RockyLinux-ANSSI-BP-028

MANUEL D’EXPLOITATION

Version	Version de l’OS applicable	Date	Commentaire	Par
1.0	9.3-1	16 Janvier 2024	Publication initiale	Chelsea Murgia mail@chelsea486 mhz.fr

[Page vide]

SOMMAIRE

5. Services actifs sur la machine

a. Pare-feu
b. Cockpit
c. OpenSSH

III – MANUEL DE MODIFICATION DE L'INSTALLATION

1. Inclure une clé publique SSH

2. Inclure un package RPM

I – MANUEL D’INSTALLATION

Le manuel d’installation a pour but de guider l’administrateur système dans le provisionnement et le déploiement d’un serveur sécurisé RockyLinux-ANSSI-BP-028.

1. Configuration matérielle minimale requise

Type de matériel	Configuration minimale requise
RAM	4096 Mo
CPU	1 vCPU, accélération matérielle AES, jeu d’instruction x86_64
Réseau	Adaptateur réseau Ethernet (connexion non requise)
Stockage	Disque VirtIO« système » de 32 Go (/dev/vda)
Système	Support UEFI activé
TPM	V2.0 activé
Virtualisation	Agent QEMU activé

2. Acquisition des fichiers d’installation

La version actuelle du système d’exploitation sécurisé est 9.3, Release 1.

a. Image disque

L’image disque doit être obtenue par GitHub :

```
$ wget https://github.com/Chelsea486MHz/RockyLinux-ANSSI-BP-028/releases/download/
v9.3-1/RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso
```

b. Somme de contrôle

La somme de contrôle SHA-256 doit être obtenue par GitHub :

```
$ wget https://github.com/Chelsea486MHz/RockyLinux-ANSSI-BP-028/releases/download/
v9.3-1/RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso.sha256sum
```

c. Signatures PGP

Les signatures PGP doivent être obtenues par GitHub :

```
$ wget https://github.com/Chelsea486MHz/RockyLinux-ANSSI-BP-028/releases/download/
v9.3-1/RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso.sig
$ wget https://github.com/Chelsea486MHz/RockyLinux-ANSSI-BP-028/releases/download/
v9.3-1/RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso.sha256sum.sig
```

d. Clé publique PGP

La clé publique de l'autrice doit être obtenue par GitHub :

```
$ wget https://github.com/Chelsea486MHz/RockyLinux-ANSSI-BP-028/releases/download/
v9.3-1/pubkey.asc
```

3. Vérification des fichiers d'installation

a. Intégrité

La vérification de l'intégrité de l'image d'installation vous permet d'établir que le fichier de l'image disque est rigoureusement identique à celui sur lequel les tests ont été effectués.

Pour vérifier l'intégrité de l'image disque :

```
$ sha256sum -c RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso.sha256sum
```

b. Signatures

La vérification des signatures vous permet d'établir que l'image d'installation et sa somme de contrôle ont été fournis par la personne contrôlant la clé PGP de l'autrice du projet, Chelsea Murgia.

Cette clé étant stockée sur une YubiKey, la vérification des signatures permet donc d'établir avec un haut niveau de confiance que les fichiers ont été émis par Chelsea Murgia.

Il est nécessaire pour cette étape d'importer la clé publique PGP de Chelsea Murgia :

```
$ gpg --import pubkey.asc
```

Pour vérifier la signature de la somme de contrôle :

```
$ gpg --verify RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso.sha256sum.sig RockyLinux-
ANSSI-BP-028-9.3-1-x86_64.iso.sha256sum
```

Pour vérifier la signature de l’image disque :

```
$ gpg --verify RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso.sig RockyLinux-ANSSI-BP-028-9.3-1-x86_64.iso
```

4. Création de la machine virtuelle

Sous Proxmox 8.1, la création d’une machine virtuelle répondant à la configuration matérielle minimale requise à l’utilisation du système d’exploitation sécurisé RockyLinux-ANSSI-BP-028 demande les options suivantes :

Nom du réglage	**Valeur du réglage**
System / Machine	q35
System / BIOS	OVMF (UEFI)
System / Qemu agent	activé
System / Add TPM	activé
Disks / Bus / Device	VirtIO Block
Disks / Disk size (GiB)	32
CPU / Type	x86-64-v2-AES
Memory / Memory (MiB)	4096
Network / Model	VirtIO (paravirtualized)

5. Installation du système d’exploitation sécurisé

L’image disque doit être introduite dans un lecteur DVD de la machine virtuelle.

Pour démarrer l’installation, il suffit de démarrer la machine virtuelle.

Si la configuration de cette dernière répond aux exigences décrites dans ce manuel, l’installation est automatique. Le système s’éteindra automatiquement après installation et l’image disque pourra être retirée.

En cas d’erreur, une entrée utilisateur sera requise.

II – MANUEL UTILISATEUR

1. La machine installée

a. Partitionnement du disque

Le partitionnement du disque répond aux exigences de l'ANSSI en matière de recommandations de configuration d'un système GNU/Linux, telles que définies dans leur document désigné ANSSI-BP-028.

Point de montage	Taille	Type
/boot	1024 Mo	XFS
/boot/efi	1024 Mo	EFI
/tmp	4096 Mo	TMPFS
swap	4096 Mo	swap
/	10240 Mo	XFS (LVM) (volgroup 1)
/home	1024 Mo	XFS (LVM) (volgroup 1)
/usr	4096 Mo	XFS (LVM) (volgroup 1)
/var	10240 Mo	XFS (LVM) (volgroup 1)
/var/tmp	1024 Mo	XFS (LVM) (volgroup 1)
/var/log	1024 Mo	XFS (LVM) (volgroup 1)
/var/log/audit	1024 Mo	XFS (LVM) (volgroup 1)
/srv	1024 Mo	XFS (LVM) (volgroup 1)
/opt	1024 Mo	XFS (LVM) (volgroup 1)

b. Conformité aux normes ANSSI-BP-028

La conformité du système déployé aux exigences de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) en matière de recommandations de configuration d'un système GNU/Linux, telles que définies dans leur document désigné ANSSI-BP-028, est établie par le logiciel OpenSCAP.

OpenSCAP réalise des tests techniques sur des exigences précises. Les exigences décrites dans le document désigné ANSSI-BP-028 ne sont pas suffisamment précises pour permettre de déléguer

entièrement l’analyse de conformité à OpenSCAP. De plus, de part la nature générale des des exigences, OpenSCAP peut être ammené à retourner des faux positifs et faux négatifs dans ses analyses.

Ainsi, il reste impératif de réaliser des audits et analyses de conformité manuellement avant de pouvoir établir avec certitude que le système répond aux exigences.

c. Niveau de sécurité

Le document désigné ANSSI-BP-028 fait état de 4 niveaux de sécurité : minimal, intermediate, enhanced, et high.

Le système RockyLinux-ANSSI-BP-028 est conforme au niveau de sécurité enhanced.

2. Configuration des utilisateurs

a. Mot de passe root

L’utilisateur root est créé pendant l’installation. Son mot de passe est root.

b. Création d’un utilisateur

La commande useradd est utilisée pour créer un nouvel utilisateur sur le système :

```
$ useradd <utilisateur>
```

Son mot de passe doit être créé :

```
$ passwd <utilisateur>
```

3. Sécurisation de la machine

a. Désactivation de la connexion SSH par mot de passe

Pour désactiver la connexion SSH par mot de passe, il faut modifier /etc/ssh/sshd_config :

```
PasswordAuthentication no
ChallengeResponseAuthentication no
PubkeyAuthentication yes
```

b. Ajout d’une clé publique SSH

Pour ajouter une clé publique SSH pour se connecter à un compte :

```
$ echo <clé-publique> >> /home/<utilisateur>/.ssh/authorized_keys
```

c. Ré-évaluation de la conformité aux normes ANSSI-BP-028

OpenSCAP peut être utilisé pour réévaluer la conformité du système après l’apport de modifications.

```
$ oscap xccdf eval --remediate --results res.xml --profile
xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced
/usr/share/xml/scap/ssg/content/ssg-rl9-ds.xml
```

d. Remédiations de sécurité

Une remédiation automatique peut être appliquée après une évaluation à l’aide du paramètre --remediate :

```
$ oscap xccdf eval --remediate --results res.xml --profile
xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced
/usr/share/xml/scap/ssg/content/ssg-rl9-ds.xml
```

4. Configuration du système

a. Nom d’hôte

Le nom d’hôte de la machine peut être changé avec la commande hostnamectl :

```
$ hostnamectl set-hostname <nom>
```

Un redémarrage est nécessaire pour compléter la procédure.

b. rsyslog

Par défaut, rsyslog est installé et configuré par OpenSCAP. Cependant, les certificats TLS à utiliser doivent être introduits manuellement.

c. sudo

La configuration de sudo dépend des utilisateurs et des usages, et doit être en conséquence complétée manuellement.

5. Services actifs sur la machine

a. Pare-feu

Un pare-feu (firewalld) est installé sur la machine. Par défaut, les ports suivants sont ouverts :

Nom	Port
ssh	22/tcp
cockpit	9090/tcp

b. Cockpit

Cockpit est une interface web d'administration. Il est exposé sur le port 9090. Par soucis de sécurité, le compte root n'est pas autorisé à s'y connecter. Il est cependant possible de l'autoriser avec la commande suivante :

```
# echo ‘ ‘ > /etc/cockpit/dissalowed-users
```

c. OpenSSH

Un serveur OpenSSH est actif sur la machine et écoute sur le port 22.

III – MANUEL DE MODIFICATION DE L’INSTALLATION

Il est possible de modifier le processus d’installation. Pour ce faire, il est nécessaire de cloner le dépôt git :

```
$ git clone https://github.com/Chelsea486MHz/RockyLinux-ANSSI-BP-028
$ cd RockyLinux-ANSSI-BP-028
```

Le processus de création d’une image d’installation nécessite Docker. L’image construite et sa somme de contrôle seront trouvables dans le répertoire build. Chaque modification demanderas de reconstruire l’image Docker avant de reconstruire l’image d’installation dans l’image Docker.

Pour reconstruire l’image Docker:

```
$ docker build -t rockylinux-bp-028-build .
```

Pour reconstruire l’image disque :

```
$ docker run --rm -v ./build:/build rockylinux-bp-028-build
```

Pour reconstruire l’image disque et garder l’image RockyLinux d’origine en cache :

```
$ docker run --rm -v ./build:/build -v ./RockyLinux:/RockyLinux rockylinux-bp-028-build
```

1. Inclure une clé publique SSH

Il est possible d’intégrer une clé publique SSH dans le processus d’installation. Pour ce faire, il faut rajouter une commande dans le fichier kickstarts/post.ks :

```
mkdir /root/.ssh
echo ‘<clé>’ > /root/.ssh/authorized_keys
```

2. Inclure un package RPM

Il est possible d’inclure un package RPM et l’installer automatiquement. Pour ce faire, il faut ajouter le nom du paquet dans le fichier packages-to-add.txt puis dans la liste des paquets du fichier kickstarts/packages.ks.