LINUX : Gestion des utilisateurs et des groupes sous Centos

Table of Contents

La gestion des utilisateurs et des groupes peut être une tâche fastidieuse. C'est pourquoi Red Hat Enterprise Linux fournit des outils et des conventions facilitant leur gestion.

Le moyen le plus simple de gérer les utilisateurs et les groupes consiste à utiliser l'application graphique User Manager (system-config-users). Pour plus d'informations sur User Manager, se reporter à la Section 32.1, «Configuration des utilisateurs et des groupes».

Les outils de ligne de commande suivants peuvent également être utilisés pour gérer des utilisateurs et des groupes:

- **useradd, usermod et userdel** Méthodes standard pour l'ajout, la suppression et la modification de comptes d'utilisateurs
- **groupadd, groupmod et groupdel** Méthodes standard pour ajouter, supprimer et modifier des groupes d'utilisateurs
- **gpasswd** Méthode standard pour l’administration du fichier /etc/group
- **pwck, grpck** Outils utilisés pour la vérification du mot de passe, du groupe et des fichiers shadow associés
- **pwconv, pwunconv** Outils utilisés pour convertir les mots de passe en mots de passe masqués et revenir aux mots de passe standard

Ajout d'un utilisateur

Pour ajouter un utilisateur au système:

Utiliser la commande useradd pour créer un compte d'utilisateur verrouillé:

```
useradd <nom d'utilisateur>
```

Déverrouiller le compte en exécutant la commande passwd pour attribuer un mot de passe et définir des instructions de vieillissement de mot de passe:

```
passwd <nom d'utilisateur>
```

Options de ligne de commande de useradd

- **-c '<comment>' <commentaire>** peut être remplacé par n'importe quelle chaîne. Cette option est généralement utilisée pour spécifier le nom complet d'un utilisateur.
- **-d <répertoire_accueil>** Répertoire de base à utiliser à la place de / home / <nom d'utilisateur> /
- **-e <date>** Date à laquelle le compte doit être désactivé au format AAAA-MM-JJ
- **-f <jours>** Nombre de jours après l'expiration du mot de passe jusqu'à la désactivation du compte. Si 0 est spécifié, le compte est désactivé immédiatement après l'expiration du mot de passe. Si -1 est spécifié, le compte n'est pas désactivé après l'expiration du mot de passe.
- **-g <nom-groupe>** Nom du groupe ou numéro du groupe pour le groupe par défaut de l'utilisateur. Le groupe doit exister avant d'être spécifié ici.
- **-G <groupe-liste>** Liste de noms de groupes ou de numéros de groupes supplémentaires (autres que ceux par défaut), séparés par des virgules, dont l'utilisateur est membre. Les groupes doivent exister avant d'être spécifiés ici.
- **-m** Crée le répertoire personnel s'il n'existe pas.
- **-M** Ne crée pas le répertoire de base.
- **-n** Ne crée pas de groupe privé d'utilisateurs pour l'utilisateur.
- **-r** Crée un compte système avec un UID inférieur à 500 et sans répertoire de base
- **-p <mot de passe>** Le mot de passe crypté avec crypt
- **-s shell de connexion de l'utilisateur**, par défaut /bin/bash
- **-u <uid> ID utilisateur de l'utilisateur**, qui doit être unique et supérieur à 499

Ajout d'un groupe

Pour ajouter un groupe au système, utiliser la commande groupadd:

```
groupadd <nom-groupe>
```

Options de ligne de commande groupadd

- **-g <gid>** ID de groupe pour le groupe, qui doit être unique et supérieur à 499
- **-r** Créer un groupe de systèmes avec un GID inférieur à 500
- **-f** Lorsqu'il est utilisé avec -g <gid> et que <gid> existe déjà, groupadd choisira un autre <gid> unique pour le groupe.

Définir la durée de validité d'une mot de passe

Pour des raisons de sécurité, il est conseillé de demander aux utilisateurs de modifier périodiquement leurs mots de passe. Cela peut être fait lors de l'ajout ou de la modification d'un utilisateur dans l'onglet Informations sur le mot de passe du gestionnaire d'utilisateurs.

Pour configurer l'expiration du mot de passe d'un utilisateur à partir d'une invite du shell, utiliser la commande **chage**, suivie d'une option du Tableau 32.3, «Options de ligne de commande chage», suivie du nom d'utilisateur de l'utilisateur.

Important : Les mots de passe masqués doivent être activés pour utiliser la commande chage.

Options de ligne de commande chage

- **-m <jours>** Spécifie le nombre minimum de jours entre lesquels l'utilisateur doit changer de mot de passe. Si la valeur est 0, le mot de passe n'expire pas.
- **-M <jours>** Spécifie le nombre maximal de jours de validité du mot de passe. Lorsque le nombre de jours spécifié par cette option, ainsi que le nombre de jours spécifié avec l'option -d, est inférieur au jour actuel, l'utilisateur doit modifier les mots de passe avant d'utiliser le compte.
- **-d <jours>** Spécifie le nombre de jours depuis le 1 janvier 1970 le mot de passe a été changé
- **-I <jours>** Spécifie le nombre de jours d'inactivité après l'expiration du mot de passe avant le verrouillage du compte. Si la valeur est 0, le compte n'est pas verrouillé après l'expiration du mot de passe.
- **-E <date>** Spécifie la date à laquelle le compte est verrouillé, au format AAAA-MM-JJ. Au lieu de la date, le nombre de jours depuis le 1er janvier 1970 peut également être utilisé.
- **-W <jours>** Spécifie le nombre de jours avant la date d'expiration du mot de passe pour avertir l'utilisateur.

Si la commande **chage** est suivie directement par un nom d'utilisateur (sans options), elle affiche les valeurs d'ancienneté du mot de passe actuelles et permet leur modification.

On peut configurer un mot de passe pour qu'il expire lors de la première connexion d'un utilisateur. Cela oblige les utilisateurs à modifier les mots de passe lors de leur première connexion.

Ce processus ne fonctionnera pas si l'utilisateur se connecte à l'aide du protocole SSH.

Verrouiller le mot de passe de l'utilisateur

Si l'utilisateur n'existe pas, utiliser la commande **useradd** pour créer le compte d'utilisateur, mais sans lui donner de mot de passe pour qu'il reste verrouillé.

Si le mot de passe est déjà activé, le verrouiller avec la commande:

```
usermod -L nom d'utilisateur
```

Forcer l'expiration immédiate du mot de passe - Taper la commande suivante:

```
chage -d 0 nom d'utilisateur
```

Cette commande définit la date à laquelle le mot de passe a été modifié pour la dernière fois à l’époque (1er janvier 1970). Cette valeur force l'expiration immédiate du mot de passe, quelle que soit la stratégie de vieillissement du mot de passe, le cas échéant.

Déverrouiller le compte - Il existe deux approches communes pour cette étape. L'administrateur peut attribuer un mot de passe initial ou un mot de passe null.

Ne pas utiliser la commande passwd pour définir le mot de passe car il désactive l'expiration immédiate du mot de passe que l'on viens de configurer.

Pour attribuer un mot de passe crypter

Démarrer l'interpréteur Python en ligne de commande à l'aide de la commande python. Il affiche les éléments suivants:

```
    Python 2.4.3 (n ° 1, 21 juillet 2006, 08:46:09)
    [GCC 4.1.1 20060718 (Red Hat 4.1.1-9)] sur linux2
    Tapez "aide", "copyright", "crédits" ou "licence" pour plus
d'informations.
    >>>
```

À l'invite, taper les commandes suivantes. Remplacer <mot de passe> par le mot de passe à chiffrer et <sel> par une combinaison aléatoire d'au moins 2 des éléments suivants: tout caractère alphanumérique, la barre oblique (/) ou un point (.):

```
    import crypt; print
    crypt.crypt ("<mot de passe>", "<sel>")
```

Le résultat est le mot de passe crypté, similaire à '12CsGd8FRcMSM'.

Appuyer sur **Ctrl-D** pour quitter l’interpréteur Python.

Sur le shell, entrer la commande suivante (en remplaçant <mot de passe crypté> par la sortie cryptée de l'interpréteur Python):

```
    usermod -p "<mot de passe crypté>" <nom d'utilisateur>
```

Sinon, on peut attribuer un mot de passe null au lieu d'un mot de passe initial. Pour ce faire, utiliser la commande suivante:

```
usermod -p "" nom d'utilisateur
```

L'utilisation d'un mot de passe nul, bien que pratique, est une pratique hautement non sécurisée, car tout tiers peut se connecter d'abord pour accéder au système à l'aide du nom d'utilisateur non sécurisé. Il faut toujours s'assurer que l'utilisateur est prêt à se connecter avant de déverrouiller un compte avec un mot de passe null.

Dans les deux cas, lors de la connexion initiale, un nouveau mot de passe est demandé à l'utilisateur.

Description du processus

Les étapes suivantes illustrent ce qui se passe si la commande useradd juan est émise sur un système sur lequel les mots de passe masqués sont activés:

Une nouvelle ligne pour juan est créée dans /etc/passwd. La ligne a les caractéristiques suivantes:

- Il commence par le nom d'utilisateur juan.
- Il y a un x pour le champ de mot de passe indiquant que le système utilise des mots de passe masqués.
- Un UID supérieur à 499 est créé. (Sous Red Hat Enterprise Linux, les UID et les GID inférieurs à 500 sont réservés à l'utilisation du système.)
- Un GID supérieur à 499 est créé.
- Les informations facultatives GECOS sont laissées vides.
- Le répertoire personnel de juan est défini sur /home/juan/.
- Le shell par défaut est /bin/bash.

Une nouvelle ligne pour juan est créée dans /etc/shadow. La ligne a les caractéristiques suivantes:

- Il commence par le nom d'utilisateur juan.
- Deux points d'exclamation (!!) apparaissent dans le champ mot de passe du fichier /etc/shadow, qui verrouille le compte.
- Si un mot de passe chiffré est passé à l'aide de l'indicateur -p, il est placé dans le fichier /etc/shadow sur la nouvelle ligne de l'utilisateur.
- Le mot de passe est défini pour ne jamais expirer.

Une nouvelle ligne pour un groupe nommé juan est créée dans /etc/group. Un groupe portant le même nom qu'un utilisateur est appelé groupe privé d'utilisateurs. La ligne présente les caractéristiques suivantes:

- Il commence par le nom de groupe juan.
- Un x apparaît dans le champ du mot de passe, indiquant que le système utilise des mots de passe de groupe d'ombres.
- Le GID correspond à celui indiqué pour l'utilisateur juan dans /etc/passwd. -

Une nouvelle ligne pour un groupe nommé juan est créée dans /etc/gshadow. La ligne a les caractéristiques suivantes:

- Il commence par le nom de groupe juan.
- Un point d'exclamation (!) Apparaît dans le champ mot de passe du fichier /etc/gshadow, qui verrouille le groupe.
- Tous les autres champs sont vides.

Un répertoire pour l'utilisateur juan est créé dans le répertoire /home/. Ce répertoire appartient à l'utilisateur juan et au groupe juan. Cependant, il dispose des privilèges de lecture, d'écriture et d'exécution uniquement pour l'utilisateur juan. Toutes les autres autorisations sont refusées.

Les fichiers du répertoire /etc/skel/ (qui contiennent les paramètres utilisateur par défaut) sont copiés dans le nouveau répertoire /home/juan/.

À ce stade, un compte verrouillé appelé juan existe sur le système. Pour l'activer, l'administrateur doit ensuite attribuer un mot de passe au compte à l'aide de la commande passwd et, éventuellement, définir des instructions de vieillissement du mot de - passe. -