SAÉ B - Déploiement d'une application

Semaine 3 - Installation et configuration de Synapse

- 1 Accès à un service HTTP sur la VM
  - 1.1 Un premier service pour tester
  - 1.2 Accès au service depuis la machine physique
- 2 Installation de Synapse
  - 2.1 Installation du paquet sous Debian
  - 2.2 Paramétrage de l'accès à distance
  - 2.3 Paramétrage spécifique pour une instance dans un réseau privé
  - 2.4 Utilisation d'une base Postgres
  - 2.5 Création d'utilisateurs
  - 2.6 Connexion à votre serveur Matrix
  - 2.7 Activation de l'enregistrement des utilisateurs
- 3 Note sur le chiffrement
- 4 Changement de machine physique

> N'oubliez pas de prendre des notes en rédigeant des procédures détaillées sur tout ce que vous faites.

1 Accès à un service HTTP sur la VM

Pour que le service que vous allez installer soit accessible de toutes les machines de TP de l'IUT, celui-ci doit *écouter* sur les interfaces réseaux de votre machine physique.

Or, vous allez installer vos services dans votre machine virtuelle. Pour rappel, le réseau virtuel principal, dans lequel se situe votre VM, n'est accessible que depuis la machine de virtualisation.

1.1 Un premier service pour tester

> Installer le serveur HTTP `nginx` dans votre machine virtuelle.
>
> Vérifier que celui-ci est démarré à l'aide de la commande `systemctl`
>
> Installer le client HTTP en mode texte `curl`
>
> Vérifier que vous pouvez accéder au serveur `nginx` **depuis la VM** à l'aide de la commande
>
> ```
> user@vm$ curl http://localhost
> ```

1.2 Accès au service depuis la machine physique

On souhaite maintenant pouvoir accéder au service qui s'exécute sur la *machine virtuelle* depuis la machine *physique*.

> Expliquer dans vos procédure, pourquoi ce n'est pas possible directement.

Pour résoudre ce problème, nous allons nous servir de la fonction *tunnel* de SSH.

> Lire la page de manuel `ssh(1)`, particulièrement l'option `-L`, et trouver une solution pour que l'URL `http://machine-physique.iutinfo.fr:9090` saisie dans le navigateur de la *machine physique* vous permette d'accéder au service `nginx` de votre *machine virtuelle*
>
> Adapter le fichier `.ssh/config` de façon à ne pas avoir à utiliser l'option `-L` systématiquement (voir le manuel `ssh_config(1)`).

2 Installation de Synapse

Il est maintenant temps d'installer Synapse, l'implémentation de référence pour un serveur Matrix.

2.1 Installation du paquet sous Debian

> Suivre les instructions sur la page dédiée à l'installation sous Debian

A l'installation, le gestionnaire de paquets vous demande le *nom de votre instance*. Vous devez indiquer `machine-physique.iutinfo.fr:8008`. Attention à bien indiquer le port `8008` et à remplacer `machine-physique` par le nom de votre machine physique (par exemple `ayou03`).

Le serveur écrira ses messages à destination de l'administrateur (les logs) dans le fichier `/var/log/matrix-synapse/homeserver.log`.

2.2 Paramétrage de l'accès à distance

Par défaut, synapse *écoute* uniquement sur l'interface de boucle locale. Pour que l'on puisse y accéder depuis l'extérieur de la machine virtuelle, il doit *écouter* également sur l'interface située dans le réseau 10.42.0.0/16.

Modifier le fichier de configuration de synapse de façon à ce qu'il *écoute* sur l'interface réseau attachée au réseau 10.42.0.0/16 en plus de la boucle locale

2.3 Paramétrage spécifique pour une instance dans un réseau privé

Notre installation est peu commune car votre serveur n'est pas accessible depuis internet. En production réelle, on voudrait qu'il le soit. Les paramètres par défaut de Synapse considèrent donc que votre serveur est accessible de l'extérieur et qu'il ne cherche pas à contacter des éléments situés sur un réseau privé. En particulier, on ne veut pas que notre serveur contacte d'autres serveurs pour obtenir des clés publiques de signatures. On va donc appliquer la documentation en affectant la variable de configuration `trusted_key_servers` à `[]`)

> ```
> If the use of a trusted key server has to be deactivated, e.g. in a
> private federation or for privacy reasons, this can be realised by
> setting an empty array (trusted_key_servers: [])
> ```

2.4 Utilisation d'une base Postgres

Par défaut, Synapse utilise une base de données au format fichier `sqlite`, ce qui est très bien pour tester, mais pas suffisant pour une instance en production.

Trouver dans la documentation les changements à appliquer à la configuration pour que votre serveur utilise une base `postgres` et pas un fichier `sqlite`

Attention : lors de la séance précédente, nous avons créé une base de données `matrix` avec les options de création par défaut. Ces options ne conviennent pas à Synapse et il refusera de démarrer si vous ne changez rien à votre base de données.

Suivre les instructions de la documentation de Synapse pour recréer cette base avec les bonnes options (vous devrez au préalable supprimer la précédente avec `dropdb(1)`

Vérifier que la base postgres a bien été utilisée en regardant le contenu de la base `matrix` après avoir redémarré le serveur synapse.

2.5 Création d'utilisateurs

Pour créer un utilisateur sur votre serveur, vous devez utiliser le script (installé avec le serveur Synapse) `register_new_matrix_user`.

Lire la documentation de Synapse et trouver comment spécifier une clé partagée d'enregistrement dans sa configuration.

Utiliser cette clé pour créer deux utilisateurs, un pour chaque membre de votre binôme.

2.6 Connexion à votre serveur Matrix

Pour vous permettre de vous concentrer sur le serveur, nous avons déployé un client Element web pour vous à l'adresse http://tp.iutinfo.fr:8888/.

Utiliser ce client dans un navigateur de la machine physique et se connecter à votre serveur. Attention, pas défaut, le client veut se connecter au serveur `matrix.org`.

Cette étape doit être faite pour les deux utilisateurs (sur deux machines physique différentes).

Créer un salon avec un utilisateur et inviter l'autre utilisateur dans le salon.

2.7 Activation de l'enregistrement des utilisateurs

Pour l'instant, votre serveur n'accepte pas les nouveaux utilisateurs.

Lire la documentation de synapse et activer l'enregistrement de nouveaux utilisateurs, sans vérification.

Créer quelques utilisateurs à l'aide du client element pour tester.

3 Note sur le chiffrement

Pour l'instant, tant que la connexion vers synapse est effectuée en HTTP (et non en HTTPS), la fédération d'instance est impossible. Il ne sera donc pas possible d'accéder à des canaux d'un serveur synapse avec un compte créé sur un autre serveur synapse.

De même, element vous indiquera une erreur à la récupération/création de clé, vous pouvez l'ignorer tant que la connexion ne sera pas faite en HTTPS.

4 Changement de machine physique

Durant la SAÉ, vous devrez probablement changer de machine physique une ou plusieurs fois.

À l'installation de Synapse, vous avez renseigné le nom du serveur comme étant `http://phys.iutinfo.fr:8008`. Comme vous

l'avez peut-être constaté, Synapse vous a indiqué que ce nom ne pouvait pas être changé à l'avenir sans avoir à recréer complètement la base de données (et donc perdre les données liées à Synapse).

Dans un déploiement classique, ce n'est pas vraiment un soucis car cette URL n'est pas censée changer. Or, dans notre déploiement, cette URL correspond à la machine physique que vous utilisez au moment de l'installation de Synapse. Si vous changez de machine physique au cours de la SAÉ, votre serveur synapse ne sera plus accessible par la même URL (car la redirection SSH permettant l'accès au service hébergé sur la VM aura changé).

Synapse se sert de cette information dans les identifiants des utilisateurs et des salons de discussion.

Si vous changez de machine physique vous devrez donc:

1. arrêter Synapse
2. modifier le fichier `/etc/matrix-synapse/conf.d/server_name.yml` pour mettre la nouvelle URL
3. détruire et recréer la base de donnée
4. recréer les utilisateurs
5. redémarrer Synapse

Vous pouvez même écrire facilement un script shell qui pourra effectuer ces modifications automatiquement.

> Il est évident que cette procédure n'est pas idéale et ne serait jamais à faire dans un vrai déploiement (on perds toutes les données), mais dans notre cas, on ne peut pas faire autrement car l'URL change pour des raisons de disponibilité des salles de TP, ce qui n'arriverait jamais sur un déploiement réel