Campus Ermitage

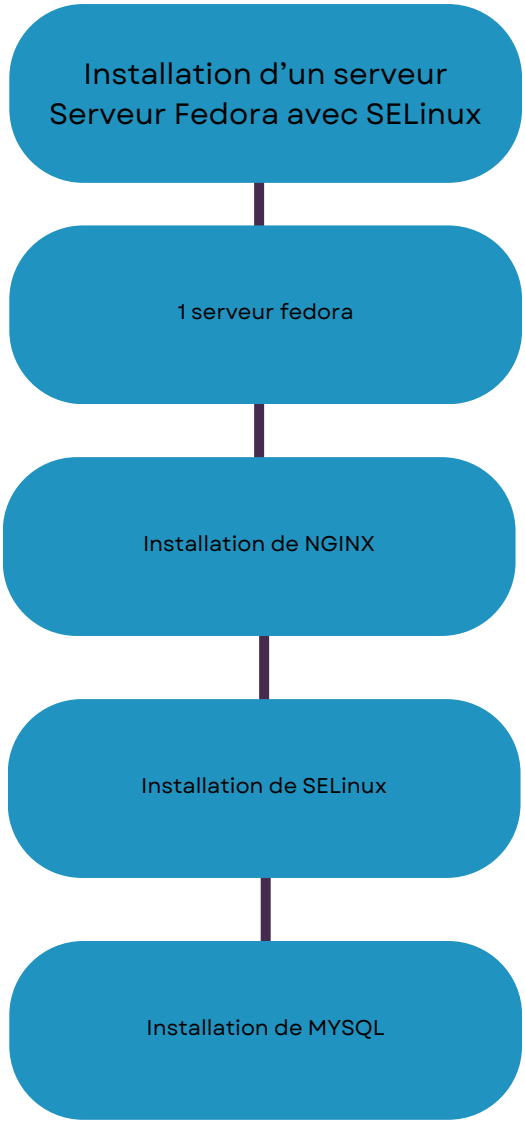
TP SISR
PROJET SELINUX

2024

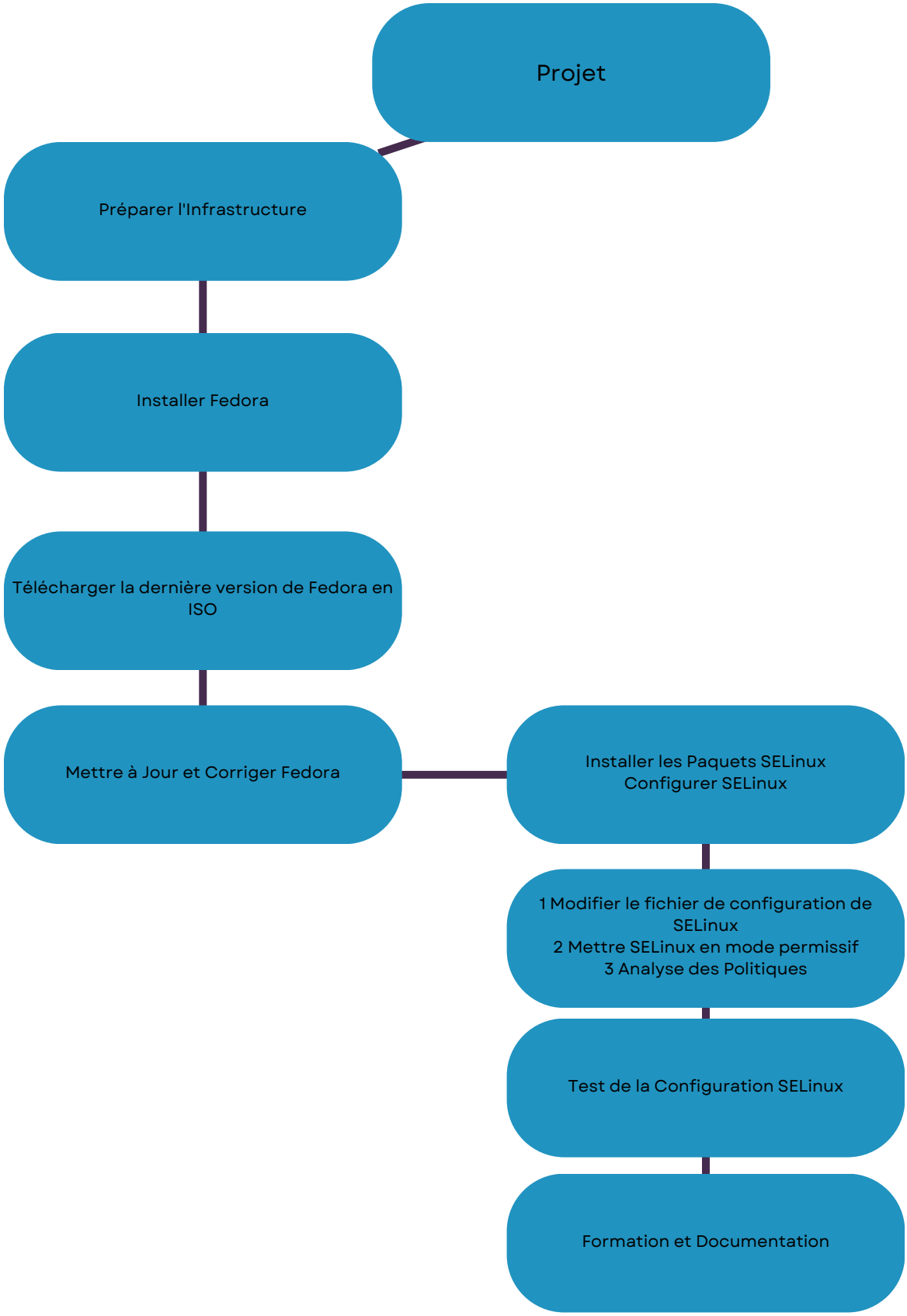
Ryan DeTree

SOMMAIRE

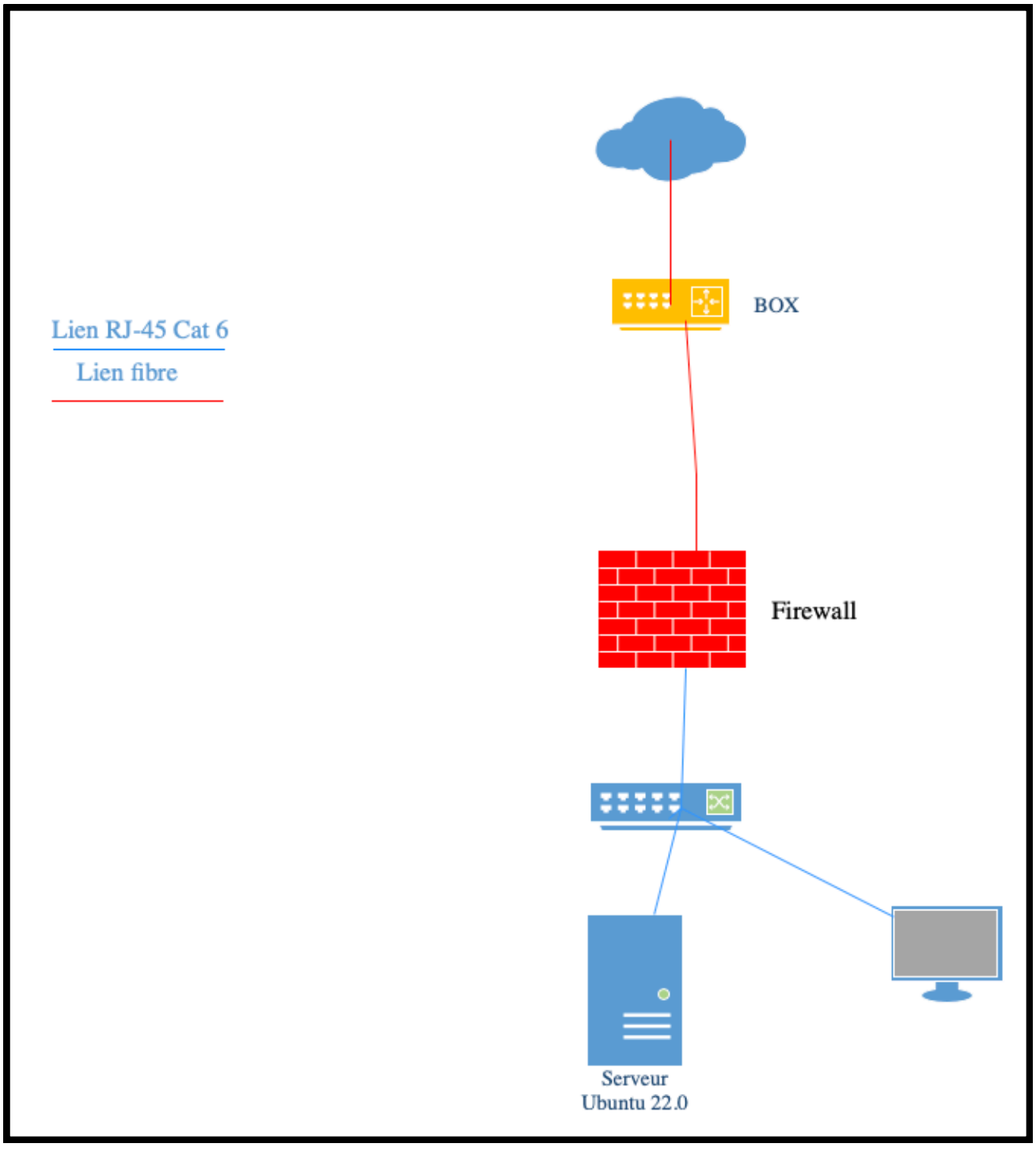
PBS (PRODUCT BREAKDOWN STRUCTURE)



WBS (WORK BREAKDOWN STRUCTURE



RESEAU ACTUEL



QU'EST CE QUE SELINUX?

SELinux, ou Security-Enhanced Linux, est une architecture de sécurité avancée intégrée profondément dans le noyau Linux.

Développé par **l'Agence de Sécurité Nationale** (NSA), il offre un mécanisme robuste pour l'application de politiques de contrôle d'accès sécurisé.

Contrairement aux mécanismes traditionnels de **contrôle d'accès discrétionnaire** (DAC), SELinux met en œuvre des **contrôles d'accès obligatoires** (MAC), qui offrent un contrôle granulaire sur les actions des utilisateurs et des processus en fonction de politiques de sécurité définies.

Chaque fichier, processus et port réseau dans SELinux est étiqueté avec un contexte de sécurité, contenant des informations sur son identité, son rôle et les autorisations associées.

PERMISSIVE, ENFORCING & DISABLED SETTINGS

La commande getenforce nous permet de voir la configuration de SELinux

- Enforcing - enabled et enforcing
- Permissive - enabled, mais pas d'enforcing (que les logs sont disponible, bien pour debug)
- Disabled - SELinux est desactiver

COMMENT SA MARCHE?

Avec la commande ls -l on peux voir les droits d'accès a un dossier.

```
root@localhost:~# ls -l
total 4
-rw-------. 1 root root 914 Apr 19 09:54 anaconda-ks.cfg
root@localhost:~#
```

SELinux apporte une couche de sécurité en plus sur les permissions de dossier et ou document.

Avec la commande ls -lZ on peux voir les details des fichier web par exemple dans cette exemple c'est du httpd_sys_content ce qui signifie que le fichier est utiliser pour un service web.

```
root@localhost:~# ls -1Z /usr/share/nginx/html/
system_u:object_r:httpd_sys_content_t:s0 50x.html
system_u:object_r:httpd_sys_content_t:s0 icons
system_u:object_r:httpd_sys_content_t:s0 index.html
system_u:object_r:httpd_sys_content_t:s0 nginx-logo.png
system_u:object_r:httpd_sys_content_t:s0 poweredby.png
root@localhost:~#
```

LES PRINCIPAUX COMPOSANTS DE SELINUX

1. Contextes de sécurité:
   - Les contextes de sécurité sont des étiquettes attribuées aux fichiers, processus, ports réseau, etc., pour définir leurs autorisations et restrictions dans un environnement SELinux. Ces contextes déterminent les actions permises ou interdites pour les objets du système.

2. Politiques SELinux:
   - Les politiques SELinux définissent les règles et les autorisations pour chaque contexte de sécurité. Elles spécifient quelles actions sont autorisées ou refusées pour chaque type d'objet et dans quelles conditions. Les politiques SELinux sont généralement définies dans des modules de politique et sont utilisées par le système pour prendre des décisions de contrôle d'accès.

3. Modules de politique:
   - Les modules de politique SELinux sont des ensembles de règles qui définissent les autorisations pour un service ou une application spécifique. Ils sont créés et gérés par les administrateurs système pour personnaliser les politiques SELinux en fonction des besoins spécifiques du système.

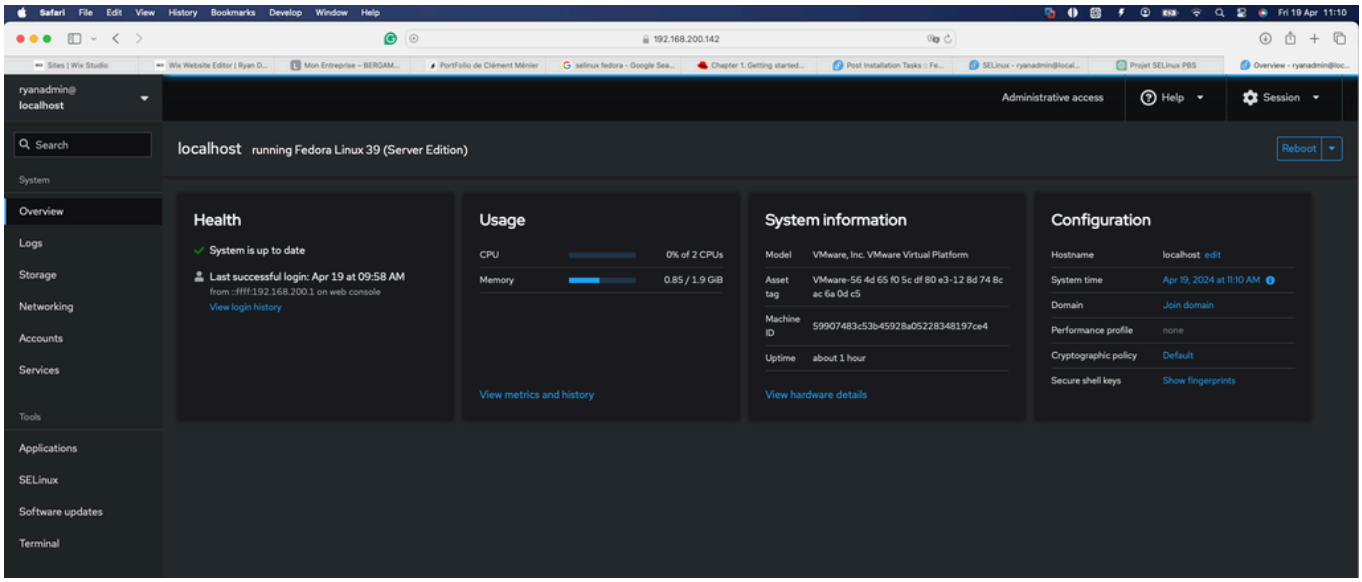
4. Règles de sécurité:
   - Les règles de sécurité définissent les autorisations et les restrictions pour chaque contexte de sécurité dans la politique SELinux. Elles précisent quelles actions sont autorisées ou refusées pour les différents objets du système en fonction de leurs contextes de sécurité.

5. Labels de sécurité:
   - Les labels de sécurité sont des informations attachées aux objets du système pour indiquer leur contexte de sécurité. Ces labels sont utilisés par SELinux pour prendre des décisions de contrôle d'accès en fonction des politiques définies.

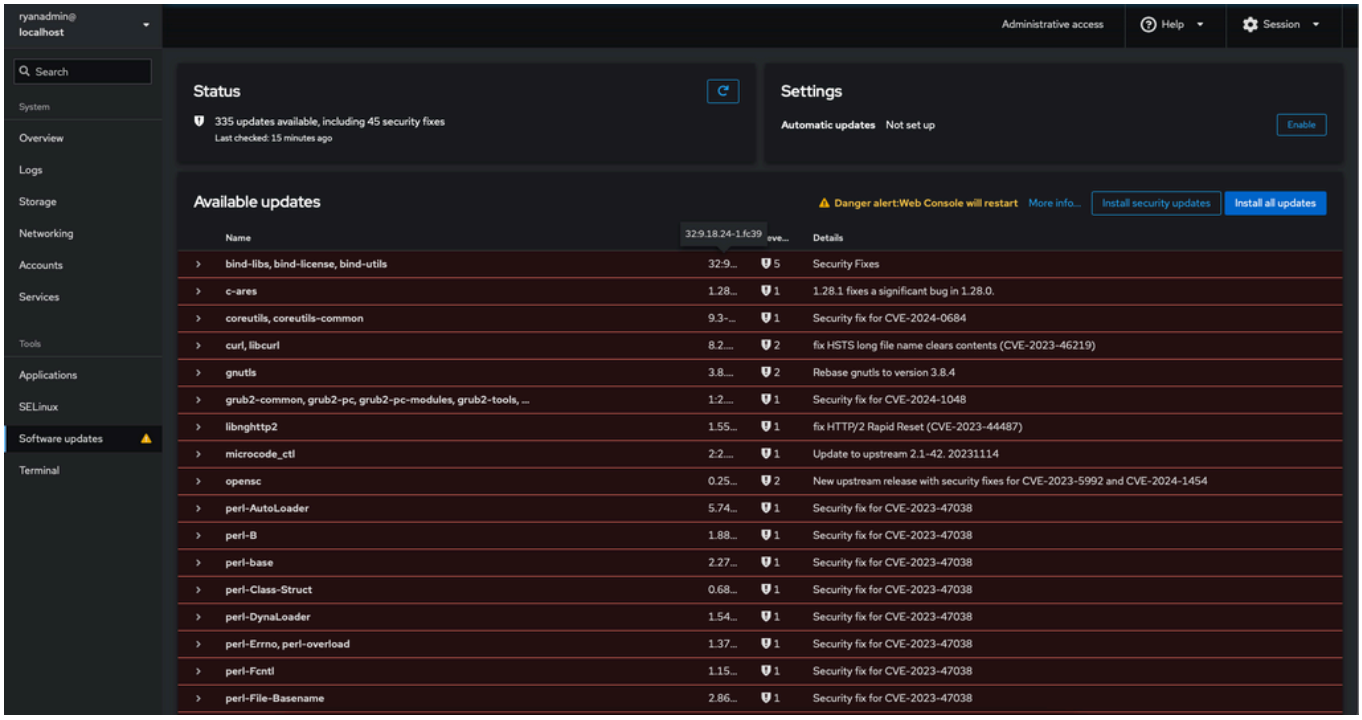
6. Audit et logs SELinux:
   - L'audit et les logs SELinux sont utilisés pour enregistrer les activités du système en ce qui concerne les politiques de sécurité SELinux. Les logs SELinux contiennent des informations sur les violations de politique, les décisions de contrôle d'accès prises par SELinux, et d'autres événements liés à la sécurité du système.

INSTALLATION & CONFIGURATION SELINUX

J'ai créé une machine virtuelle sur VMware Fusion en utilisant le iso du site de fedora. (voir dossier ressources)



Mise a jour des packets de sécurité de Fedora sur l'interface graphique (Cockpit Linux) cette option est facultatif mais fortement recommandé pour les patches de sécurité.



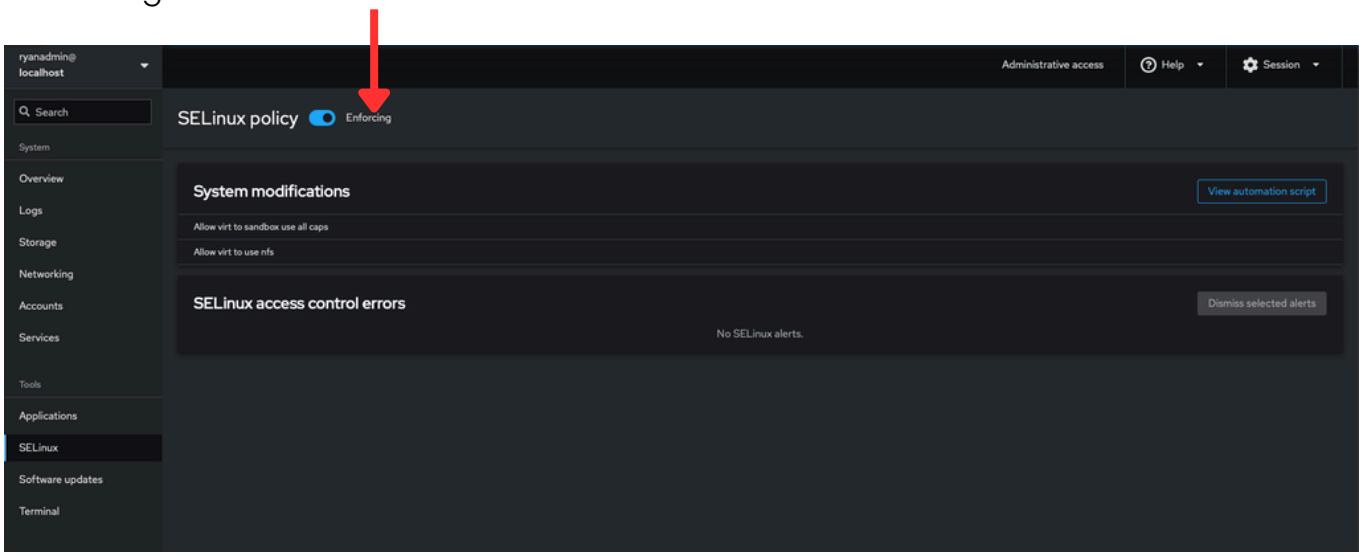
VERIFICATION DE L'ACTIVATION DE SELINUX

En root j'ai fait la commande suivante pour voir la configuration de SELinux.

vi /etc/selinux/config

```
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Ainsi que sur l'interface graphique Cockpit on peux voir dans le menu SELinux que l'enforcing est actif.



Ou encore on peux faire la commande sestatus

```
Last login: Tue May 14 10:33:18 2024
root@localhost:~# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
root@localhost:~#
```

INSTALLATION DE SETROUBLESHOOT & SETROUBLESHOOT-SERVER

Il est conseillé d'installer setroubleshoot pour pouvoir lire des erreurs dans les logs avec un visuel plus dynamique.

EXPLORATION DES OUTILS DE GESTION

Voici un résumé des commandes que l'on peux utiliser pour gérer SELinux :

semanage: Gère les paramètres SELinux liés aux politiques de sécurité.
Utilisez semanage --help pour voir les options disponibles.

seinfo: Affiche des informations sur les politiques SELinux et les contextes de sécurité.
Utilisez seinfo --help pour voir les options disponibles.

sesearch: Recherche dans la base de données des politiques SELinux pour trouver des règles spécifiques.
Utilisez sesearch --help pour voir les options disponibles.

audit2allow: Analyse les journaux SELinux pour générer des règles de module SELinux.
Utilisez audit2allow --help pour voir les options disponibles.

restorecon: Restaure les contextes SELinux par défaut sur les fichiers système.
Utilisez restorecon --help pour voir les options disponibles.

sestatus: Affiche l'état actuel de SELinux.
Utilisez sestatus --help pour voir les options disponibles.

setsebool: Modifie les paramètres SELinux booléens.
Utilisez setsebool --help pour voir les options disponibles.

Ces commandes sont les plus couramment utilisées pour gérer SELinux et ajuster ses paramètres selon les besoins de sécurité du système.

INSTALLATION HTTPD

En t'en que root faire les commandes suivantes pour installer un service web.

sudo dnf install httpd -y
sudo systemctl start httpd.service

Je veux que mes users puissent héberger leur propre serveur web a partir de leurs directoires home.

On active la fonctionnalité UserDir dans /etc/httpd/conf.d/userdir.conf

```
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    #UserDir disabled

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" line above, and uncomment
    # the following line instead:
    #
    UserDir public_html
</IfModule>

#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
<Directory "/home/*/public_html">
    AllowOverride FileInfo AuthConfig Limit Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

On redémarre le service httpd

Pour verifier le bon fonctionnement on peux faire la command
systemctl status httpd ou httpd.service

```
root@localhost:~# sudo systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
    Drop-In: /usr/lib/systemd/system/service.d
             └─10-timeout-abort.conf
     Active: active (running) since Tue 2024-05-14 14:05:30 CEST; 2s ago
```

LE USER “BREAD”

Un utilisateur “Bread” à été créé.

```
root@localhost:~# useradd bread
```

Bread crée le dossier public.html dans sont répertoire home.
Home/bread/public.html/

```
root@localhost:~# ls -ld /home/bread/
d-wx-----x. 3 bread bread 102 May 14 13:48 /home/bread/
root@localhost:~#
```

Bread crée un fichier index.html

```
bread@localhost:~$ cd public.html
bread@localhost:~/public.html$ echo "J'aime l'Ermitage d'agen" > index.html
bread@localhost:~/public.html$
```

En allant sur un navigateur et en utilisant l’adresse IP avec /~leuser cette page s’afficheras.
http://192.168.200.142/~bread

CONFIGURATION DES BOOLEANS

Le booleans nous permet d'activer des securiter pour autoriser par exemple un serveur web de d'ouvrir des fichier index.html

setsebool -P httpd_can_network_connect on -P
setsebool -P httpd_enable_homedirs on -P

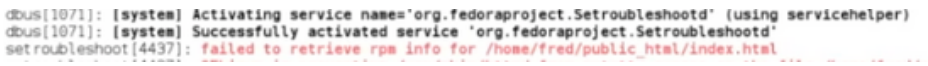
setsebool -P httpd_enable_homedirs on -P

Persisting
Si le serveur redémarre le paramètre reste activer.

Flag pour autoriser le serveur http a accéder les direction home "LABEL"

Activer ou désactiver le flag

Actuellement NGINX a accès de lire les directoire home du serveur Ubuntu.
Cette exemple c'est seulement si par exemple le serveur WEB ce trouve dans /home/userlol/monserveurwebmagnifique/x



LOGS SELINUX

```
)us[1071]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
)us[1071]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
troubleshoot[4437]: failed to retrieve rpm info for /home/fred/public_html/index.html
```

CONFIGURATION DU FICHIER INDEX.HTML

Il faut qu'on vérifie le fichier index.html sois bien un fichier httpd pour que SELinux l'autorise.

Pour cela on vas dans le dossier en question

cd /home/bread/public.html
puis
ls -lZ

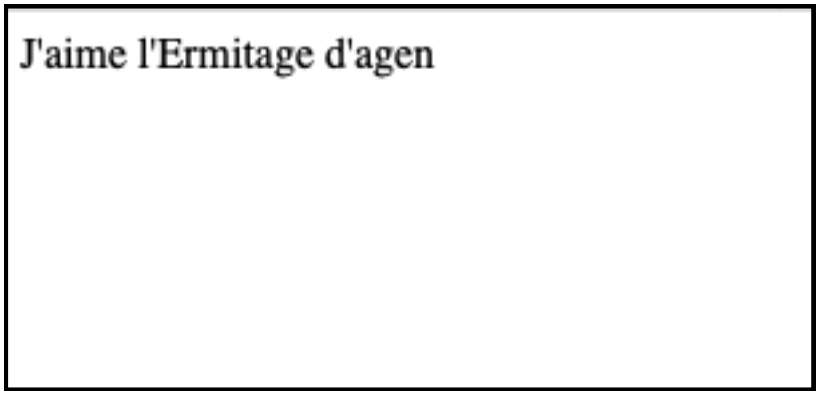
```
root@localhost:~# cd /home/bread/public.html
root@localhost:/home/bread/public.html# ls -lZ
total 4
-rw-r--r--. 1 bread bread unconfined_u:object_r:user_home_t:s0 25 May 14 13:56 index.html
root@localhost:/home/bread/public.html#
```

Le flag n'est pas bon

On doit modifier leflag pour que SELinux autorise le fichier comme fichier httpd.
Pour cela on fait la commande
chcon -Rt httpd_sys_content_T index.html ou chemin/vers/fichier

```
root@localhost:/home/bread/public.html# chcon -Rt httpd_sys_content_t index.html
root@localhost:/home/bread/public.html# ls -lZ
total 4
-rw-r--r--. 1 bread bread unconfined_u:object_r:httpd_sys_content_t:s0 25 May 14 13:56 index.html
```

Apres un reboot le serveur web est disponible.



INTÉGRATION DE SELINUX DANS UN ENVIRONNEMENT DE PRODUCTION

L'intégration de SELinux (Security-Enhanced Linux) dans un environnement de production nécessite une bonne planification.

a. Compréhension des Concepts de Base

- Documentation : Fournir des documents de référence et des guides sur SELinux à l'équipe de devellopement.

b. Évaluation de l'Environnement Actuel

- Audit du système : Identifiez les services critiques, applications et configurations actuelles.
- Compatibilité : Vérifiez la compatibilité des applications et des services avec SELinux.

Pour notre exemple ce seras un siteweb avec un acces FTP.

Avant d'integrer la securiter de SELinux en production il faudras créer un environnement de test avec de le déployer en LIVE.

a. Installation de SELinux sur la machine test

- Installer SELinux sur un environnement de test identique à la production.
- Configuration initiale : Configurer SELinux en mode permissif (setenforce 0) pour observer sans appliquer les restrictions.

b. Observation et Ajustement

- Collecte de logs : Surveillez les logs pour les alertes SELinux en utilisant audit2allow pour comprendre quelles actions seraient bloquées en mode enforcing.
- Ajustements des politiques : Créez et ajustez les politiques de sécurité pour permettre les opérations legitimes.

c. Tests Rigoureux

- Test fonctionnel : Exécutez des tests fonctionnels pour vérifier que toutes les applications et services fonctionnent comme prévu.
- Tests de sécurité : Effectuez des tests de pénétration et de sécurité pour s'assurer que SELinux renforce la sécurité sans bloquer les opérations nécessaires.

INTÉGRATION DE SELINUX DANS UN ENVIRONNEMENT DE PRODUCTION

Déploiement Progressif en Production

a. Mode Permissif en Production

- Passage en mode permissif : Déployez SELinux en mode permissif sur les serveurs de production.
- Surveillance continue : Continuer à surveiller les logs SELinux et ajustez les politiques en conséquence.

b. Transition vers le Mode Enforcing

- Phases de transition : Passez progressivement certains serveurs ou services en mode enforcing (setenforce 1).
- Validation : Validez que les systèmes fonctionnent correctement en mode enforcing sans interruption de service.

Maintien et Amélioration

a. Surveillance et Maintenance

- Surveillance : Utilisez des outils de monitoring pour surveiller les alerte et incidents lies à SELinux.

c. Documentation Continue

- Maintien de la documentation : Assurez-vous que la documentation est continuellement mise à jour pour refléter les changements dans les politiques et configurations de SELinux.

SENSIBILISATION

Déploiement Progressif en Production

a. Mode Permissif en Production

- Passage en mode permissif : Déployez SELinux en mode permissif sur les serveurs de production.
- Surveillance continue : Continuer à surveiller les logs SELinux et ajustez les politiques en conséquence.

b. Transition vers le Mode Enforcing

- Phases de transition : Passez progressivement certains serveurs ou services en mode enforcing (setenforce 1).
- Validation : Validez que les systèmes fonctionnent correctement en mode enforcing sans interruption de service.

Maintien et Amélioration

a. Surveillance et Maintenance

- Surveillance : Utilisez des outils de monitoring pour surveiller les alerte et incidents lies à SELinux.

c. Documentation Continue

- Maintien de la documentation : Assurez-vous que la documentation est continuellement mise à jour pour refléter les changements dans les politiques et configurations de SELinux.

RESSOURCE

RedHat Summit What is SELinux?
https://www.youtube.com/watch?v=_WOKRaM-HI4

Fedora Website:
https://fedoraproject.org

CONCLUSION

Coordonnées

Agen
Rue du lot

www.campusermitage.fr
groupe1@campusermitage.fr

Campus Ermitage