SUSE

Configuration des privilèges de superutilisateur avec sudo

CONTENU

Familiarisez-vous avec les bases de la configuration de **sudo** et apprenez à déléguer les privilèges de superutilisateur avec **sudo**. Cet article fournit des informations approfondies sur la configuration de **sudo** et ne donne aucun conseil sur la manière d'élaborer une stratégie **sudo** complète et sécurisée. Les stratégies liées à la sécurité sont très complexes et dépendent fortement de l'environnement pour lequel elles sont créées.

MOTIF

Certaines commandes nécessitent des privilèges d'administrateur ou `root`. L'utilisation de **sudo** vous permet de déléguer à certains utilisateurs ou groupes les privilèges nécessaires pour exécuter ces commandes.

EFFORT

La lecture de cet article vous prendra au maximum 20 minutes. L'écriture de votre première règle de configuration **sudo** ne prend que quelques minutes, mais l'établissement d'une configuration **sudo** fonctionnelle qui soit opérationnelle dans l'ensemble de votre environnement prendra beaucoup plus de temps, selon la complexité de votre configuration.

OBJECTIF

Comprendre les principes de base de la configuration **sudo**. Traiter les cas d'utilisation courants pour la configuration **sudo**. Apprendre à travailler avec des utilisateurs, des groupes d'utilisateurs et des alias dans des configurations **sudo**. Se familiariser avec les meilleures pratiques et le dépannage de **sudo**.

CONDITIONS REQUISES

- Connaissances de base de **sudo**.
- Privilèges `root`. Pour plus d'informations sur l'utilisation de **sudo** en tant qu'utilisateur standard, reportez-vous à la documentation https://documentation.suse.com/smart/systems-management/html/sudo-run-commands-as-superuser/index.html.

Date de publication : 11 déc 2025

Table des matières

1 Présentation de la configuration **sudo**

sudo fournit un moyen de déléguer de manière sécurisée et efficace des privilèges de superutilisateur à certains utilisateurs ou groupes.

Certaines opérations sur un système Linux nécessitent des privilèges d'administrateur ou `root`. Les utilisateurs privés qui gèrent leur propre système n'ont pas à déléguer de privilèges de superutilisateur, car l'administrateur et l'utilisateur ordinaire sont la même personne dans ce scénario. Toutefois, dès qu'un système fait partie d'un plus vaste environnement comptant plusieurs utilisateurs, groupes et hôtes, il devient alors essentiel de garder le contrôle de qui est autorisé à faire quoi et où. En même temps, il est important de fournir à tous les utilisateurs et groupes les privilèges nécessaires pour effectuer leurs tâches.

Important

Dans la nouvelle stratégie mise en œuvre dans le paquet `sudo-policy-wheel-auth-self`, le groupe `wheel` est utilisé pour vérifier si un utilisateur peut devenir un utilisateur `root` avec le mot de passe de l'utilisateur. Le premier utilisateur créé par le programme d'installation d'Agama est ajouté au groupe `wheel`.

En outre, lors de l'exécution de la commande **sudo** :

- Si vous faites partie du groupe `wheel`, vous êtes invité à entrer votre mot de passe utilisateur.
- Si vous ne faites pas partie du groupe `wheel`, vous êtes invité à entrer le mot de passe `root`.

sudo offre les avantage suivants :

Amélioration de la sécurité du système

sudo offre un contrôle précis sur les utilisateurs, les groupes, les hôtes et les commandes et augmente ainsi la sécurité du système en réduisant le risque de dommages intentionnels ou accidentels par un intrus ou un utilisateur système.

Suivi d'audit complet

Chaque fois qu'un utilisateur change de privilège, cette information apparaît dans le journal du système et toutes les opérations effectuées par cet utilisateur avec des privilèges élevés peuvent être retracées.

Possibilité de déléguer des tâches `root` spécifiques

À l'aide de **sudo**, les administrateurs système peuvent permettre à des utilisateurs individuels ou à des groupes d'effectuer certaines tâches sans devoir entrer le mot de passe `root` et à basculer vers le compte `root`.

2 Création de configurations **sudo** personnalisées

Apprenez à créer un simple exemple de configuration **sudo** personnalisée et à le développer étape par étape. Créez des groupes et utilisez des alias pour que votre configuration personnalisée reste simple et efficace.

Important

Lors de la migration à partir de SUSE Linux Enterprise Server for SAP Applications 15, le fichier `/etc/sudoers` est présent. Le fichier `/usr/etc/sudoers` est ignoré si le fichier `/etc/sudoers` existe. Tant que l'utilisateur n'a pas modifié le fichier `/etc/sudoers` de manière significative, la configuration du répertoire `/etc/sudoers.d/` sera toujours lue.

Lors de la migration à partir de SUSE Linux Enterprise Server for SAP Applications 15, il est recommandé aux utilisateurs qui n'ont pas modifié le fichier `/etc/sudoers` de le supprimer. Si un utilisateur a modifié le fichier `/etc/sudoers`, déplacez le fichier modifié dans le répertoire `/etc/sudoers.d`, puis supprimez-le.

Avertissement : les exemples de configuration sont fournis à des fins de démonstration uniquement

Les exemples de règles décrits ci-dessous sont fournis uniquement à des fins de démonstration. Utilisez-les pour comprendre la syntaxe générale des fichiers de configuration **sudo**. Ne les utilisez pas dans des configurations réelles, car ils ne reflètent pas la complexité de ces environnements.

2.1 Meilleures pratiques de configuration **sudo**

Avant de commencer, voici quelques règles de base pour la gestion des configurations **sudo** :

Utilisez toujours la commande `visudo -f` pour modifier le répertoire `/etc/sudoers.d/`
: Toute modification apportée à la configuration de **sudo** doit être effectuée à l'aide de la commande **visudo**. **visudo** est un outil personnalisé qui vous permet d'éditer les fichiers de configuration **sudo** et d'exécuter des vérifications de syntaxe de base, en veillant à garder la configuration intacte et fonctionnelle. Une configuration **sudo** erronée peut empêcher l'accès d'un utilisateur à son propre système.

Créez toujours les configurations personnalisées sous `/etc/sudoers.d/`
: Les configurations personnalisées doivent se trouver dans le répertoire `/etc/sudoers.d/` afin que **sudo** puisse les extraire. Les paramètres des fichiers de configuration personnalisés sont prioritaires sur ceux de la configuration par défaut dans `/usr/etc/sudoers`.

Tenez toujours compte de l'ordre dans lequel les configurations sont lues
: Pour vous assurer que les configurations personnalisées sont lues dans le bon ordre, ajoutez-leur un numéro en préfixe. Utilisez des zéros au début pour établir l'ordre dans lequel les fichiers sont lus. Par exemple, `01_myfirstconfig` est analysé avant `10_myotherconfig`. Si une directive a été définie dans un fichier qui est lu avant un autre fichier contenant des informations contradictoires, la dernière directive lue est appliquée.

Utilisez toujours des noms de fichiers descriptifs
: Utilisez des noms qui indiquent la finalité du fichier de configuration. Cela vous aide à suivre ce que votre configuration **sudo** est censée faire.

2.2 Création d'un fichier de configuration spécifique à l'utilisateur

Créez un fichier de configuration **sudo** qui permet à un utilisateur standard (`tux`) d'employer la commande **useradd** avec son propre mot de passe au lieu du mot de passe `root`.

EXEMPLE 1 : CRÉATION D'UN FICHIER DE CONFIGURATION SPÉCIFIQUE À L'UTILISATEUR

1. En tant qu'administrateur système (`root`), créez un fichier de configuration personnalisé qui contient les nouvelles directives spécifiques à l'utilisateur en démarrant **visudo**. Utilisez une numérotation ainsi qu'un nom descriptif :

```
# visudo -f /etc/sudoers.d/02_usermanagement
```

2. Créez une règle qui permet à `tux` d'exécuter le fichier binaire **`/usr/sbin/useradd`** dans tout l'environnement auquel cette configuration **`sudo`** s'applique :

```
tux❶ ALL❷ = /usr/sbin/useradd❸
```

❶ Spécifiez l'utilisateur ou le groupe. Répertoriez les utilisateurs par nom ou `#UID` et les groupes par `%GROUPNAME`. Si vous disposez de plusieurs éléments ici, séparez-les par des virgules. Pour refuser des entrées, utilisez `!`.

❷ Spécifiez un ou plusieurs hôtes (séparés par des virgules). Utilisez des noms d'hôte (complets) ou des adresses IP. Ajoutez `ALL` pour appliquer ce paramètre globalement à tous les hôtes. Utilisez `!` pour les interdictions.

❸ Spécifiez un ou plusieurs exécutables (séparés par des virgules). Lorsque vous les spécifiez, veillez à respecter les règles suivantes :

`/usr/sbin/useradd`
: Sans ajouter d'options supplémentaires, cela permet d'exécuter toutes les commandes **`useradd`** possibles.

`/usr/sbin/useradd -c`
: Si vous spécifiez explicitement une option, cette option est la seule autorisée. Aucune autre ne sera disponible pour l'utilisateur que vous avez spécifié ci-dessus.

`/usr/sbin/useradd ""`
: Cette syntaxe permet à l'utilisateur d'invoquer une simple commande **`useradd`** sans aucune option.

Dans l'exemple ci-dessus, vous pouvez autoriser toutes les options et sous-commandes ou les limiter à quelques-unes pour des raisons de sécurité, mais interdire à un utilisateur de spécifier une quelconque option est inutile dans ce contexte.

3. Enregistrez la configuration, quittez l'éditeur, puis ouvrez un deuxième shell pour vérifier si **`sudo`** respecte votre nouvelle configuration.

2.3 Création de configurations personnalisées en regroupant des éléments

Modifiez la configuration de l'*Exemple 1, « création d'un fichier de configuration spécifique à l'utilisateur »* de sorte qu'un groupe d'utilisateurs nommés puisse exécuter la commande **useradd** sans avoir besoin du mot de passe `root`. Ajoutez également **usermod** et **userdel** à la liste des commandes disponibles pour ce groupe.

EXEMPLE 2 : CRÉATION DE CONFIGURATIONS PERSONNALISÉES EN REGROUPANT DES ÉLÉMENTS

1. Pour modifier l'exemple de configuration, ouvrez-le en tant qu'administrateur système avec **visudo**.

   ```
   # visudo /etc/sudoers.d/02_usermanagement
   ```

2. Ajoutez d'autres utilisateurs à la règle dans une liste séparée par des virgules :

   ```
   tux, wilber ALL = /usr/sbin/useradd
   ```

3. Pour permettre aux utilisateurs répertoriés d'exécuter plusieurs commandes, spécifiez-les sous forme de liste séparée par des virgules :

   ```
   tux, wilber ALL = /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/userdel
   ```

4. Enregistrez la configuration, quittez l'éditeur, puis ouvrez un deuxième shell pour vérifier si **sudo** respecte votre nouvelle configuration.

2.4 simplification des configurations grâce à l'application d'alias

Les alias permettent de simplifier davantage votre configuration personnalisée de l'*Exemple 2, « Création de configurations personnalisées en regroupant des éléments »*. Le regroupement d'éléments est utile dans une certaine mesure, mais l'utilisation d'alias globaux pour les utilisateurs, les commandes et les hôtes est le moyen le plus efficace de conserver une configuration **sudo** propre et légère.

L'utilisation d'alias et de groupes au lieu de listes est une méthode bien plus efficace pour gérer les modifications apportées à votre configuration. Si un utilisateur quitte l'organisation, il suffit de le supprimer de la déclaration `User_Alias` globale de votre fichier de déclaration d'alias au lieu de passer en revue tous les fichiers de configuration personnalisés séparément. La même procédure s'applique à tout autre type d'alias (`Host_Alias`, `Cmnd_Alias` et `Runas_Alias`).

EXEMPLE 3 : SIMPLIFICATION DES CONFIGURATIONS GRÂCE À L'APPLICATION D'ALIAS

1. Créez un nouveau fichier pour stocker vos définitions d'alias globales :

```
# visudo /etc/sudoers.d/01_aliases
```

2. Ajoutez la ligne suivante pour créer l'alias `TEAMLEADERS` :

```
User_Alias    TEAMLEADERS = tux, wilber
```

3. Ajoutez la ligne suivante pour créer l'alias `USERMANAGEMENT` :

```
Cmnd_Alias    USERMANAGEMENT = /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/
userdel
```

4. Enregistrez vos modifications, puis quittez **visudo**.

5. En tant qu'administrateur système, lancez **visudo** pour modifier l'exemple de fichier de configuration :

```
# visudo -f /etc/sudoers.d/02_usermanagement
```

6. Supprimez la règle précédente et remplacez-la par la règle suivante qui utilise les alias que vous venez de définir ci-dessus :

```
TEAMLEADERS ALL = USERMANAGEMENT
```

7. Enregistrez la configuration, quittez l'éditeur, puis ouvrez un deuxième shell pour vérifier si **sudo** respecte votre nouvelle configuration.

Remarque : informations supplémentaires

Pour obtenir une description plus détaillée de la syntaxe de configuration de **sudo**, reportez-vous à la *Section 7, « Référence de configuration* **sudo** *»* et à la page de manuel de **sudo**.

3 Modification du timeout de l'invite de mot de passe **sudo**

Apprenez à modifier les paramètres de timeout pour exécuter des commandes qui nécessitent des privilèges `root` sans avoir à entrer le mot de passe `root` pour chaque commande.

Lorsque vous exécutez une commande précédée de **`sudo`** pour la première fois, vous êtes invité à entrer le mot de passe `root`. Ce mot de passe reste valide pendant un certain temps. Une fois qu'il a expiré, l'utilisateur est de nouveau invité le saisir. Pour prolonger ou raccourcir le timeout lors de l'exécution de commandes nécessitant des privilèges `root`, apportez les modifications suivantes à votre fichier de configuration **`sudo`**. Il est important de noter que l'invite pour le mot de passe `root` est destinée aux utilisateurs qui ne font pas partie du groupe `wheel`.

Avertissement : n'accordez pas un accès illimité sans mot de passe aux privilèges `root`

Pour des raisons de sécurité, n'accordez pas un accès illimité aux privilèges `root`. Définissez plutôt un timeout raisonnable pour éviter toute utilisation abusive du compte `root` par un intrus.

PROCÉDURE 1 : MODIFICATION DU TIMEOUT POUR LES INVITES DE MOT DE PASSE **sudo**

1. En tant qu'administrateur système, créez un fichier de configuration **`sudo`** pour la configuration de l'horodatage avec :

   ```
   # visudo --f=/etc/sudoers.d/timestamp_timeout
   ```

   Une fois l'authentification réussie avec le mot de passe `root`, le fichier est ouvert.

2. Activez l'édition et ajoutez la ligne `timestamp_timeout=`. Entrez une valeur pour l'horodatage.
   Par exemple, pour réduire le timeout à trois minutes, entrez :

   ```
   Defaults timestamp_timeout=3
   ```

   Si l'horodatage est défini sur zéro, vous êtes invité à entrer le mot de passe `root` pour chaque exécution d'une commande **`sudo`**.

3. Enregistrez les modifications, puis fermez le fichier.

Vous avez créé un fichier de configuration **sudo** et raccourci le paramètre de timeout pour l'exécution des commandes **sudo**.

4 Démarrage d'un shell avec des privilèges root

Démarrez un shell avec des privilèges `root` permanents à l'aide de la commande **sudo -s** ou **sudo -i**. Avec les deux commandes, vous n'êtes invité à entrer le mot de passe `root` qu'une seule fois. Il est important de noter que si l'utilisateur fait partie du groupe `wheel`, il est invité à fournir son propre mot de passe. Dans le cas contraire, il est invité à indiquer le mot de passe `root`.

4.1 Différence entre les commandes **sudo -s** et **sudo -i**

Le fait de devoir entrer **sudo** à chaque fois que vous voulez exécuter une commande en tant que `root` peut devenir fastidieux. À la place, vous pouvez utiliser l'un des mécanismes intégrés pour démarrer un shell avec des privilèges `root` permanents. Pour cela, deux options de commande sont disponibles :

- **sudo -s** lance le shell avec l'environnement de l'utilisateur actuel et offre quelques mesures de contrôle des privilèges. Pour exécuter cette commande, entrez le mot de passe `root`.
- **sudo -i** démarre le shell en tant que shell de connexion interactif avec un environnement propre. Pour exécuter cette commande, entrez le mot de passe `root`.

Avec les deux commandes, le shell démarre avec un nouvel environnement et vous êtes connecté en tant qu'utilisateur `root`. Lorsque vous exécuterez d'autres commandes dans ce shell avec des privilèges élevés, il ne sera pas nécessaire de ressaisir le mot de passe. Vous quittez cet environnement lorsque vous fermez le shell et vous devez à nouveau saisir le mot de passe pour exécuter une autre commande **sudo**.

4.2 Démarrage d'un shell avec **sudo -s**

La commande **sudo -s** lance un shell interactif sans connexion. Une fois l'authentification réussie avec le mot de passe `root`, toutes les commandes suivantes sont exécutées avec des privilèges élevés.

La variable d'environnement `SHELL` ou le shell par défaut de l'utilisateur spécifie le shell qui s'ouvre. Si cette variable est vide, le shell défini dans `/etc/passwd` est sélectionné.

Par défaut, la commande **`sudo -s`** s'exécute à partir du répertoire de l'utilisateur précédent, car l'utilisateur cible hérite de l'environnement de l'utilisateur précédent. La commande est également consignée dans votre historique.

Pour démarrer un shell avec des privilèges élevés de façon permanente, entrez la commande suivante :

```
tux:~ > sudo -s
[sudo] password for root:
root:/home/tux # exittux:~ >
```

L'invite passe de `>` à `#` .

Vous avez démarré un shell avec des privilèges élevés de façon permanente. Toutes les commandes suivantes sont exécutées sans que vous ayez à entrer de nouveau le mot de passe.

4.3 Démarrage d'un shell avec **`sudo -i`**

La commande **`sudo -i`** est similaire à l'option de ligne de commande **`sudo -s`**, mais elle lance un shell de connexion interactif. Lorsque vous utilisez la commande **`sudo -s`**, l'utilisateur cible hérite de l'environnement de l'utilisateur précédent. Vous pouvez empêcher cet héritage en utilisant la commande **`sudo -i`**, où l'utilisateur cible obtient un environnement nettoyé et démarre à partir de son propre répertoire `$HOME`.

Pour exécuter une commande avec **`sudo -i`**, entrez ceci :

```
tux:~ > sudo -i
[sudo] password for root:
root:~ # exittux:~ >
```

Vous avez démarré un shell avec des privilèges élevés en permanence et la commande est consignée dans votre historique. Toutes les commandes suivantes sont exécutées sans que vous ayez à entrer de nouveau le mot de passe.

5 Meilleures pratiques **`sudo`**

Découvrez quelques-unes des meilleures pratiques **`sudo`** pour contrôler l'accès au système et permettre aux utilisateurs d'être productifs.

Testez et auditez minutieusement vos configurations `sudo`

Pour créer une structure de configuration **`sudo`** vraiment efficace et sécurisée, établissez une routine pour effectuer régulièrement des tests et des audits. Identifiez les failles possibles et trouvez des solutions pour y remédier. Ne laissez pas la facilité d'utilisation prendre le pas sur la sécurité.

Limitez le timeout `sudo`

Pour des raisons de sécurité, n'accordez pas un accès illimité aux privilèges `root`. Définissez plutôt un timeout raisonnable pour éviter toute utilisation abusive du compte `root` par un intrus. Pour plus d'informations, reportez-vous à la *Section 3, « Modification du timeout de l'invite de mot de passe* **`sudo`** *»*.

Utilisez la commande `visudo`

Utilisez la commande **`visudo -f`** pour éditer le fichier `/usr/etc/sudoers` en toute sécurité, car elle vérifie la syntaxe du fichier avant d'enregistrer les modifications. Il s'agit d'une méthode préventive pour corriger les erreurs qui peuvent nuire au système. Outre la vérification de la syntaxe de base, vous pouvez également exécuter la commande **`visudo -c`** pour vérifier si l'ensemble de votre infrastructure de configuration **`sudo`** est analysée dans le bon ordre et sans erreur.

Gérez les utilisateurs en groupes plutôt qu'individuellement

Veillez à ce que votre configuration **`sudo`** reste la plus simple et la plus gérable possible. Gérez les utilisateurs en les ajoutant à des groupes, puis en accordant des privilèges à ces groupes plutôt qu'à des utilisateurs individuels. Cela vous permet d'ajouter ou de supprimer des utilisateurs en modifiant simplement les paramètres du groupe au lieu d'avoir à rechercher l'utilisateur dans votre configuration.

Exemple de règle qui permet à tous les utilisateurs d'un exemple de groupe `%admingrp` d'exécuter toutes les commandes :

```
%admingrp ALL = (ALL) ALL
```

Restreignez le chemin d'accès aux fichiers binaires

Avec la directive `secure_path`, limitez les zones dans lesquelles les utilisateurs peuvent exécuter des commandes. L'exemple suivant illustre le paramètre par défaut fourni avec SUSE Linux Enterprise Server for SAP Applications.

```
Defaults secure_path="/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/bin:/usr/local/sbin"
```

Préservez la transparence de la journalisation **sudo**

sudo consigne les événements dans le fichier journal standard où ses entrées peuvent facilement être ignorées. Ajoutez la règle suivante à votre configuration pour spécifier un fichier journal **sudo** dédié.

```
Defaults logfile=/var/log/sudo.log
```

6 Dépannage

Apprenez à déboguer et à résoudre les problèmes de configuration **sudo**.

6.1 Les configurations personnalisées sous `/etc/sudoers.d/` sont ignorées

La directive `#includedir` dans `/etc/sudoers` ignore les fichiers qui se terminent par le caractère `~` ou qui contiennent le caractère `.`. Cela permet d'éviter les problèmes avec les fichiers de configuration fournis par le gestionnaire de paquets (contenant `.`), ou avec les fichiers temporaires ou de sauvegarde d'un éditeur (se terminant par `~`). Assurez-vous que les noms de vos fichiers de configuration personnalisés ne contiennent ni ne se terminent par ces caractères. Si c'est le cas, renommez-les.

6.2 Conflit de directives personnalisées

L'ordre dans lequel les fichiers de configuration sont lus détermine le moment auquel une directive de configuration **sudo** est appliquée. Les directives d'un fichier situé sous `/etc/sudoers.d/` sont prioritaires sur les mêmes directives dans `/etc/sudoers`. Si les directives personnalisées indiquées dans `/etc/sudoers.d/` ne fonctionnent pas, vérifiez l'ordre dans lequel les fichiers sont lus à l'aide de **visudo -c**. Ajustez l'ordre, si nécessaire.

6.3 Verrouillage en raison d'une configuration **sudo** défaillante

Si vous avez accidentellement endommagé la configuration **sudo** de votre système et que vous vous êtes exclu de **sudo**, utilisez **su -** et le mot de passe `root` pour démarrer un shell root. Exécutez **visudo -c** pour rechercher les erreurs, puis corrigez-les à l'aide de **visudo**.

7 Référence de configuration **sudo**

Cette section fournit une référence de configuration de base de **sudo** qui vous aide à comprendre et à gérer les configurations **sudo** par défaut et personnalisées.

7.1 Syntaxe de configuration sudoers

Les fichiers de configuration `sudoers` contiennent deux types d'options : des chaînes et des indicateurs. Bien que les chaînes puissent contenir n'importe quelle valeur, les indicateurs peuvent être activés (ON) ou désactivés (OFF). Les constructions de syntaxe les plus importantes pour les fichiers de configuration `sudoers` sont les suivantes :

```
# Everything on a line after # is ignored❶
Defaults !insults # Disable the insults flag❷
Defaults env_keep += "DISPLAY HOME" # Add DISPLAY and HOME to env_keep❸
tux ALL = NOPASSWD: /usr/bin/frobnicate, PASSWD: /usr/bin/journalctl❹
```

❶ Il existe deux exceptions : `#include` et `#includedir` sont des commandes habituelles. La version la plus récente n'utilise plus le `#`. Au lieu de celui-ci, les directives d'inclusion sont désormais précédées de `@`. La notation `#` est toujours prise en charge pour des raisons de compatibilité avec les versions précédentes.

❷ Supprimez le caractère `!` pour activer l'indicateur souhaité.

❸ Indiquez la liste des variables d'environnement à conserver lorsque `env_reset` est activé.

❹ Règle complexe qui indique que l'utilisateur `tux` a besoin d'un mot de passe pour exécuter **`/usr/bin/journalctl`** et qu'il n'en a pas besoin pour exécuter **`/usr/bin/frobnicate`** sur tous les hôtes.

INDICATEURS ET OPTIONS UTILES

`env_reset`

Si cette valeur est définie, **sudo** crée un environnement minimal avec `TERM`, `PATH`, `HOME`, `MAIL`, `SHELL`, `LOGNAME`, `USER`, `USERNAME` et `SUDO_*`. En outre, les variables répertoriées dans `env_keep` sont importées de l'environnement d'appel. La valeur par défaut est ON (Activé).

```
Defaults env_reset # Turn env_reset flag ON
```

`env_keep`

Liste des variables d'environnement à conserver lorsque l'indicateur `env_reset` est ON (Activé).

```
# Set env_keep to contain EDITOR and PROMPT
Defaults env_keep = "EDITOR PROMPT"
Defaults env_keep += "JRE_HOME" # Add JRE_HOME
Defaults env_keep -= "JRE_HOME" # Remove JRE_HOME
```

`env_delete`

Liste des variables d'environnement à supprimer lorsque l'indicateur `env_reset` est OFF (Désactivé).

```
# Set env_delete to contain EDITOR and PROMPT
Defaults env_delete = "EDITOR PROMPT"
Defaults env_delete += "JRE_HOME" # Add JRE_HOME
Defaults env_delete -= "JRE_HOME" # Remove JRE_HOME
```

7.2 Règles sudoers de base

Chaque règle respecte le schéma suivant (`[]` indique les parties facultatives) :

```
#Who      Where         As whom      Tag                What
User_List Host_List = [(User_List)] [NOPASSWD:|PASSWD:] Cmnd_List
```

SYNTAXE DES RÈGLES SUDOERS

`User_List`

Un ou plusieurs identificateurs (séparés par des virgules) : un nom d'utilisateur, un groupe au format `%GROUPNAME` ou un ID utilisateur au format `#UID`. La négation peut être spécifiée avec le préfixe `!`.

`Host_List`

Un ou plusieurs identificateurs (séparés par des virgules) : un nom d'hôte (complet) ou une adresse IP. La négation peut être spécifiée avec le préfixe `!`. `ALL` est un choix courant pour `Host_List`.

`NOPASSWD:|PASSWD:`

L'utilisateur n'est pas invité à entrer de mot de passe lors de l'exécution des commandes correspondant à `Cmd_List` après `NOPASSWD:`.
`PASSWD:` est la valeur par défaut. Il ne doit être spécifié que lorsque `PASSWD:` et `NOPASSWD:` sont sur la même ligne :

```
tux ALL = PASSWD: /usr/bin/foo, NOPASSWD: /usr/bin/bar
```

`Cmnd_List`
: Un ou plusieurs spécificateurs (séparés par des virgules) : chemin d'accès à un exécutable, suivi d'un argument autorisé facultatif.

```
/usr/bin/foo     # Anything allowed
/usr/bin/foo bar # Only "/usr/bin/foo bar" allowed
/usr/bin/foo ""  # No arguments allowed
```

`ALL` peut être utilisé en tant que `User_List`, `Host_List` et `Cmnd_List`.

7.3 Simplification de `sudoers` grâce aux alias

Les administrateurs peuvent éviter de devoir gérer un ensemble de règles répétitives et individuelles en introduisant des alias pour grouper des éléments. Leur syntaxe est la même que celle des règles. Les types d'alias pris en charge sont les suivants :

`User_Alias`
: Liste de noms d'utilisateurs

`Runas_Alias`
: Groupe d'utilisateurs par UID

`Host_Alias`
: Liste de noms d'hôtes

`Cmnd_Alias`
: Liste de commandes, de répertoires et d'alias

Considérez les alias comme des listes de noms d'utilisateurs, de groupes, de commandes et d'hôtes. Pour illustrer la puissance des alias, prenez cet exemple :

```
Host_Alias    WEBSERVERS = www1, www2, www3 ❶
User_Alias    ADMINS = tux, wilber, suzanne ❷
Cmnd_Alias    REBOOT = /sbin/halt, /sbin/reboot, /sbin/poweroff ❸
ADMINS WEBSERVERS = REBOOT ❹
```

❶ Les trois serveurs sont regroupés en un seul Host_Alias `WEBSERVERS`. Vous pouvez utiliser des noms d'hôte (complets) ou des adresses IP.

❷ Comme pour les hôtes regroupés ci-dessus, des utilisateurs de groupes ou même des groupes d'utilisateurs (comme `%wheel`) sont répertoriés ici. La négation s'effectue avec le préfixe `!`, comme d'habitude.

3. Spécifie un groupe de commandes utilisées dans le même contexte.
4. Tous les alias sont regroupés dans une règle unique indiquant que tous les utilisateurs spécifiés par `User_Alias` peuvent exécuter le groupe de commandes spécifié sous `Cmnd_Alias` sur tous les hôtes nommés dans `Host_Alias`.

En résumé, les alias aident les administrateurs à ce que le fichier `sudoers` reste le plus simple et le plus gérable (et donc le plus sécurisé) possible. Si, par exemple, l'un des utilisateurs a quitté la société, vous pouvez supprimer le nom de cette personne de l'instruction `User_Alias` et de tout groupe système auquel elle appartenait une seule fois au lieu de devoir rechercher toutes les règles qui contenaient cet utilisateur spécifique.

8 Mentions légales

A GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent

copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through

arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your 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”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with…Texts.” line with this:

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

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.