



Objectifs

- Réaliser l'itération 5 de l'application Gestion Log
 - Ouvrir et filtrer les informations concernant les connexions ssh
 - Écrire les informations dans une structure
 - Sauvegarder les informations dans un nouveau fichier de log

Contenu technique

- Manipulation des structures
- Écriture dans un fichier texte

Durée 5 heures

I. Intégration des logs SSH dans la structure SSHLoggin.

I.1 Git

N'oubliez pas de vous replacer sur la branche **dev** pour cette itération.

I.2 Analyse de la structure SSHLoggin

En suivant la conception du DDC,

- Q1. Lister les champs de la structure SSHLoggin
- Q2. Lister les champs de la structure SshDateTime
- Q3. Que contient le champ `_datetime` de la structure SSHLoggin ?

I.3 Logger les connexions ssh clientes

I.3.1 Préparation

Les logs de connexion cliente ssh ne sont pas enregistrés par défaut sous Linux.

Votre RSSI vous demande de modifier la configuration de votre poste pour logger les demandes de connexion ssh.



Voici la procédure qu'il vous a demandé de suivre.

1. Ouvrir le fichier `/etc/profile`
2. Ajouter les lignes suivantes à la fin du fichier

```
function log2syslog
{
    declare command
    command=$(fc -ln -0)
    logger -p local1.notice -t bash -i -- $USER : $command
}
trap log2syslog DEBUG
```

3. Enregistrer le fichier
4. Exécuter la commande suivante

```
source /etc/profile
```

5. Vérifier que les logs de connexion apparaissent dans le fichier `/var/log/syslog`

I.4 Fonction `sshLog()`

Les informations à extraire sont de la forme

```
Mar 13 21:37:40 pc-dev bash[16685]: user1 : ssh test@srv.exemple.com -p 2222
```

- Q4. En fonction de l'exemple ci-dessus, remplir sur votre compte rendu les champs des structures `SshLogin` et `SshDateTime` avec les valeurs correspondantes.
- Q5. Déclarer la fonction `sshLog()`, ouvrir et afficher les entrées du fichier contenant les logs ssh dans votre console.

Cette fonction est un peu plus complexe que la précédente car il va falloir extraire les informations d'un flux pour remplir les champs de la structure.

Pour vous aider à « parser » le flux, vous aller vous aider des fonctions suivantes :
`gethostname()`, `getlogin_r()`, `std::find()`, `std::substr()`

- Q6. Chercher et donner la définition des fonctions ci-dessus
- Q7. Comme vous avez fait avec la fonction `sudoLog()`, filtrer les informations correspondants à des demandes de connexions ssh



I.4.1 Structure SshDateTime

Q8. Remplir les champs de la structure SshDateTime avec l'heure de la requête de connexion

I.4.2 Structure SSHLogin

La méthode ci-dessous vous aide à extraire les informations du flux en fonction des éléments à votre disposition.

Vous vous faudra utiliser les informations données par `gethostname()`, `getlogin_r`, `@` et l'option `-p` pour vous repérer dans le flux.

Q9. Remplir le champ `hostname`

Q10. Remplir le champ `username`

Q11. Isoler la partie du flux contenant les informations de connexion (`test@srv.exemple.com -p 2222`)

Q12. Isoler le nom de login et remplir le champ `sshUser`

Q13. Isoler l'adresse du serveur et remplir le champ `sshHost`

Q14. Isoler le numéro de port et remplir le champ `sshPortNumber`

I.4.3 Sauvegarde des informations

En suivant le DDC, réaliser la fonction `sauvegarderLogSSH()`

Q15. Sauvegarder les informations précédentes dans le fichier `ssh_connexion.txt` dans le répertoire de l'utilisateur.

I.5 Validation

Appeler l'enseignant pour qu'il valide votre travail

II. Dossier de validation

Vérifier que votre application répond aux exigences du cahier des charges.

Q16. Compléter le dossier de vérification `Gestion_Log_DDV.odt` (ESS002 et ESS003)



III. Outils DevOps

Afin de finaliser votre travail, n'oubliez pas :

- D'indenter correctement votre code
- De documenter le code, les fonctions et les fichiers

IV. Livrable

Sur le moodle de la section

- Votre compte rendu de TP avec les réponses aux questions de celui-ci
- La documentation générée (Télécharger l'artifact sur le pipeline)
- Le dossier de validation DDV

Sur le serveur GIT de la section

- Le projet Gestion_Log Branche dev
- Merge de la branche dev sur master
- Le tag de la version v5.0