digitális jólét nonprofit kft.

A Jitsi-meet telekonferencia szerver telepítése és konfigurálása

Tartalomjegyzék

1. Bevezetés

A Jitsi-meet nyílt forráskódú WebRTC JavaScript applikáció, mely az ún. Jitsi Videobridge nyílt forráskódú videókonferencia szolgáltatást nyújtó XMPP szerver komponensre épül. A Jitsi-meet alkalmas akár több ezer video megosztás létesítésére egy szerveren[1]. A szoftver Apache 2.0 licenc alatt érhető el és biztosítja:

- titkosított kommunikációs protokollt
- hang és video átvitelét, integrált chat szolgáltatást
- megosztott képernyő funkciót

A Jitsi-meet szerver ugyanakkor nem támogatja a fájl megosztást, azonban nyílt forráskódú szoftver révén ezen funkcionalitás más webszerver alkalmazás (pl. Openfire szerveren telepíthető Jitsi plugin[2]) telepítésével pótolható. Jelen telepítési útmutatóban azonban abból indulunk ki, hogy az online video-meeting szolgáltatásra egy már meglévő csoportmunka felület nyújtotta lehetőségek kibővítése érdekében van szükség, így a lehető legegyszerűbb, gyors, megbízható és önálló szolgáltatás telepítésére törekszünk.

2. A telepítés menete Linux operációs rendszeren

A Jitsi.org projekt hivatalos honlapján elérhető a szerver telepítését és konfigurálását lépéséről lépésre bemutató videó anyag: https://jitsi.org/news/new-tutorial-installing-jitsi-meet-on-your-own-linux-server/

A video bemutató tárgyalja:

- Szerver és elérhetőségeinek előzetes konfigurálása

1 https://jitsi.org/projects/
2 https://discourse.igniterealtime.org/t/howto-install-and-configure-jitsi-videobridge-plugin-1-2/78155

- Tűzfal beállítás
- Jitsi szoftver telepítő csomagok biztonságos letöltése
- SSL tanúsítvány létrehozása
- Webszerver konfigurálása
- Szoftverkomponensek telepítése, konfigurálása
- Az első hívás kezdeményezése

Az alábbiakban a fentiekben hivatkozott telepítési lépések tárgyaljuk. Az egyes lépésekhez adminisztrátori (super user) jogosultságok szükségesek.

2.1. Szerver és elérhetőségeinek előzetes konfigurálása

Fizikai és virtuális szerver egyaránt alkalmas a Jitsi-meet szerver telepítéséhez. A Jitsi-meet szerver futtatható felhőben futtatott szervereken, VPN hálózatokat kiszolgáló szervereken, vagy akár saját laptopunkon is. A szerver ajánlott paraméterei a Jitsi-meet szolgáltatás futtatásához:

- 1GB RAM
- 2GHz CPU
- 25GB Disk
- 10GbE Ethernet a gyártói ajánlás (mely elég egy nagyobb kapacitású kiszolgáló szerverhez), azonban kis és közép vállalati igényeket kielégíti a hagyományosan elérhető széles sávú hálózati kapcsolat is.

2.2. Tűzfal beállítása

A Jitsi-meet szerver alapbeállításként a 80-as és 443-as portokat használja TCP adatátvitelre a http és https protokollokkal. Ezeken felül UDP adatátvitelt is használ, ehhez általában elég megnyitni (alapbeállításként) a 10000-20000 közötti portokat. (A legtöbb böngésző számára, mint például a Chrome vagy a Firefox, elég megnyitni csupán a 10000-as portot) A Jitsi-meet szerver titkosított, SSL azonosítású kommunikációt valósít meg a felhasználók között, a http hívásokat automatikusan átirányítja a https csatornára. A fenti portokon ezért szükséges megnyitni a tűzfalat a szükséges kommunikációs protokollok számára. Az alábbi shell parancsokkal az iptables linuxos tűzfal csomag esetében lehet elvégezni a kívánt beállításokat

```
sudo iptables -A INPUT -m state --state NEW,ESTABLISHED -p tcp --dport 443 -j ACCEPT
```

```
sudo iptables -A INPUT -m state --state NEW,ESTABLISHED -p tcp --dport 80 -j ACCEPT
```

```
sudo iptables -A INPUT -m state --state NEW,ESTABLISHED -p udp --dport 10000 -j ACCEPT
```

Amennyiben a szerverünkön egyéb szolgáltatásokat is üzemelünk, melyek a 80-as és 443-as portokhoz köthetőek, akkor célszerű a fentiek mellett további portokat megnyitni a Jitsi-meet számára (például a 4443-at 443 helyett), majd pedig átkonfigurálni a Jitsi-meet szervert ezen portok

használatára, hogy elkerüljük a szolgáltatások ütközését. A szükséges beállításokra a Webszerver konfigurálása fejezetben adunk útmutatást. A tűzfal beállítások a

```
sudo /etc/init.d/iptables-persistent save
```

paranccsal menthetőek. További hasznos információk a tűzfal beállításával kapcsolatban például az https://bencane.com/2012/09/17/iptables-linux-firewall-rules-for-a-basic-web-server/ oldalon találhatóak.

2.3. Jitsi szoftver telepítő csomagok biztonságos letöltése

A szoftver komponensek telepítéséhez először hozzá kell adni a Jitsi repositoryt hitelesítő kulcsot az operációs rendszerünk adatbázisához:

```
wget -qO - https://download.jitsi.org/jitsi-key.gpg.key | sudo apt-key add -
```

A következő lépésben egy sources.list.d fájlt hozunk létre a Jitsi szoftverek eléréséhez.ository:

```
sudo sh -c "echo 'deb https://download.jitsi.org stable/' >
/etc/apt/sources.list.d/jitsi-stable.list"
```

Végül frissíteni kell Update your package list:

```
sudo apt-get -y update
```

2.4. SSL tanúsítvány létrehozása

Mivel a Jitsi-meet szerver titkosított https protokollt használ, beüzemeléséhez szükséges egy SSL tanúsítvány létrehozása az azonosítás a későbbiekben végzett titkosítás végett, vagy már meglévő felhasználása. A webszerver beállításain múlik, hogy éppen hol tárolja/keresi a webszerver a tanúsítványokat. Gyakori beállítás, hogy az SSL tanúsítványok a /etc/ssl, vagy a /etc/apache2/ssl könyvtárban vannak Apache web szerver esetében. Megint csak Apache webszerver esetében az aktuális elérhetősége az SSL tanúsítványok mindenkori elérhetősége az egyes VirtualHost konfigurációs fájlokban vannak tárolva (/etc/apache2/sites-available/*.conf)

SSL tanúsítvány beszerzésére több lehetőség áll fenn:

- kereskedelmi fizetős SSL tanúsítvány beszerzése
- LetsEncrypt nonprofit szolgáltató által beszerzett ingyenes SSL tanúsítvány (https://letsencrypt.org/)
- Saját magunk által generált (nem hitelesített) tanúsítvány az alábbi parancs segítségével: `sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt`

Akár melyik megoldást is választjuk, mentsük el a generált kulcs és crt fájl elérhetőségét, mert szükséges lesz azokat megadni a Jitsi-meet szerver konfigurálása során. Megjegyzendő, hogy az SSL tanúsítvány a Jitsi-meet szerver telepítése után is generálható és bekonfigurálható a telepítéssel együtt generálódó szkriptekkel. Erre a lehetőségre visszatérünk a *Szoftverkomponensek telepítése, konfigurálása* fejezetben.

2.5. Webszerver konfigurálása

A Jitsi-meet szolgáltatás képes üzemelni önálló webszerverként, de automatikusan be tudja konfigurálni a már meglévő Nginx vagy Apache webszerverünket is. A telepítés során automatikusan felismeri a már telepített webszervert és átkonfigurálja azt. Ennek során port ütközések léphetnek fel a telepítés után a már meglévő web szolgáltatásokkal, azonban ezek az ütközések könnyen feloldhatóak a létrehozott konfigurációs fájlok módosításával. (Lásd bővebben a következő fejezetet.)

Az SSL tanúsítványokon kívül a Jitsi-meet szolgáltatás telepítése során szükség lesz a webszerverünk DNS nevére, vagy IP címére. Ezt az adatot a Jitsi-meet szerver konfigurálása során fel kell használni, a kommunikációs szolgáltatás ezen címen keresztül érhető majd el. Ha a konfigurálás során DNS nevet adunk meg, akkor a szolgáltatás nem érhető el IP címmel, és fordítva.

2.6. Szoftverkomponensek telepítése, konfigurálása

A Jitsi-meet szoftver komponensek az alábbi utasításokkal telepíthetőek:

```
sudo apt-get -y install jitsi-meet
```

A telepítés során a telepítő kérdezni a szolgáltatást nyújtó szerves DNS nevét (vagy IP címét). A komponensek telepíthetőek egyenként is az alábbi utasításokkal:

```
sudo apt-get -y install jitsi-videobridge
sudo apt-get -y install jicofo
sudo apt-get -y install jigasi
```

A Jitsi-meet szolgáltatás telepítése után, ha létezett már korábbi webszerver szolgáltatásunk az adott domainhez, fel kell oldani az esetleges szolgáltatás-ütközéseket. A Jitsi-meet szerver alapbeállításként a 443-as portot használja https kommunikációra. Ennek megváltoztatására módosítani kell a webszerver kapcsolódó VirtualHost-jának beállításait. A Jitsi-meet szerver telepítése során (Apache webszerver esetében) a /etc/apache2/sites-available/MEGADOTT_DNS_NEV.conf fájlban át kell írni a

```
<VirtualHost *:443>
```

sorban a portot az általunk használni kívánt portra, például 4443-ra:

```
<VirtualHost *:4443>
```

Ezután a Jitsi-meet szerver beállításiban és át kell vezetni ezt a módosítást. A Jitsi-meet konfigurációs fájlja a */etc/jitsi/meet/MEGADOTT_DNS_NEV-config.js*

Ebben a fájlban kapcsolókkal állíthatjuk a Jitsi-meet szerver működési tulajdonságait, melyekről bő felvilágosítást adnak a benne lévő kommentek. A használatos portot a

```
bosh: '//MEGADOTT_DNS_NEV:4443/http-bind',
```

sorban kell megadni. Miután feloldottuk a port ütközéseket, a módosítások életbe léptetéséhez újra kell indítani a kapcsolódó szolgáltatásokat. Megint csak Apache webszerver esetében a kapcsolódó shell parancsok:

```
sudo /etc/init.d/apache2 restart
```

```
sudo /etc/init.d/jicofo restart
```

```
sudo /etc/init.d/jitsi-videobridge restart
```

Mivel a Jitsi-meet szolgáltatás fontos része az SSL tanúsítvány, lehetőség van annak utólagos konfigurálására is. E célt szolgálja a /usr/share/jitsi-meet/scripts/install-letsencrypt-cert.sh script, melyet adminisztrátori jogosultságokkal indítva:

- letöltődik a LetsEncrypt ingyenes SSL tanúsítvány generálását végző certbot applikáció
- generálódik az SSL tanúsítvány (ehhez meg kell adni egy kapcsolattartó email címet és domain nevet)
- módosulnak a webszerver SSL tanúsítványra vonatkozó beállításai
- újraindul a webszerver (Nginx vagy Apache) és a Jitsi-meet szerver

Amennyiben az SSL tanúsítványokat manuálisan szeretnénk beállítani, a webszerver */etc/apache2/sites-available/MEGADOTT_DNS_NEV.conf* konfigurációs fájljában kell megadni a korábban létrehozott SSL tanúsítványok eléréi útvonalát. Ehhez módosítanunk kell a

```
SSLCertificateFile          PATH_TO_SSL_CRT_FILE
```

```
SSLCertificateKeyFile       PATH_TO_SSL_KEY_FILE
```

sorokat a kapcsolódó eléréi útvonalakkal. A konfigurációs fájlok módosításával újra kell indítani a webszervert.

2.7. Az első hívás kezdeményezése

A telepített Jitsi-meet szolgáltatást kipróbálhatjuk egy webes böngésző segítségével. A böngészőben meg kell adni a bekonfigurált webszerver címét https elérési útvonallal, valamint a portot, melyen a Jitsi szolgáltatás elérhető, amennyiben ez különbözik az alapértelmezett 443-as porttól. (Egy példa a Jitsi szerver elérésére: `https://MEGADOTT_DNS_NEV:4443`)

3. A Jitsi videókonferencia szerver eltávolítása

A Jitsi szerver az alábbi paracs kiadásával távolítható el a rendszerből, konfigurációs fájlokat is beleértve:

```
$ sudo apt-get purge jigasi jitsi-meet jitsi-meet-web-config jitsi-meet-prosody jitsi-meet-turnserver jitsi-meet-web jicofo jitsi-videobridge2
```

Amennyiben a konfigurációs fájlokat meg szeretnénk tartani, a csomagokat az alábbi paranccsal tudjuk eltávolítani:

```
$ sudo apt-get remove jigasi jitsi-meet jitsi-meet-web-config jitsi-meet-prosody jitsi-meet-turnserver jitsi-meet-web jicofo jitsi-videobridge2
```

4. A telepítés menete Windows operációs rendszeren

A Jitsi-meet szerver közvetlen telepítése Windows alapú szervereken nem támogatott, azonban elérhető a Jistsi-meet szerver docker alapú változata is, mely bekonfigurálható Windoes rendszeren is. Részletekért lásd a https://github.com/jitsi/docker-jitsi-meet oldalt.