Sécurisation de SLE Micro à l'aide de Keylime

CONTENU

Keylime est un outil de mesure d'intégrité d'exécution et d'attestation de démarrage à distance basée sur TPM.

MOTIF

Cet article décrit comment configurer et exécuter Keylime sur SLE Micro.

EFFORT

La lecture de l'article prend environ 25 minutes.

OBJECTIF

Vous en saurez plus sur Keylime : son fonctionnement, sa configuration et son exécution.

CONDITIONS REQUISES

- Une instance en cours d'exécution de SLE Micro.

Date de publication : 11 déc 2025

Table des matières

1 Attestation à distance à l'aide de Keylime

Face à la demande croissante de sécurisation des périphériques contre les modifications non autorisées, l'utilisation du mécanisme de sécurité appelé *attestation à distance* (Remote Attestation, RA) s'est considérablement développée. La RA permet à un hôte (client) d'authentifier son état de chaîne de démarrage et son logiciel en cours d'exécution sur un hôte distant (vérificateur). La RA est souvent associée au chiffrement à clé publique (à l'aide de TPM2), de sorte que les informations envoyées ne peuvent être lues que par les services ayant demandé l'attestation et que la validité des données peut être vérifiée.

L'attestation à distance sur SLE Micro est implémentée par *Keylime*.

1.1 Terminologie

La technologie d'attestation à distance utilise les termes suivants :

Clé d'attestation (Attestation Key, AK)
: Clé de signature de données qui prouve que les données proviennent d'un module de plate-forme approuvée (Trusted Platform Module, TPM) réel et qu'elles n'ont pas été altérées.

Racine principale de confiance pour la mesure (Core Root of Trust for Measurement, CRTM)
: Calcule son propre hachage et le hachage de l'étape suivante du processus de démarrage, en lançant la chaîne de mesures.

Clé d'approbation (Endorsement Key, EK)
: Clé de chiffrement intégrée de façon permanente au TPM lors de sa fabrication. La partie publique de la clé et la certification stockée dans le TPM sont utilisées pour reconnaître un TPM authentique.

Architecture de gestion de l'intégrité (Integrity Management Architecture, IMA)
: Sous-système d'intégrité du kernel qui permet de détecter les modifications malveillantes apportées aux fichiers.

Démarrage mesuré (Measured Boot)
: Méthode avec laquelle chaque composant de la séquence de démarrage calcule un hachage du composant suivant avant de déléguer l'exécution de ce dernier. Le hachage étend un ou plusieurs registres de configuration de la plate-forme du TPM. Un événement est créé

avec les informations sur l'endroit où la mesure a eu lieu et ce qui a été mesuré. Ces événements sont collectés dans un journal des événements et, avec les valeurs PCR étendues, les événements peuvent être comparés aux valeurs attendues représentant un système sain.

Registre de configuration de plate-forme (Platform Configuration Register, PCR)

Emplacement mémoire dans le TPM qui, par exemple, stocke les hachages des couches de démarrage. Le PCR ne peut être mis à jour qu'à l'aide de l'opération non réversible `extend`. Il est possible d'obtenir une liste signée des valeurs PCR actuelles à l'aide de la commande **`quote`** exécutée sur le TPM. Cette liste peut être vérifiée par un tiers au cours du processus d'attestation.

Démarrage sécurisé (Secure Boot)

Chaque étape du processus de démarrage vérifie une signature cryptographique sur l'exécutable de l'étape suivante avant de le lancer.

Module de plate-forme approuvée (Trusted Platform Module, TPM)

Processeur cryptographique de sécurité autonome présent sur le système en tant que matériel ou implémenté dans le microprogramme qui fait office de racine de confiance. Le TPM fournit un PCR pour stocker les hachages des couches de démarrage. Un TPM standard fournit plusieurs fonctions, telles qu'un générateur de nombres aléatoires, des compteurs ou une horloge locale. Il stocke également 24 PCR regroupés par banques pour chaque fonction de hachage cryptographique prise en charge (SHA1, SHA256, SHA384 ou SHA512).

Remarque

Par défaut, l'utilisation d'un TPM est désactivée, de sorte que le démarrage mesuré n'a pas lieu. Pour activer l'attestation à distance, activez le TPM dans le menu EFI/BIOS.

Charge utile sécurisée

Mécanisme permettant de communiquer des données chiffrées aux agents sains. Les charges utiles sont utilisées pour fournir des clés, des mots de passe, des certificats, des configurations ou des scripts qui sont ensuite utilisés par l'agent.

1.2 Qu'est-ce que Keylime ?

Keylime est une solution d'attestation à distance qui vous permet de surveiller l'état de santé des noeuds distants à l'aide d'un TPM comme racine de confiance pour la mesure. Keylime vous permet d'effectuer diverses tâches, telles que les suivantes :

- Valider des PCR étendus pendant le démarrage mesuré.
- Créer une analyse et effectuer des assertions du journal des événements.
- Effectuer des assertions concernant la valeur de n'importe quel PCR sur le système distant.
- Surveiller la validité des fichiers ouverts ou exécutés.
- Fournir des données chiffrées aux noeuds vérifiés via des *charges utiles sécurisées*.
- Exécuter des scripts personnalisés qui sont déclenchés lorsqu'une machine échoue par rapport aux mesures attestées.

1.3 Architecture

Keylime se compose d'un agent, d'un vérificateur, d'un système de registre et d'un outil de ligne de commande (locataire). Les agents sont situés sur les systèmes à attester. Le vérificateur et le système de registre se trouvent sur des systèmes distants qui effectuent l'enregistrement et l'attestation des agents. N'oubliez pas que seul le rôle d'agent est disponible sur SUSE Linux Micro. Pour plus d'informations sur chaque composant, reportez-vous aux sections suivantes.

1.3.1 Agent Keylime

L'agent est un service qui s'exécute sur le système à attester. L'agent envoie le journal des événements, les hachages IMA et les informations sur le démarrage mesuré au vérificateur, en utilisant le TPM local comme certificateur de la validité des données.

Lorsqu'un nouvel agent est démarré, il doit d'abord s'enregistrer auprès du système de registre. Pour ce faire, il a besoin d'un certificat TLS afin d'établir la connexion. Le certificat TLS est généré par le système de registre, mais il doit être installé manuellement sur l'agent. Après l'enregistrement, l'agent envoie sa clé d'attestation et la partie publique de la clé d'approbation au système de registre. Ce dernier répond à l'agent par une question de vérification d'identité dans un processus appelé « activation des informations d'identification », qui valide le TPM de l'agent. Une fois que l'agent a été enregistré, il est prêt à être inscrit pour l'attestation.

1.3.2 Système de registre Keylime

Le système de registre est utilisé pour enregistrer les agents qui doivent être attestés. Le système de registre collecte la clé d'attestation de l'agent, la partie publique de la clé d'approbation et la certification de clé d'approbation, et vérifie que la clé d'attestation de l'agent appartient à la clé d'approbation.

1.3.3 Vérificateur Keylime

Le vérificateur effectue l'attestation réelle des agents et extrait en permanence les données d'attestation requises des agents (entre autres, les valeurs PCR, les journaux IMA et les journaux des événements UEFI).

2 Exécution de la charge de travail Keylime à l'aide de Podman

Keylime est une solution d'attestation à distance qui vous permet de surveiller l'état de santé des noeuds distants. Le *vérificateur* et le *système de registre* sont des composants essentiels de Keylime sur les systèmes distants pour effectuer l'enregistrement et l'attestation des agents Keylime.

Remarque

Le conteneur décrit dans cet article fournit un *vérificateur* et un *système de registre* de services de plan de contrôle, et un outil de ligne de commande (CLI) de *locataire* qui font partie du projet Keylime.

Avant de commencer l'installation et l'enregistrement des agents, préparez le vérificateur et le système de registre sur les hôtes distants, comme décrit dans la procédure suivante.

1. Identifiez l'image de la charge de travail Keylime.

```
# podman search keylime
[...]
registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane
```

2. Extrayez l'image à partir du registre.

```
# podman pull\
  registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane:latest
```

3. Créez le volume `keylime-control-plane` pour conserver la base de données et les certificats requis pendant le processus d'attestation.

```
# podman container runlabel install \
  registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane:latest
```

4. Démarrez le conteneur et les services associés.

```
# podman container runlabel run \
  registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane:latest
```

   Le conteneur `keylime-control-plane` est créé. Il contient les services de vérificateur et de système de registre configurés et en cours d'exécution. En interne, le conteneur expose les ports 8881, 8890 et 8891 à l'hôte en utilisant les valeurs par défaut. Validez la configuration du pare-feu pour autoriser l'accès aux ports et permettre la communication entre les conteneurs, car la CLI du locataire en a besoin.

Astuce

Si vous devez arrêter les services Keylime, exécutez la commande suivante :

```
# podman kill keylime-control-plane-container
```

2.1 Surveillance des services Keylime

Pour obtenir l'état des conteneurs en cours d'exécution sur l'hôte, exécutez la commande suivante :

```
# podman ps
```

Pour afficher les journaux des services Keylime, exécutez la commande suivante :

```
# podman logs keylime-control-plane-container
```

2.2 Exécution de la CLI locataire

L'outil CLI locataire est inclus dans le conteneur et, si le pare-feu hôte n'interfère pas avec les ports exposés par les services Keylime, vous pouvez l'exécuter à l'aide de la même image, par exemple :

```
# podman run --rm \
-v keylime-control-plane-volume:/var/lib/keylime/ \
keylime-control-plane:latest \
keylime_tenant -v 10.88.0.1 -r 10.88.0.1 --cert default -c reglist
```

2.3 Extraction du certificat Keylime

La première fois que le conteneur Keylime est exécuté, ses services créent un certificat requis par plusieurs agents. Vous devez extraire le certificat du conteneur et le copier dans le répertoire `/var/lib/keylime/cv_ca/` de l'agent.

```
# podman cp \
keylime-control-plane-container:/var/lib/keylime/cv_ca/cacert.crt
.# scp cacert.crt
AGENT_HOST:/var/lib/keylime/cv_ca/
```

Astuce

Pour plus d'informations sur l'installation de l'agent, reportez-vous à la *Section 3, « Installation de l'agent Keylime »*.

3 Installation de l'agent Keylime

Keylime est une solution d'attestation à distance qui vous permet de surveiller l'état de santé des noeuds distants. L'agent Keylime est un service qui s'exécute sur le système devant être attesté et qui envoie au vérificateur le journal des événements, les hachages IMA et les informations sur le démarrage mesuré.

L'agent Keylime n'est pas présent sur SLE Micro par défaut ; vous devez l'installer manuellement. Pour installer l'agent, procédez comme suit :

1. Installez le paquet `rust-keylime` comme suit :

```
# transactional-update pkg in rust-keylime
```

   Redémarrez ensuite le système.

2. Ajustez la configuration de l'agent par défaut.

   a. Créez un répertoire afin de stocker un nouveau fichier de configuration pour vos modifications dans `/etc/keylime/agent.conf.d/`. La configuration par défaut est stockée dans `/usr/etc/keylime/agent.conf`, mais nous vous déconseillons de modifier ce fichier, car il risque d'être écrasé dans les prochaines mises à jour système.

```
# mkdir -p /etc/keylime/agent.conf.d
```

   b. Créez un fichier `/etc/keylime/agent.conf.d/agent.conf` :

```
# cat << EOF > /etc/keylime/agent.conf.d/agent.conf
 [agent]

 uuid = "d111ec46-34d8-41af-ad56-d560bc97b2e8"❶ registrar_ip =
 "<REMOTE_IP>"❷
 revocation_notification_ip = "<REMOTE_IP>"❸
 EOF
```

   ❶ L'identificateur unique est généré chaque fois que l'agent est exécuté. Toutefois, vous pouvez définir une valeur spécifique par cette option.

   ❷ Adresse IP du système de registre.

   ❸ Adresse IP du vérificateur.

   c. Remplacez le propriétaire du répertoire `/etc/keylime/` par `keylime:tss` :

```
# chown -R keylime:tss /etc/keylime
```

   d. Modifiez les autorisations sur le répertoire `/etc/keylime/` :

```
# chmod -R 600 /etc/keylime
```

3. Copiez les certificats générés par l'autorité de certification sur le noeud de l'agent. Sur le noeud de l'agent, procédez comme suit :

   a. Préparez un répertoire pour le certificat :

   ```
   # mkdir -p /var/lib/keylime/cv_ca
   ```

   b. Copiez le certificat sur l'agent :

   ```
   # scpCERT_SERVER_ADDRESS:/var/lib/keylime/cv_ca/cacert.crt /var/lib/keylime/
   cv_ca
   ```

   c. Remplacez le propriétaire du certificat par `keylime:tss` :

   ```
   # chown -R keylime:tss /var/lib/keylime/cv_ca
   ```

4. Démarrez et activez `keylime_agent.service` :

   ```
   # systemctl enable --now keylime_agent.service
   ```

4 Enregistrement de l'agent Keylime

Keylime est une solution d'attestation à distance qui vous permet de surveiller l'état de santé des noeuds distants. L'agent Keylime est un service qui s'exécute sur le système devant être attesté et qui envoie au vérificateur le journal des événements, les hachages IMA et les informations sur le démarrage mesuré.

Vous pouvez enregistrer un nouvel agent à l'aide de la CLI locataire ou en modifiant la configuration du vérificateur. À l'aide du locataire sur l'hôte du vérificateur, exécutez la commande suivante :

```
# keylime_tenant -v 127.0.0.1 \
  -tAGENT \ ❶
  -u UUID \ ❷
  --cert default \
  -c add
  [--include PATH_TO_ZIP_FILE] ❸
```

❶ *AGENT* est une adresse IP de l'agent à enregistrer.

❷ *UUID* est l'identificateur unique de l'agent.

❸ Le fichier transmis par l'option `include` est utilisé pour fournir des données de charge utile secrètes à l'agent. Pour plus d'informations, reportez-vous à la *Section 5, « Charges utiles sécurisées Keylime »*.

Vous pouvez lister les agents enregistrés à l'aide de la commande **`reglist`** sur l'hôte du vérificateur comme suit :

```
# keylime_tenant -v 127.0.0.1 \
  --cert default \
  -c reglist
```

Pour supprimer un agent enregistré, spécifiez l'agent à l'aide des options `-t` et `-u` et de la commande `-c delete` comme suit :

```
# keylime_tenant -v 127.0.0.1 \
  -tAGENT \
 -u UUID \
  -c delete
```

5 Charges utiles sécurisées Keylime

Keylime est une solution d'attestation à distance qui vous permet de surveiller l'état de santé des noeuds distants.

5.1 Qu'est-ce qu'une charge utile sécurisée ?

Une charge utile sécurisée Keylime vous permet de fournir des données chiffrées à des agents sains. Les charges utiles sont utilisées pour fournir des clés, des mots de passe, des certificats, des configurations ou des scripts qui sont utilisés par l'agent Keylime à un stade ultérieur.

5.2 Comment fonctionne une charge utile sécurisée ?

Une charge utile sécurisée est fournie à l'agent dans un fichier `zip` qui doit contenir un script shell nommé `autorun.sh`. Le script n'est exécuté que si l'agent a été correctement enregistré et vérifié. Pour distribuer le fichier `zip`, utilisez l'option `--include` de la commande **`keylime_tenant`**.

Par exemple, le script `autorun.sh` suivant crée une structure de répertoires et y copie les clés SSH. L'archive `zip` associée doit inclure ces clés SSH.

```
> cat autorun.sh
#!/bin/bash

 mkdir -p /root/.ssh/
 cp id_rsa* /root/.ssh/
 chmod 600 /root/.ssh/id_rsa*
 cp /root/.ssh/id_rsa.pub /root/.ssh/authorized_keys
```

6 Activation du suivi IMA pour Keylime

Keylime est une solution d'attestation à distance qui vous permet de surveiller l'état de santé des noeuds distants. *L'architecture de gestion de l'intégrité* (Integrity Management Architecture, IMA) est un sous-système d'intégrité du kernel qui permet de détecter les modifications malveillantes des fichiers.

Lorsque vous utilisez la technologie IMA, le kernel calcule un hachage des fichiers consultés. Le hachage est ensuite utilisé pour étendre le PCR 10 dans le TPM et également pour consigner la liste des fichiers consultés. Le vérificateur peut demander une citation signée à l'agent pour que le PCR 10 obtienne les journaux de tous les fichiers consultés, y compris les hachages de fichiers. Les vérificateurs comparent ensuite les fichiers consultés avec une liste d'autorisation locale de fichiers approuvés. Si l'un des hachages n'est pas reconnu, le système est considéré comme non sécurisé et un événement de révocation est déclenché.

Avant que Keylime puisse collecter des informations, IMA/EVM doit être activé. Pour activer le processus, démarrez un kernel de l'agent avec les paramètres `ima_appraise=log` et `ima_policy=tcb` :

1. Mettez à jour l'option `GRUB_CMDLINE_LINUX_DEFAULT` avec les paramètres dans `/etc/default/grub` :

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="ima_appraise=log ima_policy=tcb"
   ```

2. Regénérez `grub.cfg` en exécutant :

   ```
   # transactional-update grub.cfg
   ```

3. Redémarrez votre système.

La procédure ci-dessus utilise la stratégie IMA du kernel par défaut. Pour éviter de surveiller un trop grand nombre de fichiers et donc de générer de longs journaux, créez une nouvelle stratégie personnalisée. Pour plus de détails, reportez-vous au document Keylime documentation (https://keylime-docs.readthedocs.io/en/latest/user_guide/runtime_ima.html).

Pour indiquer les hachages attendus, utilisez l'option `--allowlist` de la commande **`keylime_tenant`** lors de l'enregistrement de l'agent. Pour afficher les fichiers exclus ou ignorés, utilisez l'option `--exclude` de la commande **`keylime_tenant`** :

```
# keylime_tenant --allowlist
    -v 127.0.0.1 \
    -uUUID
```

7 Informations supplémentaires

- La page d'accueil de Keylime se trouve à l'adresse https://keylime.dev.
- La documentation Keylime la plus récente est disponible à l'adresse https://keylime.readthedocs.io/en/latest/.
- Pour une présentation générale des technologies IMA/EVM, reportez-vous au document https://en.opensuse.org/SDB:Ima_evm#Introduction.
- Pour plus d'informations sur la création d'une stratégie IMA de kernel, reportez-vous au document https://keylime-docs.readthedocs.io/en/latest/user_guide/runtime_ima.html.

8 Mentions légales

Toutes les informations de cet ouvrage ont été regroupées avec le plus grand soin. Cela ne garantit cependant pas sa complète exactitude. Ni SUSE LLC, ni les sociétés affiliées, ni les auteurs, ni les traducteurs ne peuvent être tenus responsables des erreurs possibles ou des conséquences qu'elles peuvent entraîner.

A Licence de Documentation Libre GNU

0. PRÉAMBULE

La présente Licence entend rendre un manuel, un guide ou tout autre document utile et fonctionnel « libre » de tout droit afin de garantir que toute personne soit effectivement libre de le copier et de le redistribuer, avec ou sans modification, à des fins commerciales ou non. En second lieu, cette Licence conserve à l'auteur et à l'éditeur un moyen de bénéficier du crédit de son travail, sans être considéré comme responsable des modifications réalisées par des tiers.

La présente Licence est une sorte de « copyleft », ce qui signifie que les travaux dérivés du document doivent eux aussi offrir les mêmes libertés que l'original. Elle complète la Licence publique générale GNU, qui est une licence copyleft conçue pour les logiciels libres.

Nous avons conçu cette Licence afin qu'elle soit utilisée pour les manuels de logiciels libres. En effet, qui dit logiciel libre dit documentation libre : un programme proposé librement doit être accompagné de manuels offrant les mêmes libertés que le logiciel original. Mais cette Licence ne se limite pas aux manuels des logiciels ; elle peut s'utiliser pour tout travail sous forme de texte, quel qu'en soit le sujet et qu'il soit ou non publié sous forme d'ouvrage imprimé. Nous recommandons cette Licence principalement pour les travaux dont l'objectif est la formation ou devant servir de référence.

1. DOMAINE D'APPLICATION ET DÉFINITIONS

Cette licence s'applique à tout manuel ou à tout autre travail, sur tout support, contenant une notification placée par le propriétaire du copyright indiquant qu'il peut être distribué conformément aux termes de cette Licence. Cette notification accorde une licence internationale, libre de droits et de durée illimitée, d'utilisation de ce travail conformément aux conditions indiquées

par les présentes. Le « Document » fait référence à ce manuel ou à ce travail. Tout membre du public est un détenteur de licence, et est désigné par l'appellation « Vous ». Vous acceptez la licence si vous copiez, modifiez ou distribuez le travail d'une manière nécessitant une autorisation selon les lois relatives au droit d'auteur.

Une « Version Modifiée » du Document désigne un travail contenant le Document ou une partie du Document, soit mot pour mot, soit avec des modifications et/ou traduit dans une autre langue.

Une « Section Secondaire » est une annexe nommée ou une section liminaire du Document qui traite exclusivement de la relation des éditeurs ou des auteurs du Document au sujet global du Document (ou à des sujets associés) et ne contient rien qui pourrait relever directement de ce sujet global. (Ainsi, si le Document est une partie d'un manuel de mathématiques, une Section Secondaire ne peut rien expliquer des mathématiques.) La relation peut être une question de relation historique avec le sujet ou avec des questions associées, ou de nature légale, commerciale, philosophique, éthique ou politique les concernant.

Les « Sections Invariantes » sont des Sections secondaires dont les titres sont désignés, comme étant ceux de Sections Invariantes, dans la notification indiquant que le Document est publié dans le cadre de la présente Licence. Si une section ne correspond pas à la définition ci-dessus de Secondaire, elle ne peut pas être désignée en tant qu'Invariante. Le Document peut ne contenir aucune Section Invariante. Si le Document n'identifie aucune Section Invariante, il n'y en a aucune.

Les « Textes de Couverture » sont certains courts passages de Texte de la Première de Couverture ou Texte de la Dernière de Couverture, dans la notification indiquant que le Document est publié dans le cadre de la présente Licence. Le Texte de la Première de Couverture doit comporter au plus 5 mots et le Texte de la Dernière de Couverture doit en comporter au plus 25.

Une copie Transparente du Document signifie une copie lisible par la machine, représentée dans un format dont la spécification est à la disposition du public, adaptée à la révision directe du document avec des éditeurs de texte génériques ou (pour les images composées de pixels) des programmes de peinture génériques ou (pour les dessins) certains éditeurs de dessin largement diffusés, et adaptée à la saisie dans des formateurs de texte ou pour la traduction automatique dans un ensemble de formats adaptés à la saisie dans des formateurs de texte. Une copie réalisée dans un autre format de fichier Transparent dont le balisage, ou l'absence de balisage, a été organisé pour déjouer ou décourager la modification ultérieure n'est pas Transparent. Un format d'image n'est pas Transparent s'il est utilisé pour une quantité importante de texte. Une copie qui n'est pas Transparente est dite Opaque.

Les exemples de formats adaptés aux copies Transparentes incluent l'ASCII standard sans balisage, le format de saisie Texinfo, le format de saisie LaTeX, le format SGML ou XML utilisant un DTD publiquement disponible, et le format HTML simple conforme à la norme, le format PostScript ou PDF conçu pour la modification par l'homme. Les exemples de formats d'image transparents incluent PNG, XCF et JPG. Les formats Opaques incluent les formats propriétaires qui ne peuvent être lus et modifiés que par des traitements de textes propriétaires, le format SGML ou XML pour lequel les outils de DTD et/ou de traitement ne sont généralement pas disponibles, et le HTML généré en machine, le format PostScript ou PDF produit par certains traitements de texte à des fins de sortie seulement.

La « Page de titre » signifie, pour un ouvrage imprimé, la page de titre proprement dite ainsi que les pages suivantes nécessaires pour contenir, lisiblement, les informations que la présente Licence exige de faire apparaître dans la page de titre. Pour les travaux dont les formats ne comportent pas de page de titre en tant que telle, « Page de titre » signifie le texte situé à proximité du titre du travail, avant le début du corps du texte.

Une section « Intitulée XYZ » signifie une sous-unité nommée du Document dont le titre est soit précisément XYZ, soit contient XYZ entre parenthèses à la suite du texte qui traduit XYZ dans une autre langue. (À cet endroit XYZ représente un nom de section spécifique mentionné ci-dessous, tel que « Remerciements », « Dédicaces », « Recommandations » ou « Historique ».) Pour « Conserver le Titre » d'une telle section lorsque vous modifiez le Document, cela signifie qu'il reste une section « Intitulée XYZ » conformément à la présente définition.

Le Document peut comporter des Limitations de Garantie à côté de la notification indiquant que la Licence s'applique au Document. Ces Limitations de Garantie sont considérées comme étant incluses car il y est fait référence dans la présente Licence, mais uniquement au titre des limitations de garantie : toute autre implication que pourrait avoir ces Limitations de Garantie est nulle et n'a aucun effet sur la signification de cette Licence.

2. COPIE MOT POUR MOT

Vous pouvez copier et distribuer le Document sur n'importe quel support, commercialement ou non, pourvu que cette Licence, les mentions de copyright et la mention de licence indiquant que cette Licence s'applique au Document soient reproduites sur toutes les copies, et que vous n'ajoutiez aucune autre condition à celles de cette Licence. Vous ne pouvez pas utiliser de mesures techniques pour empêcher ou contrôler la lecture ou la copie ultérieure des copies

que vous effectuez ou distribuez. Toutefois, vous pouvez accepter une compensation en échange des copies. Si vous distribuez un grand nombre de copies, vous devez respecter les conditions énoncées à la section 3.

Vous pouvez également prêter des copies, sous les mêmes conditions que celles indiquées ci-dessus, et afficher des copies publiquement.

3. COPIE EN QUANTITÉ

Si vous publiez des copies imprimées (ou des copies sur un support ayant des couvertures imprimées) du Document, à plus de 100 tirages, et que la mention de licence du Document exige des Textes de Couverture, vous devez inclure les copies dans des couvertures portant, clairement et de façon lisible, tous ces Textes de Couverture : les deux couvertures doivent également vous identifier clairement et de façon lisible comme l'éditeur de ces copies. La première de couverture doit présenter le titre complet, tous les mots de ce titre étant également lisibles et visibles. Vous pouvez également ajouter des informations aux couvertures. La copie avec des modifications limitées aux couvertures, tant qu'elles préservent le titre du Document et respectent ces conditions, peut être considérée comme une copie mot pour mot dans ses autres aspects.

Si les textes requis pour l'une ou l'autre des couvertures sont trop volumineux pour tenir de façon lisible, vous devez placer les premiers (autant qu'il en tient raisonnablement) sur la couverture réelle, et continuer le reste sur les pages adjacentes.

Si vous publiez ou distribuez des copies Opaques du Document avec une numérotation supérieure à 100, vous devez inclure une copie Transparente lisible en machine avec chaque copie Opaque, ou indiquer dans ou avec chaque copie Opaque un emplacement de réseau informatique auquel le public utilisant le réseau peut accéder pour télécharger, en utilisant des protocoles réseau publics standard, une copie Transparente complète du Document, sans informations supplémentaires. Si vous choisissez la dernière option, vous devez respecter des étapes raisonnables, lorsque vous commencez la distribution de copies Opaques en quantité, pour vous assurer que cette copie Transparente restera ainsi accessible à l'emplacement indiqué au moins un an après la dernière distribution d'une copie Opaque (directement ou par l'intermédiaire de vos agents ou de vos distributeurs) de cette édition au public.

Il est demandé, mais pas obligatoire, de contacter les auteurs du Document bien avant de redistribuer un grand nombre de copies, pour leur permettre de vous en fournir une version actualisée.

4. MODIFICATIONS

Vous pouvez copier et distribuer une Version Modifiée du Document conformément aux conditions des sections 2 et 3 ci-dessus, pourvu que vous diffusiez la Version Modifiée en respectant précisément cette Licence, la Version Modifiée jouant le rôle du Document, accordant ainsi la licence de distribution et de modification de la Version Modifiée à quiconque en possède une copie. En outre, vous devez procéder de la façon suivante dans la Version Modifiée :

A. Utiliser dans la Page de Titre (et sur les couvertures le cas échéant) un titre distinct de celui du Document et de ceux des versions précédentes (qui devraient être répertoriés dans la section Historique du Document). Vous pouvez utiliser le même titre qu'une version précédente si l'éditeur d'origine de cette version vous en donne l'autorisation.

B. Indiquer sur la Page de Titre, en tant qu'auteurs, une ou plusieurs personnes ou entités responsable de la paternité des modifications de la Version Modifiée, ainsi qu'au moins cinq des principaux auteurs du Document (tous ses principaux auteurs, s'ils sont moins de cinq), sauf s'ils vous dispensent de cette obligation.

C. Indiquer sur la Page de Titre le nom de l'éditeur de la Version Modifiée, en tant qu'éditeur.

D. Conserver toutes les mentions de copyright du Document.

E. Ajouter une mention de copyright appropriée pour vos modifications à côté des autres mentions de copyright.

F. Inclure, immédiatement après les mentions de copyright, une mention de licence donnant au public l'autorisation d'utiliser la Version Modifiée conformément aux termes de cette Licence, sous la forme indiquée dans l'Addendum ci-dessous.

G. Conserver dans cette mention de licence la liste complète des Sections Invariantes et des Textes de Couverture fournie dans la mention de licence du Document.

H. Inclure une copie non modifiée de cette Licence.

I. Conserver la section intitulée « Historique », Conserver son Titre et lui ajouter un élément indiquant au moins le titre, l'année, les nouveaux auteurs et l'éditeur de la Version Modifiée comme indiqué dans la Page de Titre. S'il n'existe pas de section Intitulée Historique dans le Document, créez-en une qui mentionne le titre, l'année, les nouveaux auteurs et l'éditeur du Document comme indiqué dans sa Page de Titre, puis ajoutez un élément décrivant la Version Modifiée comme indiqué dans la phrase qui précède.

J. Conserver l'emplacement réseau, le cas échéant, fourni dans le Document pour l'accès public à une copie Transparente du Document, ainsi que les emplacements réseau fournis dans le Document pour les versions précédentes sur lequel il était basé. Ils peuvent être placés dans la section Historique. Vous pouvez omettre un emplacement réseau pour un travail qui a été publié au moins quatre ans avant le Document lui-même, ou si l'éditeur d'origine de la version auquel il fait référence en donne l'autorisation.

K. Pour toute section intitulée « Remerciements » ou « Dédicaces », conserver le Titre de la section, et conserver dans la section toute la substance et le ton de chacun des remerciements et/ou dédicaces des contributeurs mentionnés.

L. Conserver toutes les Sections Invariantes du Document, sans modifications de leurs textes ni de leurs titres. Les numéros de section ou leur équivalent ne sont pas considérés comme faisant partie des titres de section.

M. Supprimer toute section intitulée « Recommandations ». Une telle section ne peut être incluse à la Version Modifiée.

N. Ne pas modifier le titre d'une section existante dont le titre est « Recommandations » ou ne pas créer de conflit avec le titre d'une Section Invariante.

O. Conserver les Limitations de Garantie.

Si la Version Modifiée comporte de nouvelles sections liminaires ou des annexes qui en font des Sections Secondaires et ne contiennent aucune information copiée à partir du Document, vous pouvez si vous le souhaitez désigner certaines ou toutes ces sections comme invariantes. Pour ce faire, ajoutez leurs titres à la liste des sections invariantes de la mention de licence de la version modifiée. Ces titres doivent être distincts des autres titres de section.

Vous pouvez ajouter une section intitulée « Recommandations », pour autant qu'elle ne contienne rien d'autre que des recommandations de votre Version Modifiée par différentes parties (par exemple, des déclarations d'évaluation par vos pairs ou indiquant que le texte a été approuvé par une organisation comme définition ou norme faisant autorité).

Vous pouvez ajouter un passage pouvant atteindre cinq mots comme Texte de la Première de Couverture, et un passage pouvant atteindre vingt-cinq mots comme Texte de Dernière de Couverture, à la fin de la liste des Textes de Couverture de la Version Modifiée. Un seul passage de Texte de la Première de Couverture et de Texte de Dernière de Couverture peut être ajouté par (ou par l'intermédiaire d'accords effectués par) une entité quelconque. Si le Document inclut déjà un texte de couverture pour la même couverture, précédemment ajouté par vous ou par

un accord effectué par l'entité pour le compte de laquelle vous agissez, vous ne pouvez pas en ajouter d'autre ; mais vous pouvez remplacer l'ancien, avec l'autorisation explicite de l'éditeur qui avait ajouté l'ancien.

Le ou les auteur(s) et éditeur(s) du Document n'accordent pas par cette Licence l'autorisation d'utiliser leurs noms pour la publicité de ou pour revendiquer ou insinuer la signature d'une quelconque Version Modifiée.

5. COMBINAISON DE DOCUMENTS

Vous pouvez combiner le Document à d'autres documents diffusés dans le cadre de cette Licence, conformément aux termes définis dans la section 4 ci-dessus pour les versions modifiées, pourvu que vous incluiez à la combinaison toutes les Sections Invariantes de tous les documents d'origine, non modifiés, et que vous les répertoriiez tous comme Sections Invariantes de votre travail combiné dans sa mention de licence, et que vous conserviez toutes ses Limitations de Garantie.

Le travail combiné ne doit contenir qu'une copie de cette Licence, et plusieurs Sections Invariantes identiques peuvent être remplacées par une seule copie. S'il existe plusieurs Sections Invariantes portant le même nom mais avec un contenu différent, rendez le titre de chacune de ces sections unique en ajoutant à la fin de celui-ci, entre parenthèses, le nom de l'auteur ou de l'éditeur d'origine de cette section s'il est connu, ou sinon un numéro unique. Effectuez le même ajustement aux titres des sections dans la liste des Sections Invariantes de la mention de licence du travail combiné.

Dans le travail combiné, vous devez compiler les sections intitulées « Historique » des différents documents originaux, afin de ne plus former qu'une section intitulée « Historique » ; de la même manière, compilez les sections intitulées « Remerciements » et « Dédicaces ». Vous devez supprimer toutes les sections intitulées « Recommandations ».

6. ENSEMBLES DE DOCUMENTS

Vous pouvez réaliser un ensemble constitué du Document et d'autres documents diffusés dans le cadre de cette Licence, et remplacer les copies individuelles de cette Licence dans les différents documents par une copie unique incluse à l'ensemble, pourvu que vous respectiez les règles de cette Licence concernant la copie mot pour mot de chacun des documents dans tous leurs autres aspects.

Vous pouvez extraire un document unique d'un tel ensemble, et le distribuer individuellement dans le cadre de cette Licence, pourvu que vous insériez une copie de cette Licence dans le document extrait, et que vous respectiez cette Licence dans tous ses autres aspects concernant la copie mot pour mot de ce document.

7. AGRÉGATION AVEC DES TRAVAUX INDÉPENDANTS

Une compilation du Document ou de ses dérivés avec d'autres documents ou travaux séparés et indépendants, dans ou sur un volume de stockage ou un support de distribution, est appelé un « agrégation » si le copyright résultant de la compilation n'est pas utilisé pour limiter les droits légaux des utilisateurs de la compilation au-delà de ce qu'autorisent les travaux individuels. Lorsque le Document est inclus dans une agrégation, cette Licence ne s'applique pas aux autres travaux de l'agrégation qui ne sont pas eux-mêmes des travaux dérivés du Document.

Si l'obligation relative au Texte de Couverture de la section 3 est applicable à ces copies du Document, si le Document est inférieur à la moitié de l'agrégation dans son ensemble, les Textes de Couverture du Document peuvent être placés sur les couvertures qui regroupent le Document au sein de l'agrégation, ou l'équivalent électronique des couvertures si le Document est au format électronique. Sinon, ils doivent apparaître sur les couvertures imprimées qui regroupent l'agrégation complète.

8. TRADUCTION

La traduction étant considérée comme une sorte de modification, vous êtes autorisé à distribuer des traductions du Document conformément aux dispositions de la section 4. Le remplacement des Sections Invariantes par des traductions nécessite une autorisation spéciale de leurs détenteurs de copyright, mais vous pouvez inclure des traductions de certaines ou de toutes les Sections Invariantes en plus des versions originales de ces Sections Invariantes. Vous pouvez inclure une traduction de cette Licence, toutes les mentions de licence du Document et toutes les Limitations de Garantie, pourvu que vous incluiez également la version anglaise d'origine de cette Licence et les versions d'origine de ces mentions et de ces limitations. En cas de désaccord entre la traduction et la version originale de cette Licence ou d'une mention ou d'une limitation, la version d'origine prévaut.

Si une section du Document est intitulée « Remerciements », « Dédicaces » ou « Historique », l'obligation (section 4) de conserver son Titre (section 1) nécessitera généralement de changer le titre réel.

9. RÉSILIATION

Vous ne pouvez copier, modifier, accorder une sous-licence, ou distribuer le Document excepté dans le strict respect de cette Licence. Toute autre tentative de copier, modifier, accorder une sous-licence, ou distribuer le Document est nulle et met automatiquement fin à vos droits relatifs à cette Licence. Toutefois, les parties qui ont reçu de votre part des copies, ou des droits dans le cadre de cette Licence ne verront pas leurs licences annulées si elles respectent strictement les termes de cette licence.

10. FUTURES RÉVISIONS DE LA PRÉSENTE LICENCE

La Free Software Foundation peut publier des versions nouvelles, révisées, de la Licence de Documentation Libre GNU de temps à autre. Ces nouvelles versions seront semblables en esprit à la présente version, mais elles peuvent différer dans ses détails pour répondre à de nouveaux problèmes ou à de nouveaux besoins. Reportez-vous à la page https://www.gnu.org/copyleft/.

Chaque version de la Licence reçoit un numéro distinctif. Si le Document spécifie qu'un numéro de version particulier de cette Licence ou de toute autre version ultérieure s'y applique, vous avez la possibilité de respecter les termes et conditions de cette version spécifiée ou de toute autre version ultérieure publiée (autrement que sous forme de brouillon) par la Free Software Foundation. Si le Document ne spécifie pas de numéro de version de cette Licence, vous pouvez choisir n'importe quelle version publiée (autrement que sous forme de brouillon) par la Free Software Foundation.

ANNEXE : comment utiliser la présente Licence pour vos documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

Si vous avez des Sections Invariantes, Textes de Première de Couverture et Textes de Dernière de Couverture, remplacez la ligne « with...Texts » par :

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

Si vous avez des Sections Invariantes sans Textes de Couverture, ou une autre combinaison des trois, fusionnez ces deux alternatives pour vous adapter à la situation.

Si votre document contient des exemples inhabituels de code programme, nous vous recommandons de diffuser ces exemples en parallèle sous votre choix de la licence de logiciel libre, telle que la Licence publique générale GNU, pour en permettre l'utilisation comme un logiciel libre.