

# Guide d'Installation et d'Utilisation

Projet : SAÉ 3.02 — Solution de consultation centralisée de journaux systèmes

Yacine Ben Omrane Étudiant en 2ème année de BUT Réseaux et Télécommunications  
Parcours Cybersécurité

## 1. Installation :

L'installation a été automatisée au maximum, mais le lancement nécessite une activation manuelle de l'environnement Python sécurisé.

### 1.1 Installation automatique

Tout d'abord, il faut lancer le script qui prépare la machine, installe la base de données et configure les droits.

Rendre le script exécutable (si nécessaire)

```
chmod +x install.sh
```

Lancer l'installation

```
./install.sh
```

*Le script affichera "Installation Terminée" une fois les opérations finies.*

### 1.2 Activer l'environnement Virtuel (Important)

Une fois l'installation finie, une étape manuelle est nécessaire pour entrer dans l'environnement virtuel Python (là où les librairies Flask et Paramiko sont installées).

Activer l'environnement virtuel :

Tapez la commande suivante. Vous verrez (venv) apparaître au début de votre ligne de commande.

```
qamu@Serveur - SAE302:~/sae302$ source venv/bin/activate
(venv) qamu@Serveur - SAE302:~/sae302$
```

### 1.3 Configuration de l'utilisateur système (**Important**)

Par défaut, l'application est configurée pour se connecter en SSH avec l'utilisateur **qamu**. Si votre session Linux utilise un autre nom d'utilisateur, vous devez modifier cette configuration dans le code, sinon la récupération des logs distants échouera.

1. Ouvrez le fichier **app.py** avec un éditeur de texte :  
`nano app.py`
2. Repérez les lignes 13 et 14 au début du fichier :

```
# Identifiants SSH pour les connexions aux serveurs
SSH_USER = 'qamu'
SSH_PASSWORD = 'qamu'
```

3. Remplacez '**qamu**' par votre nom d'utilisateur et votre mot de passe de session Linux.

Et pour ce qui est du mot de passe pour la base de donnée il n'y a pas de problème car le script **install.sh** crée automatiquement un utilisateur MariaDB nommé **sae302** avec le mot de passe **qamu**

## 2. Utilisation :

### 2.1 Exécuter le script python :

Tout d'abord, il faut vérifier si le script est exécutable. Ensuite, faire la commande `python3 app.py` pour pouvoir lancer l'application :

```
(venv) qamu@Serveur-SAE302:~/sae302$ python3 app.py
* Serving Flask app 'app'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://192.168.122.100:5000
Press CTRL+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 952-629-277
```

Le terminal doit afficher : [Running on http://127.0.0.1:5000](http://127.0.0.1:5000)

### 2.2 Connexion à l'interface

Ouvrez un navigateur Web et allez à l'adresse : <http://localhost:5000>

Utilisez les identifiants administrateur par défaut (injectés par le script) :

- **Identifiant : admin**
- **Mot de passe : admin123**

Ces identifiants sont modifiables par la suite, donc une fois sur l'application, il faudra se rendre dans la section utilisateur :

**Ajouter un utilisateur**

Nom d'utilisateur:

Mot de passe:

Minimum 6 caractères

Rôle:

**Ajouter**

Et ensuite, pour des raisons de sécurité, il est préférable de supprimer l'ancien administrateur qui a été créé par défaut pour accéder à la page :

**Liste des utilisateurs**

Sélection	ID	Nom	Rôle
<input checked="" type="radio"/>	1	admin <small>Vous</small>	administrateur
<input type="radio"/>	3	Nouveau admin	administrateur

**Modifier** **Supprimer**

## 2.3 Petit souci fréquent : Impossible de lire les logs

Si quand on clique sur "Afficher les journaux", il ne se passe rien ou qu'il voit une erreur "Permission Denied", c'est normal. C'est la sécurité de Linux qui bloque l'accès au fichier **/var/log/syslog**.

Pour régler ça, il faut donner le droit de lecture à l'utilisateur, mais ça dépend d'où vient le problème :

Si vous n'arrivez pas à lire les logs d'une machine distante (ex: Hote1) Là, c'est l'utilisateur qu'on utilise pour la connexion SSH (défini dans le code) qui se fait bloquer sur l'autre machine. Il faut aller sur la machine distante (Hote1) et taper :

**sudo usermod -aG adm qamu**

(Remplacez **qamu** par le nom de l'utilisateur que vous utilisez pour le SSH).