

Nagy rendelkezésre állású web hoszting, föderációs hitelesítéssel

Molnár Péter
molnarp@niif.hu

NIIF

2016. március 31.



- ▶ Biztonság
- ▶ Egyszerűség
- ▶ Kényelem
- ▶ Föderáció támogatása
- ▶ Teljesítmény, skálázódás, magas rendelkezésre állás: *fürtözés*

Web hoszting

Az NIIF webhoszting backend

Föderációs hitelesítés

3S: Saml, Shib, Ssp

Nagy rendelkezésre állás

Linux Virtual Server



Következik

Web hoszting

Az NIIF webhoszting backend

Föderációs hitelesítés

3S: Saml, Shib, Ssp

Nagy rendelkezésre állás

Linux Virtual Server



Linux-Apache-MySQL-PHP

- ▶ Linux 3.2
 - ▶ Debian alapok
 - ▶ ansible-el telepített és karbantartott
 - ▶ egyforma VM-ek
- ▶ Apache 2.2
 - ▶ mod-fcgid
 - ▶ mod-shib2
- ▶ Adatbázis kiszolgáló
 - ▶ MySQL
 - ▶ MariaDB előkészületben
 - ▶ RAID10-be épített SSD lemeztömb
- ▶ PHP 5.4
 - ▶ php5-mysql



Feltöltés

- ▶ SFTP kapcsolat
- ▶ Állományrendszer jogok

```
    /.....chroot
├── etc
├── log..... APACHE NAPLÓK
├── include -> protected/include
├── protected..... ÍRHATÓ SFTP-N
│   ├── include
│   ├── tmp
│   └── www..... WEBROOT
├── tmp -> protected/tmp
└── www -> protected/www
```



Biztonság

- ▶ Külön site és apache felhasználó
- ▶ MySQL külön felhasználó
- ▶ Központi, LDAP hitelesítés
- ▶ NFS, *root_squash*
- ▶ Futtatás *chroot*-al
- ▶ Futtatás külön felhasználóval *suexec*-el
- ▶ Nincs SSH shell
- ▶ Tűzfal *iptables*-szel
 - ▶ Kifelé nem engedélyezünk kapcsolatot alaphelyzetben
 - ▶ Felhasználónként külön szabályok



Teljesítmény

- ▶ Fcgi tuning: memória szivárgás, túlterhelés ellen

Folyamatok kezelése Apache példányonként

- ▶ Maximális folyamatszám
- ▶ Folyamat létrehozási gyakoriság

Folyamatok kezelése VirtualHost-onként

- ▶ Min-max folyamatszám
- ▶ Kiszolgált kérések maximális száma
- ▶ Tétlen folyamatok megszüntetése
- ▶ Sokáig futó folyamatok megszüntetése
- ▶ Maximális folyamat élettartam

- ▶ Sulinet webmail teljesítmény: kb. 200000 kérés egy nap



Következik

Web hoszting

Az NIIF webhoszting backend

Föderációs hitelesítés

3S: Saml, Shib, Ssp

Nagy rendelkezésre állás

Linux Virtual Server

Apache



Minden webnode-on azonos beállítások és munkamenet állapot szükséges

Két lehetséges Single-Sign-On irány

- ▶ Alkalmazásonként külön SAML kezelés és SP implementáció (vagy más SSO)
- ▶ A webkiszolgálóra bízni (például: apache2-mod-shib, mod-wsgi)

Shibd



Minden webnode-on azonos beállítások és munkamenet állapot szükséges

- ▶ MySQL, PostgreSQL, Oracle, MSSQL sessionstore
- ▶ A megvalósítás unixODBC alapú¹

¹<http://www.unixodbc.org>



Shibd beállítása

/etc/shibboleth2.xml részletek:²

```
1 <SPConfig xmlns="urn:mace:shibboleth:2.0:native:sp:config">
2   ...
3   <OutOfProcess>
4     <Extensions>
5       <Library path="odbc-store.so" fatal="true"/>
6       <Library path="plugins.so" fatal="true"/>
7     </Extensions>
8   </OutOfProcess>
9   ...
10  <StorageService type="ODBC" id="db" cleanupInterval="900">
11    <ConnectionString>
12      DRIVER=MySQL;SERVER=$host;UID=$user;PWD=$pw;DATABASE=$db;APP=Shibboleth
13    </ConnectionString>
14  </StorageService>
15  <SessionCache type="StorageService" StorageService="db" cacheTimeout="3600"
16    inprocTimeout="900" cleanupInterval="900"/>
17  <ReplayCache StorageService="db"/>
18  <ArtifactMap StorageService="db" artifactTTL="180"/>
19  ...
20  <Sessions postData="ss:db" relayState="ss:db" ... >
21  ...
```

Megjegyzés: a szükséges táblákat létre kell hozni előre.

²<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPODBCStorageService>



Felmerült problémák

Debian 7 (wheezy) és 8 (jessie) rendszereken futottunk bele megbízhatósági gondokba.

- ▶ Véletlenszerű összeomlások történtek a shibd esetén.
- ▶ A *unixodbc* frissítésre szorult.
- ▶ 2015. augusztusban megjelent 2.3.3-as verzió már stabilan működik.
- ▶ A deb csomagot magunk építettük.

Következik



Web hoszting

Az NIIF webhoszting backend

Föderációs hitelesítés

3S: Saml, Shib, Ssp

Nagy rendelkezésre állás

Linux Virtual Server



Linux Virtual Server működése

Mi az LVS?

- ▶ IP terhelés elosztó
 - ▶ Nagy rendelkezésre állású kiépítés lehetséges
-
- ▶ Aszimmetrikus forgalom
 - ▶ Nat
 - ▶ Tunnel
 - ▶ Direct routing
 - ▶ Súlyozott round-robin választás



Linux Virtual Server NAT

A publikus, szolgáltatás elérési cím és a valós kiszolgálók között címfordítás megvalósításával.

- ▶ Teljes forgalom áthalad a terheléelosztón.
- ▶ A valós kiszolgáló lehet más hálózati szegmensben is.
- ▶ Belső címek használhatók.
- ▶ Bármilyen TCP/IP-t ismerő operációs rendszer.
- ▶ Egy-két tucat csomópontig.
- ▶ Jelentékeny rendszer-erőforrást használ a címfordítás.



Linux Virtual Server IP Tunnel

IP alagút a terheléelosztó és a valós kiszolgálók között.

- ▶ Teljes forgalom áthalad a terheléelosztón.
- ▶ Némi hálózati overhead.
- ▶ Több, mint 100 valós kiszolgálóig.
- ▶ A kiszolgálónak ismernie kell az IP Tunneling-et.
- ▶ Bárhol a hálózatban.
- ▶ Nagy teljesítmény.
- ▶ Sok valós kiszolgálóval is működik.



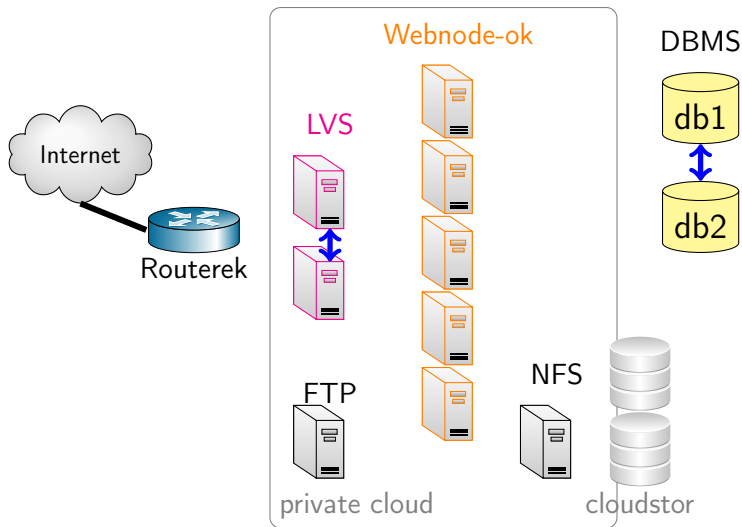
Linux Virtual Server Direct Routing

A forgalom aszimetriájának kihasználása.

- ▶ Direct routing
- ▶ A forgalom csak az ügyfél -> kiszolgáló része (tipikusan kérések és ACK)
- ▶ Közös L2 szegmens
- ▶ Nagy teljesítmény.
- ▶ Sok valós kiszolgálóval is működik.

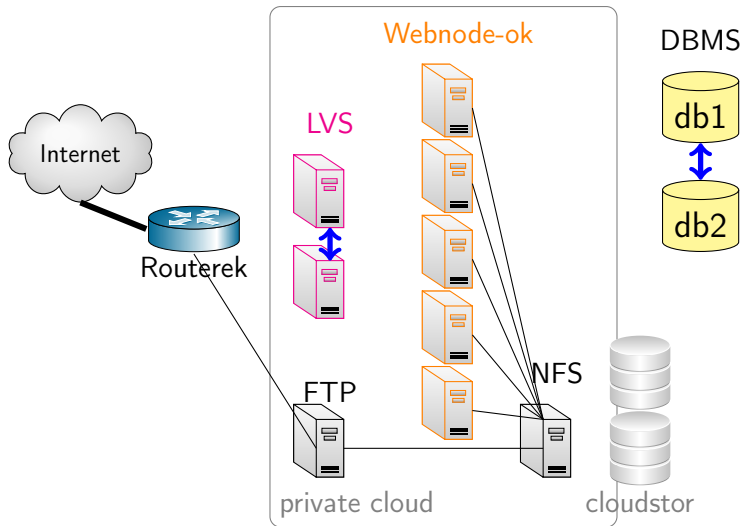


Cluster



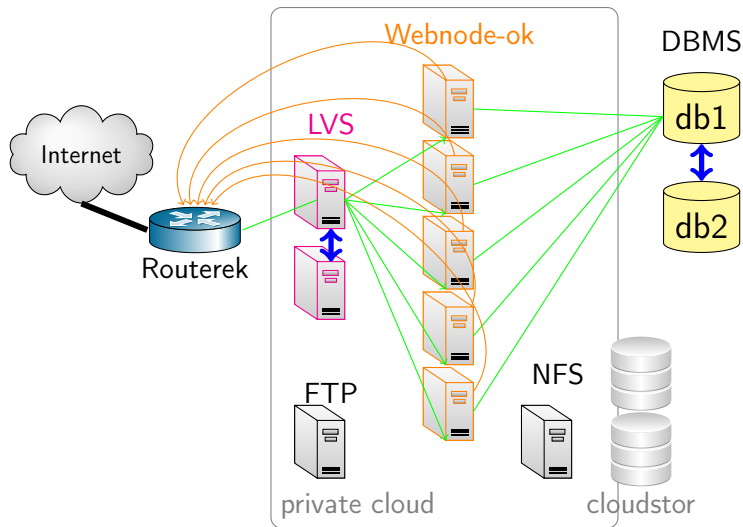


Cluster



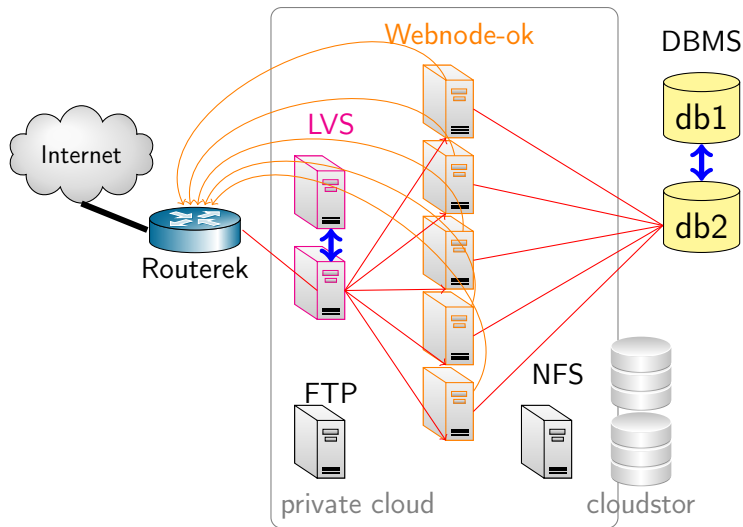


Cluster



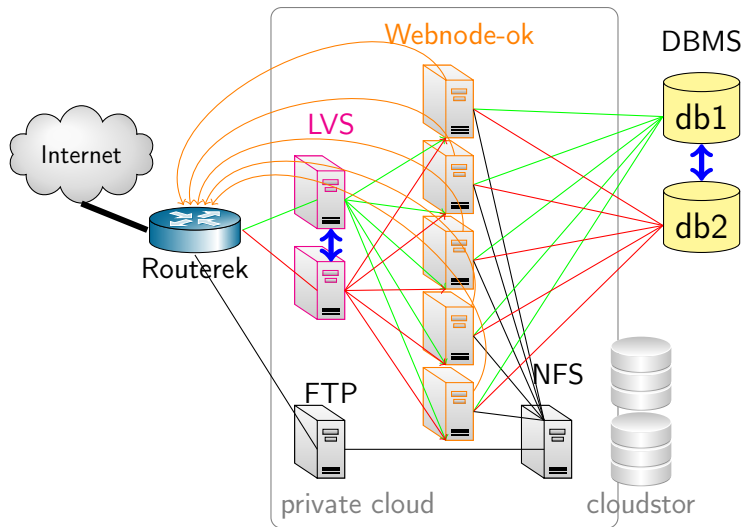


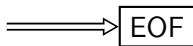
Cluster





Cluster





End of file. . .