Code Affaire : **1-12-AIA-1900** N° Marché ou N° Cde : **2018 – 19 31 033 000 – 00 00**

Classification : **Non Protégé**

Diffusion interne : (Diffuse aux personnes concernées au sein de sa structure)

Diffusion externe :

Rédigé par **N. CERVERA**	Vérifié par **O. SELLIER**	Approuvé par **JC. PEREZ**	Approuvé par
Visa NICOLAS CERVERA Signature numérique de NICOLAS CERVERA Date : 2023.02.24 10:24:03 +01'00'	Visa OLIVIER SELLIER Signature numérique de OLIVIER SELLIER Date : 2023.02.24 14:28:27 +01'00'	Visa	Visa

Procédure d'installation et de justification de la Station Sol du Système FRANC – Version SSI

REVISIONS

IND.	DATE	SECR.	REDACTEUR	OBJET
00	**08/08/2022**		**J. PIGNOLET**	**Version Initiale**
01	**28/12/2022**		**N. CERVERA**	**Ajout du tableau de justification en annexe validé par AIACP/SDT/PC (JC PEREZ)**

Table des matières

ANNEXES

N°	Intitulé
1	TABLEAU DE JUSTIFICATION SSI

1. Identification

Ce document constitue la procédure d'installation de la Station Sol du Système FRANC dans sa version SSI.

La Station Sol est constituée du PC portable durci fourni par la société 6TA (référence ARP998) dont voici un aperçu :

En plus de l'OS, la Station Sol contient les logiciels suivants :

- AccueilFRANC-STD2 : IHM d'Accueil FRANC Standard 2
- PlayerXS : Logiciel de Restitution FRANC Standard 2
- FormatageSSI : IHM de Formatage SSI FRAnC Standard 2
- LectureTABMNT : IHM de lecture des tables de maintenance d'un coffret FRANC

2. Documents

2.1. DOCUMENTS APPLICABLES

Rep.	Intitulé	Référence	Indice	Date
[A1]	Instructions d'installation SSI Linux	DP072596NTE008	00	27/10/2021
[A2]	Recommandations de Configuration d'un système Gnu/linux	ANSSI-BP-028	1.2	22/02/2019

2.2. DOCUMENTS DE REFERENCE

Rep.	Intitulé	Référence	Indice	Date
[R1]	FCL Logiciel AccueilFRANC-STD2	DP072596FCL016	00	25/01/21
[R2]	FCL Logiciel PlayerXS	DP072596FCL015	00	25/01/21
[R3]	FCL Logiciel FormatageSSI-STD2	DP072596FCL017	01	10/03/21

3. Terminologie et sigles utilisés

Terme	Définition
FRANC	French Recorder Analyser Numeric Computer
OS	Operating System

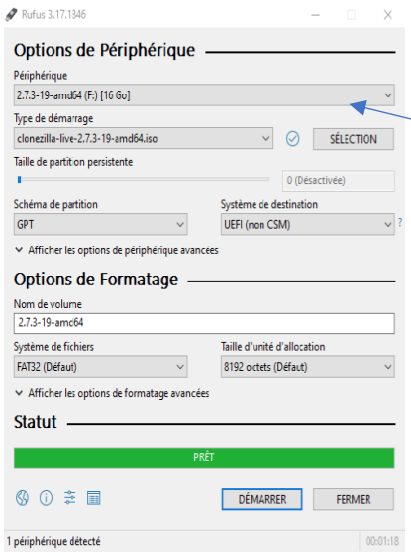
4. Procédure d'installation

4.1. CREATION D'UNE CLE DE DEMARRAGE

Il s'agit de la distribution linux **Kubuntu 20.04.4**.
Il faut dans un premier temps télécharger l'image ISO **kubuntu-20.04.4-desktop-amd64.iso** sur le site de Kubuntu, à l'adresse suivante : *http://cdimage.ubuntu.com/kubuntu/releases/20.04.4/release/.* Sinon il faut utiliser l'image ISO présente sur le serveur : \\srv-filer01.global.ad\AFFAIRES_DIGILOG\1-12-AIA-1900\TECHNIQUE\SSI\01-ISO\Kubuntu_20.04.4.

Pour créer une clé bootable, il nous faut l'image ISO précédemment citée et le logiciel Rufus (OS Windows) disponible sur Internet ou \\srv-filer01.global.ad\AFFAIRES_DIGILOG\1-12-AIA-1900\TECHNIQUE\SSI\00-OUTILS\Rufus.
On note également qu'il est nécessaire de disposer d'une clef USB que la procédure va effacer, les données présentes sur la clef seront effacées. Il est préconisé d'utiliser des clefs USB3.

1) Brancher la clef USB
2) Lancer Rufus
3) Sélectionner la clef USB dans l'option « Périphérique »
4) Sélectionner l'ISO dans l'option « Type de démarrage »
5) Sélectionner le schéma de partition « GPT »
6) Nommer la clef « Kubuntu-20.04.4 »



Sélectionner la clef USB

Sélectionner l'ISO

Sélectionner le schéma GPT

7) Laisser les autres paramètres par défaut
8) Système de destination : **UEFI**
9) Système de fichier : **FAT32**
10) Taille d'unité d'allocation : **4096 octets**
11) Démarrer la création de la clef
12) Quand la création est terminée, fermer Rufus et éjecter la clef

Nommer la clé

Démarrer la création de la clef

4.2. INSTALLATION DE L'OS

Booter sur la clé USB en démarrant le système avec la clé branchée (si besoin forcer le boot dessus à partir du BIOS).
Choisir l'entrée de menu « Start Kubuntu », puis vient une analyse sur les fichiers sur la clé.
Une fois sur le bureau, sélectionner un affichage en français, puis le choix « Try Kubuntu » (cela permettra de configurer l'affichage à la taille de l'écran 4K pour une meilleure lisibilité de l'écran).
Une fois sur le bureau, aller dans le menu *Apparence → Police → Police de caractères* et cocher « Forcer le PPP de la police » et mettre 176.
Lancer l'installation en lançant le raccourci sur le bureau « Install Kubuntu ».
Lors de l'installation, effectuer les choix suivants :

- Langue française + disposition clavier français
- Installation minimale
- Pas d'installation de logiciels tiers
- Pas de connexion à internet
- Partitionnement manuel sur le point d'amorçage /dev/nvme0n1 avec les infos suivantes (sur la base d'un disque NVME de 512Go):

Partition	Montage	Taille	Note
nvme0n1p1	/boot (ext2)	600Mo	
nvme0n1p2	/	10Go	
nvme0n1p3	/usr	20Go	A augmenter/réduire selon besoin si des apps utilisateurs sont installées ici
nvme0n1p4	/opt	30Go	A augmenter/réduire selon besoin si des apps utilisateurs sont installées ici
nvme0n1p5	/var	100Go	
nvme0n1p6	/var/log	125Go	Donner une taille conséquente car les outils SSI génèrent bcp de logs
nvme0n1p7	/var/tmp	20Go	Fichiers temporaires conservés après extinction
nvme0n1p8	/tmp	10Go	Si possible en tmpfs pour que le dossier se vide à chaque re-boot
nvme0n1p9	SWAP	8Go	Si possible à la même taille que la taille de la RAM du système
nvme0n1p10	EFI	600Mo	
nvme0n1p11	/home	Le reste	Ne pas trop réduire la taille car les vidéos FRANC peuvent temporairement être stockées sur l'OS

- Toutes les partitions (exceptée « /boot ») sont en ext4
- Renseigner les tailles du tableau et laisser le logiciel arrondir (ne pas s'efforcer de tomber sur une taille précise) : 600Mo seront arrondis à 598Mo par exemple.
- Ne pas utiliser de miroir réseau
- Choisir le fuseau horaire « Paris - France »
- Entrer les valeurs suivantes pour la configuration du compte utilisateur principal :
  - Nom: MAINTENANCE
  - Nom d'utilisateur: maintenance
  - Mot de passe: cf. fichier « password.txt »
  - Nom du poste: francE2C-stationSOL
  - Mot de passe à chaque connexion

A l'issue de l'installation la clé USB peut être retirée et le PC redémarré pour effectuer les opérations décrites dans les paragraphes suivants.

4.3. CONFIGURATION DE L'OS

4.3.1. ADAPTATION DE LA TAILLE DE LA POLICE A L'ECRAN 4K

Lancer le logiciel « Configuration du système » puis aller dans le menu *Apparence* → *Police* → *Police de caractères* et cocher « Forcer le PPP de la police » et mettre 176.

4.3.2. AJOUT DES OUTILS / LIBRAIRIES POUR LES LOGICIELS FRANC-STATION SOL

Le poste devant rester hors-ligne (règle SSI), les paquets suivants doivent être récupérés depuis le répertoire SSI sur le réseau (\\srv-filer01.global.ad/AFFAIRES_DIGILOG/1-12-AIA-1900/TECHNIQUE/BINAIRES/Logiciels/OFFLINE-DEPS-STATION_SOL/ESSENTIAL) sur une clé USB:

Liste-Offline-Deps-StationSol.txt

- Brancher la clé USB sur un des ports USB du poste.
- Monter la clé ('x' correspond au device qui vient d'apparaître et 'y' à sa partition) :

```
sudo mount /dev/sdxy /mnt
```

- Se déplacer vers le point de montage de la clé USB dans le dossier contenant les .deb:

```
cd /chemin/vers/le/répertoire/OFFLINE-DEPS-STATION_SOL/ESSENTIAL
```

- Installer toutes les packages (plusieurs fois selon l'ordre d'installation dû aux dépendances) :

```
sudo dpkg -i *.deb
```

  - Attention: les paquets "libnvidia-compute-*.deb" doivent être installés dans l'ordre décroissant de version (470 -> 418) sinon il y a un problème de dépendances.

NB : si les packages sont obsolètes ou introuvables, il faut exécuter ces commandes sur un poste en-ligne pour télécharger les packages :

- Se placer dans le dossier "/var/cache/apt/archives" :

```
cd /var/cache/apt/archives
```

- Installer apt-rdepends:

```
sudo apt-get install apt-rdepends
```

- Télécharger uniquement les packages nécessaires (cf. liste).
  - Soit :

```
sudo apt download $(apt-rdepends nomPackage | grep -v "^ ")
```

  - Soit :

```
sudo apt -f install --download-only nomPackage
```

  - Soit pour télécharger tous les packages nécessaires suivant la liste fournie (fichier présent dans le dossier parent de celui des .deb) :

```
xargs sudo apt-get install --download-only < Liste-Offline-Deps-StationSol.txt
```

4.4. INSTALLATION DES LOGICIELS FRANC

4.4.1. INSTALLATION DES PAQUETS LOGICIELS

Les paquets d'installation des logiciels FRANC sont dans le répertoire des binaires du projet :
\\srv-filer01.global.ad/AFFAIRES_DIGILOG/1-12-AIA-1900/TECHNIQUE/BINAIRES/Logiciels/1.Segment_SOL/

Installer les logiciels FRANC disponibles dans chaque dossier de logiciel:

```
cd chemin/vers/le/logiciel
sudo dpkg -i nomDuLogiciel.deb
```

- Dossier "1.Segment_SOL\04.LectureTABMNT"
- Dossier "1.Segment_SOL\10.PlayerXS"
- Dossier "1.Segment_SOL\11.AccueilFRANC-STD2"
- Dossier "1.Segment_SOL\12.FormatageSSI-STD2"

Remarque : pour le logiciel PlayerXS, il est également nécessaire d'installer la librairie de décompression (IpxGpuCodec) dont le paquet est situé dans le même répertoire que celui du PlayerXS.

4.4.2. MISE EN PLACE DES FICHIERS CHIFFRES DE PROTECTION

Afin de protéger les logiciels contre de multiples installations, lors du démarrage d'un logiciel celui-ci vérifie que le numéro de série du disque de la machine correspond à celui indiqué lors de la génération du setup d'installation.
Le numéro de série attendu est stocké dans un fichier crypté devant se trouver dans le répertoire parent du binaire, nommé « serial.gpg ».

Or en suivant cette note technique, on a utilisé directement les paquets d'installation (fichiers .deb) et non les fichiers de setup d'installation (fichiers .franc), donc le fichier contenant le numéro de série n'existe pas.
==> il faut donc le créer en suivant la méthode suivante :

a) récupération du numéro de série du disque :

```
lsblk -no serial /dev/nvme0n1
```

Où sdX correspond au device associé au disque de l'OS (utiliser la commande df pour récupérer le nom de device : device associé au point de montage '/')

b) création du fichier chiffré contenant le numéro de série attendu :

```
echo "num_série" > /tmp/serial.txt
echo FRANC_atos_2020 | gpg --batch --yes --passphrase-fd 0 -o /tmp/serial.gpg -c /tmp/serial.txt
```

c) terminer par la copie du fichier chiffré dans le répertoire parent du binaire :
Pour chaque logiciel FRANC, faire la commande suivante :

```
sudo cp /tmp/serial.gpg /opt/Atos/<nom du logiciel>/serial.gpg
```

NB : les numéros de série des NVME présents dans les stations SOL sont :

- N/S 0001 (prototype): G107580666
- N/S 0002: H061790503
- N/S 0003: H061790494
- N/S 0004: H061790500
- N/S 0005: H061790483

4.5. CREATION DE L'UTILISATEUR « FRANC »

Lancer le logiciel « Configuration du système », puis se rendre dans le menu *Personnalisation* → *Détails du compte* → *Gestionnaire des utilisateurs* :
Cliquer sur « Nouvel utilisateur », puis renseigner les champs suivants :

- Nom de l'utilisateur = franc
- Nom réel = FRANC
- Pas d'adresse mail
- Cliquer sur « Définir un mot de passe » et mettre : cf. fichier « password.txt »
- Cocher « Activer les privilèges d'administrateur pour cet utilisateur »

4.6. CONFIGURATION DU COMPTE UTILISATEUR « FRANC »

Fermer la session « alse » et ouvrir une nouvelle session avec l'utilisateur « franc ».

Lancer le logiciel « Configuration du système » :

- Espace de travail → Démarrage et arrêt : pour « Session de bureau », sélectionner « Démarrer avec une session vide »
- Apparence → Police → Police de caractères : cocher « Forcer le PPP de la police » et mettre 176
- Matériel → Economie d'énergie : décocher « Economie d'énergie pour l'écran »
- Espace de travail → Démarrage et arrêt → Démarrage automatique : cliquer sur "Ajouter un programme" et choisir /opt/Atos/AccueilFRANC-STD2/bin/AccueilFRANC-STD2
- Espace de travail → Gestion des fenêtres → Règles de la fenêtre : cliquer sur « Nouveau... » pour créer une nouvelle règle :
  - Dans l'onglet « Correspondance de fenêtre » :
    - Champ « Description », mettre par ex. Accueil FRANC
    - Champ « Types de fenêtres » tout laisser sélectionné
  - Dans l'onglet « Apparence et corrections », sélectionner « Ignorer les raccourcis globaux »,
  - Sélectionner « Forcer » et cliquer sur Oui
- Suppression de la barre des tâches / tableau de bord :
  - Click droit dessus --> Modifier Tableau de bord...
  - Cliquer sur « Supprimer Tableau de bord » à gauche de la barre
- Et pour fermer la session (puisqu'il n'y a plus de tableau de bord), faire click droit n'importe où sur le bureau et choisir Quitter…

5. Mise en place des recommandations SSI

Sur la base du document de l'ANSSI en version 1.2 disponible sur le serveur (\\srv-filer01.global.ad\AFFAIRES_DIGI-LOG\1-12-AIA-1900\TECHNIQUE\SSI\03-DOCS\linux_configuration-fr-v1.2.pdf) ou en ligne sur le site de l'ANSSI (https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/), les recommandations pour sécuriser le poste sont appliquées et sont justifiées dans les paragraphes suivants. Les preuves d'application des recommandations sont aussi disponibles sur le serveur : \\srv-filer01.global.ad\AFFAIRES_DIGILOG\1-12-AIA-1900\TECHNIQUE\SSI\02-PREUVES-RECO-ANSSI.

5.1. R1 (MIRE) : MINIMISATION DES SERVICES INSTALLES

Liste faîte des services démarrés nécessaires au fonctionnement des logiciels FRANC via la commande:

```
systemctl list-units --type=service
```

R01-Liste-Services-with_Systemctl.txt

5.2. R2 (MIRE) : MINIMISATION DE LA CONFIGURATION

La présence de tous nos services en cours d'exécution est justifiable donc notre système respecte ces règles.

La commande suivante permet de vérifier ce point :

```
systemctl list-units --type=service --state=running
```

R02-Liste-Services_Running-with_Systemctl.t

5.3. R5 (MIRE) : PRINCIPE DE DEFENSE EN PROFONDEUR

Les 4 principes sont :

1) Authentification nécessaire avant d'effectuer des opérations, notamment quand elles sont privilégiées ;
2) Journalisation centralisée d'évènements au niveau systèmes et services ;
3) Priorité à l'usage de services qui implémentent des mécanismes de cloisonnement et/ou de séparation de privilèges ;
4) Utilisation de mécanismes de prévention d'exploitation

Les trois premiers points sont validés du fait de la distribution Kubuntu et le point « Mécanismes de prévention d'exploitation » consiste à cloisonner les applications qui peuvent apporter des modifications graves au système ou à fournir des infos à distance: cela n'est pas le cas dans notre application car les logiciels FRANC sont hors-ligne et ne sont pas malveillants.

5.4. R8 (MIRE) : MISES A JOUR REGULIERES

Ces mises-à-jour ne sont à effectuer que sur le compte « maintenance » uniquement si un problème apparaît sur l'OS durant son utilisation.

5.5. R9 (IRE) : CONFIGURATION MATERIELLE

Le client valide de ne pas appliquer cette recommandation.

5.6. R10 (IRE) : ARCHITECTURE 32 ET 64 BITS

Par sa nature, la distribution Kubuntu 20.04.4 fonctionne avec une architecture 64 bits.

5.7. R12 (IRE) : PARTITIONNEMENT TYPE

Le partitionnement type appliqué (par modification du fichier « /etc/fstab ») est le suivant :

R12-fstab.txt

Point de montage	Options	Description
/		Partition racine, contient le reste de l'arborescence.
/boot	nosuid,nodev,noexec (noauto optionnel)	Contient le noyau et le chargeur de démarrage. Pas d'accès nécessaire une fois le boot terminé (sauf mise à jour).
/opt	nosuid,nodev (ro optionnel)	Packages additionnels au système. Montage en lecture seule si non utilisé.
/tmp	nosuid,nodev,noexec	Fichiers temporaires. Ne doit contenir que des éléments non exécutables. Nettoyer par le système à chaque reboot.
/home	nosuid,nodev,noexec	Contient les HOME utilisateurs. Montage en lecture seule si non utilisé.
/usr	nodev	Contient la majorité des utilitaires et fichiers système.
/var	nosuid,nodev,noexec	Partition contenant des fichiers variables pendant la vie du système (mails, fichiers PID, bases de données d'un service).
/var/log	nosuid,nodev,noexec	Contient les logs du système.
/var/tmp	nosuid,nodev,noexec	Fichiers temporaires conservés après extinction.

5.8. R14 (MIRE) : INSTALLATION DE PAQUETS REDUITE AU STRICT NECESSAIRE

Les paquets installés sont réduits au maximum, ce sont ceux nécessaires pour les logiciels FRANC ainsi que ceux nécessaires pour la SSI.

5.9. R15 (MIRE) : CHOIX DES DEPOTS DE PAQUETS

Le téléchargement des paquets nécessaires aux logiciels FRANC et à la procédure SSI s'est fait via un autre poste sous distribution Ubuntu 20.04 LTS connecté aux dépôts officiels Linux et ces mêmes paquets ont été transmis au poste SSI concerné par une clé USB sécurisée pour une installation offline.

5.10. R18 (MIRE) : ROBUSTESSE DU MOT DE PASSE ADMINISTRATEUR

Le premier utilisateur créé lors de l'installation du linux est l'utilisateur «maintenance » (accès utilisateur sudo pour commande système).

L'autre compte utilisateur créé (« franc ») pour les opérationnels aura ces accès seulement pour les logiciels FRANC.

Les mots de passe sont de type « passphrase » pour les utilisateurs "franc" et "maintenance" (validés par "cracklib-check" de PAM).

Le fichier « /etc/passwd » dispose des lignes pour « maintenance » et « franc » leur permettant de se connecter eux seulement. La modification de la ligne pour l'utilisateur « root » permet de l'empêcher l'accès au bash :

```
root:x:0:0:root:/root:/sbin/nologin
```

R18-passwd.txt

Il faut rajouter dans le fichier « /etc/ssh/ssh_config » la ligne empêchant l'utilisateur « root » de se connecter en SSH :

```
PermitRootLogin no
```

R18-ssh_config.txt

Il faut empêcher l'utilisateur « root » de se connecter localement via la commande :

```
sudo passwd –lock root
```

5.11. R19 (IRE) : IMPUTABILITE DES OPERATIONS D'ADMINISTRATION

L'administrateur du poste est l'utilisateur « maintenance », l'utilisateur « root » est désactivé et les élévations de droits se font via « sudo ».

5.12. R21 (IRE) : DURCISSEMENT ET SURVEILLANCE DES SERVICES SOUMIS A DES FLUX ARBITRAIRES

Le client valide de ne pas appliquer cette recommandation.

5.13. R22 (IRE) : PARAMETRAGE DES SYSCTL RESEAU

Selon les recommandations de l'ANSSI, l'IPV6 est désactivé et le paramétrage de l'IPV4 est sécurisé dans le fichier « /etc/sysctl.conf » :

R22-sysctl_conf-Edit.t
xt

5.14. R23 (IRE) : PARAMETRAGE DES SYSCTL SYSTEME

Selon les recommandations de l'ANSSI, le paramétrage sécurisé du kernel est fait dans le fichier « /etc/sysctl.conf » :

R23-sysctl_conf-Edit.t
xt

5.15. R27 (IRE) : DESACTIVATION DES COMPTES DE SERVICES

Seuls les comptes « maintenance » et « franc » sont actifs.

5.16. R30 (MIRE) : APPLICATIONS UTILISANT PAM

La liste des services présents dans le dossier « /etc/pam.d/ » contient les applications utilisant PAM prouvant qu'elles sont réduites au minimum :

R30-Liste-PAM-Services.txt

5.17. R31 (IRE) : SECURISATION DES SERVICES RESEAU D'AUTHENTIFICATION PAM

Quand l'authentification se déroule au travers d'un service distant (réseau), le protocole d'authentification utilisé par PAM doit être sécurisé (chiffrement du flux, authentification du serveur distant, mécanismes d'anti-rejeu, etc.).

Il faut bloquer un compte pendant 5 minutes après 3 tentatives de mot de passe échoué. Pour cela, on modifie le fichier « /etc/pam.d/login » en y ajoutant ces lignes :

```
# Block account for 5 minutes (300 seconds) after 3 password fails
auth    required    pam_tally.so deny=3 lock_time=300
```

R31-PAM-login.txt

Pour changer les règles de complexité des mots de passe, il faut éditer le fichier « /etc/pam.d/passwd » en y ajoutant ces lignes :

```
password    required    pam_cracklib.so minlen=12 minclass=3 \
                        dcredit=0 ucredit=0 lcredit=0        \
                        ocredit=0 maxrepeat=1                \
                        maxsequence=1 gecoscheck             \
                        reject_username enforce_for_root
```

R31-PAM-passwd.txt

5.18. R32 (MIRE) : PROTECTION DES MOTS DE PASSE STOCKES

Par défaut, le stockage des mots de passe sur Kubuntu 20.04.4 est sécurisé par un SHA-512.

Pour augmenter la protection des mots de passe stockés, il faut éditer la ligne suivante dans le fichier « /etc/pam.d/common-password » :

```
password        [success=1 default=ignore]      pam_unix.so obscure sha512 rounds=65536
```

R32-PAM-common_passwd.txt

De plus, il faut modifier le fichier « /etc/login.defs »:

```
ENCRYPT_METHOD  SHA512
SHA_CRYPT_MIN_ROUNDS 65536
```

R32-login_defs.txt

5.19. R33 (IRE) : SECURISATION DES ACCES AUX BASES UTILISATEURS DISTANTES

Le service LDAP n'est pas présent dans la conf de NSS (« /etc/nsswitch.conf ») ainsi que dans les configurations pour l'authentification: la connexion ne peut se faire que localement :

R33-nssswitch_conf.tx
t

5.20. R34 (IRE) : SEPARATION DES COMPTES SYSTEME ET D'ADMINISTRATEUR DE L'ANNUAIRE

La séparation n'est pas nécessaire car les services sont non-configurés pour.

5.21. R36 (IRE) : DROITS D'ACCES AUX FICHIERS DE CONTENU SENSIBLE

Selon l'ANSSI :

---

1) *Les fichiers systèmes sensibles doivent avoir comme propriétaire le compte root afin d'éviter qu'un changement de droits puisse être effectué par un utilisateur non privilégié ;*

2) *Quand ce fichier doit être accessible à un utilisateur non root (exemple : base de mot de passe de serveur web), l'utilisateur associé au serveur doit être membre d'un groupe dédié (exemple : www-group) qui aura un droit d'accès en lecture seule à ce fichier ;*

3) *Le reste des utilisateurs ne doit posséder aucun droit.*

Les fichiers sans utilisateur ou groupe propriétaire doivent être :

- Assignés à un utilisateur/groupe qui existe si on souhaite conserver le fichier
- Supprimés

Pour trouver les fichiers qui répondent aux deux conditions (pas d'utilisateur et pas de groupe propriétaire), on utilise la commande et s'il n'y a pas de retour tout est bon:

```
find / -type f \( -nouser -o -nogroup \) -ls 2>/dev/null
```

5.22. R37 (MIRE) : EXECUTABLES AVEC BITS SETUID ET SETGID

Il faut autoriser ces droits que pour les fichiers qui sont possédés (et exécutables) par le groupe « sudo » (qui pourront donc être limités par l'accès au groupe « sudo » et l'utilisation de la commande su/sudo).

Il est recommandé de faire un scan des fichiers avec ces droits après chaque mise à jour. On peut même le faire après chaque installation de programme pour être vraiment prévoyant.

Pour lister les fichiers sur le système avec les droits *'setuid'/'setgid'*, on utilise la commande:

```
find / -type f -perm /6000 -ls 2>/dev/null
```

Il y a ensuite un ensemble de recommandations de l'ANSSI pour des fichiers spécifiques :

Exécutable	Commentaire

/bin/mount	À désactiver, sauf si absolument nécessaire pour les utilisateurs.
/bin/netreport	À désactiver.
/bin/ping6	(IPv6) Idem ping.
/bin/ping	(IPv4) Retirer droit setuid, sauf si un programme le requiert pour du monitoring.
/bin/su	Changement d'utilisateur. Ne pas désactiver.
/bin/umount	À désactiver, sauf si absolument nécessaire pour les utilisateurs.
/sbin/mount.nfs4	À désactiver si NFSv4 est inutilisé.
/sbin/mount.nfs	À désactiver si NFSv2/3 est inutilisé.
/sbin/umount.nfs4	À désactiver si NFSv4 est inutilisé.
/sbin/umount.nfs	À désactiver si NFSv2/3 est inutilisé.
/sbin/unix_chkpwd	Permet de vérifier le mot de passe utilisateur pour des programmes non-root. À désactiver si inutilisé.
/usr/bin/at	À désactiver si atd n'est pas utilisé.
/usr/bin/chage	À désactiver.
/usr/bin/chfn	À désactiver.
/usr/bin/chsh	À désactiver.
/usr/bin/crontab	À désactiver si cron n'est pas requis.
/usr/bin/fusermount	À désactiver sauf si des utilisateurs doivent monter des partitions FUSE.
/usr/bin/gpasswd	À désactiver si pas d'authentification de groupe.
/usr/bin/locate	À désactiver. Remplacer par mlocate et slocate.
/usr/bin/mail	À désactiver. Utiliser un mailer local comme ssmtp.
/usr/bin/newgrp	À désactiver si pas d'authentification de groupe.
/usr/bin/passwd	À désactiver, sauf si des utilisateurs non-root doivent pouvoir changer leur mot de passe.
/usr/bin/pkexec	À désactiver si PolicyKit n'est pas utilisé.
/usr/bin/procmail	À désactiver sauf si procmail est requis.
/usr/bin/rcp	Obsolète. À désactiver.
/usr/bin/rlogin	Obsolète. À désactiver.
/usr/bin/rsh	Obsolète. À désactiver.
/usr/bin/screen	À désactiver.
/usr/bin/sudo	Changement d'utilisateur. Ne pas désactiver.
/usr/bin/sudoedit	Idem sudo.
/usr/bin/wall	À désactiver.
/usr/bin/X	À désactiver sauf si le serveur X est requis.

/usr/lib/dbus-1.0/dbusdaemon-launch-helper	À désactiver quand D-BUS n'est pas utilisé.
/usr/lib/openssh/sshkeysign	À désactiver.
/usr/lib/pt_chown	À désactiver (permet de changer le propriétaire des PTY avant l'existence de devfs).
/usr/libexec/utempter/utempter	À désactiver si le profil utempter SELinux n'est pas utilisé.
/usr/sbin/exim4	À désactiver si Exim n'est pas utilisé.
/usr/sbin/suexec	À désactiver si le suexec Apache n'est pas utilisé.
/usr/sbin/traceroute	(IPv4) Idem ping.
/usr/sbin/traceroute6	(IPv6) Idem ping

Une amélioration de la commande permet de lister en filtrant sur les fichiers qui sont dans les recommandations :

```
find / -type f -perm /6000 -ls 2>/dev/null | grep -E
'/bin/mount|/bin/netreport|/bin/ping6|/bin/ping|/bin/su|/bin/umount|/sbin/mount.nfs4|/sbi
n/mount.nfs|/sbin/umount.nfs4|/sbin/umount.nfs|/sbin/unix_chkpwd|/usr/bin/at|/usr/bin/cha
ge|/usr/bin/chfn|/usr/bin/chsh|/usr/bin/crontab'
```

À la suite du résultat, il faut désactiver le *'setuid'* et le *'setgid'* avec les commandes suivantes :

```
Pour désactiver setuid : chmod u-s nom_fichier
Pour désactiver setgid : chmod g-s nom_fichier
```

R37-Liste-Droits-setuid_setgid-Before.txt R37-Liste-Droits-setuid_setgid-After.txt

5.23. R39 (IRE) : REPERTOIRES TEMPORAIRES DEDIES AUX COMPTES

Le client valide de ne pas appliquer cette recommandation.

5.24. R40 (IRE) : STICKY BIT ET DROITS D'ACCES EN ECRITURE

L'ANSSI fournit les commandes utiles pour lister les droits d'écritures sur les répertoires et les fichiers.

La commande suivante permet de lister l'ensemble des répertoires modifiables par tous et sans *'sticky bit'* :

```
find / -type d \( -perm -0002 -a \ ! -perm -1000 \) -ls 2>/dev/null
```

La commande ne doit rien retourner pour valider ce point.

Il faut aussi s'assurer que le propriétaire du répertoire est bien root, sans quoi l'utilisateur propriétaire pourra à loisir modifier son contenu et ce malgré le *'sticky bit'*.

La commande suivante permet de lister l'ensemble des répertoires modifiables par tous et dont le propriétaire n'est pas root :

```
find / -type d -perm -0002 -a \ ! -uid 0 -ls 2>/dev/null
```

La commande ne doit rien retourner pour valider ce point.

Il faut lister les répertoires pour lesquels tous les utilisateurs ont les droits d'écriture mais pour lesquels le *'sticky bit'* n'est pas activé via la commande:

```
find / -type f -perm -0002 -ls 2>/dev/null
```

Le résultat de la commande permet de regrouper les fichiers en quatre catégories :

/proc/sys/...

/proc/fs/…

/proc/<>/...

/sys/kernel/...

R40-Liste-Sticky_Bit.txt

Ces types de fichiers sont temporaires et seront supprimés au redémarrage, il n'y a donc pas de problème dans notre situation.

5.25. R42 (MIRE) : SERVICES ET DEMONS RESIDENTS EN MEMOIRE

Il faut lister les services installés via la commande:

```
systemctl list-units --type=service
```

R42-Liste-Services_Demons_Before.txt

R42-Liste-Services_Demons_After.txt

Dans notre cas, il faut désactiver les services suivants via les commandes:

```
systemctl mask avahi-daemon
systemctl disable avahi-daemon
systemctl stop avahi-daemon
```

5.26. R43 (IRE) : DURCISSEMENT ET CONFIGURATION DU SERVICE SYSLOG

Le client valide de ne pas appliquer cette recommandation.

5.27. R44 (IRE) : CLOISONNEMENT DU SERVICE SYSLOG PAR CHROOT

Le client valide de ne pas appliquer cette recommandation.

5.28. R46 (IRE) : JOURNAUX D'ACTIVITE DE SERVICE

Le client valide de ne pas appliquer cette recommandation.

5.29. R47 (IRE) : PARTITION DEDIEE POUR LES JOURNAUX

Le client valide de ne pas appliquer cette recommandation.

5.30. R48 (IRE) : CONFIGURATION DU SERVICE LOCAL DE MESSAGERIE

Le client valide de ne pas appliquer cette recommandation.

5.31. R49 (IRE) : ALIAS DE MESSAGERIE DES COMPTES DE SERVICE

Le client valide de ne pas appliquer cette recommandation.

5.32. R55 (IRE) : CAGE CHROOT ET PRIVILEGES D'ACCES DU SERVICE CLOISONNE

Le client valide de ne pas appliquer cette recommandation.

5.33. R56 (IRE) : ACTIVATION ET UTILISATION DE CHROOT PAR UN SERVICE

Le client valide de ne pas appliquer cette recommandation.

5.34. R57 (IRE) : GROUPE DEDIE A L'USAGE DE SUDO

Il faut créer un groupe « sudogrp » pour que seuls les utilisateurs de ce groupe puissent utiliser *'sudo'* via la commande:

```
sudo groupadd sudogrp
```

Il faut restreindre l'accès à *'sudo'* aux seuls membres du groupe via les commandes:

```
sudo usermod -a -G sudogrp maintenance
sudo usermod -a -G sudogrp franc
```

Il faut d'abord repasser en tant qu'utilisateur « root » après l'avoir débloqué via les commandes:

```
sudo passwd –unlock root
sudo nano /etc/passwd → la ligne de « root » doit passer de « /sbin/nologin » à « /bin/bash »
sudo -i
```

Il faut changer les permissions du fichier « /usr/bin/sudo » pour permettre le *'setuid'* via les commandes:

```
chown root:sudogrp /usr/bin/sudo
chmod 4750 /usr/bin/sudo
```

Il faut vérifier que les permissions sont bien prises en compte via la commande :

```
ls -lah /usr/bin/sudo
```

R57-Droits-sudo.txt

Il faut vérifier que les utilisateurs « maintenance » et « franc » appartient bien au groupe « sudogrp » et peut exécuter *'sudo'* via la commande:

```
groups maintenance franc
```

R57-groups.txt

Il faut ensuite faire l'opération inverse pour re-bloquer l'utilisateur « root » via les commandes :

```
exit
sudo passwd –lock root
sudo nano /etc/passwd → la ligne de « root » doit passer de « /bin/bash »  à « /sbin/nologin »
```

5.35. R58 (IRE) : DIRECTIVES DE CONFIGURATION SUDO

Le client valide de ne pas appliquer cette recommandation.

5.36. R59 (MIRE) : AUTHENTIFICATION DES UTILISATEURS EXECUTANT SUDO

Par défaut à l'installation de la distribution Kubuntu, le système demande que l'utilisateur soit authentifié avant de pouvoir exécuter une commande en tant que *'sudo'*.

5.37. R60 (IRE) : PRIVILEGES DES UTILISATEURS CIBLES POUR UNE COMMANDE SUDO

Pour toute commande, il est configuré que des droits utilisateurs simples et minimaux soient appliqués aux utilisateurs « maintenance » et « franc » afin d'éviter une escalade de privilège.

5.38. R62 (IRE) : DU BON USAGE DE LA NEGATION DANS UNE SPECIFICATION SUDO

Il n'y a pas de commandes spécifiques dans le fichier « /etc/sudoers ».

5.39. R63 (IRE) : ARGUMENTS EXPLICITES DANS LES SPECIFICATIONS SUDO

Dans le fichier de configuration de *'sudo'* (« /etc/sudoers »), toutes les commandes précisent strictement les arguments autorisés à être utilisés pour les utilisateurs « maintenance » et « franc ».

L'utilisation de * n'est pas utilisé et l'absence d'argument est spécifié par la présence d'une chaine de caractères vide ("").

R63-sudoers.txt

5.40. R64 (IRE) : DU BON USAGE DE SUDOEDIT

Le client valide de ne pas appliquer cette recommandation.

6. Archivage de l'OS

6.1. SAUVEGARDE ET RESTAURATION DE L'OS AVEC CLONEZILLA

Pour finir, réaliser une sauvegarde du système avec Clonezilla.

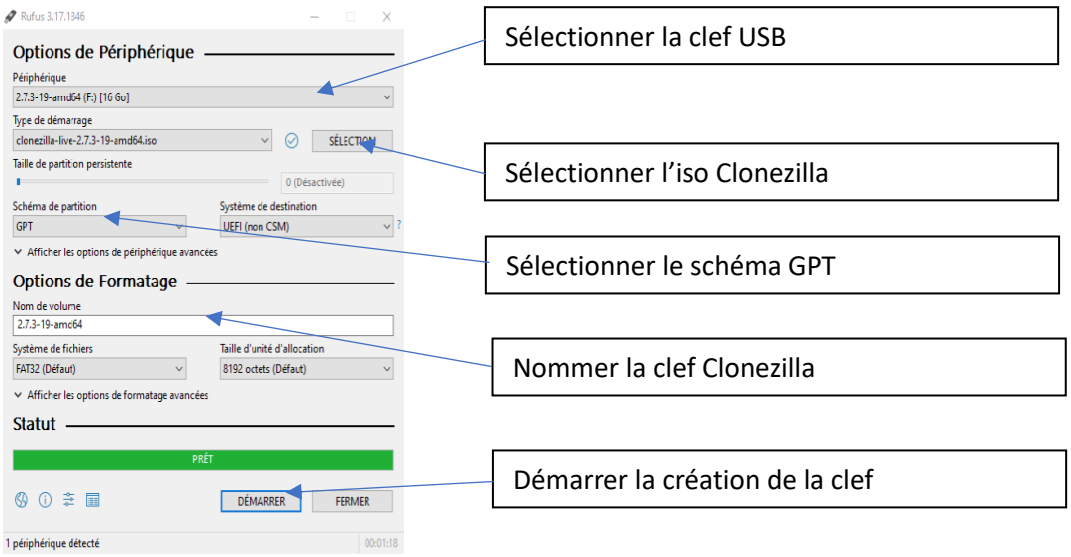
6.1.1. CREER UNE CLE CLONEZILLA

Les FOSS nécessaires à la création d'une clef bootable Clonezilla sont fournis avec la livraison Phenix dans le répertoire SSI_TOOLS/Clonezilla.

- Rufus : un outil permettant de créer des clefs bootables
- Clonezilla : l'outil de sauvegarde et restauration

On note également qu'il est nécessaire de disposer d'une clef USB que la procédure va effacer, les données présentes sur la clef seront effacées. Il est préconisé d'utiliser des clefs USB3.

1. Brancher la clef USB
2. Lancer Rufus
3. Sélectionner la clef USB dans l'option « Périphérique »
4. Sélectionner l'ISO Clonezilla dans l'option « Type de démarrage »
5. Sélectionner le schéma de partition « GPT »
6. Nommer la clef « Clonezilla »



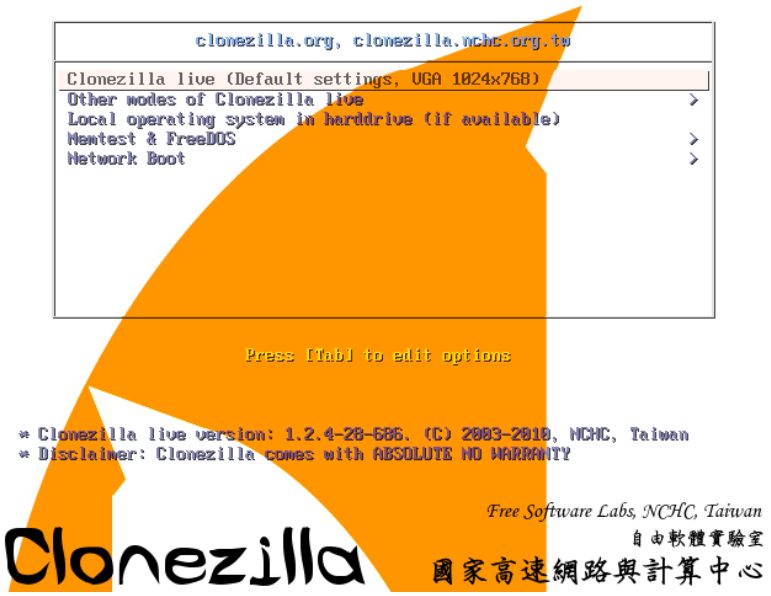
7. Laisser les autres paramètres par défaut
    a. Système de destination : UEFI
    b. Système de fichier : FAT32
    c. Taille d'unité d'allocation : 4096 octets
8. Démarrer la création de la clef
9. Quand la création est terminée, fermer Rufus et éjecter la clef

6.1.2. SAUVEGARDE D'UNE IMAGE SYSTEME

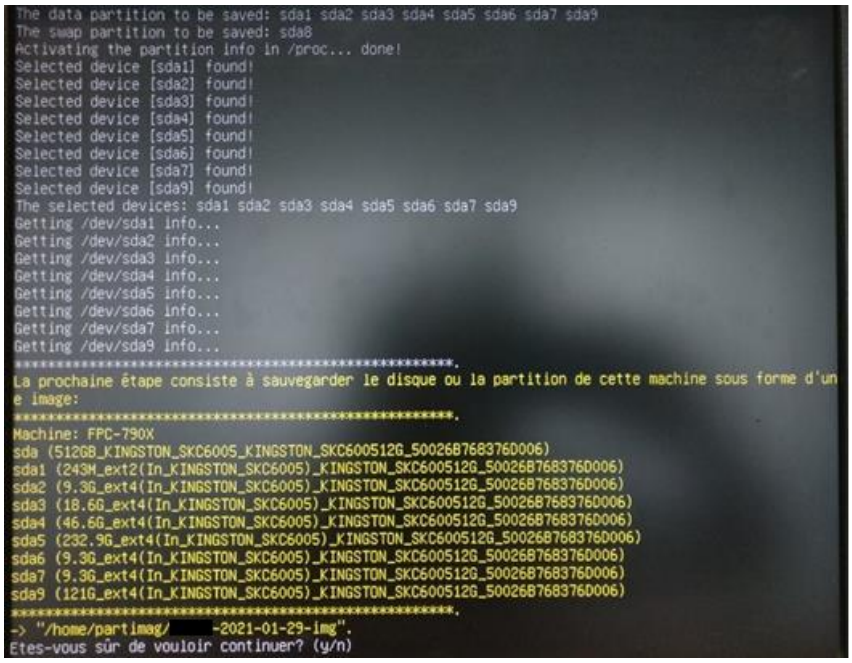
Pour sauvegarder une image système, il est nécessaire d'avoir à disposition une clé bootable Clonezilla ainsi qu'une clé pour stocker l'image résultante (prévoir une place conséquente, une image fait environ 20Go).

Le logiciel est disponible sur Internet ou sur le serveur : \\srv-filer01.global.ad\AFFAIRES_DIGILOG\1-12-AIA-1900\TECHNIQUE\SSI\00-OUTILS\Clonezilla.

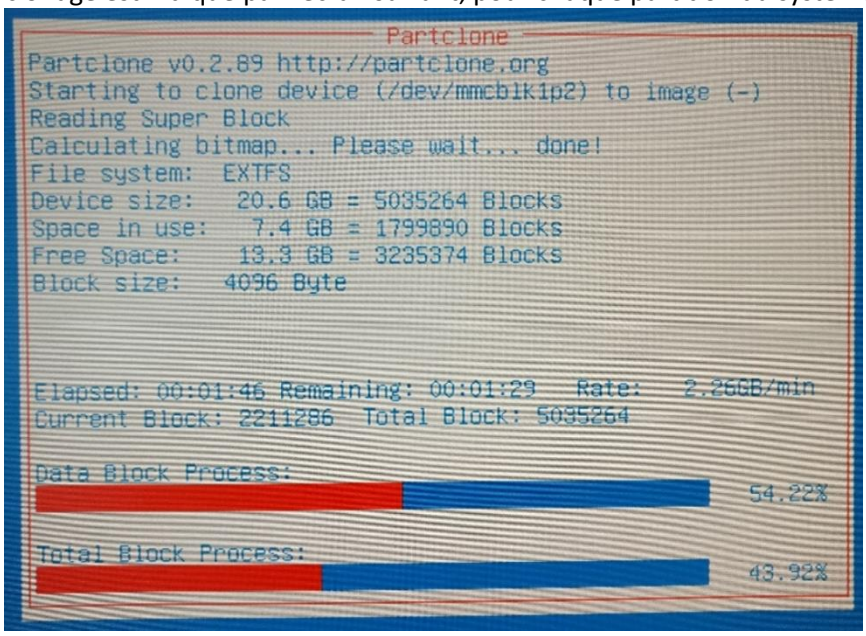
Au démarrage du serveur/poste, accéder au BIOS et démarrer sur la clé Clonezilla en mode UEFI.



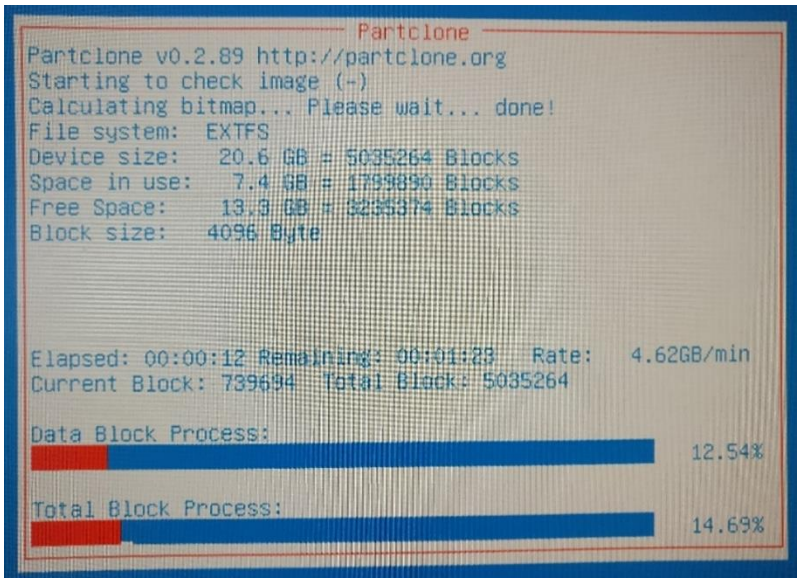
1. Dans Clonezilla, sélectionner la première option.
2. Sélectionner le langage et la disposition du clavier.
3. Sélectionner **Start_Clonezilla**.
4. Sélectionner **device-image**.
5. Sélectionner **local_dev**.
6. Sélectionner **savedisk**.
7. Choisir le disque associé à la clé USB où l'on veut stocker l'image.
8. Nommer l'image.
9. Sélectionner les disques à sauvegarder (sélectionner avec la barre d'espace puis entrée pour valider).
   i. Il est possible de restaurer qu'un des disques ou les deux.
   ii. /dev/nvme0n1pX, avec X le numéro de la partition, correspond au découpage de l'OS.
10. Le scan des partitions se réalise puis taper sur **y** puis **entrée**.



Le déroulement du clonage est indiqué par l'écran suivant, pour chaque partition du système.



Une vérification de l'image créée est alors réalisée.

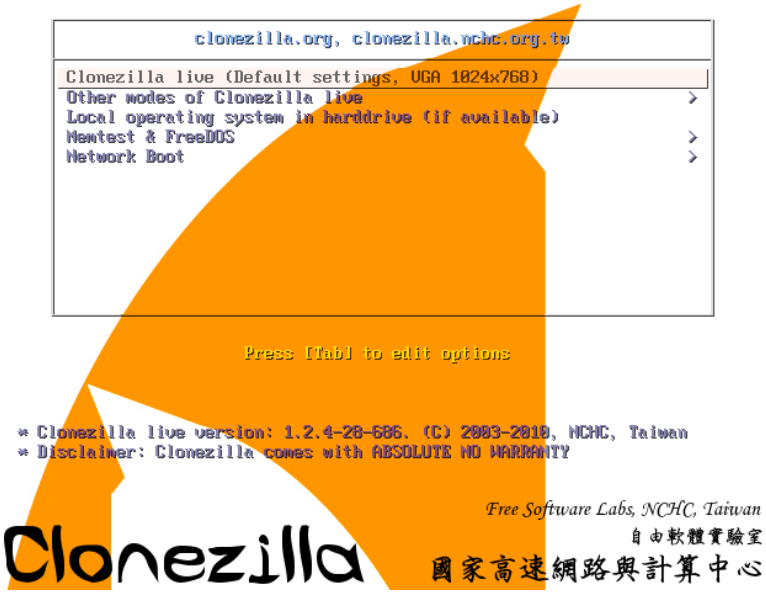


A la fin, choisir d'éteindre ou de redémarrer le poste.

6.1.3. RESTAURATION A PARTIR D'UNE IMAGE CLONEZILLA

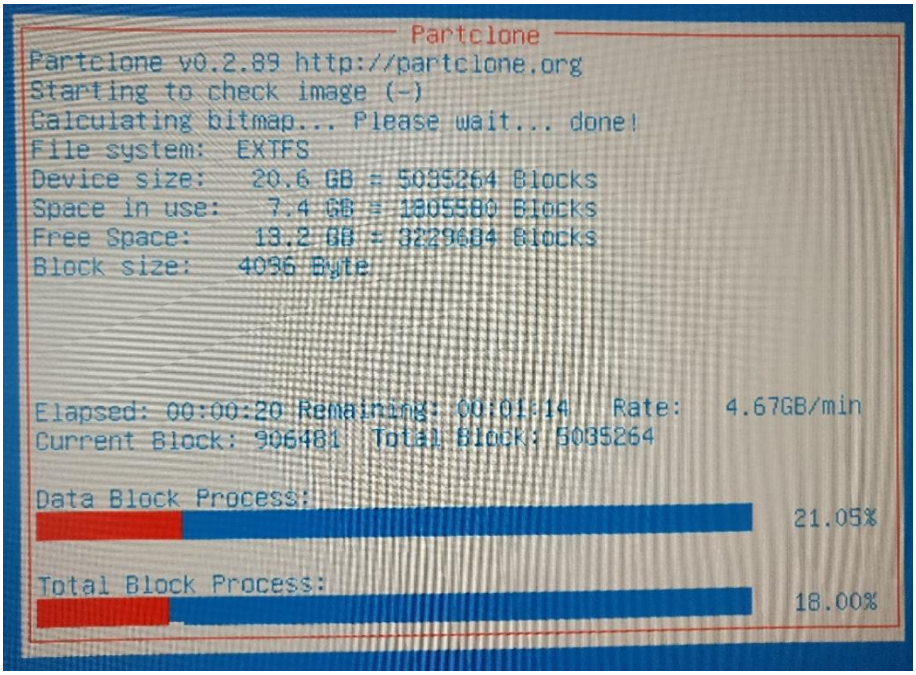
Pour restaurer une image système, il est nécessaire d'avoir à disposition une clé bootable Clonezilla ainsi que la clé contenant l'image.

Au démarrage du serveur/poste, accéder au BIOS et démarrer sur la clé Clonezilla en mode UEFI.

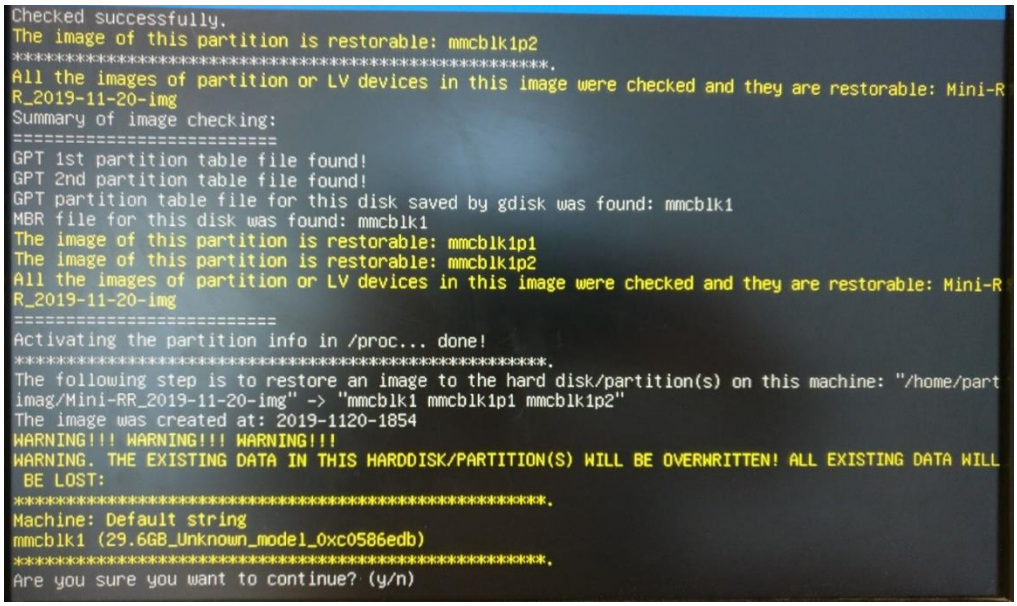


1. Dans Clonezilla, sélectionner la première option.
2. Sélectionner le langage et la disposition du clavier.
3. Sélectionner **Start_Clonezilla**.
4. Sélectionner **device-image**.
5. Sélectionner **local_dev**.

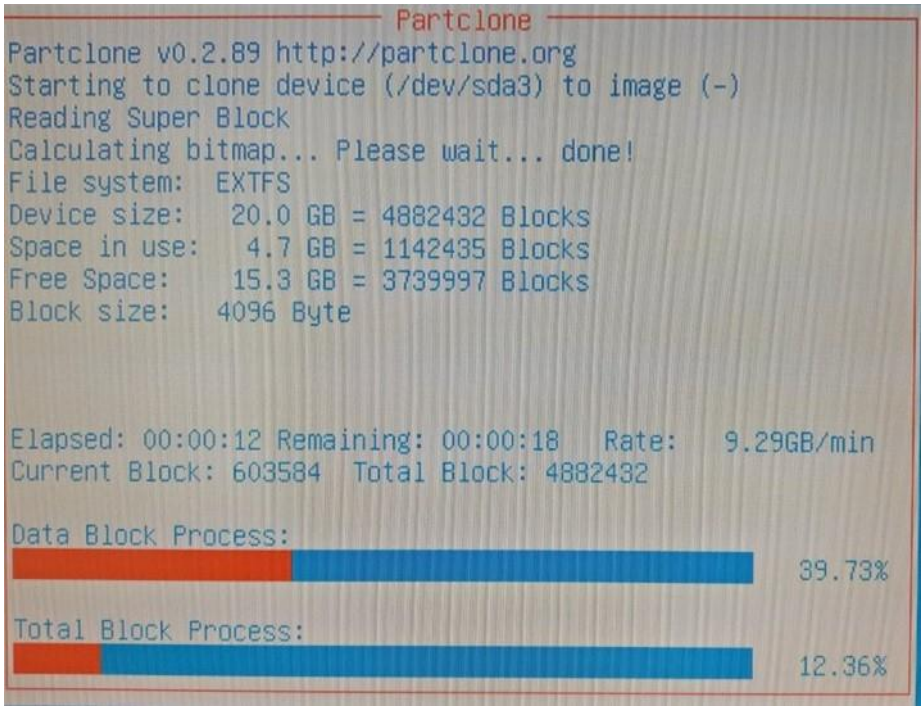
6. Sélectionner **restoredisk**.
7. Choisir le disque associé à la clé USB où l'image est stockée.
8. Sélectionner le dossier contenant l'image.
9. Sélectionner l'image à restaurer.
10. Sélectionner les disques à restaurer (sélectionner avec la barre d'espace puis entrée pour valider).
    i. Il est possible de restaurer qu'un des disques ou les deux.
    ii. /dev/nvme0n1pX, avec X le numéro de la partition, correspond au découpage de l'OS.
11. Une vérification de l'image est d'abord effectuée.



Puis une double demande de confirmation pour démarrer la restauration est demandée.



La restauration de l'image est ensuite réalisée, pour chaque partition du ou des disques concernés.



A la fin, choisir d'éteindre ou de redémarrer le poste.

TABLEAU DE JUSTIFICATION SSI

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
CCTP-ADD01	SEGMENT SOL : Recommandations de configuration d'un système GNU/Linux, référencé DAT-NT-28/ANSSI/SDE/NP du 12/01/2016, avec une conformité atteinte pour niveau intermédiaire.	Conforme	Recommandations suivies lors du portage
CCTP-ADD01-1	R1 - M I R E Minimisation des services installés Seuls les composants strictement nécessaires au service rendu par le système doivent être installés. Tout service (particulièrement en écoute active sur le réseau) est un élément sensible. Seuls ceux connus et requis pour le fonctionnement et la maintenance doivent être résidents. Ceux dont la présence ne peut être justifiée doivent être désactivés, désinstallés ou supprimés	Conforme	La liste des services installés est donnée dans le fichier R01-Liste-Services-with_systemctl.txt (p12/33)
CCTP-ADD01-2	R2 - I R E Minimisation de la configuration Les fonctionnalités configurées au niveau des services démarrés doivent être limitées au strict nécessaire	Conforme	La liste de la configuration est donnée dans le fichier R02-Liste-Services_Running-with_systemctl.txt (p12/33)
CCTP-ADD01-3	R5 - M I R E Principe de défense en profondeur Sous Unix et dérivés, la défense en profondeur doit reposer sur une combinaison de barrières qu'il faut garder indépendantes les unes des autres. Par exemple : – authentification nécessaire avant d'effectuer des opérations, notamment quand elles sont privilégiées ; – journalisation centralisée d'évènements au niveau systèmes et services ; – priorité à l'usage de services qui implémentent des mécanismes de	Conforme	Les trois premiers points sont validés du fait de la distribution Kubuntu et le point « Mécanismes de prévention d'exploitation » consiste à cloisonner les applications qui peuvent apporter des modifications graves au système ou à fournir des infos à distance : cela n'est pas le cas dans notre application car les

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
	cloisonnement et/ou de séparation de privilèges ; – utilisation de mécanismes de prévention d'exploitation		logiciels FRANC sont hors-ligne et ne sont pas malveillants (p12/33).
CCTP-ADD01-4	R10 - I R E Architecture 32 et 64 bits Lorsque la machine le supporte, préférer l'installation d'une distribution GNU/Linux en version 64 bits plutôt qu'en version 32 bits	Conforme	Par sa nature, la distribution Kubuntu 20.04.4 fonctionne avec une architecture 64 bits (p13/33).
CCTP-ADD01-5	R12 - I R E Partitionnement type Le partitionnement type recommandé est le suivant : Point de montage Options Description / <sans option> Partition racine, contient le reste de l'arborescence /boot nosuid,nodev,noexec (noauto optionnel) Contient le noyau et le chargeur de démarrage. Pas d'accès nécessaire une fois le boot terminé (sauf mise à jour) /opt nosuid,nodev (ro optionnel) Packages additionnels au système. Montage en lecture seule si non utilisé /tmp nosuid,nodev,noexec Fichiers temporaires. Ne doit contenir que des éléments non exécutables. Nettoyé après redémarrage /srv nosuid,nodev (noexec,ro optionnels) Contient des fichiers servis par un service type web, ftp, etc. /home nosuid,nodev,noexec Contient les HOME utilisateurs. Montage en lecture seule si non utilisé /proc hidepid=1 Contient des informations sur les processus et le système /usr nodev Contient la majorité des utilitaires et fichiers système /var nosuid,nodev,noexec Partition contenant des fichiers variables pendant la vie du système (mails, fichiers PID, bases de données d'un service) /var/log nosuid,nodev,noexec Contient les logs du système /var/tmp nosuid,nodev,noexec Fichiers temporaires conservés après extinction	Conforme	La liste de la configuration est donnée dans le fichier R12-fstab.txt (p13/33).
CCTP-ADD01-6	R14 - M I R E Installation de paquets réduite au strict nécessaire Le choix des paquets doit conduire à une installation aussi petite que possible, se bornant à ne sélectionner que ce qui est nécessaire au besoin.	Conforme	Les paquets installés sont réduits au maximum, ce sont ceux nécessaires pour les logiciels FRANC ainsi que ceux nécessaires pour la SSI (p13/33).

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
CCTP-ADD01-7	R15 - M I R E Choix des dépôts de paquets Seuls les dépôts officiels à jour de la distribution doivent être utilisés.	Conforme	Le téléchargement des paquets nécessaires aux logiciels FRANC et à la procédure SSI s'est fait via un autre poste sous distribution Ubuntu 20.04 LTS connecté aux dépôts officiels Linux et ces mêmes paquets ont été transmis au poste SSI concerné par une clé USB sécurisée pour une installation offline (p13/33).
CCTP-ADD01-8	R18 – M I R E Robustesse du mot de passe administrateur Le mot de passe root doit être suffisamment robuste compte tenu des recommandations présentes dans la note « Recommandations de sécurité relatives aux mots de passe ». Ce mot de passe doit être unique et propre à chaque machine.	Conforme	Le MdP est donnée dans le fichier R18-passwd.txt avec config SSH (R18-ssh_config.txt) (p14/33)
CCTP-ADD01-9	R19 - I R E Imputabilité des opérations d'administration Chaque administrateur doit posséder un compte dédié (local ou distant), et ne pas utiliser le compte root comme compte d'accès pour l'administration du système. Les opérations de changement de privilèges devront reposer sur des exécutables permettant de surveiller les activités réalisées (par exemple sudo).	Conforme	L'administrateur du poste est l'utilisateur « maintenance », l'utilisateur « root » est désactivé et les élévations de droits se font via « sudo » (p14/33).
CCTP-ADD01-10	R22 - M I R E Paramétrage des sysctl réseau Ces sysctl sont données pour un hôte « serveur » typique qui n'effectue pas de routage et ayant une configuration IPv6 minimaliste (adressage statique). Quand IPv6 n'est pas utilisé il convient de le désactiver en mettant l'option net.ipv6.conf.all.disable_ipv6 à 1. Elles sont présentées ici telles que rencontrées dans le fichier /etc/sysctl.conf :	Conforme	Données dans le fichier R22-sysctl_conf-Edit.txt (p14/33).
CCTP-ADD01-11	R23 - M I R E Paramétrage des sysctl système Voici une liste de sysctl système recommandées (au format /etc/sysctl.conf) :	Conforme	La liste est détaillées dans le fichier R23-sysctl_conf-Edit.txt (p14/33).
CCTP-ADD01-12	R27 - M I R E Désactivation des comptes de services. Les comptes de service doivent être désactivés.	Conforme	Seuls les comptes « maintenance » et « franc » sont actifs (p14/33).

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
CCTP-ADD01-13	R30 - M I R E Applications utilisant PAM Le nombre d'applications utilisant PAM doit être réduit au strict nécessaire afin de limiter l'exposition d'éléments d'authentification sensibles.	Conforme	Le nombre d'applications est listé dans le fichier R30-Liste-PAM-Services.txt (p15/33)
CCTP-ADD01-14	R31 - M I R E Sécurisation des services réseau d'authentification PAM Quand l'authentification se déroule au travers d'un service distant (réseau), le protocole d'authentification utilisé par PAM doit être sécurisé (chiffrement du flux, authentification du serveur distant, mécanismes d'anti-rejeu, etc.).	Conforme	Les données sont dans les fichiers R31-PAM-login.txt et R31-PAM-passwd.txt (p15/33)
CCTP-ADD01-15	R32 - M I R E Protection des mots de passe stockés Tout mot de passe doit être protégé par des mécanismes cryptographiques évitant de les exposer en clair à un attaquant récupérant leur base : – hachage du mot de passe par une fonction de hachage considérée comme sûre (SHA256, SHA-512), avec un sel et un nombre de tours assez grand (65536) ; – fonction de dérivation de clé sur le mot de passe et combinée à une fonction de hachage considérée comme sûre (selon le Référentiel Général de Sécurité 10) afin d'obtenir une empreinte valide pour un aléa donné ; – chiffrement par une clé secrète (éventuellement protégée au travers d'un HSM auquel l'application accède).	Conforme	Procédure listée dans les fichiers R32-PAM-common_passwd.txt et R32-login_defs.txt (p15/33)
CCTP-ADD01-16	R33 – I R E Sécurisation des accès aux bases utilisateurs distantes Lorsque les bases utilisateurs sont stockées sur un service réseau distant (type LDAP), NSS doit être configuré pour établir une liaison sécurisée permettant au minimum d'authentifier le serveur et de protéger le canal de communication.	NA	Connexion uniquement réalisée localement voir fichier R33-nssswitch_conf.txt (p15/33)
CCTP-ADD01-17	R34 - M I R E Séparation des comptes système et d'administrateur de l'annuaire Il est recommandé de ne pas avoir de recouvrement de compte entre ceux utilisés par le système d'exploitation et ceux utilisés pour administrer l'annuaire. L'usage de comptes administrateur d'annuaire pour effectuer des requêtes d'énumération de comptes par NSS doit être prohibé.	NA	La séparation n'est pas nécessaire car les services sont non-configurés pour (p16/33).

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
CCTP-ADD01-18	R36 - I R E Droits d'accès aux fichiers de contenu sensible Les fichiers à contenu sensible ne doivent être lisibles que par les utilisateurs ayant le strict besoin d'en connaître.	Conforme	Les fichiers sans utilisateur ou groupe propriétaire doivent être : • Assignés à un utilisateur/groupe qui existe si on souhaite conserver le fichier • Supprimés Pour trouver les fichiers qui répondent aux deux conditions (pas d'utilisateur et pas de groupe propriétaire), on utilise la commande et s'il n'y a pas de retour tout est bon (p16/33) : **find / -type f \(-nouser -o -nogroup \) -ls 2>/dev/null**
CCTP-ADD01-19	R37 - M I R E Exécutables avec bits setuid et setgid Seuls les programmes spécifiquement conçus pour être utilisés avec les bits setuid (ou setgid) peuvent avoir ces bits de privilèges positionnés.	Conforme	La liste des droits est donnée dans les fichiers R37-Liste-Droits-setuid_setgid-Before.txt et R37-Liste-Droits-setuid_setgid-After.txt (p16/33).
CCTP-ADD01-20	R40 - I R E Sticky bit et droits d'accès en écriture Tous les répertoires accessibles en écriture par tous doivent avoir le sticky bit armé	Conforme	La liste est donnée dans le fichier R40-Liste-Sticky_Bit.txt (p18/33)
CCTP-ADD01-21	R42 - M I R E Services et daemons résidents en mémoire Seuls les démons réseau strictement nécessaires au fonctionnement du système et du service qu'ils rendent doivent être résidents et n'être en écoute que sur les interfaces réseau adéquates. Les autres démons doivent être désactivés et autant que possible désinstallés.	Conforme	La liste des services et daemons est donnée dans les fichiers R42-Liste-Services_Demons_Before.txt et R42-Liste-Services_Demons_After.txt (p19/33)
CCTP-ADD01-22	R57 - I R E Groupe dédié à l'usage de sudo Un groupe dédié à l'usage de sudo doit être créé. Seuls les utilisateurs membres de ce groupe doivent avoir le droit d'exécuter sudo.	Conforme	Les droits sont listés dans les fichiers R57-Droits-sudo.txt et R57-groups.txt (p20/33)

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
CCTP-ADD01-23	R59 - M I R E Authentification des utilisateurs exécutant sudo Une authentification de l'utilisateur appelant doit être effectuée avant toute exécution de commande par sudo. Le mot-clé NOPASSWD ne doit pas être utilisé.	Conforme	Par défaut à l'installation de la distribution Kubuntu, le système demande que l'utilisateur soit authentifié avant de pouvoir exécuter une commande en tant que *'sudo'* (p21/33).
CCTP-ADD01-24	R60 - I R E Privilèges des utilisateurs cible pour une commande sudo Les utilisateurs cible d'une règle doivent autant que possible être un utilisateur non privilégié (c'est-à-dire non root).	Conforme	Pour toute commande, il est configuré que des droits utilisateurs simples et minimaux soient appliqués aux utilisateurs « maintenance » et « franc » afin d'éviter une escalade de privilège (p21/33).
CCTP-ADD01-25	R62 - I R E Du bon usage de la négation dans une spécification sudo Les spécifications de commandes ne doivent pas faire intervenir de négation	Conforme	Il n'y a pas de commandes spécifiques dans le fichier « /etc/sudoers » (p21/33).
CCTP-ADD01-26	R63 - I R E Arguments explicites dans les spécifications sudo Toutes les commandes du fichier sudoers doivent préciser strictement les arguments autorisés à être utilisés pour un utilisateur donné. L'usage de * (wildcard) dans les règles doit être autant que possible évité. L'absence d'arguments auprès d'une commande doit être spécifiée par la présence d'une chaîne vide ("").	Conforme	La liste des commandes est donnée dans le fichier R63-sudoers.txt (p21/33)
CCTP-ADD03	Le démarrage et l'exécution du système d'exploitation FRANC Std2 SOL sont réalisés en RAM physique et virtuelle.	Conforme	Démarrage et exécution en RAM avec utilisation mémoire cache du processeur. RAM = RAM physique (mémoire vive + mémoire cache) + RAM virtuelle (swap). Justification par analyse. Nb : Analyse du swap (disque dur vu comme extension RAM) lors de la mise en veille.

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
CCTP-ADD04	La station de restitution sol FRANC STD2 possèdera une liste blanche permettant de filtrer les médias connectés : - Média FRANC STD2 - Disques SATA archivage - Clés USB	Conforme	Utilisation règles udev sous *Linux: filtre selon un device ID - vérifier la possibilité de filtrage pour les matériels SATA - maintenance de la liste blanche par l'AIA en cas d'ajout de médias
CCTP-ADD05	Une clé USB sera fourni et dédiée pour la mise à jour software de la station de restitution SOL.	NA	Mise à jour software sous profil "administrateur", uniquement en usine par Avantix. Pas de processus sécurisé de mise à jour implémenté au niveau du système FRANC. Le processus sécurisé est défini au niveau organisationnel par Avantix (en usine).
CCTP-ADD06	Installation d'un logiciel qui détecte la présence éventuelle d'un logiciel malveillant ou d'un virus avant leur introduction dans le FRANC Std2 bord	Conforme	Repose sur l'intégration d'une liste blanche afin de ne pas connecter des médias USB non autorisés.
CCTP-ADD07	BIENS 02 Le poste de travail 1. Il est interdit à l'utilisateur d'apporter des modifications à la configuration de sa station, d'y installer des logiciels ou des périphériques non autorisés. 2. L'utilisation de périphériques sans fil (clavier, souris, …) est interdite sur un poste de travail classifié. Elle est interdite par défaut sur un poste non classifié, sauf si le besoin opérationnel, voire médical, la justifie. Dans ce cas, l'autorisation formelle est accordée par le chef d'organisme et conservée dans le dossier de sécurité. 3. En dehors d'éventuelles applications métiers, il est interdit d'exécuter des logiciels flash, appelés aussi « logiciels portables » (jeux en particulier) sur les postes de travail fournis par l'administration, même s'ils ne modifient pas	Conforme	L'utilisateur ne pourra pas modifier la configuration de la station sol FRANC. Opérations de mises à jour de l'OS uniquement en usine, par le constructeur (Avantix). Pas d'antivirus prévu car utilisation d'un OS LINUX EMBEDDED limité. La station sol n'est pas prévu pour être connectée à un réseau par l'utilisateur.

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
	la configuration du poste de travail. **4. Chaque station de travail (stations isolées ou en réseau fermé) dispose d'un antivirus avec un processus de mise à jour défini.** 5. En dehors des cas d'incidents de sécurité traités au chapitre 6, section V, seuls les postes prévus pour le nomadisme (stations d'accueil) et enregistrés auprès du CSSI/OSSI peuvent être librement déconnectés et reconnectés au réseau par l'utilisateur.		
CCTP-ADD08	BIENS 03 Verrouillage du compte utilisateur - Après 6 tentatives de connexion infructueuses, un compte utilisateur se verrouille pour une durée de 30 minutes. L'administrateur en est informé par une remontée d'alarme. Le déverrouillage du compte avant l'expiration du délai nécessite une action de l'administrateur. - En cas d'impossibilité technique, l'AH peut déroger si des mesures techniques et/ou organisationnelles réduisent le risque.	Conforme	Fonction intégrée dans le logiciel station sol, pour gestion des exigences SSI : - Gestion des MdP, - Verrouillage compte utilisateur, - Verrouillage automatique, - Journalisation, - Protection fichiers MdP et journaux (cryptés)
CCTP-ADD09	BIENS 04 Avertissement à l'ouverture de session Avant l'ouverture d'une session sur un système permettant d'accéder à des informations classifiées, l'utilisateur est informé du niveau de classification, de la ou des habilitations requises, que seuls les utilisateurs autorisés peuvent accéder au système et que celui-ci peut être surveillé pour détecter les utilisations non autorisées.	Conforme	
CCTP-ADD10	BIENS 05 Verrouillage automatique du poste 1. Les postes de travail et les serveurs informatiques se verrouillent automatiquement après au maximum 10 minutes d'inactivité. Le déverrouillage nécessite alors une nouvelle authentification de l'utilisateur. 2. Le verrouillage automatique s'accompagne de l'affichage de l'écran de veille. Celui-ci indique le niveau maximum de classification des informations traitées et fait apparaître que les activités sur le système d'information font l'objet d'une surveillance, dans le respect des lois. 3. Pour certains postes de supervision ou dans les salles de réunions, le délai de verrouillage peut être porté à 1 heure. La note d'organisation SSI de l'organisme doit en faire état et préciser les mesures de réduction du risque associées (présence permanente par exemple).	Conforme	

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
	4. Exceptionnellement, certains systèmes (systèmes d'arme temps réel, contrôle aérien local, etc.) peuvent n'implémenter ni écran de veille ni verrouillage automatique. Ce risque est alors formellement accepté lors de l'homologation et est atténué par des mesures organisationnelles. 5. Ces paramètres ne sont modifiables que par un administrateur.		
CCTP-ADD11	INFO 01 Marquage de l'information Les informations sont marquées conformément à leur niveau de sensibilité ou de classification, et à leur appartenance.	Conforme	Les information vidéo (classifiées DR-SF), sont sauvegardées sur le SSD extractible classifié. Ce dernier sera marqué "DR-SF" à l'aide d'une étiquette durcie.
CCTP-ADD12	Inclure dans la procédure de mise en ordre de marche et d'utilisation une procédure de réinstallation de l'OS + logiciel de restitution. (Fournir le temps de la manipulation)	PC	Uniquement pour le logiciel applicatif de restitution. L'utilisateur ne pourra pas modifier la configuration de la station sol FRANC. Opérations de mises à jour OS uniquement en usine, par le constructeur (Avantix) : pas de réinstallation de l'OS par l'utilisateur.
CCTP-ADD13	BIENS 44 Configuration des postes de travail 1. Chaque station de travail bénéficie d'un processus de mise à jour du système d'exploitation et des logiciels. 2. Seuls les logiciels nécessaires au fonctionnement et au travail susceptible d'être réalisé sur la station sont installés. Cette règle s'applique aussi aux **administrateurs** qui n'ont pas plus que d'autres le droit de détenir des logiciels illicites (logiciels de « craquage » de clés notamment). 3. Les connexions sans-fil (Wifi, Bluetooth, etc.) sont désactivées par défaut et ouvertes seulement si nécessaire. Leur utilisation est auditée. 4. Les ports permettant de connecter des périphériques sont ouverts au strict nécessaire et dans le respect des PES du système. Leurs accès sont audités. 5. Les fonctions d'autorun et d'autoplay sont désactivées.	Conforme	Mise à jour du système d'exploitation et des logiciels lors d'opérations de maintenance "administrateur" (corrective ou évolutive) par le constructeur, en usine. Règles appliquées aux administrateurs : Processus défini / suivi au niveau organisationnel par Avantix. Mise en place MdP pour protéger l'accès au BIOS.

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
	6. L'accès au BIOS de chaque poste de travail ou serveur informatique est verrouillé par un mot de passe détenu par l'OSSI de l'organisme d'appartenance de l'administrateur (CIRISI, etc.). 7. Le BIOS de chaque poste de travail ou serveur informatique est paramétré pour n'autoriser le démarrage qu'à partir du disque dur (hors opérations d'administration ou dispositif agréé).		
CCTP-ADD14	INFO 37 **Protection des journaux** 1. Sur les SI classifiés, les journaux stockant les informations d'imputation doivent être protégés en intégrité et en disponibilité.	Conforme	Cf. CCTP-ADD08. Journaux à sauvegarder cryptés. Evt SSI : cf. CCTP-ADD18 (INFO 45).
CCTP-ADD15	INFO 42 Authentifiants d'administration - Les mots de passe d'administration respectent la règle INFO44 et sont composés au minimum de 14 caractères.	Conforme	MdP "Admin" géré uniquement par Avantix, en usine.
CCTP-ADD16	INFO 43 Fichiers de mots de passe Les fichiers contenant des mots de passe ne sont accessibles qu'aux seuls administrateurs concernés et sont protégés, lors de leur stockage, conformément aux règles en vigueur (au minimum en étant chiffrés à l'aide du logiciel ACID Cryptofiler).	Conforme	Chiffrement des mots de passe via busybox/passwd (Solution logicielle). La clef de chiffrement sera dérivée du mot de passe "utilisateur". Acid non prévu.
CCTP-ADD17	INFO 44 Règles relatives au mot de passe **utilisateur** 1. Lors de la création d'un compte, **le mot de passe initial** doit être aléatoire et unique. Si les circonstances l'imposent un mot de passe plus simple mais à usage unique peut être envisagé. 2. Pour garantir la robustesse du mot de passe utilisateur (hors code PIN), celui-ci : - est composé au minimum de 9 caractères ; - inclut au moins trois des catégories suivantes : lettre majuscule, lettre minuscule, chiffre arabe (0 à 9), caractère spécial (sous réserve que le système d'exploitation le permette) ;	Conforme	Lors de la création d'un compte (sortie usine), le mot de passe initial sera "simple" et "à usage unique", commun à tous les matériel. Il sera ensuite personnalisé / géré par le SIAé. Processus sécurisés définis au niveau organisationnel par le SIAé

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
	- ne contient pas tout ou partie de l'identifiant, du nom de l'utilisateur, de son rôle ou de son grade		
CCTP-ADD18	INFO 45 Journalisation des évènements de sécurité 1. Des dispositifs de journalisation doivent permettre de conserver une trace des événements de sécurité observés sur le système d'information durant 12 mois glissants, 2. Pour les SI classifiés, l'imputation des actions doit permettre de disposer de suffisamment de traces pour mener les investigations dans le cas de suspicion de compromission conformément à [DIR TRACES]. 3. Les événements de sécurité relatifs au SI qui doivent être journalisés sont au minimum : - les connexions et déconnexions au SI et leur nature (locale, à distance notamment) ; - la création, la modification et la suppression de comptes ; - actions sur le système (démarrage/redémarrage/arrêt) ; - modification de la configuration d'un logiciel de sécurité (pare-feu, antivirus, chargement d'une base de signature, …) ; - pour les SI classifiés : la création, la suppression et la modification des journaux ; - pour les SI classifiés : la modification de droits techniques, des droits utilisateurs et administrateurs sur le système d'information ; - pour les SI classifiés : la modification des droits d'accès à l'information (s'ils ne sont pas intégrés dans les droits d'accès utilisateurs) ;	Conforme	Pas de connexion à distance vers un SI. Evt SSI traités : - démarrage, redémarrage, arrêt DE L'APPLICATION FRANC, - création, suppression et modification des journaux, - modification des droits d'accès à l'information : changement de Mdp utilisateur.
CCTP-ADD19	INFO 46 Journalisation des opérations d'administration 1. Les opérations de gestion et d'administration des systèmes d'information doivent être journalisées, authentifiées et contrôlées. 2. Sur les intranets* les actions d'administration d'un système d'information doivent être enregistrées. Les traces de ces actions sont stockées pour une durée minimale de 12 mois. Elles sont protégées en intégrité, soit par un stockage sur un système séparé dont les comptes à privilèges sont détenus	NA	Non applicable : les opérations de gestion et/ou d'administration de la station SOL FRANC sont réalisés uniquement en usine, par le constructeur. Pas d'intranet prévu.

EXIGENCES	DESCRIPTION	CONFORMITE	JUSTIFICATION
	par un administrater de sécurité soit par un enregistrement dans un « coffre-fort numérique ».		

Légende :

- PC : Partiellement Conforme
- NA : Non Applicable