

SELinux

CONTENU

La rubrique fournit des informations de base concernant Security-Enhanced Linux.

MOTIF

Vous voulez comprendre SELinux et comment le configurer sous SLE Micro.

EFFORT

La lecture de l'article prend environ 40 minutes.

Date de publication : 11 déc 2025

Table des matières

1	À propos de SELinux	2
2	Obtention de SELinux	2
3	Modes SELinux	2
4	Contexte de sécurité SELinux	6
5	Présentation de la stratégie SELinux	7
6	Attributs booléens SELinux	9
7	Outils de gestion de SELinux	11
8	Mentions légales	21
A	Licence de Documentation Libre GNU	21

1 À propos de SELinux

SELinux a été développé en tant que solution de sécurité Linux supplémentaire qui utilise l'infrastructure de sécurité du kernel Linux. L'objectif était de permettre une stratégie de sécurité plus granulaire allant au-delà des contrôles d'accès discrétionnaires (Discretionary Access Controls - DAC) standard, des autorisations de fichier traditionnelles du propriétaire/du groupe/du monde et de lecture/d'écriture/d'exécution.

SELinux utilise des étiquettes jointes aux objets (par exemple, des fichiers et des sockets réseau) et les utilise pour les décisions d'accès.

L'action par défaut de SELinux consiste à refuser tout accès. SELinux n'autorise que les opérations spécifiquement autorisées dans la stratégie SELinux. Une autre caractéristique de SELinux qui renforce la sécurité est que SELinux permet un confinement strict des processus à tel point que les processus ne peuvent pas accéder aux fichiers d'autres processus sur le même système.

SELinux a été conçu pour améliorer les solutions de sécurité existantes et non pour les remplacer. Par exemple, le contrôle d'accès discrétionnaire (DAC) est toujours d'application, même si le système utilise SELinux. En cas de refus d'accès par DAC, SELinux n'est alors pas utilisé, puisque l'accès a déjà été bloqué en amont par un autre mécanisme.

2 Obtention de SELinux

SELinux est installé par défaut lors de l'installation de SLE Micro par YaST ou fait partie des images prédéfinies.

Si SELinux n'est pas configuré sur votre système, exécutez la commande suivante :

```
# transactional-update setup-selinux
```

Redémarrez votre système une fois la commande terminée. La commande installe la stratégie SELinux si elle n'est pas installée, définit le mode SELinux enforcing, puis reconstruit initrd.

3 Modes SELinux

SELinux peut être exécuté dans l'un des trois modes suivants : disabled, permissive ou enforcing.

L'utilisation du mode disabled signifie qu'aucune règle de la stratégie SELinux n'est appliquée et que votre système n'est pas protégé. Nous vous déconseillons donc d'utiliser le mode disabled.

Avec le mode permissive, SELinux est actif, la stratégie de sécurité est chargée, le système de fichiers est étiqueté et des entrées sont consignées en cas de refus d'accès. Toutefois, la stratégie n'est pas appliquée et aucun accès n'est donc réellement refusé.

En mode enforced, la stratégie de sécurité est appliquée. Chaque accès qui n'est pas explicitement autorisé par la stratégie est refusé.

Pour plus d'informations sur la procédure pour passer d'un mode SELinux à un autre, reportez-vous à la [Section 3.1, « Modification du mode SELinux »](#)

3.1 Modification du mode SELinux

Vous pouvez changer de mode SELinux de façon temporaire ou permanente.

3.1.1 Changement temporaire du mode SELinux

Pour définir temporairement SELinux en mode permissive ou enforcing, utilisez la commande **setenforce**.

La commande **setenforce** présente la syntaxe suivante :

```
# setenforceMODE_ID
```

où MODE_ID est 0 pour le mode permissive ou 1 pour le mode enforced.

N'oubliez pas que vous ne pouvez pas désactiver SELinux à l'aide de la commande **setenforce**.

3.1.2 Modification permanente du mode SELinux

Pour que les modifications apportées au mode SELinux restent applicables après le redémarrage du système, modifiez le fichier de configuration /etc/selinux/config. Dans ce fichier, vous pouvez également désactiver SELinux sur votre système. Toutefois, cette opération n'est pas recommandée. Si vous pensez que SELinux est peut-être à l'origine de certains problèmes sur votre système, passez alors en mode permissive et déboguez votre système.

Dans le fichier /etc/selinux/config, modifiez la valeur de SELINUX en disabled, permissive ou enforced comme suit :

```
SELINUX=disabled
```

Les modifications apportées au fichier seront appliquées après le prochain redémarrage.



Remarque : réétiquetage de votre système après avoir quitté le mode disabled

Si vous désactivez SELinux sur votre système et que vous le réactivez par la suite, veillez à réétiqueter votre système. Lorsque SELinux est désactivé et que vous apportez des modifications à votre système de fichiers, les modifications ne sont plus prises en compte dans le contexte (par exemple, les nouveaux fichiers n'ont aucun contexte). Par conséquent, vous devez réétiqueter votre système à l'aide de la commande **restorecon**, du paramètre de démarrage `autorelabel` ou en créant un fichier qui déclenchera le réétiquetage au prochain démarrage. Pour créer le fichier, exécutez la commande suivante :

```
# touch /etc/selinux/.autorelabel
```

Après le redémarrage, le fichier `/etc/selinux/.autorelabel` est remplacé par un autre fichier d'indicateur (`/etc/selinux/.relabelled`) pour empêcher le réétiquetage lors des redémarrages suivants.

3.1.3 Vérification du mode SELinux actif

Pour vérifier le mode, exécutez la commande suivante :

```
# getenforce
```

La commande doit renvoyer `permissive` ou `enforced` selon l'ID de mode `MODE_ID` fourni.

3.2 Vérification du fonctionnement de SELinux

Pour apporter des modifications de configuration, il peut être utile de passer en mode permissif. Pendant ce temps, les utilisateurs risquent d'étiqueter les fichiers de manière incorrecte et provoquer des problèmes lors du retour au mode d'application.

Pour rétablir l'état sécurisé du système, procédez comme suit :

1. Réinitialisez le contexte de sécurité :

```
> sudo restorecon -R /
```

2. Passez en mode d'application en définissant `SELINUX=enforcing` dans le fichier à l'emplacement suivant `/etc/selinux/config`.
3. Redémarrez le système, puis reconnectez-vous.
4. Exécutez la commande `sestatus -v`. Vous devriez obtenir une sortie similaire à ce qui suit :

```
> sudosestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:        enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    requested(insecure)
Max kernel policy version:    33

Process contexts:
Current context:               unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
Init context:                  system_u:system_r:init_t:s0
/usr/sbin/sshd                 system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:          unconfined_u:object_r:user_tty_device_t:s0
/etc/passwd                    system_u:object_r:passwd_file_t:s0
/etc/shadow                    system_u:object_r:shadow_t:s0
/bin/bash                      system_u:object_r:shell_exec_t:s0 \
-> system_u:object_r:shell_exec_t:s0
/bin/login                     system_u:object_r:login_exec_t:s0
/bin/sh                        system_u:object_r:bin_t:s0 \
-> system_u:object_r:shell_exec_t:s0
/sbin/agetty                   system_u:object_r:bin_t:s0 \
-> system_u:object_r:getty_exec_t:s0
/sbin/init                     system_u:object_r:bin_t:s0 -> \
system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                 system_u:object_r:sshd_exec_t:s0
```

5. Si le système ne fonctionne pas correctement, vérifiez les fichiers journaux à l'emplacement suivant : `/var/log/audit/audit.log`. Pour plus d'informations, reportez-vous à la documentation [SELinux troubleshooting \(https://documentation.suse.com/smart-supported.html\)](https://documentation.suse.com/smart-supported.html).

4 Contexte de sécurité SELinux

Le contexte de sécurité est un ensemble d'informations assignées à un fichier ou à un processus. Il se compose de l'utilisateur SELinux, de son rôle, du type, du niveau et de la catégorie. Ces informations servent à prendre des décisions en matière de contrôle d'accès.

CHAMPS DE CONTEXTE SELINUX

utilisateur SELinux

Identité définie dans la stratégie qui est autorisée pour un ensemble spécifique de rôles et pour une plage de *niveau* spécifique. Chaque utilisateur Linux est assigné à un seul utilisateur SELinux. Toutefois, un utilisateur SELinux peut avoir plusieurs rôles.

SELinux n'utilise pas la liste des comptes utilisateur gérée par Linux dans le fichier à l'emplacement `/etc/passwd`, mais utilise sa propre base de données et son assignation. Par convention, le nom de l'identité a le suffixe `_u`, par exemple : `user_u`.

Lorsqu'un nouveau compte Linux est créé et que l'utilisateur SELinux n'est pas assigné au compte, l'utilisateur SELinux par défaut est utilisé. Habituellement, la valeur par défaut est `unconfined_u`. Pour consulter la procédure de modification de la valeur par défaut, reportez-vous à la [Section 7.5.2, « Commande `semanage login` »](#).

rôle

Définit un ensemble d'autorisations qu'un utilisateur peut se voir accorder. Un rôle définit les *types* auxquels un utilisateur assigné à ce rôle peut accéder. Par convention, le nom du rôle a le suffixe `_r`, par exemple : `system_r`.

type

Le type transmet des informations sur la façon dont certains fichiers et processus peuvent interagir. Un processus est constitué de fichiers d'un type SELinux bien spécifique et ne peut pas accéder aux fichiers qui ne sont pas de ce type. Par convention, le nom du type a le suffixe `_t`, par exemple : `var_t`

niveau

Attribut facultatif qui spécifie la plage de niveaux d'autorisation dans le cadre d'une sécurité à plusieurs niveaux.

catégorie

Attribut facultatif qui vous permet d'ajouter des catégories à des processus, à des fichiers et à des utilisateurs. Un utilisateur peut alors accéder aux fichiers d'une même catégorie.

Voici un exemple de contexte SELinux :

```
allow user_t bin_t:file {read execute gettattr};
```

Cet exemple de règle indique que l'utilisateur qui possède le type de contexte `user_t` (cet utilisateur est appelé l'objet source) est autorisé à accéder aux objets du *fichier* de classe dont le type de contexte est `bin_t` (la cible), à l'aide des autorisations `read`, `execute` et `gettattr`.

5 Présentation de la stratégie SELinux

La stratégie est le composant clé de SELinux. Votre stratégie SELinux définit des règles qui spécifient les objets qui peuvent accéder aux fichiers, répertoires, ports et processus d'un système. Pour ce faire, un contexte de sécurité est défini pour l'ensemble de ces éléments.

Une stratégie SELinux contient un grand nombre de règles. Pour faciliter leur gestion, les stratégies sont souvent divisées en modules. De cette façon, l'administrateur peut activer ou désactiver la protection pour différentes parties du système.

Lors de la compilation de la stratégie pour votre système, vous aurez le choix entre une stratégie modulaire ou monolithique. La stratégie monolithique est une stratégie gigantesque qui servira à protéger l'ensemble de votre système. Nous vous recommandons vivement d'utiliser une stratégie modulaire plutôt qu'une stratégie monolithique. Les stratégies modulaires sont beaucoup plus simples à gérer.

SLE Micro est fourni avec la stratégie SELinux `targeted`.

5.1 Utilisation des modules SELinux

En tant qu'administrateur, vous pouvez activer ou désactiver des modules. Cela peut être utile si vous souhaitez désactiver uniquement une partie de la stratégie SELinux et que vous ne souhaitez pas exécuter un service spécifique sans la protection SELinux.

Pour afficher tous les modules de stratégie SELinux en cours d'utilisation, exécutez la commande :

```
semodule -l
```

Une fois que vous avez obtenu le nom du module que vous souhaitez désactiver, exécutez la commande :

```
> sudo semodule -d MODULENAME
```

Pour activer le module de stratégie, exécutez la commande :

```
> sudo semodule -e MODULENAME
```

5.2 Création de stratégies pour les conteneurs

SLE Micro est fourni avec une stratégie qui, par défaut, n'autorise pas les conteneurs à accéder aux fichiers en dehors des données de conteneur. En revanche, tous les accès au réseau sont autorisés. En règle générale, les conteneurs sont créés avec des montages liés et doivent pouvoir accéder à d'autres répertoires, tels que `/home` ou `/var`. Vous souhaitez peut-être avoir la possibilité d'autoriser l'accès à ces répertoires ou, au contraire, de limiter certains ports au conteneur, même si SELinux est utilisé sur votre système. Dans ce cas, vous devez créer de nouvelles règles de stratégie qui activent ou désactivent l'accès. SLE Micro fournit l'outil Udica pour ce faire.

La procédure suivante décrit comment créer une stratégie personnalisée pour vos conteneurs :

1. Assurez-vous que SELinux est en mode d'application. Pour plus d'informations, reportez-vous à la [Section 3.1, « Modification du mode SELinux »](#).

2. Démarrez un conteneur à l'aide des paramètres suivants :

```
# podman run -v /home:/home:rw -v /var:/var:rw -p 21:21 -it sle15 bash
```

Le conteneur s'exécute avec la stratégie par défaut qui n'autorise pas l'accès aux points de montage, mais ne limite pas les autres ports.

3. Vous pouvez quitter le conteneur.

4. Obtenez l'ID du conteneur :

```
# podman ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
e59f9d0f86f2	registry.opensuse.org/devel/bci/tumbleweed/containerfile/opensuse/bci/ruby:latest	/bin/bash	8 minutes ago	Up 8 seconds ago	0.0.0.0:21->21/tcp	zen_ramanujan

5. Créez un fichier JSON qu'Udica utilisera pour créer une stratégie personnalisée pour le conteneur :

```
# podman inspect e59f9d0f86f2 >OUTPUT_JSON_FILE
```


Par exemple, remplacez `OUTPUT_JSON_FILE` par `container.json`.

6. Exécutez Udica pour générer une stratégie en fonction des paramètres du conteneur :

```
# udica -j OUTPUT_JSON_FILE CUSTOM_CONTAINER_POLICY
```

Par exemple :

```
# udica -j container.json custom_policy
```

7. Selon les instructions fournies, chargez les modules de stratégie en exécutant :

```
# semodule -i custom_policy.cil /usr/share/udica/templates/  
{base_container.cil,net_container.cil,home_container.cil}
```

8. Exécutez un conteneur avec le nouveau module de stratégie en utilisant l'option `--security-opt` comme suit :

```
# podman run --security-opt label=type:custom_policy.process -v /home:/home:rw -v /  
var:/var:rw -p 21:21 -it sle15 bash
```

6 Attributs booléens SELinux

Les attributs booléens SELinux prennent en charge une approche flexible de gestion des stratégies. Par exemple, les attributs booléens vous permettent de désactiver une stratégie spécifique d'un serveur, tout en maintenant la même stratégie active sur un autre. Autrement dit, un attribut booléen peut être interprété comme un paramètre de règle de stratégie. Au lieu de modifier une stratégie particulière, vous pouvez la désactiver. Dans le code de la stratégie, les attributs booléens sont appelés *variables programmables*. Étant donné que les attributs booléens sont inclus dans la stratégie, ils sont disponibles dès qu'une stratégie est chargée.

Les modifications apportées aux valeurs booléennes peuvent être permanentes ou temporaires et dans ce cas, ne durer que jusqu'à la fin de la session.

SELinux propose des outils qui vous permettent de lister et d'afficher les détails ou de modifier l'état des attributs booléens. Reportez-vous aux sections suivantes pour plus de détails.

6.1 Utilisation d'attributs booléens

6.1.1 Liste des attributs booléens

Vous pouvez utiliser la commande **getsebool** ou **semanage** pour lister les attributs booléens actuellement définis. Pour lister tous les attributs booléens actuellement définis, ainsi que leur état, exécutez la commande suivante :

```
# getsebool -a

abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
...
```

Pour obtenir plus de détails sur des attributs booléens spécifiques, vous pouvez utiliser la commande **semanage** comme suit :

```
# semanage boolean -l
```

SELinux boolean	State	Default	Description
abrt_anon_write	(off , off)		Allow abrt to anon write
abrt_handle_event	(off , off)		Allow abrt to handle event
abrt_upload_watch_anon_write	(on , on)		Allow abrt to upload watch anon write

Pour obtenir l'état d'un attribut booléen individuel, vous pouvez utiliser la commande suivante :

```
# getseboolBOOLEAN_NAME
```

Vous pouvez également utiliser la commande **grep** sur la sortie **semanage boolean** :

```
# semanage boolean -l | grepBOOLEAN_NAME
```

6.1.2 Affichage/masquage des attributs booléens

Les commandes **setsebool** et **semanage** peuvent être utilisées pour changer la valeur des attributs booléens. Vous pouvez modifier l'état d'un attribut booléen de façon permanente ou temporaire (jusqu'à la fin de la session). Pour modifier temporairement une valeur booléenne, exécutez la commande suivante :

```
# setseboolBOOLEAN_NAMEBOOLEAN_VALUE
```

où `BOOLEAN_VALUE` est soit `on`, soit `off`.

Pour modifier une valeur booléenne de façon permanente, exécutez l'une des deux commandes suivantes :

```
# setsebool -PBOOLEAN_NAMEBOOLEAN_VALUE
```

Vous pouvez également utiliser la commande `semanage` :

```
# semanage boolean -m --BOOLEAN_VALUEBOOLEAN_NAME
```

où `BOOLEAN_VALUE` est soit `on`, soit `off`

Un seul attribut booléen peut activer ou désactiver plusieurs règles de stratégie. Pour afficher les règles de stratégie activées ou désactivées par les attributs booléens, employez l'outil `sedispol` qui permet d'analyser le fichier de stratégie :

```
# sedispol /etc/selinux/targeted/policy/policy.32
```

Les règles de stratégie étant généralement très volumineuses, nous vous recommandons de définir un fichier de sortie en sélectionnant `f` et en spécifiant un nom de fichier. Après avoir spécifié le nom du fichier, appuyez sur `6`. Vous pouvez ensuite inspecter le fichier.

7 Outils de gestion de SELinux

SLE Micro vous fournit des outils pour gérer SELinux sur votre système. Si les outils décrits ci-dessous ne sont pas installés sur votre système, installez-les en exécutant :

```
# transactional-update pkg install policycoreutils-python-utils
```

Une fois l'installation réussie, redémarrez le système.

7.1 Utilisation de l'option `Z`

Lorsque SELinux est installé et configuré, vous pouvez utiliser l'option `-Z` dans les commandes standard telles que `ls`, `id`, ou `ps`. Cette option vous permet d'afficher le contexte de sécurité des fichiers ou des processus. Par exemple, pour la commande `ls` :

```
> ls -Z /etc/shadow

system_u:object_r:shadow_t:s0 /etc/shadow
```

7.2 Commande **chcon**

Le nom de la commande **chcon** signifie « change context » (modifier le contexte). La commande peut modifier l'ensemble du contexte de sécurité d'un fichier par la valeur fournie dans l'interface de ligne de commande ou n'en modifier que certaines parties. Vous pouvez également fournir un fichier pour qu'il serve de référence.

Pour modifier l'ensemble du contexte de sécurité d'un fichier, la syntaxe de la commande se présente comme suit :

```
# chconSECURITY_CONTEXTFILENAME
```

où :

- SECURITY_CONTEXT est au format : SELinux_USER:ROLE:TYPE:LEVEL:CATEGORY. Par exemple, le contexte peut être : `system_u:object_r:httpd_config_t:s0`.
- FILENAME est le chemin d'accès au fichier dont le contexte doit être modifié.

Pour définir un contexte de sécurité en fonction d'un fichier fourni à titre de référence, exécutez **chcon** comme suit :

```
# chcon --reference=REFERENCE_FILEFILENAME
```

où :

- REFERENCE_FILE est le chemin d'accès à un fichier qui doit servir de référence.
- FILENAME est le chemin d'accès au fichier dont le contexte doit être modifié.

Vous pouvez également modifier uniquement une partie du contexte de sécurité. La syntaxe générale de la commande **chcon** est la suivante :

```
# chconCONTEXT_OPTIONCONTEXT_PARTFILENAME
```

Les options et arguments ont la signification suivante :

- En fonction de la partie du contexte, CONTEXT_OPTION peut être l'un des éléments suivants :

-u resp --user

Indique qu'un contexte utilisateur SELinux sera modifié dans le fichier fourni :

```
# chcon -u system_u logind.conf
```

-r resp --role

Seule la partie role (rôle) sera modifiée dans le contexte du fichier fourni :

```
# chcon -r object_r logind.conf
```

-t resp --type

Seule la partie type (type) sera modifiée dans le contexte du fichier fourni :

```
# chcon -t etc_t logind.conf
```

-l resp --range

Seule la partie range (plage) du contexte de sécurité sera modifiée :

```
# chcon -l s0 logind.conf
```

- CONTEXT_PART est la valeur spécifique du contexte de sécurité à définir.
- FILENAME est un chemin d'accès au fichier dont le contexte sera modifié.



Remarque : utilisation de **chcon** sur des liens symboliques

Par défaut, lorsque vous modifiez le contexte de sécurité d'un lien symbolique, le contexte du lien cible est modifié et le contexte du lien symbolique n'est **pas** modifié. Pour forcer **chcon** à modifier le contexte du lien symbolique et non de la cible du lien, utilisez l'option --no-dereference ci-dessous :

```
# chcon --no-dereference -u system_u -t etc_t network.conf
```

Vous pouvez modifier le contexte de tous les fichiers d'un répertoire à l'aide de l'option récursive :

```
# chcon --recursive system_u:object_r:httpd_config_t:s0 conf.d
```

7.3 Commandes **getenforce** et **setenforce**

La commande **getenforce** renvoie le mode SELinux actuel : Enforcing, Permissive ou Disabled.

```
# getenforce
```

Permissive

La commande **setenforce** change temporairement le mode SELinux en mode d'application ou permissif. Vous ne pouvez pas utiliser cette commande pour désactiver SELinux. N'oubliez pas que la modification ne reste active que jusqu'au prochain redémarrage. Pour modifier l'état de façon permanente, lisez la description de la [Section 3.1, « Modification du mode SELinux »](#).

```
# setenforceMODE_ID
```

où MODE_ID est 0 pour le mode permissive ou 1 pour le mode enforced.

7.4 Script **fixfiles**

Le script vous permet d'effectuer la tâche suivante avec le contexte de sécurité :

- Vérifier si le contexte est correct
- Modifier les étiquettes de contexte de fichier incorrectes
- Renommer votre système si vous avez ajouté une nouvelle stratégie

La syntaxe du script est la suivante :

```
# fixfiles [OPTIONS] ARGUMENT
```

où :

- OPTIONS peut être l'une des commandes suivantes :

-l LOGFILE

Enregistre la sortie dans le fichier fourni.

-o OUTPUT_FILE

Enregistre les noms de tous les fichiers dont le contexte de fichier diffère de celui par défaut dans le fichier de sortie fourni.

-F

Force une réinitialisation du contexte.

- ARGUMENT peut être l'une des commandes suivantes :

check

Affiche le contexte du fichier précédent et du fichier actuel pour une étiquette incorrecte sans apporter de modifications.

relabel

Réétiquette les contextes de fichier incorrects en fonction de la stratégie actuellement chargée.

restore

Restaure les valeurs par défaut des contextes de fichier incorrects.

verify

Dresse une liste de tous les fichiers dont les étiquettes de contexte de fichier sont incorrectes sans apporter de modifications.

7.5 Commande **semanage**

La commande **semanage** peut être utilisée pour configurer des parties de la stratégie sans devoir recompiler la stratégie à partir des sources. La commande vous permet d'effectuer les tâches suivantes :

- Gérer les attributs booléens à l'aide de l'argument boolean. Pour plus d'informations concernant les attributs booléens, reportez-vous à la section *Section 6.1, « Utilisation d'attributs booléens »*.
- Ajuster le contexte des fichiers à l'aide de l'argument fcontext.
- Gérer les assignations d'utilisateurs à l'aide de l'argument login.
- Gérer les utilisateurs SELinux à l'aide de l'argument user.
- Gérer les modules de stratégie SELinux à l'aide de l'argument module.

La syntaxe générale de la commande se présente comme suit :

```
# semanageARGUMENTOPTIONS [OBJECT_NAME]
```

où :

- ARGUMENT est l'un des opérateurs suivants : **login**, **user**, **fcontext**, **boolean**, **module**.
- OPTIONS dépend de l'argument ARGUMENT fourni. Ces options sont décrites dans la rubrique *Options courantes*.
- OBJECT_NAME en fonction de l'argument ARGUMENT fourni, il peut s'agir d'un nom de connexion, d'un nom de module, d'un nom de fichier ou d'un utilisateur SELinux.

OPTIONS COURANTES

-a, --add

Ajoute un objet fourni.

-h, --help

Affiche l'aide de la commande.

--extract

Affiche les commandes utilisées pour modifier le système (attributs booléens, contexte de fichier, etc.).

-l, --list

Dresse la liste de tous les objets.

-m, --modify

Modifie l'objet fourni.

-n, --noheading

Modifie la sortie de l'opération établissant la liste en omettant les titres.

-s, --seuser

Spécifie l'utilisateur SELinux.

D'autres options sont spécifiques à des commandes **semanage** particulières et sont décrites dans les sections correspondantes.

7.5.1 Commande **semanage fcontext**

La commande **semanage fcontext** vous permet d'effectuer les tâches suivantes :

- Demander les définitions des contextes de fichiers
- Ajouter des contextes aux fichiers
- Ajouter vos propres règles

Les modifications apportées au contexte de fichier à l'aide de la commande **semanage fcontext** ne nécessitent pas de modification ni de recompilation de la stratégie.

En plus des options courantes décrites dans la rubrique *Options courantes*, la commande **semanage fcontext** utilise les options suivantes :

-e, --equal

Cette option vous permet d'utiliser le contexte du chemin d'accès fourni pour étiqueter les fichiers dans un autre répertoire (chemin cible fourni). Par exemple, vous voulez assigner le même contexte que /home à un autre répertoire privé /export/home. Si vous utilisez cette option, vous devez fournir les chemins source cible :

```
# semanage fcontext -a -e /home /export/home
```

-f, --ftype

Spécifiez un type de fichier. Utilisez l'une des valeurs suivantes :

- a : tous les fichiers. Il s'agit aussi de la valeur par défaut
- b : un périphérique de bloc
- c : un périphérique de caractères
- d : un répertoire
- f : fichiers normaux
- l : un lien symbolique
- p : un canal nommé
- s : un socket

7.5.2 Commande **semanage login**

La commande **semanage login** vous permet d'effectuer les tâches suivantes :

- Assignment d'utilisateurs Linux à un utilisateur SELinux spécifique. Par exemple, pour assigner l'utilisateur Linux *tux* à l'utilisateur sysadm_u exécutez la commande :

```
# semanage login -a -s sysadm_u tux
```

- Assignment d'un groupe d'utilisateurs Linux à un utilisateur SELinux spécifique. Par exemple, pour assigner les utilisateurs du groupe *writers* (utilisateurs disposant de droits en écriture) à l'utilisateur user_u, exécutez la commande :

```
# semanage login -a -s user_u %writers
```

Le groupe est ensuite répertorié dans la sortie de **semanage login -l**, précédé du caractère %.

N'oubliez pas que le groupe d'utilisateurs doit être primaire, car l'assignation d'utilisateurs SELinux à des groupes supplémentaires peut entraîner des assignations incompatibles.

```
# semanage login -m -s staff_u %writers
```

- Assignation d'utilisateurs Linux à une plage de sécurité SELinux MLS/MCS spécifique.
- Modification de l'assignation déjà créée. Pour ce faire, remplacez simplement l'option **-a** par **-m** dans les commandes précédentes.
- Définition de l'utilisateur SELinux par défaut pour les nouveaux utilisateurs Linux. Par défaut, l'utilisateur SELinux est habituellement **unconfined_u**. Pour modifier la valeur sur **staff_u**, exécutez la commande :

```
# semanage login -m -s staff_u __default__
```

7.5.3 Commande **semanage boolean**

La commande **semanage boolean** permet de contrôler les attributs booléens dans la stratégie SELinux.

Le synopsis de la commande se présente comme suit :

```
semanage boolean [-h] [-n] [ --extract |  
--deleteall | --list [-C] | --modify ( --on | --off | -1 | -0 ) boolean ]
```

En plus des options courantes, vous pouvez utiliser les options spécifiques suivantes dans la commande **semanage boolean** :

--list -C

Permet d'afficher une liste des modifications locales apportées aux attributs booléens.

-m --on | -1

Permet d'activer l'attribut booléen fourni.

-m --off | -0

Permet de désactiver l'attribut booléen fourni.

-D, --deleteall

Permet de supprimer toutes les modifications locales apportées aux attributs booléens.

L'utilisation la plus courante de la commande consiste à activer ou à désactiver un attribut booléen spécifique. Par exemple, pour activer l'attribut booléen `authlogin_yubikey`, exécutez :

```
# semanage boolean -m on authlogin_yubikey
```

7.5.4 Commande `semanage user`

La commande `semanage user` contrôle l'assignation entre l'utilisateur SELinux, les rôles et les niveaux MLS/MCS.

En plus des options courantes décrites dans la rubrique *Options courantes*, la commande `semanage use` utilise les options suivantes :

`-R [ROLES], --roles [ROLES]`

Liste des rôles SELinux. Vous pouvez placer plusieurs rôles entre guillemets et les séparer par des espaces ou utiliser plusieurs fois `-R`.

Cette commande vous permet d'effectuer les tâches suivantes :

- Dresser la liste de l'assignation des utilisateurs SELinux aux rôles en exécutant la commande :

```
# semanage user -l
```

- Modifier les rôles assignés à l'utilisateur SELinux `user_u` :

```
# semanage user -m -R "system_r unconfined_r user_r"
```

- Assigner à l'utilisateur `admin_u` le rôle `staff_r` et une catégorie `s0` :

```
# semanage user -a -R "staff_r -r s0 admin_u"
```

- Créer un nouvel utilisateur SELinux, par exemple, `admin_u` avec le rôle `staff_r`. Vous devez également définir le préfixe d'étiquetage pour cet utilisateur à l'aide de l'option `-P` :

```
# semanage user -a -R "staff_r" -P admin admin_u
```

7.5.5 Commande `semanage module`

La commande `semanage module` peut installer, supprimer, désactiver ou activer des modules de stratégie SELinux.

En plus des options courantes décrites dans la rubrique *Options courantes*, la commande **semanage** **fcontext** utilise les options suivantes :

-d, --disable

Pour désactiver le module de stratégie SELinux fourni :

```
# semanage module --disable MODULE_NAME
```

-e, --enable

Pour activer le module de stratégie SELinux fourni :

```
# semanage module --enable MODULE_NAME
```

7.6 Commande **sestatus**

La commande **sestatus** obtient l'état d'un système sur lequel SELinux est exécuté.

La syntaxe générique de la commande est la suivante :

```
sestatus [OPTION]
```

Lorsqu'elle est exécutée sans options ni arguments, la commande génère les informations suivantes :

```
# sestatus

SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    requested (insecure)
Max kernel policy version:    33
```

La commande peut accepter les options suivantes :

-b

Affiche l'état des attributs booléens sur le système.


-v

Affiche le contexte de sécurité des fichiers et des processus répertoriés dans le fichier /etc/sestatus.conf.

8 Mentions légales

Copyright © 2006–2025 SUSE LLC et contributeurs. Tous droits réservés.

Il est autorisé de copier, distribuer et/ou modifier ce document conformément aux conditions de la licence de documentation libre GNU version 1.2 ou (à votre discrétion) 1.3, avec la section permanente qu'est cette mention de copyright et la licence. Une copie de la version de licence 1.2 est incluse dans la section intitulée « Licence de documentation libre GNU ».

Pour les marques commerciales SUSE, consultez le site Web <https://www.suse.com/company/legal/> . Toutes les autres marques de fabricants tiers sont la propriété de leur détenteur respectif. Les symboles de marque (®, ™, etc.) désignent des marques commerciales de SUSE et de ses sociétés affiliées. Des astérisques (*) désignent des marques commerciales de fabricants tiers.

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

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Toute personne est autorisée à copier et distribuer des copies exactes de cette Licence, mais n'a pas le droit de les modifier.

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 répertoriez 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.