## L’agence Red Sun Studio

Red Sun Studio est l’agence d’intelligence centrale (AIC) de la ville de Laval. Elle emploie plus de 10 employés et le reste des détails est top secret. D’ailleurs, vous en savez déjà trop…

## La demande

Récemment, l’agence a décidé de mettre à jour ses infrastructures. Voici les détails de leur nouvelle configuration pour leur serveur d’accès aux données (fichiers).

Il y aura 4 comptes (« usagers ») ayant des accès aux données sur le serveur :

Useradd

* redPublic
* redTrainee
* redAgent
* redAdmin

Voici la hiérarchie des répertoires de l’agence :

Mkdir

/usr/local/**RedSS /dropZone/**

/usr/local/**RedSS/docs/**

/usr/local/**RedSS/ops/**

Le dossier **redSS** doit être seulement accessible pour ces 4 comptes. Si l’usager, disons« noob », essaie d’y accéder, un message d’erreur doit être lancé (permission denied).

Le dossier **dropZone** permet simplement aux 4 comptes la permission d’y déposer des fichiers. Seul **redAdmin** à la capacité de pouvoir lister les fichiers du répertoire. **dropZone** sera utilisé lorsque des agents de RedSS voudront y déposer des informations sur les habitants de Laval.

Le dossier **docs** possède de la documentation accessible à tous. Seul **redAdmin** peut y déposer des fichiers.

Le dossier **ops** possède des informations pour le compte **redAgent**. Il ne doit être accessible en lecture que par **redAgent**, **redAdmin** et **redTrainee.** Seul **redAdmin** peut y ajouter/supprimer des fichiers. **redPublic** n’a aucun droit sur ce répertoire.

Il n’est pas permis d’ajouter/modifier/supprimer des répertoires/fichiers dans le dossier **RedSS**.

Au départ, le dossier **docs** contiendra un seul fichier, **guidelines.txt**. Ce fichier est disponible en lecture par les comptes red\* et seul **redAdmin** le modifier. Ce fichier n’est pas un script exécutable.

1. Set permissions for the **redSS** directory:

bashCopy code

sudo chown -R redAdmin:redAdmin /usr/local/RedSS sudo chmod 700 /usr/local/RedSS

This sets the owner and group of the directory to **redAdmin** and gives read, write, and execute permissions to only the owner (**redAdmin**).

1. Set permissions for the **dropZone** directory:

bashCopy code

sudo chown -R redAdmin:redAdmin /usr/local/RedSS/dropZone sudo chmod 770 /usr/local/RedSS/dropZone

This sets the owner and group of the directory to **redAdmin** and gives read, write, and execute permissions to both the owner and group.

1. Set permissions for the **docs** directory:

bashCopy code

sudo chown -R redAdmin:redAdmin /usr/local/RedSS/docs sudo chmod 750 /usr/local/RedSS/docs

This sets the owner and group of the directory to **redAdmin** and gives read, write, and execute permissions to the owner, and read and execute permissions to the group.

1. Set permissions for the **ops** directory:

bashCopy code

sudo chown -R redAdmin:redAdmin /usr/local/RedSS/ops sudo chmod 750 /usr/local/RedSS/ops

This sets the owner and group of the directory to **redAdmin** and gives read, write, and execute permissions to the owner, and read and execute permissions to the group.

1. Create the **guidelines.txt** file in the **docs** directory:

bashCopy code

sudo touch /usr/local/RedSS/docs/guidelines.txt sudo chown redAdmin:redAdmin /usr/local/RedSS/docs/guidelines.txt sudo chmod 640 /usr/local/RedSS/docs/guidelines.txt

This creates the file and sets the owner and group to **redAdmin**, allowing read and write permissions for the owner, and read permissions for the group.

## alisation du mandat

Pour créer l’architecture répondant à la demande précédente, aidez-vous du compte « root ».

### Étape 1 – Création des comptes et groupes

Créez les comptes RedSS et donnez à ces comptes les groupes nécessaires.

Vos commandes de création des comptes :

useradd redPublic

useradd redTrainee

useradd redAgent

useradd redAdmin

groupadd redGroup

usermod –a –G redGroup redPublic // ajoute le groupe à l’usager

usermod –a –G redGroup redTrainee

usermod –a –G redGroup redAgent

usermod –a –G redGroup redAdmin

groupadd redOps // Pour le dossier ops qui n’est pas accessible à redPublic

usermod –a –G redOps redTrainee

usermod –a –G redOps redAgent

usermod –a –G redOps redAdmin

Note : On peut ajouter un groupe à un usager avec : usermod –a –G *groupe* *usager*

### Étape 2 –Le répertoire RedSS

Créez et sécurisez le répertoire /usr/local/RedSS

Commandes :

mkdir /usr/local/RedSS

chmod 750 RedSS // 5 = On ne peut ajouter/supprimer fichiers dans RedSS

chgrp redGroup RedSS // Ceux qui ne font pas parti du groupe RedSS ne peut pas y

avoir accès

### Étape 3 – Le répertoire dropZone

Créez le répertoire /usr/local/RedSS/dropZone.

Modifiez le propriétaire/groupe du répertoire et donnez-lui les bonnes permissions pour répondre à la demande.

Commandes:

mkdir dropZone

chgrp redPublic dropZone // avec droit pour déposer

chown redAdmin dropZone // avec tous les droits

chmod 730 dropZone // wx pour que redPublic puisse y déposer des fichiers

Note : Pour déposer des fichiers, on ne peut donner seulement le droit «w», il faut donner «wx».

### Étape 4 – Le répertoire docs

Créez le répertoire /usr/local/RedSS/docs

Modifiez le propriétaire/groupe du répertoire et donnez-lui les bonnes permissions pour répondre à la demande.

Commandes:

mkdir docs

chown redAdmin docs // Pour les droits d’écriture

chgrp redGroup docs // Pour les droits de lecture

chmod 750 docs

### Étape 5 – Le répertoire ops

Créez le répertoire /usr/local/RedSS/ops

Modifiez le propriétaire/groupe du répertoire et donnez-lui les bonnes permissions pour répondre à la demande.

Commandes:

mkdir ops

chown redAdmin ops

chgrp redOps ops

chmod 750 ops

### Étape 6 – Le fichier guidelines.txt

Créez le fichier guidelines.txt dans le dossier docs.

Modifiez le propriétaire/groupe du fichier et donnez-lui les bonnes permissions pour répondre à la demande.

Commandes:

touch docs/guidelines.txt

chown redAdmin docs/guidelines.txt

chgrp redGroup docs/guidelines.txt

chmod 640 docs/guidelines.txt

### Étape 7 – Les tests

Effectuez les tests suivants. Si un test échoue, réparez votre/vos erreur(s).

Il est impossible d’écrire, de se déplacer ou de lire avec un compte qui n’est pas red\* dans le dossier RedSS.

Tests :

su frederic

touch RedSS/test.txt

cd RedSS/

ls RedSS

Tout sera “Permission denied”

Les agents de RedSS sont capables de déposer des fichiers dans dropZone, mais ils sont incapables de faire un « ls ». RedAdmin à tous les droits sur ce répertoire.

Tests :

su redPublic

touch dropZone/test.txt

ls –l dropZone/test.txt (erreur)

su redAdmin

ls –l dropZone/test.txt (ok)

Il est possible pour redAdmin d’ajouter des fichiers dans docs. Les autres comptes red\* peuvent consulter ces documents, mais ils ne peuvent ajouter/supprimer des fichiers dans ce répertoire.

Tests :

su redAdmin

touch docs/test.txt

su redAgent/redPublic/redTrainee

touch docs/test2.txt (erreur)

ls –l docs

redPublic ne peut pas lire ou se déplacer dans le répertoire ops. Les autres comptes peuvent aller et lire le répertoire ops. Seul redAdmin peut y créer des fichiers.

Tests :

su redPublic

cd ops (access denied)

su redAgent

cd ops

ls ops

su redAdmin

touch ops/test.txt

redAdmin est le seul qui peut écrire dans le fichier guidelines.txt, mais les autres comptes red\* peuvent le consulter.

Tests :

su redAdmin

nano docs/guidelines.txt (sauvegarder fonctionne)

su redAgent

nano docs/guidelines.txt (fonctionne en lecture seulement)