnek megfelelő rendelkezésre állással - a hívó szolgáltatás helyére transzparens módon - biztosítja.

### Adatbázis kiszolgáló szolgáltatás (DBaaS)

Az Adatbázis szolgáltatások PaaS szintű kiegészítő szolgáltatások, ezért általánosságban igazak rájuk a 3.2 fejezetben ismertetettek. Mivel az adatbázis szolgáltatás kiegészítő szolgáltatás,

* Szükséges egy olyan ellátási szolgáltatás elem megléte, amelyik igénybe veszi majd az adatbázis szolgáltatásait.
* Felhőn kívülre nem szolgáltatjuk.

A PaaS szintű szolgáltatásokhoz hasonlóan a DBaaS szolgáltatások esetén általánosan elmondható, hogy a NISZ által biztosított szintig az üzemeltetést a NISZ végzi. Ez azt is jelenti többek között, hogy a NISZ rendszeres, előre bejelentett, tervezhető időközönként telepíti a javítócsomagokat (patch) először a dev, teszt, oktatói környezetekben, majd az éles környezetben is. A NISZ csak egy stabil verziójú szoftver kiadást üzemeltet a különböző adatbázis szolgáltatásokban. Virtuális szervereken szolgáltatott DBaaS szolgáltatás (mongoDB, MariaDB, PostgreSQL) esetében amennyiben egy rendszer számára nem megfelelő a NISZ által üzemeltetett verzió, úgy lehetőség van a továbbiakban az adott szolgáltatást ellátó virtuális gépet átminősíteni IaaS szintre, melyet a bérlő maga is üzemeltethet vagy a NISZ Zrt.-vel az IaaS szint feletti részre külön üzemeltetési szerződést köthet. (Ennek egyedi ára várhatóan meghaladja PaaS szinten igénybe vett szolgáltatás árát.)

A fizikai infrastruktúrán nyújtott DBaaS szolgáltatások (Oracle, MS SQL) esetén nincs lehetőség az ilyen jellegű átminősítésre. Ezeknél a szolgáltatásoknál kötelező és egységes verzióváltás kerül kikényszerítésre, melyre a bérlő rendszereit időben fel kell készíteni és az új verziójú kiadásokat támogatniuk kell.

Az Oracle speciális, integrált adatbázis-kezelő és tároló rendszerén valójában nem is szoros értelemben vett DBaaS lesz kialakítva, mivel a bérlők az Oracle adatbázisok futtató környezetéhez is hozzáférést szereznek. A tervezett megoldás a szolgáltató hatáskörében az integrált eszköz klaszter funkcióit és az adattároló réteget (ASM-et) tartja meg, míg a bérlőknek IaaS-hoz közelítő lehetőségei és feladatai lesznek a konkrét adatbázispéldányok üzemeltetésében. Előbbiek miatt a DBaaS szolgáltatások kapcsán jelentős különbségek lehetnek a felügyeleti eszközök kialakításában és feladatkörök elhatárolásában.

*Az Oracle kivételével*, a többi szolgáltatás kapcsán elmondható, hogy - az alkalmazás-kiszolgáló PaaS szolgáltatásokhoz hasonlóan – a bérlő adminisztrátorának nem lesz operációs rendszer szintű hozzáférése. Így a „3.3 PaaS szintű ellátási szolgáltatások” alfejezetben leírtaknak megfelelően a futtató környezet karbantartása és felügyelete teljes körűen a szolgáltató kezében marad. Ekkor (*az Oracle kivételével*) a kapcsolódó egyéb szolgáltatások igénybe vétele (pl. NAS csatolása és a hozzáférések kiosztása) is a szolgáltató támogatásával, illetve a felhőmenedzsment portál felületén vagy bejelentés alapján történhet. Ahogy az adatbázisszerver végezhet strukturált állományokból való betöltéseket, illetve NAS-ra kimutatásokat tárolhat és publikálhat, ugyanúgy átmeneti állományokat is képezhet objektumtárból letöltött dokumentumok mentéséhez és archiválásához. Ezen állományok kezeléséhez a bérlőnek *nincsen az adott hoszton belül közvetlen kontrollja*, így az adott szerveren a konzisztens konfigurációk és állapotok agent alapú mentését sem végezheti sajátos intézkedések nélkül.

A felhőben biztosított mentés és archiválás, illetve helyreállítás kialakításának általános szempontjait a 3.5.11 Mentés szolgáltatás és 3.5.12 Archiválás szolgáltatás alfejezetek tartalmazzák. Mivel az archiválás - az utóbb hivatkozott alfejezetben vázoltak szerint – a mentéshez analóg módon valósul meg, az alábbiakban nincs külön részletezve.

#### Oracle adatbázis platform

Oracle adatbázis platformot a KAK Felhő, Oracle Exadata-n szolgáltat. A két telephelyen azonos méretű hardvereken, azonos számú Oracle Database Machine és Oracle Storage Server node-okból álló redundáns fürtök adják a fizikai erőforrásokat. A fizikai Storage szervereken telepített Oracle tároló virtualizációs megoldás fogja össze a tároló erőforrásokat, és egyúttal biztosítja az adatok node-ok közötti elosztott tárolásának és elérésének redundáns megoldását, magas rendelkezésre állását. A szolgáltatás szintű magas rendelkezésre állást (HA) az adatbázis kiszolgálókon (database machine) futó Oracle RAC klaszter, míg a két telephely közötti adattárolási redundanciát az Oracle Dataguard eszköz IP feletti aszinkron/szinkron replikációval biztosítja.

Az Exadata ASM rétegének üzemeltetése a NISZ végzi. Az ASM-et a NISZ a 3.2 fejezetnek megfelelően rendszeresen frissíti.

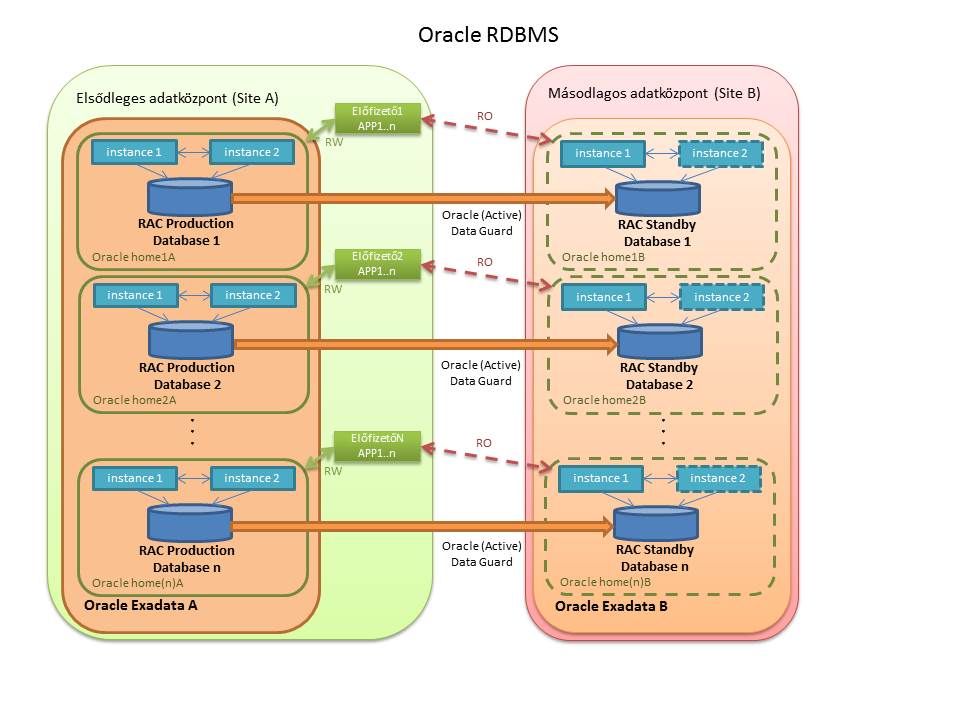
A több bérlős megoldást az Oracle RAC alatt bérlőnként elkülönített RDBMS futtató környezetekben (oracle home), szolgáltatásonként külön létre hozott Oracle adatbázisok jelentik, az alábbiak szerint:

* minden Oracle RAC node-on a felhasználás, rendelkezésre állás és karbantartás igényei szerint minden bérlő számára egy vagy több Oracle RDBMS futtató környezet telepítendő;
* egy Oracle RDBMS futtató környezet adja az alatta futó bérlői szolgáltatások számára az adatbázis-kiszolgáló rendszer szintű kereteit, amely több felhasználói adatbázis futtatását, egyben az adattárolás és elérés adatbázis szintű izolációját biztosítja;
* a teljes bérlői szolgáltatást az egyazon Oracle RDBMS adatbázishoz tartozó, - a szolgáltatás feldolgozási és a rendelkezésre állás igényei szerint - egy vagy több node-on párhuzamosan elindított, és az Oracle RAC fürtözési megoldáson keresztül összekapcsolt adatbázis-kiszolgáló példányok együttese alkotja;

Egy bérlői DBaaS szolgáltatás példány egy olyan Oracle RDBMS adatbázis, amely az egy-vagy több Oracle RAC node-on, külön adatbázis-kiszolgáló példányon keresztül elérhető az alkalmazások számára:

* minden bérlő saját oraclehome –al rendelkezik, saját oracle bináris környezettel, biztosítva a független patch–elés lehetőségét. Megjegyzés: a minimum és maximum patch szintet a NISZ által üzemeltetett ASM aktuális verziójának kompatibilitási mátrixa adja meg.
* a bérlők számára csak az adatbázis szintű hozzáférés biztosított (adminisztrátori (root) jogosultsággal operációs rendszerszintű elérés nem lehetséges);
* az adatbázis katasztrófatűrését (DR konfigurációját) az adott Oracle adatbázis telephely szintű aszinkron/szinkron, Oracle Dataguard replikációja határozza meg (a tartalék telephelyen működő aszinkron/szinkron fizikai standby adatbázis);
  + az Active Dataguard konfiguráció esetén a fizikai standby riportolási igényekre is felhasználható;

A fenti konfigurációt a lenti ábra szemlélteti.



Az Oracle mentése RMAN-on keresztül lehetséges IBM Spectrum Protect mentőrendszer segítségével. A Spectrum Protect TDPO modulja SBTAPI-n keresztül kommunikál az RMAN-nal, mely lefordítja az Oracle mentési utasításait.

Teljes, és inkrementális mentések online, és offline mentés esetében is a következőkre vonatkozhatnak:

-adatbázisok

-táblaterek

-adat fájlok

-arhiv logok

-control file-ok

Az IBM Spectrum Protect integrált eszközöket biztosít az Oracle adatbázisok különféle technológiákhoz és stratégiákhoz illeszkedő mentésére.

Az Oracle szolgáltatások kapcsán a mentés és archiválás lényeges jellemzői az alábbiak:

* mivel az adatbázisszerverek bérlői elhatárolása nem VM szinten történik, itt nincs image alapú mentés
* a bérlő számára minden megoldás elérhető az IBM Spectrum Protect integrált megoldásaival
* a DBaaS keretében működő adatbázisok point-in-time helyreállításához a IBM Spectrum Protect biztosít eszközöket, amely az adott platformhoz illeszkedő agent alapú megoldást jelent:
  + az IBM Spectrum Protect Oracle platformhoz integrált eszközei lehetőséget biztosítanak az adatbázisok teljes illetve inkrementális mentéséhez
  + az IBM Spectrum Protect-ben a tranzakció naplók rendszeres mentésére az előbbihez hasonlóan egy külön eljárást érhető el
  + a bérlő által készített mentések visszaállítására ugyancsak az IBM Spectrum Protect integrált eszközeivel van lehetősége
* az agent alapú megoldás két formában elérhető a bérlő számára
  + az Oracle RMAN mentés adminisztrációs eszközén keresztül (mivel az a fentebb vázolt módon az SP-hez van integrálva)
  + az IBM Spectrum Protect felületein keresztül
* a bérlő számára a konzisztens mentések szempontjából lényeges konfigurációs elemek (NAS könyvtárak, illetve egyéb állományok) is elérhetők operációs rendszer szinten, amelyek mentésére ugyancsak az IBM Spectrum Protect agent ad lehetőséget
* a konzisztens mentések végrehajtása minden esetben a bérlő felelőssége
* Oracle esetén – az operációs rendszeri hozzáférés miatt – a NISZ a „3.5.11 Mentés szolgáltatás” fejezerben ismertetett mentések közül csak az egyedi mentést szolgáltatja a NISZ, a támogatott mentést nem.

Az, hogy a két gépteremben található Oracle példányok között Data Guard segítségével kialakított DR megoldás illeszkedjen a 2.3.2 fejezetben ismertetett támogatott DR megoldások közé, a bérlő feladata és felelőssége. Az Oracle szolgáltatáshoz tarozó tenant napló állományokhoz az Oracle Enterprise Manager Cloud Controll-on keresztül lehetséges a hozzáférés.

#### Microsoft SQL adatbázis platform

Az MS SQL platform szolgáltatás futtatásához szükséges számítási erőforrásokat dedikált (rack-mount) szerverek, míg az adatok tárolására szolgáló tárterület a szerverekhez SAN (Storage Area Network) hálózaton keresztül csatolt külső, központi tároló egységek biztosítják.

A két telephelyen azonos méretű hardvereken, azonos számú dedikált szerverből álló adatbázis fürtök adják a fizikai erőforrásokat, amelyek közül minden esetben az elsődleges telephelyen futó (master) adatbázis példányok biztosítják az éles alkalmazások igényeit. A szolgáltatás szintű magas rendelkezésre állást és a katasztrófatűrő megoldást is a telephelyek között átnyúló MS SQL AOAG (AlwaysON Availability Group) fürtözési technológia adja.

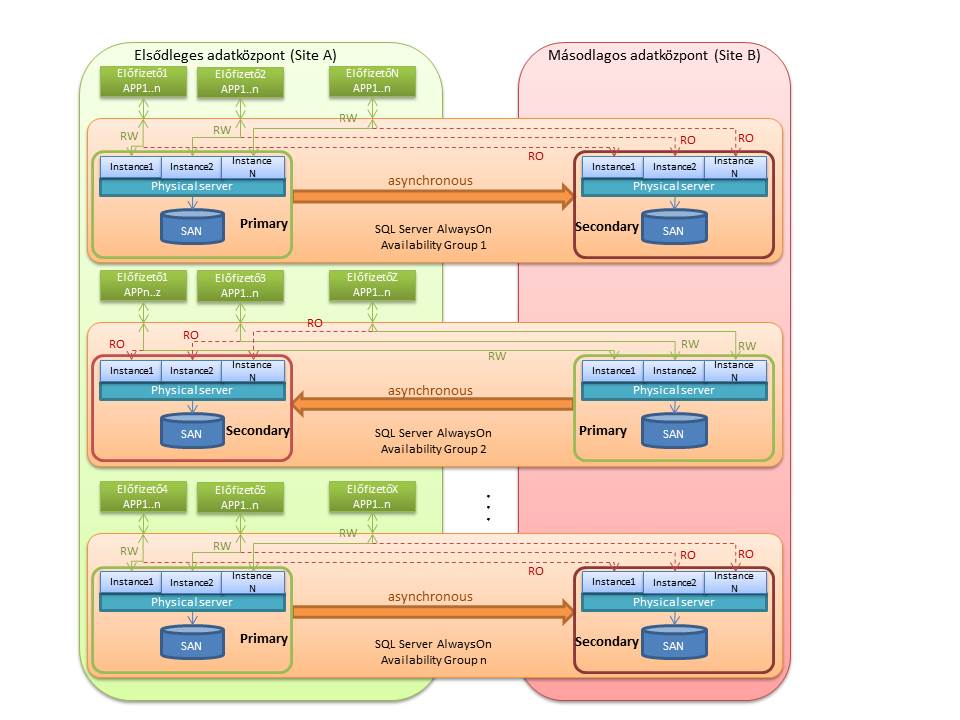
A bérlői DBaaS szolgáltatás egy fizikai szerveren kialakított MS SQL server istance:

* az adatok tárolása a SAN tárolókon történik,
* egy bérlő, több instace-t is bérelhet,
* a bérlő csak az általa bérelt MS SQL erőforrásokat éri el. Az operációs rendszert nem.
* a magas rendelkezésre állást (HA) és katasztrófa tűrést (DR) a kiépített „SQL Server AlwaysOn

Availability Group” biztosítja.

* A másodlagos (secondary) példány olvasási (RO) műveletekre elérhető lehet, így csökkentve az elsődleges (primary) példány leterheltségét.

A fenti leírást a lenti ábra szemlélteti.



Az SQL Server Agent Logokhoz hozzáférés biztosított Management Studio-n keresztül.

Az IBM Spectrum Protect integrált eszközöket biztosít az MS-SQL adatbázisok különféle technológiákhoz (Legacy, VSS) és stratégiákhoz illeszkedő mentésére. Az MS-SQL szolgáltatások kapcsán a mentés és archiválás lényeges jellemzői az alábbiak:

* mivel az adatbázisszerverek bérlői elhatárolása nem VM szinten történik, nincs image alapú mentés
* a DBaaS keretében működő adatbázisok point-in-time helyreállításához a IBM Spectrum Protect biztosít eszközöket, amely az adott platformhoz illeszkedő agent alapú megoldást jelent:
  + az IBM Spectrum Protect MS-SQL platformhoz integrált eszközei lehetőséget biztosítanak az adatbázisok teljes illetve inkrementális mentéséhez
  + az IBM Spectrum Protect-ben a tranzakció naplók rendszeres mentésére az előbbihez hasonlóan egy külön eljárást érhető el
* az agent alapú megoldás két formában elérhető a bérlő számára
  + a *támogatott* mentés beállítása és ütemezése a szolgáltató felelőssége
    - ebben az esetben is a felhőmenedzsment felületén kiválasztható, de nem biztosít a bérlő számára rugalmas ütemezési lehetőséget
    - az igény szerinti, ad-hoc mentés kezdeményezésére is van lehetőség
    - mindkét esetben a példány előkészítése a DBaaS-ek esetén is a bérlő feladata
    - a helyreállítás itt is bejelentés alapján történhet
  + a bérlőnek az adott példányok kapcsán *egyedi* ütemezésű, illetve egyéb kapcsolódó komponensekkel összehangolt mentések végrehajtására az IBM Spectrum Protect-en keresztül van lehetősége
    - ekkor sincs elérése operációs rendszer szinten, ezért a szolgáltató által biztosított eszközöket alkalmazhatja az IBM Spectrum Protect kezelő felületein
    - az általa vagy a szolgáltató által készített mentések visszaállítására ugyancsak az IBM Spectrum Protect felületén van lehetősége
* a bérlő számára a konzisztens mentések szempontjából lényeges konfigurációs elemek (NAS könyvtárak, illetve egyéb állományok) regisztrációja alapján azok agent alapú mentése a bérlő IBM Spectrum Protect tenant hozzáférésével lehetséges.
* a konzisztens mentések végrehajtása minden esetben a bérlő felelőssége

#### MariaDB és PostgreSQL RDBMS DBaaS szolgáltatások

A MariaDB és PostgreSQL adatbázis szerver platform bérlői szolgáltatásonként külön VM-eken települnek, így a szerver virtualizáció a szeparációt és a magas rendelkezésre állást is fizikai szinten biztosítja. A magas rendelkezésre állás és katasztrófa elhárítás követelményeit a platform szinten elérhető Multi-Master replikáció támogatja magasabb szinten. Minden bérlői szolgáltatás esetén - az igényekhez illeszkedően - több szinkron és aszinkron példány alkalmazható oldal irányú skálázás biztosítására, illetve a telephelyek közötti aszinkron replikációval a katasztrófa jellegű meghibásodások kezelésére.

* Külön VM-ként települ VMware-en vagy OpenStack-en,
* Szeparációt és a magas rendelkezésre állást is biztosítja,
* A bérlő csak az általa bérelt SQL erőforrásokat éri el, az operációs rendszert nem (DB admin jelszavát kapja meg, operációs rendszer root jogot nem),
* A menedzselés az adatbázis kezelők natív eszközeivel végezheti el, nem az önkiszolgáló portál felületére kivezetve,
* A lokális adatbázis naplókhoz – a PaaS szolgáltatásnál ismertetett módon – a bérlő hozzáfér.

DR szempontjából a példány létrehozásakor az ügyfél által, a 2.3.2 fejezetben ismertetett és támogatott DR megoldások közül kiválasztottaknak megfelelően kerül létrehozásra a környezet.

Az MariaDB és Postgres szolgáltatások kapcsán a mentés és archiválás lényeges jellemzői az alábbiak:

* mivel az adatbázisszerverek bérlői elhatárolása VM szinten történik, az image alapú, *támogatott* mentés a felhőmenedzsment önkiszolgáló felületén keresztül biztosított
  + ez a megoldás természetesen nem alkalmas sem több VM-en elosztott adatbázisok mentésére, sem point-in-time helyreállítások végrehajtására
  + a helyreállítás ebben az esetben is bejelentés alapján történhet
* a DBaaS keretében működő adatbázisok point-in-time helyreállításához a szolgáltató biztosít eszközöket, amely az adott platformhoz és konfigurációhoz illeszkedő agent alapú megoldást jelent:
  + az adatbázisok teljes illetve inkrementális mentését az adott platform és az IBM Spectrum Protect eszközeinek együttes alkalmazásával támogatja (közvetlen SP integráció hiányában az adatbázis eszközeivel a mentést ideiglenes állományokban letárolja, majd ezekre az SP fájl szintű mentését alkalmazza)
  + a tranzakció naplók rendszeres mentésére az előbbihez hasonlóan egy külön eljárást alakít ki
* az agent alapú megoldás két formában elérhető a bérlő számára
  + a *támogatott* mentés beállítása és ütemezése a szolgáltató felelőssége
    - ebben az esetben is a felhőmenedzsment felületén kiválasztható, de nem biztosít a bérlő számára rugalmas ütemezési lehetőséget
    - az igény szerinti, ad-hoc mentés kezdeményezésére is van lehetőség
    - mindkét esetben a példány előkészítése a DBaaS-ek esetén is a bérlő feladata
    - a helyreállítás itt is bejelentés alapján történhet
  + a bérlőnek az adott példányok kapcsán *egyedi* ütemezésű, illetve egyéb kapcsolódó komponensekkel összehangolt mentések végrehajtására az IBM Spectrum Protect-en keresztül van lehetősége
    - ekkor sincs elérése operációs rendszer szinten, ezért a szolgáltató által biztosított eszközöket alkalmazhatja az IBM Spectrum Protect kezelő felületein
    - az általa vagy a szolgáltató által készített mentések visszaállítására ugyancsak az IBM Spectrum Protect felületén van lehetősége
* a bérlő számára a konzisztens mentések szempontjából lényeges konfigurációs elemek (NAS könyvtárak, illetve egyéb állományok) regisztrációja alapján azok agent alapú mentése a bérlő IBM Spectrum Protect tenant hozzáférésével lehetséges.
* a konzisztens mentések végrehajtása minden esetben a bérlő felelőssége

#### MongoDB NoSQL DBaaS szolgáltatás

A MongoDB adatbázis szerver platform bérlői szolgáltatásonként külön VM-eken települ, így a szerver virtualizáció a szeparációt infrastruktúra szinten, és a magas rendelkezésre állást is alap szinten biztosítja. A magas rendelkezésre állás és katasztrófa elhárítás követelményeit a platform szinten elérhető replikációs megoldás támogatja. Minden bérlői szolgáltatás esetén - az igényekhez illeszkedően - több példány alkalmazható oldal irányú skálázás biztosítására, illetve a telephelyek közötti aszinkron replikációval a katasztrófa jellegű meghibásodások kezelésére.

Szolgáltatásonként több VM példány létesítése történik a DR modellnek való megfelelésnek megfelelően. A több példánynak a replikáción kívül az úgynevezett sharding funkciója is van, ez az adatbázisban tárolt adatok tárolásának valamely kulcs értékek mentén való partícionálása (a párhuzamos adatfeldolgozások minél nagyobb mértékű konkurenciájának kiszolgálására, oldalra történő skálázás).

A kiszolgálás célja szerint a MongoDB kérhető kétféle storage engine-nel:

* Perzisztens: az adatok tartós tárolásáról gondoskodni kell
* In-memory: az adatok kizárólag a memóriában kerülnek tárolásra

A lokális MongoDB logokhoz – a PaaS szolgáltatásnál ismertetett módon – a bérlő hozzáfér.

MongoDB mentése IBM Spectrum Protect segítségével történik. Mivel produktív környezetben a MongoDB replikát használunk, ebből adódóan a mentés a dedikált replikáról készül. A mentés első fázisában LVM snapshot készül a fájlrendszerről, mely tartalmazza a MongoDB fájlokat ( az adatbázis fájlok és a journal-ok ugyanazon a volume-on kell hogy legyenek), és az így létrehozott snapshot tömörítés után követően, mentésre (agent alapú) kerül IBM SP által.

Az MariaDB és Postgres szolgáltatások kapcsán a mentés és archiválás lényeges jellemzői az alábbiak:

* mivel az adatbázisszerverek bérlői elhatárolása VM szinten történik, az image alapú, *támogatott* mentés a felhőmenedzsment önkiszolgáló felületén keresztül biztosított
  + ez a megoldás természetesen nem alkalmas sem több VM-en elosztott adatbázisok mentésére, sem point-in-time helyreállítások végrehajtására
  + a helyreállítás ebben az esetben is bejelentés alapján történhet
* a DBaaS keretében működő adatbázisok helyreállításához a szolgáltató biztosít eszközöket, amely az adott platformhoz és konfigurációhoz illeszkedő agent alapú megoldást jelent:
  + az adatbázisok teljes mentését a MongoDB lehetőségeinek és az IBM Spectrum Protect eszközeinek (fent vázolt) együttes alkalmazásával támogatja
* az agent alapú megoldás két formában elérhető a bérlő számára
  + a *támogatott* mentés beállítása és ütemezése a szolgáltató felelőssége
    - ebben az esetben is a felhőmenedzsment felületén kiválasztható, de nem biztosít a bérlő számára rugalmas ütemezési lehetőséget
    - az igény szerinti, ad-hoc mentés kezdeményezésére is van lehetőség
    - mindkét esetben a példány előkészítése a DBaaS-ek esetén is a bérlő feladata
    - a helyreállítás itt is bejelentés alapján történhet
  + a bérlőnek az adott példányok kapcsán *egyedi* ütemezésű, illetve egyéb kapcsolódó komponensekkel összehangolt mentések végrehajtására az IBM Spectrum Protect-en keresztül van lehetősége
    - ekkor sincs elérése operációs rendszer szinten, ezért a szolgáltató által biztosított eszközöket alkalmazhatja az IBM Spectrum Protect kezelő felületein
    - az általa vagy a szolgáltató által készített mentések visszaállítására ugyancsak az IBM Spectrum Protect felületén van lehetősége
* a bérlő számára a konzisztens mentések szempontjából lényeges konfigurációs elemek (NAS könyvtárak, illetve egyéb állományok) regisztrációja alapján azok agent alapú mentése a bérlő IBM Spectrum Protect tenant hozzáférésével lehetséges.
* a konzisztens mentések végrehajtása minden esetben a bérlő felelőssége

### Adatközponti alap szoftver infrastruktúra szolgáltatások

Az adatközpontokban szokásos szoftver infrastruktúra elemek szolgáltatásait nyújtja a kialakított megoldás:

* SMTP szolgáltatás belső- vagy Internet felé küldendő levelezéshez,
* NTP szolgáltatás,
* DNS szolgáltatás.

DNS szolgáltatás alatt a következőket értjük:

* A Felhő a saját DNS-eiben bejegyzésre kerül egy privát TLD (.kak),
* Ennek egy aldomainjében minden virtuális gép kap egy automatikusan generált nevet (xy123.vm.kak),
* A tenant adminisztrátornak lehetősége van aldomaint regisztrálni, ami alá felveheti a saját bejegyzéseit (webszerver.sohivatal.kak),
* A tenanthoz tartozó publikus IP címekhez a tenant admin által megadott reverse DNS-t szolgáltatjuk,

## Üzleti szolgáltatásonként a hozzájuk rendelhető kiegészítő szolgáltatások táblázata

|  | Fix publikus IP cím | Objektumtár szolgáltatás | Tárhely | Fájlkiszolgáló (NAS) | Terheléselosztás | SSL terminálás, | Naplógyűjtés | Naplóelemzés[[2]](#footnote-3) | Teljesítmény- és állapotfigyelés szolgáltatás[[3]](#footnote-4) | Webalkalmazás-tűzfal (WAF) | Mentés, visszaállítás szolgáltatás[[4]](#footnote-5) | Archiválás szolgáltatás | Adatközponti alap szoftver-infrastruktúra szolgáltatások (NTP, DNS[[5]](#footnote-6)) | Adatközponti alap szoftver-infrastruktúra szolgáltatások (SMTP Gateway) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hosting | igen | nem | nem | nem | nem | nem | nem | nem | nem | nem | nem | nem | nem | nem |
| Virtuális gép | igen | igen | igen | igen | igen | igen | igen | nem | nem | igen | igen | igen | alapból kapja a szolg. | igen |
| Virtuális adatközpont | igen | igen | igen | igen | igen | igen | igen | nem | nem | igen | igen | igen | alapból kapja a szolg. | igen |
| Docker konténer | igen | igen | nem | igen | igen | igen | igen | nem | nem | igen | nem[[6]](#footnote-7) | nem | alapból kapja a szolg. | igen |
| Alkalmazás-kiszolgáló szolgáltatás/futtató környezet | igen | igen | igen | igen | igen | igen | igen[[7]](#footnote-8) | nem | nem | igen | igen | igen | alapból kapja a szolg. | igen |
| Adatbázis-kiszolgáló szolgáltatás (DBaaS) Oracle platform szolgáltatás | nem | nem | igen | nem | nem | nem | igen6 | nem | nem | NA | igen | igen | alapból kapja a szolg. | igen |
| Adatbázis-kiszolgáló szolgáltatás (DBaaS) Microsoft SQL platform szolgáltatás | nem | nem | igen | nem | nem | nem | Igen[[8]](#footnote-9) | nem | igen | NA | igen | igen | alapból kapja a szolg. | igen |
| Adatbázis-kiszolgáló szolgáltatás (DBaaS) Mongo DB NoSQL platform szolgáltatás | nem | nem | igen | nem | nem | nem | igen6 | nem | nem | NA | igen | igen | alapból kapja a szolg. | igen |
| Adatbázis-kiszolgáló szolgáltatás (DBaaS) MariaDB platform szolgáltatás | nem | nem | igen | nem | nem | nem | igen6 | nem | nem | NA | igen | igen | alapból kapja a szolg. | igen |
| Levelezés, csoportmunka[[9]](#footnote-10) | NA | nem | alapból kapja a szolg.[[10]](#footnote-11) | alapból kapja a szolg. | alapból kapja a szolg. | alapból kapja a szolg. | alapból kapja a szolg. | alapból kapja a szolg. | alapból kapja a szolg. | alapból kapja a szolg. | alapból kapja a szolg. | Igen | NA | NA |
| Dokumentumkezelé | igen | igen | igen | igen | igen | igen | igen[[11]](#footnote-12) | nem | nem | igen | igen | igen | alapból kapja a szolg. | igen |
| Tartalomkezelés (CMS) | igen | igen | igen | igen | igen | igen | igen10 | nem | nem | igen | igen | igen | alapból kapja a szolg. | igen |
| Oktatási keretrendszer (elearning) | igen | igen | igen | igen | igen | igen | igen10 | nem | nem | igen | igen | igen | alapból kapja a szolg. | igen |

## 

# Architekturális illeszkedés követelményei

Az újonnan kialakításra kerülő rendszereknek virtuális gépek horizontális bővítésével skálázhatónak kell lennie. A felhőben létrehozható maximális kapacitások virtuális gépenként:

|  |  |  |
| --- | --- | --- |
| Megnevezés | Igénylési egység | Maximálisan igényelhető |
| Virtuális processzor | 1 db | 16 db |
| Virtuális memória | 1 GB | 128 GB |
| Virtuális Tárhely[[12]](#footnote-13) | 50GB | Maximum 2 TB-os egységekben kiegészítő szolgáltatás keretében |

A kliens rétegben böngészőben futó webes alkalmazás elvárt. A rendszer biztosítson lehetőséget az adatok archiválásának megoldására.

A rendszer elemeinek minimálisan a következő rétegeket kell megkülönböztetnie:

1. *Megjelenítés:* Front-end szerver: Egy webszerver, ami az ügyféli felületet alkotó (statikus vagy dinamikusan előállított) weboldalakat szolgáltatja.
2. *Üzleti logika:* Alkalmazásszerver: Az alkalmazásszerver a dinamikus tartalmak előállítását és feldolgozását végzi. Tipikusan itt kapnak helyet a Java EE, PHP, ASP.NET, stb. alkalmazások.
3. *Perzisztencia:* Adatbázisszerver, Objektumtár, Fájlkiszolgáló: Az adatok tárolását és hozzáférését teszi lehetővé.

Elfogadható olyan megoldás is, ahol az üzleti logika réteg és a megjelenítés nem különül el külön szerverre.

Az alkalmazás szerver rétegben preferált a JVM, .NET, Python, és PHP technológiák valamelyikének alkalmazása.

A rendszernek Windows vagy gyártói támogatással rendelkező Enterprise Linux operációs rendszerek fölött kell működnie.

Kivételt képeznek a Docker konténerek, ezek belsejében alkalmazott „base” operációs rendszerre illetve a használt alkalmazás szerver technológiára nincs megkötés, viszont az üzemeltetés nem végez hibakeresést vagy hibaelhárítást a konténeren belül.

A skálázhatóság és a katasztrófatűrő architektúra egyszerű kialakítása miatt elvárt, hogy az alkalmazás szerver réteg adatot lokálisan ne tároljon. Adattárolásra csak adatbázis, és/vagy ObjectStore, és/vagy (nem preferáltan) NAS használata elfogadott.

A rendszerek a „3.5.13 Adatbázis kiszolgáló szolgáltatás (DBaaS)” fejezetben leírásra került adatbázisokat használhatják szolgáltatásként, vagy pedig IaaS felett kell a saját adatbázis megoldásukat megvalósítani.

Elvárás, hogy az olyan műveletek, amelyek adatbázis kezelőben nem valósíthatóak meg hatékonyan, arra felhő alapú, skálázható megoldást kell használni. Jellemző példa az adatbázisban történő szövegkeresés, amelyre léteznek horizontálisan skálázódó, felhőbe illeszthető kereső motorok is, mind kereskedelmi, mind ingyenes licenccel.

# Szakrendszer fejlesztőjének feladata és felelősségei

A Kormányzati Adatközpontba migrálandó szakrendszerek szempontjából a szakrendszer tulajdonosának feladata és felelőssége az alábbi elvek figyelembe vétele.

## Biztonsági besorolás meghatározása

A kormányzati adatközpont használata esetén az Ügyfél/Adatgazda feladata a 2013. évi L. törvény (Ibtv.) 7.§ (2) bekezdése alapján eljárni és rendszere bizalmasság, sértetlenség és rendelkezésre állás szempontjából történő, kockázatelemzésen alapuló biztonsági osztályba sorolása. A NISZ által nyújtott szolgáltatási szintig a biztonsági osztályra vonatkozó követelményeknek történő megfelelést a NISZ biztosítja. Az e feletti szintek esetében a követelmények teljesítése az Ügyfél/Adatgazda feladata és felelőssége.

A meghatározott biztonsági besorolás hatással lehet a rendszer architekturális kialakítására, a használt biztonsági megoldásokra és az SLA szintjére is. A KAK Felhő kialakítása a NISZ által nyújtott szolgáltatási szintig támogatja a legmagasabb, az 5-ös biztonsági osztályra előírt követelményeknek történő megfelelést, viszont a konkrét kialakítás során az Ügyfél felelőssége, hogy a rendelkezésre álló szolgáltatások felhasználásával elektronikus információs rendszerében milyen biztonsági megoldásokat alkalmaz.

A felhő architektúra sajátosságaiból adódóan a KAK Felhő által biztosított szolgáltatások tervezett tartalma szükségszerűen nem feleltethető meg minden egyes, a 41/2015. (VII. 15.) BM rendeletben foglalt védelmi intézkedésnek, emiatt ezekben az esetekben az adott szakrendszernek a biztonsági besorolása által elvárt követelmények maradéktalan teljesítéséhez szükséges biztonsági megoldás megvalósítása az Ügyfél felelőssége, illetve a szakrendszer fejlesztőjének a feladata. Ilyen, a KAK Felhő által önálló szolgáltatásként nem biztosított – több követelményben is érintett – védelmi intézkedés elem a többtényezős hitelesítés, valamint a kriptográfiai védelem.

A rendszer SLA szintjének meghatározása szintén az Ügyfél feladata, figyelembe véve a rendszer biztonsági besorolását is. Az Ügyfél felelős azért is, hogy a rendszer egésze alkalmas legyen a meghatározott SLA szinten való üzemelésre, a NISZ SLA-t az általa üzemeltetett szolgáltatásokra vállal.

## Vírusvédelem

A KAK Felhő vírusvédelmi szolgáltatást csak azoknál a szolgáltatás katalógus elemeknél biztosít, ahol ez külön említve van. Azon szolgáltatások esetében, ahol a KAK Felhő ezt nem biztosítja, a vírusvédelem megvalósítása az Ügyfél feladata.

## Közreműködés az infrastruktúra tervezésében, adatszolgáltatás

Adatszolgáltatás szükséges a szakrendszer fejlesztője részéről a központi felhőszolgáltató számára az alkalmazás informatikai infrastruktúrájának megtervezéséhez, az alábbiak tekintetében:

* + az alkalmazás komponenseinek azonosítása (pl.: alkalmazás szerverek, adatbázisok, local traffic manager-ek, címtárak stb.),
  + az alkalmazás VLAN-okra tagolódása,
  + egyéb rendszerekkel történő belső és külső kapcsolódás (interfészek),
  + virtuális gépek száma és paramétereik,
  + tároló kapacitási igény,
  + felhasználók tervezett száma (maximum illetve konkurens ügyfél),
  + rendelkezésre állás megvalósításának módja,
  + preferált hypervisor szolgáltatás,
  + alkalmazott operációs rendszerek, adatbázisok, alkalmazásszerverek,
  + mentési rend megadása, mentendő területek kijelölése,
  + fő alkalmazási funkciók, megoldások és tervezett technikai megvalósításuk.

A fent rögzített pontok alapján a központi felhőszolgáltató által megtervezett architektúra kapcsán a központi felhőszolgáltató és a szakrendszer fejlesztőjének megállapodása szükséges. A fejlesztés során a szakrendszer fejlesztőjének érvényesíteni kell a központi felhőszolgáltató által megtervezett architektúra folyományaként meghatározott alkalmazás szintű követelményeket.

Ügyfél feladata a szükséges szakrendszeri módosítások, fejlesztések megtervezése és kivitelezése, a felhőszolgáltatásokba való betelepülés eszközeinek megtervezése és kivitelezése, valamint a betelepülés szakrendszeri szintű forgatókönyvének összeállítása, a szolgáltatási szerződésben rögzítettek alapján esetlegesen a forgatókönyv tesztelése és végrehajtása az alábbiak szerint:

* + a betelepülés során alkalmazott eszközök, telepítési anyagok fejlesztői szintű tesztelése minden esetben az intézmény feladata,
  + az elfogadási tesztek, illetve betelepülés lépéseinek tényleges végrehajtása a felek közötti szolgáltatási szerződésben rögzített intézményi szakrendszer üzemeltetési és alkalmazástámogatási feladatainak függvénye.

## EWS csatlakozás

A felhő infrastruktúrát igénybe vevő alkalmazásoknak kötelező jelleggel kapcsolódniuk kell a Nemzeti Kibervédelmi Intézet által üzemeltetett Early Warning System (EWS) rendszerhez. Ennek keretében az NKI úgynevezett tapokat helyez el a felhő infrastruktúrában, melyek az egyes vlanok forgalmát elemzik anélkül, hogy megváltoztatnák azt. Az elemzés sikerének feltétele, hogy a tap titkosítás nélküli adatfolyamhoz kapcsolódhasson. Ez két módon lehetséges:

* amennyiben vlanon belül nincs titkosított forgalom, minden titkosított adatfolyam terminálása a perimeter eszközön történik, úgy az EWS csatlakozás feltételeit a NISZ biztosítja;
* ellenkező esetben a titkosítás nélküli adatfolyam átadása az NKI elemző rendszere felé a tenant bérlőjének feladata és felelőssége.

# A KAK Felhő bővítése

A KAK Felhő „befogadó” felhőként került megtervezésre, azaz a leginkább költséges rétegekben vendor lock-in nélkül bővíthető. Lehetséges integrálni mind újonnan beszerzett hardver elemeket, mind az esetleges felhőbe költöző régi alkalmazások alatti még használható számítási- és tárolási kapacitásokat.

A KAK Felhő a 1004/2016. (I.18.) Korm. határozat (A Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról) II. mellékletének 13. sorában nevesített szakrendszerek számára biztosít erőforrást, a következő módon:

* Biztosítja a szükséges hardver erőforrásokat
* Oracle DBaaS szolgáltatás esetén biztosítja az Oracle licenceket, a biztosított licencek a „6.7.2 Oracle” fejezetben kerültek felsorolásra.
* MS SQL DBaaS szolgáltatás esetén biztosítja a „6.7.1 Microsoft SQL” fejezetben meghatározott licenceket.
* A Felhő OpenStack lábán biztosít egy gyártói támogatással rendelkező Linux guest operációs rendszert a virtuális gépekhez (szerződéskötés után tudjuk pontosan specifikálni)
* Biztosítja a monitorozáshoz szükséges PVSR licenceket
* Biztosítja a naplógyűjtést és a naplóelemzést

Minden más komponenst, licencet (például operációs rendszer licenc, applikációs szerver licenc) a 1004/2016. (I.18.) Korm. határozatban nevesített beköltöző szakrendszernek kell biztosítani.

Amennyiben a beköltöző rendszer nem szerepel a felsorolásban, a megfelelő kapacitás biztosítása szükséges a futtatásához. A kapacitás biztosítás során az egyes rétegekben az alábbi fejezetekben felsorolt szempontokat és költségelemeket szükséges figyelembe venni.

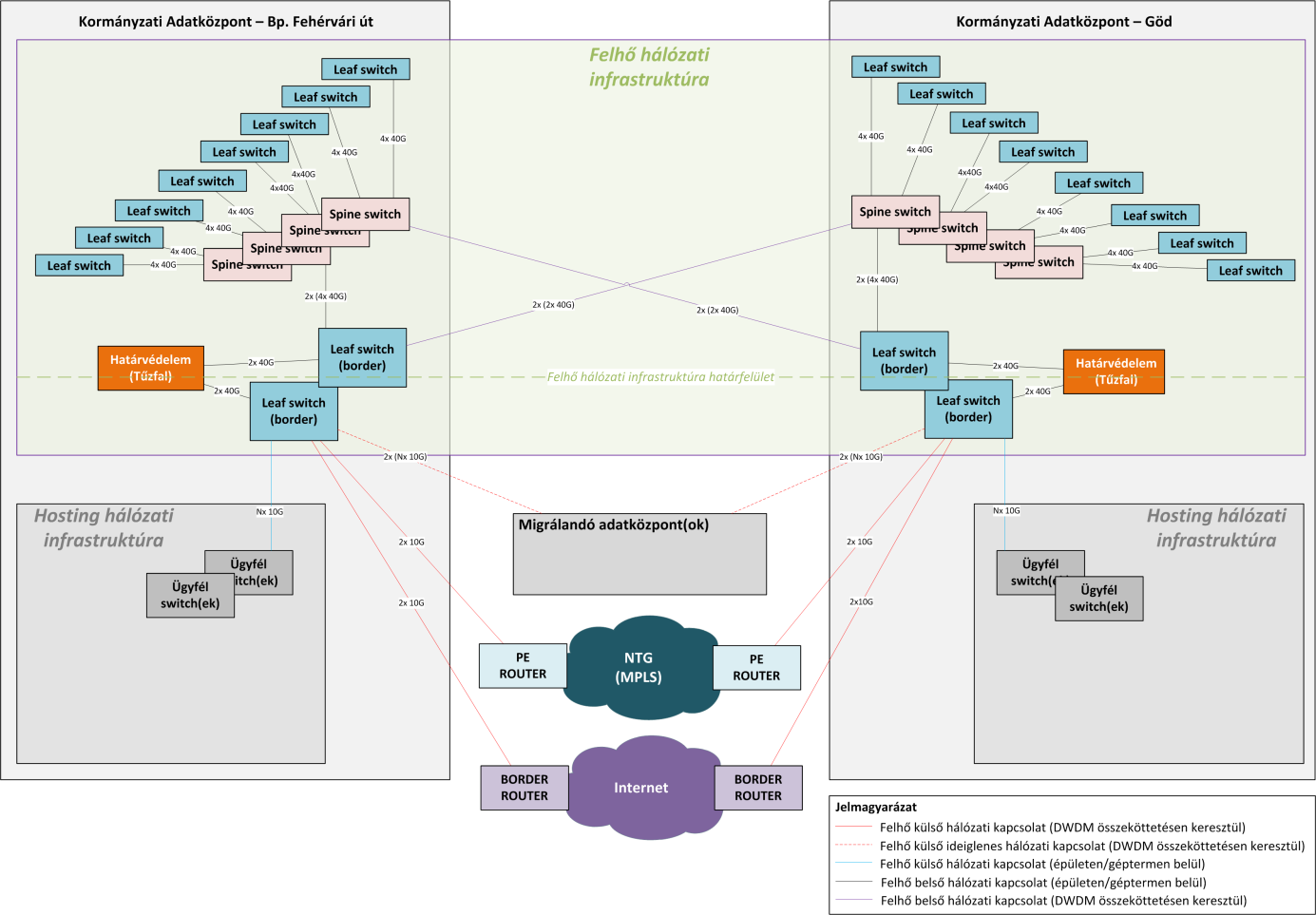
*Fontos megjegyezni, hogy a több rendszer konszolidációja során fellépő párhuzamos bővítések kiaknázásában (leverage effect) rejlő lehetőségek miatt nem szükséges minden beszerzést minden esetben elvégezni; a felhasználható szabad kapacitások ügyében minden esetben egyeztetni kell a NISZ-szel.*

Az adatközpontok elvárt kialakításából adódóan a bővítéseknek minden esetben a két telephelyen szimmetrikusan kell megtörténnie.

## WAN

Az adatközpont az NTG és az internet felöl is redundáns 20 – 20 Gbps-os kapcsolatokon keresztül érhető el. A teljes sávszélességen a KAK Felhő és a Hosting környezet osztozik. Mind a két adatközponti környezet esetén meg kell határozni, hogy az adatközpontba költöző rendszernek mekkora WAN irányú (NTG, Internet) hálózati sávszélességre van szükség, vagyis mekkora sávszélességgel lesz elérhető az NTG illetve az internet irányából.

A KAK Felhő környezet a fent említett külső irányokból előre definiált szabályok alapján, tűzfalon keresztül érhető el. Ebből adódóan a felhő infrastruktúrát hálózati szempontból kizárólag IP protokoll (L3 szinten) felett lehet elérni. Egy külső telephely és a KAK Felhő között L2 kapcsolat kiépítésére nincs lehetőség.



7. ábra KAK hálózati architektúra

## LAN

Az adatközponti LAN hálózat kétrétegű, Leaf & Spine architektúra szerint épül fel. A két adatközpont között redundáns 160Gbps összeköttetés biztosítja a kapcsolatot. Az ügyfél eszközei a Leaf rétegbe kapcsolódnak, ahol 48x 1/10GE portos switchek helyezkednek el, melyekhez GE (multimódusú optika, vagy rezes RJ45), vagy 10GE (multimódusú optika) interfészeken keresztül kapcsolódhatnak. Minden LAN hálózatba kötött kliens oldali eszköz esetén lehetőség van a kapcsolatokat két különálló fizikai switchben végződtetni, ez által biztosítva a hálózati redundanciát. A hálózati LAN szolgáltatás igénybevételéhez a kliens oldali interfészek típusának és számosságának függvényében az ügyfélnek kell biztosítania az adatközponti csatlakozáshoz szükséges hálózati (optikai vagy réz) portokat.

Abban az esetben, ha a Leaf rétegben nincs elégséges számú szabad port, akkor az ügyfélnek biztosítania kell az architektúra bővítését.

## Menedzsment hálózat

A NISZ által végrehajtandó infrastruktúra üzemeltetési feladatok ellátásához szükséges menedzsment kapcsolatait a produktív LAN hálózattól független (Out of Band) menedzsment hálózat szolgálja ki. A hálózat elemei 48x 10/100/1000 Mbps portos switchek, melyek RJ45-ös interfészeken keresztül biztosítják a menedzsment rendszerekhez való hozzáférést. Minden menedzsment hálózatba kötött eszköz esetén lehetőség van a kapcsolatokat két különálló fizikai switchben végződtetni, ez által biztosítva a hálózati redundanciát.

Abban az esetben, ha a menedzsment switchekben nincs elégséges számú szabad port, akkor az ügyfélnek gondoskodni kell a switchek bővítéséről.

## SAN

A NISZ két, a KAK telephelyein átnyúló fabric-et használ, amelyeket telephelyenként két-két központi SAN Director hajt meg. Amennyiben a tárolókapacitás új SAN eszközzel kerül bővítésre, vagy nem OpenStack alapú számítási kapacitás kerül beszerzésre, úgy a SAN directorok porttal, vagy kártyával és porttal történő bővítése szükségessé válhat.

A KAK Felhő-ben kizárólag 16Gbites SAN portokkal való bővítés lehetséges.

Abban az esetben, ha a SAN directorokon nincs elégséges számú szabad port, akkor az ügyfélnek gondoskodni kell ezek bővítéséről.

## Tároló kapacitás

### SAN alapú tároló kapacitás

A SAN alapú tároló kapacitás bővítésekor két lehetséges megoldás adódik:

* A meglevő tároló bővítése új diszkekkel, diszk polcokkal, esetleg szükség esetén backend és frontend directorokkal, illetve a diszkek használatba vételéhez és tükrözéséhez szükséges licencekkel.
* Storage virtualizáció segítségével az új tároló virtuális kapacitásként való bekötése a NISZ-szel történt szakmai egyeztetést követően lehetséges.

Amennyiben új tároló bekötése storage virtualizáció segítségével kerül kiválasztásra, a tárolóval szembeni minimális elvárások a következők:

* multipathing,
* redundáns működés (hibatűrő és terheléselosztó),
* legyen integrálható felügyeleti rendszerbe SNMP v3-n keresztül és saját menedzsment szoftverrel rendelkezzen)
  + teljesítménymonitorozás valós időben és historikusan
  + távoli menedzsment képesség
* teljes mértékben működjön együtt a tároló virtualizációs megoldással,
* RAID 1/5/6 támogatás,
* forró tartalék lemezek fiókonként vagy tömbönként (cross-spare) definiálhatók legyenek, vagy más technológiával kiválthatóak (pl.: wide-striping),
* kritikus hibapont nélküli (No-SPOF) architektúra,
* FC protokoll és interfészek kezelése,
* működés közbeni (hostolt rendszerek zavartalan működésével):
  + firmware/microcode/bináris upgrade a vezérlőkön és a lemezeken
  + konfigurációs változtatások a lemez kiosztás megváltoztatása
  + LUN migráció, Volume / LUN méret növelés
  + egyik kontroller cseréje
* infrastruktúra menedzsment eszköz biztosítása, legalább az alábbi képességekkel:
  + felügyelet és konfiguráció
  + infrastruktúra menedzsment
  + külső felügyeleti, monitoring rendszer felé kapcsolat lehetősége

### OpenStack tároló kapacitás

Az OpenStack tároló kapacitás bővítése két módon lehetséges:

* A meglevő tárolók bővítése új diszkekkel, diszk polcokkal, esetleg szükség esetén backend és frontend directorokkal, illetve a diszkek használatba vételéhez és tükrözéséhez szükséges licencekkel,
* új OpenStack kompatibilis eszköz üzembe állítása.

A második pont esetén az új eszköznek a következő kritériumoknak kell megfelelnie ahhoz, hogy probléma nélkül integrálható legyen az OpenStack környezetbe:

* Legyen lehetőség bizonyos területek site-ok közötti tükrözésére (DR védelem) aszinkron módon. A tükrözéshez rendelkezésre áll mind FC mind Ethernet interfész.
* A megoldás támogassa a NISZ által futtatott OpenStack kiadást,
* Legyen integrálható felügyeleti rendszerbe SNMP v3-n keresztül, valamint rendelkezzen saját menedzsment szoftverrel is. A menedzsment szoftver biztosítsa a következőket:
  + teljesítménymonitorozás valós időben és historikusan,
  + távoli menedzsment képesség,
  + felügyelet és konfiguráció,
  + infrastruktúra menedzsment,
  + külső felügyeleti, monitoring rendszer felé kapcsolat lehetősége,
* A tárolónak a host-ok felé történő kommunikációra iSCSI protokollal 10Gbit-es Ethernet hálózatot kell használnia.
* A tároló támogassa az NFS protokollt a hostok felé történő kommunikációra.
* A megoldás oldalanként redundáns felépítésű legyen a főbb alkotó elemeiben, azaz vezérlő, tápegység, adat utak a diszk dobozokhoz legyenek redundánsak,
* a tároló támogassa a thin/virtual provisioninget,
* a tároló támogassa a snapshot létrehozást teljesítményvesztés nélkül (vagy minimális teljesítményvesztéssel),
* audit log továbbítható legyen naplókiszolgálók felé,
* rendelkezzen Silent Data Corruption (SDC) elleni natív védelemmel,
* legyen lehetőség a 10Gbit-es hálózati portok későbbi bővítésére,
* támogassa az adatkötetek (volume/LUN) online mozgatását RAID set-ek között (terhelés újraelosztása),
* software és firmware frissítéseket szolgáltatás kiesés nélkül lehessen elvégezni mind array, mind diszk szinten,
* támogassa a Quality of Service-t tenant/volume/LUN/file szinten,
* adjon lehetőséget az adatok SSD rétegben történő cachelésére,
* a megoldásnak rendelkeznie kell OpenStack Cinder driverrel a NISZ által aktuálisan használt OpenStack verzióhoz, a driver által támogatott minimális funkcionalitás a következő:
  + Create Volume
  + Delete Volume
  + Attach Volume
  + Detach Volume
  + Extend Volume
  + Create Snapshot
  + Delete Snapshot
  + List Snapshots
  + Create Volume from Snapshot
  + Create Volume from Image
  + Create Volume from Volume (Clone)
  + Create Image from Volume
  + Volume Migration (host assisted)
* A tárolónak rendelkeznie kell a NISZ által az OpenStack blokkban használt kereskedelmi Linux hardver kompatibilitási tanúsítványával.

## Számítási kapacitás

A számítási kapacitást nagy teljesítményű blade szerverekkel, illetve az ezekhez tartozó blade keretekkel biztosítjuk. A KAK Felhő projektben összesen 32 core-os, 768GB RAM-mal ellátott pengék vannak használatban mind az OpenStack, mind a VMware blokkon belül. Az N+1 redundancia egyszerű biztosíthatósága érdekében a bővítés során hasonló paraméterekkel rendelkező pengék hozzáadása szükséges.

Amennyiben az OpenStack blokk kerül bővítésre, úgy a pengéknek és a keretnek redundáns, 2x10Gbit ethernet csatlakozással kell rendelkezniük; a VMware kapacitás bővítésekor redundáns 2x10Gbit ethernet és 2x16Gbit FC csatlakozás szükséges.

A fentieken kívüli minimum elvárások a blade kerettel szemben:

* A keretek penge befoglaló sűrűsége a lehető legnagyobb legyen (fizikai méret (U) / pengeszám), de ne igényeljen különleges, egyedi hűtést,
* rendelkezzen redundáns menedzsment modullal,
* rendelkezzen távoli menedzsment lehetőséggel a keretre és a pengékre,
* redundáns IPMI 2.0 menedzsment interfésszel rendelkezzen, a pengékre is használható módon.
* Redundáns, az összes szerverhelyet (slot) kiszolgálni képes legalább portonként 10 GbE Ethernet kapcsolót tartalmazzon, amely mindegyike támogatja a következő funkcionalitást:
  + Az összes üzembe helyezhető szerver beköthető 24x10 Gbps Ethernet sebességgel,
  + legalább 4 port 10 Gbps sebességű csatlakozási lehetőséget biztosít a külső eszközök eléréséhez, SFP+ multi modusú dual LC/LC vonali meghajtó (transceiver) fogadására képes.
  + Támogatja az IEEE 802.1Q VLAN szabványt, egy időben egyszerre legalább 1000 VLAN kialakítható,
  + támogatja az IEEE 802.3ad Link Aggregation szabványt,
  + SNMP-vel menedzselhető.
* Hot-plug képesség biztosítandó a pengékre, tápegységekre, ventillátorokra, IO interfészekre,
* tápellátás és a hűtés tekintetében teljes redundanciával kell, hogy rendelkezzen,
* nagy energiahatékonyságú tápegység (>90%) biztosítása szükséges,a keretben az I/O modulokat a teljes kiépítettségre kell kiépíteni és licencelni.
* Menedzselhetőség: távoli kiszolgáló menedzselhetőség biztosítása és a szükséges licencek szállítása.
* IPMI 2.0 protokoll támogatása szükséges,
* a keretben nem kitöltött penge helyeket megfelelő módon zárni kell, hogy a keret szellőzése hatékony maradjon.

Elvárások a pengeszerverekkel kapcsolatban:

* 2 CPU foglalatos, x86 architektúrájú pengeszerverek, Intel processzorral,
* egy szerverben 2 CPU, összesen legalább 32 core számítási erőforrás legyen, amelyhez programok, virtuális gépek rendelhetők. Csak fizikai core számítható be, logikai core nem.
* legalább 512GB ECC védett RAM, minimum DDR4 2133MHz-es DIMM sebesség,
* csatlakozási lehetőségek a kommunikációs infrastruktúrára (egymástól független, fizikailag dedikált csatornákkal),
* ***OpenStack esetén:*** Boot-oláshoz szükséges 128GB méretű SSD vagy SATA DOM modul,
* hálózati elérés (LAN) biztosítása legalább 2 db x 10Gbps pengénként, lehetőség biztosítása a hálózati csatoló virtualizálására, legalább 4 virtuális eszköz fizikai portonként,
* Menedzselhetőség: távoli kiszolgáló menedzselhetőség biztosítása és a szükséges licencek szállítása.
* IPMI 2.0 protokoll támogatás elvárt,
* a következő virtualizációs és operációs rendszerek támogatása, futtatási képessége:
* Hypervisor rétegek:
  + KVM, Hyper-V, VMware vSphere 6, XenDocker
* Operációs rendszerek:
  + Red Hat Enterprise Linux 6+
  + Suse Linux Enterprise 11+
* ***OpenStack esetén:*** A szervereknek rendelkeznie kell a NISZ által az OpenStack blokkban használt kereskedelmi Linux hardver kompatibilitási tanúsítványával.

A számítási kapacitás igénylésekor a bérlőnek szükséges az adott blokkhoz illeszkedő VMware illetve OpenStack licencek beszerzése is. OpenStack esetén a NISZ által az OpenStack blokkban használt kereskedelmi linux host és az unlimited guest licenc beszerzése is a bérlő feladata.

## Adatbázis farmok bővítése DBaaS szolgáltatás esetén

A KAK Felhő -ben az Oracle és MS SQL adatbázisok fizikai gépeken kerülnek futtatásra. Amennyiben ezek bővítésére van szükség, akkor az egyen szilárd architektúra megtartása érdekében a már a farmban levő gépek specifikációjához hasonló szerverekkel lehetséges.

### Microsoft SQL

A minimális elvárás az adatbázis szerverek felé:

* Forma: a megrendelő által biztosított rackbe szerelhető maximum 2U magas, 2 processzor befogadására alkalmas szerver,
* egy szerverben 2 CPU, összesen 16 core számítási erőforrás legyen, amelyhez programok, virtuális gépek rendelhetők. Csak fizikai core számítható be, logikai core nem. A szállítandó processzor: Intel Xeon E5-2667 v4, vagy ezzel egyenértékű. Az egyenértékűség feltétele, hogy az alábbi paraméterekben a megadott értéket vagy jobbat biztosítsa az egyenértékűként megajánlott termék:
  + Core szám: 8
  + CINT2006 Rates baseline: 886
  + CFP2006 Rates baseline: 737
  + Max Memory Bandwidth: 76,8 GB/s
  + Intel QPI Speed: 9,6 GT/s
* Memória: 512 GB RAM ECC minimum DDR4, memória bővítési lehetőség összesen 24 darab slotig.
* A konfiguráció a megadott memória méret kétszereséig memóriamodul csere nélkül bővíthető legyen.
* Beépített tárolók:
  + 1 darab RAID 10 tömb legalább 4 darab, minimum 400GB SSD lemezzel, és
  + minimum 1 db, legalább 1,3 TB kapacitású írás intenzív PCIe csatolós alkalmazás gyorsító kártya (ioMemory), az írási és az olvasási műveletek gyorsítására.
* Hardveres RAID vezérlő, adatvesztés ellen flash-el védett, minimum 2GB gyorsító tárral, a következő elvárásokkal:
  + 12Gb/s SAS technológia támogatása,
  + hagyományos (mechanikus) és SSD lemezek támogatása,
  + menet közbeni lemezcsere és új lemez fogadásának támogatása,
  + legalább a következő RAID szintek támogatása: 1, 10, 5, 50, 6, 60,
  + menet közbeni RAID szint átalakítás, tömb kibővítés
  + menet közbeni logikai kötet kiterjesztés és Stripe size migráció,
  + korlátlan Online spare lemez kijelölhetőség,
  + felhasználó által meghatározható olvasási/írási cache arány,
  + S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology) támogatás.
* Hálózati csatolók:
  + tároló csatlakozás (SAN-FC): csatlakozás legalább 2 db x 16 Gbps FC,
  + hálózati csatlakozás (LAN): legalább 4 db x 10Gbps SFP+ multi modusú dual LC/PC vonali meghajtó (transceiver) fogadására képes.
* Teljes körű távoli menedzsment biztosítása (grafikus képernyő átvételt is beleértve) „agent” nélkül, virtuális média használattal együtt.
* Menedzselhetőség: távoli kiszolgáló menedzselhetőség biztosítása grafikus felülettel, integrált távoli konzol, és virtuális média támogatás. Amennyiben a funkció biztosításához, valamilyen komponens szükséges, akkor az ajánlat részét kell, hogy képezzék, melyet az eszköz árába beleszámítva kell biztosítani**.** A menedzsment szoftver funkciói minimum a következő területeket fedjék le:
  + a szerver installációjának támogatása
  + szerverek monitorozása
  + esemény menedzsment (konfigurálható riasztási szintek)
  + teljesítmény menedzsment, amiben a CPU, memória, fájl rendszer és hálózati terhelések rögzítése megtörténik
  + preventív hiba beazonosítás, online diagnosztika
  + a szerverek RAID konfigurációjának menedzsmentje
  + teljesítmény (tápellátás) monitorozás és intelligens fogyasztás menedzsment
  + BIOS, Firmware frissítés lehetősége
  + a felhasználók (rendszergazdák) szerepkör szerinti megkülönböztetésének lehetősége
* Dedikált menedzsment port RJ-45 porton keresztül, minimum integrált 4GB flash memóriával amely támogatja a gépek távoli menedzsmentjét (IPMI 2.0 kompatibilis), grafikus elérést biztosít,
* A szervereknek rendelkeznie kell az alábbi szoftver verziók vagy újabb verziók hardver kompatibilitási tanúsítványával:
  + Operációs rendszerek:
    - Microsoft Windows Server 2012+
    - Red Hat Enterprise Linux 6+
    - Suse Linux Enterprise 11+
* Tápellátás: redundáns kialakítású, működés közben cserélhető (hot-plug), minimum 750W, minimum 96% hatékonyságú tápegység, ami a teljes kiépítettség esetén is biztosítja egy tápegység kiesése esetén a működést, „80 Plus Titanium” minősítésű tápegységekkel.
* Hűtés: Hot-plug hűtő ventilátor (N+1 redundanciával).
* A rack szervereket beépítő kerettel, sínnel és kábelvezetővel szükséges szállítani.
* Egy szerver csatlakoztatásához szükséges kábelek:
  + 4 darab 15m LC/LC OM4 patch kábel
  + 2 darab 10m LC/LC OM4 patch kábel
  + 1 darab 15m 1 Gbps Ethernet Cat6 UTP patch kábel

A fizikai bővítés mellett a bérlőnek kell a szükséges az operációs rendszer, illetve az MS SQL megfelelő licencbővítésről is gondoskodni a következő licencek beszerzésével:

* Microsoft Core Infrastructure Server Standard + SA
* Microsoft SQL Server 2016 Enterprise

### Oracle

Az Oracle Exadata X6-2 bővítése szükséges további számítási illetve tárolási kapacitással, illetve a szükséges mennyiségű Oracle licenccel. Licencekből a következők beszerzése szükséges adatbázis szerver bővítése esetén:

* Oracle Database Enterprise Edition - Processor Perpetual
* Oracle Real Application Clusters - Processor Perpetual
* Oracle Diagnostics Pack - Processor Perpetual
* Oracle Partitioning - Processor Perpetual
* Oracle Tuning Pack - Processor Perpetual
* Oracle Cloud Management Pack for Oracle Database - Processor Perpetual
* Oracle Database Lifecycle Management Pack - Processor Perpetual
* Oracle Advanced Security - Processor Perpetual
* Oracle Active Data Guard - Processor Perpetual

Szükséges licencek storage node bővítése esetén:

* Exadata Storage Server Software - Disk Drive Perpetual

## Szükséges licencek

A bővítés során fellépő egyéb licenc szükségletek az alábbi fejezetekben található:

### Felhő automatizálási rendszer licencek

A NISZ által használt felhő automatizálási rendszer licencekkel való lekövetése. A pontos típus és licenc kérdések a későbbiekben kerülnek publikálásra.

### Virtuális gépek licencei

A NISZ nem biztosít operációs rendszer, vírusirtó, alkalmazás kiszolgáló, illetve egyéb, a virtuális gépeken futó szoftver licenceket.

Ez alól kivétel az OpenStack blokkban a használt kereskedelmi Linux operációs rendszer (a pontos típust szerződés kötés után tudjuk definiálni), melyből az OpenStack felett korlátlan számú futtatható.

### Támogató rendszerek licencei

A szolgáltatások nyújtásához kapcsolódó támogatóeszköz licenszeket (jegykezelő, konfigurációmenedzsment, számlázási rendszerek, stb.) a szolgáltatások egységárai tartalmazzák. Ezzel kapcsolatos beszerzési szükséglet nem terheli a Megrendelőt.

# Kormányzati hoszting szolgáltatás

## Szolgáltatás általános ismertetés

A szolgáltatás célja, hogy lehetőséget biztosítson a Bérlők számára saját informatikai eszközök elhelyezésére a Szolgáltató által működtetett géptermekben.

A TIER-3-as követelményeknek megfelelő adatközpont nagybiztonságú fizikai és műszaki üzemeltetési környezetet biztosít a kijelölt eszközök számára. Megrendelőnek lehetősége van akár kéthelyszínes elhelyezést is kérni (például rendkívüli, előre nem látható esemény esetén történő működésképességének Bérlő saját hatáskörében történő fenntartása céljából).

A szolgáltatás részét képezi a Megrendelő központi kiszolgáló informatikai eszközeinek a Szolgáltató által biztosított géptermi létesítményben történő elhelyezése és megfelelő fizikai környezet biztosítása. Igény esetén Szolgáltató operátori asszisztenciát nyújt a Bérlőnek. Az elhelyezés bérleti konstrukcióban történik, amelyhez kapcsolódóan az elszámolás az elfoglalt hely és energia fogyasztás alapján történik.

## Fizikai biztonsági környezet jellemzői

Központi infrastruktúra elhelyezése:

* egy vagy kéthelyszínes,
* folyamatosan monitorozott, redundáns kiépítettség, állandó hőmérsékletet és páratartalmat biztosító klimatizált,
* normál vagy EM védelemmel ellátott, (kiemelt EM védelemmel ellátott, csak igazoltan minősített adatok esetén)
* két független forrásból történő tápellátással rendelkező, dízelgenerátorral támogatott szünetmentes áramellátás mellett üzemelő,
* korszerű, automata jelző és oltó rendszerekkel ellátott,
* élő erővel, kamerával és fizikai védelemmel védett géptermi környezetben történik.

Igény esetén, külön kérésre, ennek pénzügyi vonzatát is figyelembe véve, eseti jellegű mérlegelés mellett és a fizikai lehetőségek figyelembe vételével lehetőség van a géptermi területi fizikai lehatárolására.

## Szolgáltatások megvalósításának műszaki feltételei

* A Hosting hálózati szolgáltatáshoz internet és NTG elérés tartozik, melyet telephelyenként – a redundancia miatt – két 1/10GE porton keresztül lehet igénybe venni. A szolgáltatáshoz nem tartozik LAN, SAN, illetve tűzfal szolgáltatás sem, így a Bérlőnek kell gondoskodnia a rendszerelemek (szerverek, tárolók, …) etherntes és FC portjainak aggregációjáról, illetve a teljes rendszer adatforgalmának felügyeletéről, beleértve a felügyeleti forgalmat is.
* NTG szolgáltatás igénybe vételekor alapesetben a Bérlő hosting környezetéhez közvetlenül kapcsolódó Border Leaf eszköz lesz a CE router, melynek üzemletetését a NISZ fogja ellátni. Amennyiben a Bérlő saját maga szeretné a CE funkcionalitást üzemeltetni, abban az esetben a saját CE router beszerezéséről magának kell gondoskodnia.
* Kéthelyszínes elhelyezés esetén, a telephelyeken felépített környezetek összekapcsolása és az adott rendszerre vonatkozó kapcsolatok kiépítése a Bérlő feladata. A két helyszín között hálózati szempontból az NTG-én kizárólag IP protokoll (L3 szinten) feletti kapcsolat építhető ki. Amennyiben a Megrendelőnek a két telephely között Ethernetes (L2 szint) vagy natív FC kapcsolatra van szüksége, az bérelt vonalon (sötét szál) keresztül valósítható meg.
* A Hosting szolgáltatáshoz nem kapcsolható egységes központi naplózás, rendszerfelügyelet. Ezeket a Bérlőnek a saját eszközei segítségével kell megvalósítania.

## Géptermi környezet

### Eszközök elhelyezése

Eszközök gépterembe történő elhelyezése a következő két módon valósítható meg:

1. Bérlő által biztosított szabványos méretű, 600 mm x 1200 mm alapterületű, 47U magas rackszekrény elhelyezés (rackszekrény hely db)
2. Az eszközöket a géptermekbe beépített rack szekrényekbe lehet elhelyezni a lentiek szerint:
   * Kialakítás: rack szekrények hideg zárt rack folyosóban
   * Rendelkezésre állnak 600 mm x 1200 mm alapterületű, 47U magas rack-szekrények (rackhely unit db)
   * legalább 10-15% szabadon hagyott, beépíthető kapacitás (például 47 U magas szekrénynél 6-10 U szabadon kell, hogy maradjon, a beszerelési tervben ezt figyelembe kell venni)

* Rack-szekrényenként lehetőleg azonos kategóriájú termékek kerüljenek csak pl.
  + penge keret és penge szerverek
  + tároló

### PDU-k csatlakozása

PDU-k csatlakozását a terv szerinti eszköz eloszlás alapján, bérlő biztosítja az alábbiak szerint

* *csatlakozás az ellátó-hálózathoz minden esetben:*
  + EN 60309 32A 3 PH (IEC309 32A 3 fázis) (2 db/ rack, lehetőség 2 \* 2 db/rack)
* belső elosztás *javaslat:*
  + IEC320 C19 (anya) – nagyobb teljesítményű eszközökhöz, ahol indokolt
  + IEC320 C13 (anya)
* rack-szekrényenként a beszerelési terv alapján elhelyezett eszközöknek megfelelő mennyiségű aljzat (PDU)
* redundáns elosztás minden rack-szerkényben.

### Redundáns elektromos energia ellátás

Olyan villamos energia ellátás, amely mögött többpontos energia ellátás és vészenergia megoldások állnak rendelkezésre (generátor, akkumulátor).

Az elhelyezett eszközök tápellátását Szolgáltató biztosítja:

* Szünetmentes 230 V AC +/- 10%
* 50 Hz +/- 5%
* Teljesítményfelvétel: átlagosan 6 kW/ 47U (rack) , (egyedi esetekben maximum 12 kW)

A tápellátás szabványos 230/400 V váltakozófeszültségű hálózatról történik

### Klimatizálás

Az elhelyezett eszközök hűtését a Szolgáltató biztosítja:

Hőmérséklet tartomány:

* működési: 0 …… 40 C
* tárolási: -20 ….. +60 C

Páratartalom: max. 95% lecsapódásmentesen.

A hűtési igény nem haladhatja meg a rack-szekrényenként a 12 kW (egyes esetekben a 16 kW-t).

1. Mivel a Felhő bizonyos részeire unlimited guest licenc is beszerzésre kerül, az operációs rendszer tekintetében a többszörös licencelést elkerülendő egyeztetni szükséges a NISZ-szel. [↑](#footnote-ref-2)
2. Biztonsági napló állományok gyűjtését és elemzését a NISZ üzemeltetési szintjéig alapból magában foglalja a szolgáltatás. Hozzáférés a megrendelő számára a Naplóelemzési részben részletezettek szerint történhet. [↑](#footnote-ref-3)
3. Kizárólag alapinformációk biztosít a kiegészítő szolgáltatás, amely a szolgáltatás saját dashboard-ján jelenik meg. [↑](#footnote-ref-4)
4. Mentéssel kapcsolatos bővebben információkat lásd jelen dokumentum adott fejezetében [↑](#footnote-ref-5)
5. Névfeloldási szolgáltatás mellett Megrendelőnek lehetősége van saját domain név regisztrációra NISZ Ellátási szolgáltatáskatalógusában részletezett módon. Emellett saját lokális sub-domain név hozzárendelés történik. [↑](#footnote-ref-6)
6. A docker konténer állapotmentes, így mentésre nincs szükség. Alternatívaként tárhely alapú kiegészítő szolgáltatásokra lehet felhasználói paraméterezéssel mentéseket elhelyezni [↑](#footnote-ref-7)
7. Megjegyzés: Megrendelő korlátozott ideig a lokális naplókhoz hozzáfér jelen kiegészítő szolgáltatás nélkül is [↑](#footnote-ref-8)
8. Megjegyzés: Naplógyűjtés feltételeiről és hozzáférhetőségéről jelen üzleti szolgáltatás részletes leírásában találhatóak információk [↑](#footnote-ref-9)
9. Jelen szolgáltatások esetén az „alapból adja a szolg.” megjegyzés a NISZ üzemeltetési felelősségi körbe tartozóan a NISZ üzemeltetés számára nyújtja a kiegészítő szolgáltatást. Megrendelőnek nincs hozzáférése. [↑](#footnote-ref-10)
10. A megrendelt mennyiségű szolgáltatáshoz szükséges (block device alapú) tárhely kerül hozzárendelésre. Megrendelő a tárhelyhez nem fér hozzá közvetlenül. Igény esetén ticket alapon kell kérnie. [↑](#footnote-ref-11)
11. Megjegyzés: Megrendelő korlátozott ideig a lokális naplókhoz hozzáfér jelen kiegészítő szolgáltatás nélkül is. [↑](#footnote-ref-12)
12. A virtuális gép OS tárhelye (disk) nem módosítható (Linux operációs rendszer esetén 30GB, Microsoft Windows esetén pedig 128GB) [↑](#footnote-ref-13)