Gestion des compte et environnements utilisateur dans Oracle® Solaris 11.1

Référence : E36537–01
Octobre 2012

ORACLE®

130327@25097

Table des matières

Préface

Le manuel *Gestion des compte et environnements utilisateur dans Oracle Solaris 11.1* fait partie d'un ensemble de documents qui fournit une grande part des informations sur l'administration du système Oracle Solaris. Ce manuel contient des informations sur les systèmes SPARC et x86.

Il part du principe que vous avez terminé les tâches suivantes :

- Installation du logiciel Oracle Solaris
- Configuration de tous les logiciels de gestion de réseau que vous avez l'intention d'utiliser

Pour Oracle Solaris, les nouvelles fonctionnalités pouvant intéresser les administrateurs système sont traitées dans les sections intitulées *Nouveautés concernant...* dans les chapitres correspondants.

Remarque – Cette version d'Oracle Solaris prend en charge les systèmes reposant sur les architectures de processeur SPARC et x86. Pour connaître les systèmes pris en charge, reportez-vous aux *Oracle Solaris OS: Hardware Compatibility Lists*. Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

Pour connaître les systèmes pris en charge, reportez-vous aux listes de la page *Oracle Solaris OS: Hardware Compatibility Lists*.

Utilisateurs de ce manuel

Ce manuel s'adresse aux personnes chargées d'administrer un ou plusieurs systèmes exécutant Oracle Solaris. Pour utiliser ce manuel, vous devez posséder une à deux années d'expérience en matière d'administration de systèmes UNIX. Une formation en administration de systèmes UNIX peut se révéler utile.

Accès à Oracle Support

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P–1 Conventions typographiques

Type de caractères	Description	Exemple
`AaBbCc123`	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `nom_machine% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *nom_fichier*.
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie des éléments stockés localement. *N'enregistrez pas* le fichier. **Remarque :** en ligne, certains éléments mis en valeur s'affichent en gras.

Invites de shell dans les exemples de commandes

Le tableau suivant présente l'invite système UNIX par défaut et l'invite superutilisateur pour les shells faisant partie du SE Oracle Solaris. L'invite système par défaut qui s'affiche dans les exemples de commandes dépend de la version Oracle Solaris.

TABLEAU P–2 Invites de shell

Shell	Invite
Bash shell, korn shell et bourne shell	`$`
Bash shell, korn shell et bourne shell pour superutilisateur	`#`
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`

◆ ◆ ◆ CHAPITRE 1

1 Gestion des comptes et des environnements utilisateur (présentation)

Les informations contenues dans ce chapitre sont répertoriées ci-après :

Pour plus d'informations sur les tâches de gestion des comptes et des environnements utilisateur, reportez-vous au Chapitre 2, "Gestion des comptes utilisateur avec l'interface de ligne de commande (tâches)" et au Chapitre 3, "Gestion des comptes utilisateur dans l'interface graphique du Gestionnaire d'utilisateurs (tâches)".

Nouveautés et modifications concernant la gestion des comptes et des environnements utilisateur

La liste suivante répertorie les fonctionnalités introduites ou modifiées dans cette version.

Modifications en matière de sécurité ayant une incidence sur la gestion des comptes utilisateur

Dans cette version, les fonctions suivantes ont changé :

- Amélioration des transitions d'état pour la commande `password`. Cette modification clarifie les comptes utilisateur pouvant et ne pouvant pas être verrouillés. Les principales modifications affectent les définitions de propriétés `LK` et `NL`, comme suit :

  `LK` Le compte est verrouillé. La commande `passwd -l` a été exécutée ou le compte a été automatiquement verrouillé car le nombre d'échecs d'authentification maximal a été atteint. Reportez-vous aux pages de manuel `policy.conf(4)` et `user_attr(4)`.

  `NL` Le compte est configuré pour une authentification non UNIX. La commande `passwd -N` a été exécutée. À partir de cette version, les comptes possédant cet état peuvent être verrouillés via l'exécution de la commande `passwd -l`, et déverrouillés via l'exécution de la commande `passwd -u`.
- Autorisations qualifiées. Il est possible de définir plus précisément les autorisations pour les appliquer à des objets spécifiques tels que des groupes, des zones ou des noms de fichiers. Reportez-vous à la section "Editeur d'administration (`pfedit`)" à la page 13.
- La commande `profiles` a été modifiée pour gérer les profils de droits à l'échelle d'une étendue locale et LDAP. La modification directe des fichiers RBAC (contrôle d'accès basé sur les rôles) n'est plus prise en charge.
- Dans cette version, vous avez la possibilité de définir une stratégie PAM (module d'authentification enfichable) par utilisateur (`pam_policy`) dans un profil de droits. Le paramètre `pam_policy` doit être soit un chemin d'accès absolu à un fichier au format `pam_conf`(4), soit le nom d'un fichier au format `pam.conf`(4) figurant dans le fichier `/etc/security/pam_policy`. Reportez-vous à la section `pam_user_policy(5)`.

  Au lieu de définir la stratégie PAM dans un profil de droits, vous pouvez définir directement le paramètre `pam_policy` dans l'entrée utilisateur `user_attr` en exécutant la commande `useradd` ou `usermod`. Reportez-vous à l'Exemple 2–1.
- Les utilisateurs et les rôles auxquels est attribué le profil de droits User Security peuvent créer des comptes utilisateur, mais également déléguer une partie de leurs droits à d'autres comptes, sans prendre le rôle `root`.

Pour plus d'informations, reportez-vous à la Partie III, "Rôles, profils de droits et privilèges" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Présentation de l'interface graphique du Gestionnaire d'utilisateurs

Vous pouvez désormais configurer et gérer des utilisateurs, des rôles et des groupes dans l'interface graphique du Gestionnaire d'utilisateurs Oracle Solaris. Cette interface graphique, disponible sur le bureau, fait partie du projet Visual Panels. Dans cette version, l'interface graphique du Gestionnaire d'utilisateurs remplace celle de la console de gestion Solaris. Vous pouvez effectuer quasiment les mêmes tâches dans l'interface graphique du Gestionnaire d'utilisateurs et dans l'interface de ligne de commande, et notamment exécuter les fonctions correspondant aux commandes `useradd`, `usermod`, `userdel`, `roleadd`, `rolemod` et `roledel`.

Pour obtenir des instructions sur le fonctionnement de l'interface graphique du Gestionnaire d'utilisateurs, reportez-vous au Chapitre 3, “Gestion des comptes utilisateur dans l'interface graphique du Gestionnaire d'utilisateurs (tâches)” et à l'aide en ligne.

Editeur d'administration (`pfedit`)

Dans cette version, un éditeur d'administration (`pfedit`) permet de modifier les fichiers système. Si elle est définie par l'administrateur système, la valeur de cet éditeur est `$EDITOR`. Si l'éditeur n'est pas défini, sa valeur par défaut est la commande `vi`.

Démarrez l'éditeur comme suit :

```
$ pfedit system-filename
```

Pour modifier des fichiers système en exécutant la commande `pfedit`, vous (ou votre rôle) devez disposer de l'autorisation `solaris.admin.edit/`*system-filename* sur chaque fichier concerné. L'intégration de l'autorisation `auth-sysfilename` dans un profil de droits existant simplifie les procédures regroupant des modifications apportées à des fichiers standard et des commandes SMF (utilitaire de gestion des services). Par exemple, si l'autorisation `solaris.admin.edit/etc/security/audit_warn` vous a été attribuée, vous pouvez modifier le fichier `audit_warn`.

La commande `pfedit` permet de modifier la plupart des fichiers de configuration stockés dans le répertoire `/etc` et ses sous-répertoires, mais également des fichiers de configuration d'application comme GNOME et Firefox. En revanche, la commande `pfedit` *ne permet pas* de modifier les fichiers système qui accordent à l'utilisateur des droits sur une large portion d'un système, comme le fichier `/etc/security/policy.conf`. Vous devez disposer d'un accès `root` pour modifier ces fichiers. Reportez-vous à la page de manuel `pfedit`(1M) et au Chapitre 3, “Contrôle de l'accès aux systèmes (tâches)” du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Sous-répertoire /var/user/$USER

Chaque fois qu'un utilisateur se connecte et réussit à s'authentifier par le biais du module pam_unix_cred, un répertoire /var/user/$USER est créé de manière explicite s'il n'existe pas déjà. Ce répertoire permet aux applications de stocker les données persistantes associées à un utilisateur spécifique sur le système hôte. Le répertoire /var/user/$USER est créé lors de l'établissement initial des informations d'identification, mais également au cours de l'authentification secondaire lorsque les utilisateurs changent en exécutant les commandes su, ssh, rlogin et telnet. Le répertoire /var/user/$USER ne nécessite aucune administration. Toutefois, les utilisateurs doivent savoir pourquoi et comment ce répertoire est créé sous le répertoire /var.

Modifications apportées à la commande groupadd

Un administrateur disposant de l'autorisation solaris.group.manage peut créer un groupe. Au moment de la création d'un groupe, le système attribue l'autorisation solaris.group.assign/*groupname* à l'administrateur, ce qui lui permet d'exercer un contrôle total sur ce groupe. L'administrateur peut ensuite modifier ou supprimer ce groupe, selon les besoins. Pour plus d'informations, reportez-vous aux pages de manuel groupadd(1M) et groupmod (1M).

Notification relative au nombre d'échecs de connexion

Le système informe désormais les utilisateurs des échecs d'authentification, même si le compte utilisateur n'est pas configuré pour appliquer les tentatives de connexion ayant échoué. Les utilisateurs qui ne parviennent pas à s'authentifier correctement reçoivent un message semblable au suivant lors d'une authentification réussie :

```
Warning: 2 failed authentication attempts since last successful
authentication. The latest at Thu May 24 12:02 2012.
```

Pour supprimer ces notifications, créez un fichier ~/.hushlogin.

Définition des comptes utilisateur et des groupes

Les informations suivantes sont décrites dans cette section :

Une tâche d'administration système de base consiste à configurer un compte utilisateur pour chaque utilisateur sur un site. En général, un compte utilisateur inclut les informations dont un utilisateur a besoin pour se connecter et utiliser un système, sans disposer du mot de passe `root` du système. Les composants d'un compte d'utilisateur sont décrits dans la section "Composants d'un compte utilisateur" à la page 15.

Lorsque vous configurez un compte utilisateur, vous pouvez ajouter l'utilisateur à un groupe d'utilisateurs prédéfini. Une utilisation type des groupes consiste à configurer des autorisations de groupe sur un fichier et un répertoire et permettre l'accès uniquement aux utilisateurs appartenant à ce groupe.

Par exemple, vous pouvez disposer d'un répertoire contenant des fichiers confidentiels dont l'accès doit être limité à un nombre réduit d'utilisateurs. Vous pouvez configurer un groupe appelé `topsecret` qui inclut les utilisateurs travaillant sur le projet `topsecret`. En outre, vous pouvez configurer les fichiers `topsecret` avec une autorisation de lecture réservée au groupe `topsecret`. De cette manière, seuls les utilisateurs du groupe `topsecret` seront en mesure de lire les fichiers.

Un type spécial de compte utilisateur, appelé un *rôle*, accorde des privilèges spéciaux à des utilisateurs sélectionnés. Pour plus d'informations, reportez-vous à la section "Contrôle d'accès basé sur les rôles (présentation)" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Composants d'un compte utilisateur

Les sections suivantes décrivent les différents composants d'un compte utilisateur.

Noms d'utilisateur (de connexion)

Les noms d'utilisateurs, aussi appelés *login names* permettent aux utilisateurs d'accéder à leurs propres systèmes et à des systèmes distants disposant de privilèges d'accès appropriés. Vous devez choisir un nom d'utilisateur pour chaque compte utilisateur que vous créez.

Essayez de mettre en place une méthode standard d'affectation des noms d'utilisateur afin d'en faciliter le suivi. En outre, les utilisateurs doivent pouvoir les mémoriser facilement. Une méthode simple consiste à prendre l'initiale du prénom et les sept premières lettres du nom de famille. Par exemple, Ziggy Ignatz devient `zignatz`. En cas de doublons, vous pouvez utiliser l'initiale du prénom, l'initiale du deuxième prénom et les six premières lettres du nom de famille de l'utilisateur. Par exemple, `Ziggy Top Ignatz` devient `ztignatz`.

Si des doublons persistent, essayez de créer un nom d'utilisateur selon le modèle suivant :

- initiale du prénom, initiale du deuxième prénom et cinq premières lettres du nom de famille de l'utilisateur ;
- numéro 1, 2 ou 3, et ainsi de suite, jusqu'à ce qu'à l'obtention d'un nom unique.

Remarque – Tout nouveau nom d'utilisateur doit être différent des alias de messagerie déjà connu du système ou d'un domaine NIS. Dans le cas contraire, les messages risquent d'être remis à l'alias plutôt qu'à l'utilisateur réel.

Pour des instructions détaillées sur la configuration des noms (de connexion) utilisateur, reportez-vous à la section "Recommandations relatives à l'affectation des noms d'utilisateur, ID utilisateur et ID de groupe" à la page 22.

Numéros d'identification de l'utilisateur

Un numéro d'identification de l'utilisateur (UID) est associé à chaque nom d'utilisateur. L'ID utilisateur identifie le nom d'utilisateur par rapport à n'importe quel système sur lequel l'utilisateur tente de se connecter. L'ID utilisateur est utilisé par les systèmes pour identifier les propriétaires des fichiers et répertoires. Si vous créez des comptes utilisateur pour un seul individu sur un certain nombre de systèmes différents, utilisez toujours le même nom et ID utilisateur. De cette façon, l'utilisateur peut déplacer facilement des fichiers entre les systèmes sans rencontrer de problèmes de propriété.

Un ID utilisateur doit être un nombre entier inférieur ou égal à 2147483647. Les ID utilisateur sont requis pour les comptes utilisateur standard et les comptes système spéciaux. Le tableau suivant répertorie les ID utilisateurs qui sont réservés aux comptes utilisateur et comptes système.

TABLEAU 1–1 ID utilisateur réservés

ID utilisateur	Comptes utilisateur ou de connexion	Description
0 – 99	`root`, `daemon`, `bin`, `sys`, etc.	Réservés au système d'exploitation
100 – 2147483647	Utilisateurs standard	Comptes destinés à un usage général
60001 et 65534	`nobody` et `nobody4`	Utilisateurs anonymes NFS
60002	`noaccess`	Utilisateurs qui ne sont pas de confiance

N'attribuez pas d'ID utilisateur compris entre 0 et 99. Ces ID utilisateur sont réservés à l'usage d'Oracle Solaris. Par définition, `root` a toujours l'ID utilisateur 0, `daemon` l'ID utilisateur 1, le

pseudo-utilisateur `bin` l'ID utilisateur 2. En outre, vous devez attribuer aux connexions `uucp` et connexions pseudo-utilisateur, telles que `who`, `tty` et `ttytype`, des ID utilisateur faibles pour qu'elles figurent au début du fichier `passwd`.

Pour des instructions supplémentaires sur la configuration des ID utilisateur, reportez-vous à la section "Recommandations relatives à l'affectation des noms d'utilisateur, ID utilisateur et ID de groupe" à la page 22.

Comme pour les noms (de connexion) utilisateur, vous devez adopter un modèle pour l'assignation d'ID utilisateur uniques. Certaines entreprises attribuent des numéros d'employé uniques. Les administrateurs ajoutent ensuite un chiffre au numéro d'employé pour créer un ID utilisateur unique pour chaque employé.

Pour réduire les risques de sécurité, évitez de réutiliser les ID utilisateur de comptes supprimés. Si vous devez réutiliser un ID utilisateur, veillez à tout effacer de sorte que le nouvel utilisateur ne soit pas affecté par des attributs définis pour un ancien utilisateur. Par exemple, un ancien utilisateur s'est peut-être vu refuser l'accès à une imprimante en étant inclus dans une liste des accès refusé à l'imprimante. Cependant, cet attribut peut être inapproprié pour le nouvel utilisateur.

Utilisation d'ID utilisateur et ID de groupe de grande valeur

Les ID utilisateur et ID de groupe (GID) peuvent se voir affecter jusqu'à la valeur maximale d'un entier signé ou 2147483647.

Le tableau suivant décrit les restrictions liées aux ID utilisateur et ID de groupe.

TABLEAU 1–2 Récapitulatif des restrictions liées aux ID utilisateur et ID de groupe de grande valeur

ID utilisateur ou ID de groupe	Restrictions
262144 ou supérieur	Les utilisateurs exécutant la commande `cpio` avec le format d'archives par défaut pour copier un fichier voient s'afficher un message d'erreur pour chaque fichier. Ainsi, les ID utilisateur et ID de groupe sont définis sur `nobody` dans l'archive.
2097152 ou supérieur	Les utilisateurs exécutant la commande `cpio` au format `-H odc` ou la commande `pax -x cpio` pour copier des fichiers reçoivent un message d'erreur pour chaque fichier. Ainsi, les ID utilisateur et ID de groupe sont définis sur `nobody` dans l'archive.
1000000 ou supérieur	Les utilisateurs exécutant la commande `ar` ont des ID utilisateur et ID de groupe définis sur `nobody` dans l'archive.
2097152 ou supérieur	Les utilisateurs exécutant la commande `tar`, la commande `cpio -H ustar` ou la commande `pax -x tar` ont des ID utilisateur et ID de groupe définis sur `nobody`.

Groupes UNIX

Un *groupe* est un ensemble d'utilisateurs pouvant partager des fichiers et des ressources système. Par exemple, des utilisateurs travaillant sur le même projet peuvent former un groupe. Un groupe est traditionnellement connu comme groupe UNIX.

Chaque groupe doit disposer d'un nom, d'un ID et d'une liste des noms d'utilisateur appartenant au groupe. Un ID de groupe identifie le groupe en interne sur le système.

Les deux types de groupes auxquels un utilisateur peut appartenir sont les suivants :

- **Groupe principal** : groupe assigné par le système d'exploitation aux fichiers créés par l'utilisateur. Chaque utilisateur doit appartenir à un groupe principal.
- **Groupes supplémentaires :** autres groupes auxquels un utilisateur appartient. Les utilisateurs peuvent appartenir à 1024 groupes supplémentaires au maximum.

Pour consulter des instructions détaillées sur la configuration des noms de groupe, reportez-vous à la section "Recommandations relatives à l'affectation des noms d'utilisateur, ID utilisateur et ID de groupe" à la page 22.

Il peut arriver qu'un groupe secondaire d'utilisateur ne soit pas important. Par exemple, la propriété des fichiers reflète le groupe principal, et pas les groupes secondaires. Toutefois, d'autres applications peuvent se baser sur l'appartenance d'un utilisateur à un groupe secondaire. Par exemple, un utilisateur doit être un membre du groupe `sysadmin` (groupe 14) pour utiliser le logiciel Admintool dans les versions précédentes de Solaris. Cependant, peu importe si le groupe 14 est le groupe principal actif de l'utilisateur.

La commande `groups` répertorie les groupes auxquels appartient un utilisateur. Un utilisateur ne peut avoir qu'un groupe principal à la fois. Toutefois, un utilisateur peut remplacer son groupe principal à l'aide de la commande `newgrp` par n'importe quel autre groupe auquel il appartient.

Lorsque vous ajoutez un compte utilisateur, vous devez assigner un groupe principal à l'utilisateur ou accepter le groupe par défaut `staff` (groupe 10). Le groupe principal doit déjà exister. Si le groupe principal n'existe pas, indiquez le groupe par un ID de groupe (GID) Les noms d'utilisateur ne sont pas ajoutés aux groupes principaux. Si des noms d'utilisateur étaient ajoutés aux groupes principaux, la liste deviendrait trop longue. Avant de pouvoir assigner des utilisateurs à un nouveau groupe secondaire, vous devez créer le groupe et lui assigner un ID de groupe.

Les groupes peuvent être locaux pour un système ou gérés par un service de noms. Afin de simplifier l'administration des groupes, vous devez utiliser un service de noms, tel que NIS ou d'un service d'annuaire, tel que LDAP. Ces services vous permettent de gérer de façon centralisée les appartenances aux groupes.

Mots de passe utilisateur

Vous pouvez spécifier un mot de passe utilisateur lorsque vous ajoutez l'utilisateur. Vous pouvez également imposer à l'utilisateur de spécifier un mot de passe lorsque celui-ci se connecte pour la première fois au système. Bien que les noms d'utilisateur soient connus publiquement, les mots de passe doivent être tenus secrets et transmis uniquement aux utilisateurs. Un mot de passe doit être assigné à chaque compte utilisateur.

Les mots de passe utilisateur doivent respecter la syntaxe suivante :

- La longueur du mot de passe doit au moins correspondre à la valeur identifiée par la variable `PASSLENGTH` dans le fichier `/etc/passwd`. Par défaut, cette valeur est fixée à 6.

  Dans cette version, `SHA256` est l'algorithme de hachage du mot de passe par défaut. Par conséquent, la limitation de huit caractères pour les mots de passe utilisateur ne s'applique plus, contrairement aux versions précédentes d'Oracle Solaris. La limite de huit caractères s'applique uniquement aux mots de passe qui utilisent l'ancien algorithme `crypt_unix`(5), lequel a été conservé à des fins de compatibilité ascendante avec les éventuelles entrées de fichier `passwd` et cartes NIS existantes.

  Le nombre maximal de caractères pour un mot de passe dépend de l'algorithme utilisé : soit `crypt_unix` pour les mots de passe anciens, soit `SHA256` pour tous les autres. En cas de changement d'un mot de passe du type `crypt_unix`, la longueur maximale est fixée à 8 caractères, à moins que le fichier `policy.conf` n'impose le remplacement de l'algorithme.

  Le nouveau mot de passe doit suivre les règles de complexité dans la limite du nombre de caractères autorisé pour l'algorithme mis en oeuvre. Ainsi, lorsque l'algorithme `crypt_unix` est utilisé, si vous tapez un mot de passe de 20 caractères, celui-ci doit respecter les règles de complexité dans la plage des 8 premiers caractères. S'il s'agit d'un autre algorithme, il faut respecter les règles de complexité au niveau du mot de passe entier, c'est-à-dire dans la plage des 20 caractères saisis dans cet exemple.
- Chaque mot de passe doit se plier aux contraintes configurées dans le fichier `/etc/default/passwd`.
- Il ne faut pas inclure les mots de passe dans le dictionnaire configuré, comme indiqué dans le fichier `/etc/default/passwd`.
- En ce qui concerne les comptes utilisateur dans des services de noms qui prennent en charge la vérification de l'historique des mots de passe, si cet historique est déjà défini, les nouveaux mots de passe ne doivent pas figurer dans l'historique précédent.

Les règles de mot de passe sont décrites de manière détaillée dans la page de manuel `passwd(1)`.

Pour accroître la sécurité de votre système informatique, les utilisateurs doivent changer leur mot de passe régulièrement. Pour maintenir un niveau de sécurité élevé, vous devez demander aux utilisateurs de modifier leur mot de passe toutes les six semaines. Pour un niveau de sécurité moins élevé, un changement tous les trois mois est suffisant. Il est recommandé de modifier les connexions d'administration système (telles que `root` et `sys`) une fois par mois, ou chaque fois qu'une personne connaissant le mot de passe `root` quitte l'entreprise ou change d'affectation.

Dans de nombreux cas, les failles de sécurité informatique sont liées à la possibilité de deviner le mot de passe d'un utilisateur légitime. Vous devez vous assurer que les utilisateurs ne définissent par leur mot de passe à partir de noms propres, noms, noms de connexion, ou éléments pouvant être devinés par quiconque les connaissant un peu.

Choix appropriés pour des mots de passe :

- Phrases (`beammeup`).
- Série de mots dénués de sens et composée des premières lettres de chaque mot d'une phrase. Par exemple, `swotrb` pour `SomeWhere Over The RainBow`.
- Mots dont des lettres sont remplacés par des nombres ou des symboles. Par exemple, `sn00py` pour `snoopy`.

N'utilisez pas les types de mots de passe suivants :

- votre nom (écrit à l'endroit, à l'envers ou de manière désordonnée) ;
- noms de membres de votre famille ou d'animaux de compagnie ;
- numéros d'immatriculation de voiture ;
- numéros de téléphone ;
- numéros de sécurité sociale ;
- numéros d'employé ;
- mots liés à un passe-temps ou un centre d'intérêts ;
- thèmes saisonniers, comme Noël en décembre ;
- n'importe quel mot figurant dans le dictionnaire.

Répertoires personnels

Le répertoire personnel est la portion d'un système de fichiers allouée à un utilisateur pour le stockage de fichiers privés. La quantité d'espace alloué à un répertoire personnel dépend du type de fichiers créés par l'utilisateur, ainsi que de leur taille et leur nombre.

Un répertoire personnel peut se situé sur le système local de l'utilisateur ou sur un serveur de fichiers distant. Dans les deux cas, par convention, le répertoire personnel doit être créé en tant que `/export/home/`*username*. Pour un site de grande taille, vous devez stocker les répertoires personnels sur un serveur. Utilisez un système de fichiers distinct pour chaque utilisateur. Par exemple, `/export/home/alice` ou `/export/home/bob`. En créant des systèmes de fichiers distincts pour chaque utilisateur, vous pouvez définir les propriétés ou les attributs en fonction des besoins de chaque utilisateur.

Quel que soit l'emplacement de leur répertoire personnel, les utilisateurs y ont généralement accès par le biais d'un point de montage nommé `/home/`*username*. Lorsqu'AutoFS est utilisé pour monter des répertoires personnels, vous n'êtes pas autorisé à créer des répertoires sous le point de montage `/home` sur un système. Le système reconnaît le statut spécial de `/home` lorsqu'AutoFS est actif. Pour plus d'informations sur le montage automatique des répertoires personnels, reportez-vous à la section "Présentation des tâches d'administration Autofs" du manuel *Gestion de systèmes de fichiers réseau dans Oracle Solaris 11.1*.

Pour utiliser un répertoire personnel en tout point du réseau, vous devez toujours faire référence au répertoire personnel en tant que `$HOME`, et pas en tant que `/export/home/`*username*. Ce dernier est propre à la machine. En outre, les liens symboliques créés dans le répertoire personnel d'un utilisateur doivent utiliser des chemins d'accès relatifs (par exemple, `../../../x/y/x`) pour que les liens restent valides quel que soit l'endroit où le répertoire personnel est monté.

Pour plus d'informations sur l'ajout des répertoires personnels lorsque vous créez des comptes utilisateur avec l'interface de ligne de commande, reportez-vous à la section "Instructions relatives à la configuration des comptes utilisateur" à la page 47.

Services de noms

Si vous gérez des comptes utilisateur pour un site de grande taille, vous pouvez être amené à utiliser un service de noms ou d'annuaire tel que LDAP ou NIS. Un service de noms ou d'annuaire vous permet de stocker des informations de compte utilisateur de manière centralisée au lieu de les stocker dans tous les fichiers `/etc` du système. Lorsque vous utilisez un service de noms ou d'annuaire pour leurs comptes, les utilisateurs peuvent passer d'un système à l'autre avec le même compte sans que leurs informations ne soient dupliquées sur chaque système. L'utilisation d'un service de noms ou d'annuaire garantit également la cohérence des informations des comptes utilisateur.

Environnement de travail de l'utilisateur

Outre le répertoire personnel destiné à créer et stocker des fichiers, les utilisateurs doivent bénéficier d'un environnement leur permettant d'accéder aux outils et ressources dont ils ont besoin pour effectuer leur travail. Lorsqu'un utilisateur se connecte à un système, son environnement de travail est déterminé par les fichiers d'initialisation. Ces fichiers sont définis par le shell de démarrage de l'utilisateur, et peut varier en fonction de la version.

Une bonne stratégie de gestion de l'environnement de travail des utilisateurs consiste à fournir des fichiers d'initialisation personnalisés (comme `.bash_profile`, `.bash_login`, `.kshrc` ou `.profile`) dans le répertoire personnel des utilisateurs.

Remarque – N'utilisez pas de fichiers d'initialisation système, tels que `/etc/profil` ou `/etc/.login` pour gérer un environnement de travail d'utilisateur. Ces fichiers sont stockés localement sur les systèmes et ne sont pas administrés de façon centralisée. Si, par exemple, AutoFS est utilisé pour monter le répertoire personnel d'utilisateur à partir de n'importe quel système sur le réseau, vous devez modifier les fichiers d'initialisation système sur chaque système afin de garantir un environnement cohérent chaque fois qu'un utilisateur se déplace d'un système à l'autre.

Pour plus d'informations sur la personnalisation des fichiers d'initialisation utilisateur pour les utilisateurs, reportez-vous à la section "Personnalisation de l'environnement de travail d'un utilisateur " à la page 31.

Pour plus d'informations sur la procédure de personnalisation des comptes utilisateur via la fonction RBAC (contrôle d'accès basé sur les rôles), reportez-vous à la section "Contrôle d'accès basé sur les rôles (présentation)" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Recommandations relatives à l'affectation des noms d'utilisateur, ID utilisateur et ID de groupe

Les noms d'utilisateur, ID utilisateur et ID de groupe doivent être uniques au sein de votre organisation, qui peut s'étendre sur plusieurs domaines.

Gardez à l'esprit les recommandations suivantes lorsque vous créez des noms d'utilisateur ou de rôle, des ID utilisateurs et des ID de groupe :

- **Noms d'utilisateur :** les noms d'utilisateur doivent être composés de deux à huit lettres et chiffres. Le premier caractère doit être une lettre. Au moins un des caractères doit être une lettre minuscule.

  Remarque – Même si les noms d'utilisateur peuvent inclure un point (.), un trait de soulignement (_), ou un trait d'union (-), l'utilisation de ces caractères n'est pas recommandée car ils peuvent provoquer des problèmes avec certains logiciels.

- **Comptes système :** n'utilisez pas les noms d'utilisateur, les ID utilisateur ou les ID de groupe contenus dans les fichiers par défaut `/etc/passwd` et `/etc/group`. N'utilisez pas d'ID utilisateur et de groupe compris entre 0 et 99. Ces numéros sont réservés à l'usage d'Oracle Solaris et ne doivent pas être utilisés. Notez que cette restriction s'applique également aux chiffres qui ne sont actuellement pas en cours d'utilisation.

  Par exemple, `gdm` est le nom d'utilisateur et de groupe réservé au démon du gestionnaire d'affichage GNOME et ne doit pas être utilisé pour un autre utilisateur. Pour obtenir la liste complète des entrées `/etc/passwd` et `/etc/group` par défaut, reportez-vous au Tableau 1–3 et au Tableau 1–4.

  Les comptes `nobody` et `nobody4` ne doivent jamais être utilisés pour l'exécution de processus. Ces deux comptes sont réservés à l'utilisation par NFS. L'utilisation de ces comptes pour l'exécution de processus peut entraîner des risques inattendus pour la sécurité. Les processus devant s'exécuter avec un autre compte que root doivent utiliser les comptes `daemon` ou `noaccess`.

- **Configuration des comptes système** : la configuration des comptes système par défaut ne doit jamais être modifiée. Ceci inclut la modification du shell de connexion d'un compte système qui est actuellement verrouillé. La seule exception à cette règle est la définition d'un mot de passe et de paramètres de vieillissement du mot de passe pour le compte `root`.

Remarque – La modification du mot de passe d'un compte utilisateur verrouillé modifie le mot de passe, mais ne déverrouille plus par la même occasion le compte concerné. Une deuxième étape est désormais nécessaire pour déverrouiller le compte et requiert l'utilisation de la commande `passwd -u`.

Emplacement de stockage des informations de compte utilisateur et de groupe

Les informations suivantes sont décrites dans cette section :

Selon la stratégie de votre site, les informations de compte utilisateur et de groupe peuvent être stockées dans les fichiers `/etc` de votre système local ou dans un service de noms ou d'annuaire comme suit :

- Les informations du service de noms NIS sont stockées dans des cartes.
- Les informations du service d'annuaire LDAP sont stockées dans des fichiers de base de données indexées.

Remarque – Pour éviter toute confusion, l'emplacement des informations de compte utilisateur et de groupe est qualifié de manière générique de *fichier* plutôt que de *base de données*, *tableau* ou *carte*.

La plupart des informations de compte utilisateur sont stockées dans le fichier `passwd`. Les informations sur les mots de passe sont stockées comme suit :

- dans le fichier `passwd` lorsque vous utilisez NIS ;
- dans le fichier `/etc/shadow` lorsque vous utilisez des fichiers `/etc` ;
- dans le conteneur `people` lorsque vous utilisez LDAP.

Le vieillissement du mot de passe est disponible lorsque vous utilisez LDAP, mais pas NIS.

Les informations relatives aux groupes sont stockées dans le fichier `group` pour NIS et dans des fichiers. Pour LDAP, les informations de groupe sont stockées dans le conteneur `group`.

Champs du fichier `passwd`

Les champs dans le fichier `passwd` sont séparés par des deux-points et contiennent les informations suivantes :

username:*password*:*uid*:*gid*:*comment*:*home-directory*:*login-shell*

Par exemple :

```
kryten:x:101:100:Kryten Series 4000 Mechanoid:/export/home/kryten:/bin/csh
```

Pour obtenir une description complète des champs dans le fichier `passwd`, reportez-vous à la page de manuel `passwd(1)`.

Fichier `passwd` par défaut

Le fichier par défaut `passwd` contient des entrées pour les démons standard. Des démons sont des processus qui sont habituellement démarrés au moment de l'initialisation afin d'effectuer certaines tâches à l'échelle du système, telles que l'impression, l'administration réseau ou la surveillance de port.

```
root:x:0:0:Super-User:/root:/usr/bin/bash
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
dladm:x:15:65:Datalink Admin:/:
netadm:x:16:65:Network Admin:/:
netcfg:x:17:65:Network Configuration Admin:/:
smmsp:x:25:25:SendMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/var/lib/gdm:
zfssnap:x:51:12:ZFS Automatic Snapshots Reserved UID:/:/usr/bin/pfsh
upnp:x:52:52:UPnP Server Reserved UID:/var/coherence:/bin/ksh
xvm:x:60:60:xVM User:/:
mysql:x:70:70:MySQL Reserved UID:/:
openldap:x:75:75:OpenLDAP User:/:
webservd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/:/usr/bin/pfksh
svctag:x:95:12:Service Tag UID:/:
unknown:x:96:96:Unknown Remote UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
ftp:x:21:21:FTPD Reserved UID:/:
dhcpserv:x:18:65:DHCP Configuration Admin:/:
aiuser:x:60003:60001:AI User:/:
pkg5srv:x:97:97:pkg(5) server UID:/:
```

TABLEAU 1–3 Entrées du fichier `passwd` par défaut

Nom d'utilisateur	Identifiant utilisateur	Description
`root`	`0`	Réservé au compte superutilisateur
`daemon`	`1`	Démon système générique associé à des tâches de routine
`bin`	`2`	Démon d'administration associé à l'exécution de fichiers binaires du système pour effectuer des tâches de routine
`sys`	`3`	Démon d'administration associé à la journalisation système ou des fichiers de mise à jour dans des répertoires temporaires
`adm`	`4`	Démon d'administration associé à la journalisation du système
`lp`	`71`	Réservé au démon d'imprimante ligne
`uucp`	`5`	Affecté au démon associé aux fonctions `uucp`
`nuucp`	`9`	Affecté à un autre démon associé aux fonctions `uucp`
`dladm`	`15`	Réservé à l'administration de liaison de données
`netadm`	`16`	Réservé à l'administration réseau
`netcfg`	`17`	Réservé à l'administration de la configuration réseau
`smmsp`	`25`	Affecté au démon du programme d'envoi de message Sendmail
`listen`	`37`	Affecté au démon d'écoute réseau
`gdm`	`50`	Affecté au démon du gestionnaire d'affichage de GNOME
`zfssnap`	`51`	Réservé aux instantanés automatiques
`upnp`	`52`	Réservé au serveur UPnP
`xvm`	`60`	Réservé à l'utilisateur xVM
`mysql`	`70`	Réservé à l'utilisateur MySQL
`openldap`	`75`	Réservé à l'utilisateur OpenLDAP
`webservd`	`80`	Réservé à l'accès WebServer
`postgres`	`90`	Réservé à l'accès PostgresSQL
`svctag`	`95`	Réservé à l'accès au registre de balises de service
`unknown`	`96`	Réservé aux utilisateurs distants ne pouvant pas être mappés dans les ACL NFSv4

TABLEAU 1–3 Entrées du fichier `passwd` par défaut *(Suite)*

Nom d'utilisateur	Identifiant utilisateur	Description
`nobody`	`60001`	Réservé à un utilisateur à accès anonyme NFS
`noaccess`	`60002`	Réservé à un utilisateur sans accès
`nobody4`	`65534`	Réservé à un utilisateur à accès anonyme NFS SunOS 4.x
`ftp`	`21`	Réservé à l'accès FTP
`dhcpserv`	`18`	Réservé à un utilisateur de serveur DHCP
`aiuser`	`60003`	Réservé à un utilisateur AI
`pkg5srv`	`97`	Réservé au serveur de dépôt `pkg`(5)

Champs du fichier `shadow`

Les champs dans le fichier `shadow` sont séparés par le signe deux-points et contiennent les informations suivantes :

username:*password*:*lastchg*:*min*:*max*:*warn*:*inactive*:*expire*

L'algorithme de hachage du mot de passe par défaut est `SHA256`. Le hachage du mot de passe pour l'utilisateur est similaire à l'exemple suivant :

```
$5$cgQk2iUy$AhHtVGx5Qd0.W3NCKjikb8.KhOiA4DpxsW55sP0UnYD
```

Pour obtenir une description complète des champs du fichier `shadow`, reportez-vous à la page de manuel `shadow`(4).

Champs du fichier `group`

Les champs dans le fichier `group` sont séparés par des deux-points et contiennent les informations suivantes :

group-name:*group-password*:*gid*:*user-list*

Par exemple :

```
bin::2:root,bin,daemon
```

Pour une description complète des champs dans le fichier `group`, reportez-vous à la page de manuel `group`(4).

Fichier `group` par défaut

Le fichier `group` par défaut contient les groupes système suivants qui prennent en charge des tâches à l'échelle du système, telles que l'impression, l'administration réseau ou la messagerie électronique. La plupart de ces groupes ont des entrées correspondantes dans le fichier `passwd`.

```
root::0:
other::1:root
bin::2:root,daemon
sys::3:root,bin,adm
adm::4:root,daemon
uucp::5:root
mail::6:root
tty::7:root,adm
lp::8:root,adm
nuucp::9:root
staff::10:
daemon::12:root
sysadmin::14:
games::20:
smmsp::25:
gdm::50:
upnp::52:
xvm::60:
netadm::65:
mysql::70:
openldap::75:
webservd::80:
postgres::90:
slocate::95:
unknown::96:
nobody::60001:
noaccess::60002:
nogroup::65534:
ftp::21
pkg5srv::97:
```

TABLEAU 1–4 Entrées du fichier `group` par défaut

Nom de groupe	ID de groupe	Description
`root`	`0`	Groupe superutilisateur
`other`	`1`	Groupe facultatif
`bin`	`2`	Groupe d'administration associé à l'exécution de fichiers binaires du système
`sys`	`3`	Groupe d'administration associé à la journalisation du système ou à des répertoires temporaires
`adm`	`4`	Groupe d'administration associé à la journalisation du système
`uucp`	`5`	Groupe associé aux fonctions `uucp`
`mail`	`6`	Groupe de messagerie électronique

TABLEAU 1–4 Entrées du fichier `group` par défaut *(Suite)*

Nom de groupe	ID de groupe	Description
`tty`	7	Groupe associé aux périphériques `tty`
`lp`	8	Groupe d'imprimante ligne
`nuucp`	9	Groupe associé aux fonctions `uucp`
`staff`	10	Groupe d'administration générale
`daemon`	12	Groupe associé aux tâches de routine
`sysadmin`	14	Groupe d'administration utile pour les administrateurs système
`smmsp`	25	Démon du programme Sendmail d'envoi de message
`gdm`	50	Groupe réservé au démon du gestionnaire d'affichage de GNOME
`upnp`	52	Groupe réservé au serveur UPnP
`xvm`	60	Groupe réservé à l'utilisateur xVM
`netadm`	65	Groupe réservé à l'administration réseau
`mysql`	70	Groupe réservé à l'utilisateur MySQL
`openldap`	75	Réservé à l'utilisateur OpenLDAP
`webservd`	80	Groupe réservé à l'accès WebServer
`postgres`	90	Groupe réservé à l'accès PostgresSQL
`slocate`	95	Groupe réservé à l'accès à emplacement sécurisé
`unknown`	96	Groupe réservé aux groupes distants ne pouvant pas être mappés dans les ACL NFSv4
`nobody`	60001	Groupe assigné pour un accès NFS anonyme
`noaccess`	60002	Groupe assigné à un utilisateur ou un processus ayant besoin d'accéder à un système par le biais d'une application, mais sans se connecter
`nogroup`	65534	Groupe assigné à un utilisateur qui n'est membre d'aucun groupe connu
`ftp`	21	Groupe assigné pour l'accès FTP
`pkg5srv`	97	Groupe affecté au serveur de dépôt `pkg`(5)

Commandes permettant d'obtenir des informations sur les comptes utilisateur

Le tableau suivant décrit les commandes que les administrateurs système peuvent exécuter pour obtenir des informations sur les comptes utilisateur. Ces informations sont stockées dans différents fichiers sous le répertoire `/etc`. Mieux vaut exécuter ces commandes (et non la commande `cat`) pour obtenir des informations sur les comptes utilisateur.

TABLEAU 1–5 Commandes à exécuter pour obtenir des informations sur les utilisateurs

Commande	Description	Référence aux pages de manuel
`auths`	Répertorie et gère les autorisations.	`auths(1)`
`getent`	Extrait la liste des entrées de la base de données d'administration. Ces informations proviennent généralement d'une ou de plusieurs sources spécifiées pour la base de données `/etc/nsswitch.conf`.	`getent(1M)`
`logins`	Affiche des informations sur les utilisateurs, les rôles et les connexions au système. La sortie est contrôlée par les options de commande ajoutées et peut inclure un utilisateur, un rôle, une connexion au système, un identificateur unique, la valeur du champ du compte `passwd`, un groupe principal, un ID de groupe principal, plusieurs noms de groupes, plusieurs ID de groupes, un répertoire personnel, un shell de connexion et des paramètres de durée de vie du mot de passe.	`logins(1M)`
`profiles`	Répertorie et gère les profils de droits.	`profiles(1)`
`roles`	Affiche les rôles attribués à un utilisateur.	`roles(1)`

TABLEAU 1–5 Commandes à exécuter pour obtenir des informations sur les utilisateurs *(Suite)*

Commande	Description	Référence aux pages de manuel
`userattr`	Affiche la première valeur trouvée pour `attribute_name`. Si un utilisateur n'est pas spécifié, il est extrait de l'ID utilisateur effectif du processus. Les noms d'attribut sont définis dans les pages de manuel `user_attr`(4) et `prof_attr` (4). **Remarque –** Cette commande est une nouveauté d'Oracle Solaris 11.	Example 2–1

Commandes permettant de gérer les utilisateurs, les rôles et les groupes

Remarque – L'interface graphique de la console de gestion Solaris et la ligne de commande associée ne sont plus prises en charge.

Les commandes suivantes sont disponibles pour gérer les utilisateurs, les rôles et les groupes.

TABLEAU 1–6 Commandes permettant de gérer les utilisateurs, les rôles et les groupes

Page de manuel pour les commandes	Description	Pour plus d'informations
`useradd`(1M)	Crée des utilisateurs localement ou dans un référentiel LDAP.	"Ajout d'un utilisateur" à la page 49
`usermod`(1M)	Modifie les propriétés de l'utilisateur localement ou dans un référentiel LDAP. Si les propriétés de l'utilisateur sont liées à la sécurité, telles que l'affectation de rôles, cette tâche peut être limitée à votre administrateur de la sécurité ou au rôle `root`.	"Modification d'un utilisateur" à la page 50 "Modification des attributs de sécurité d'un utilisateur" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*
`userdel`(1M)	Supprime un utilisateur du système ou du référentiel LDAP. Peut impliquer un nettoyage supplémentaire, tel que la suppression de la tâche `cron`.	"Suppression d'un utilisateur" à la page 51

TABLEAU 1–6 Commandes permettant de gérer les utilisateurs, les rôles et les groupes *(Suite)*

Page de manuel pour les commandes	Description	Pour plus d'informations
`roleadd`(1M) `rolemod`(1M) `roledel`(1M)	Gère les rôles localement ou dans un référentiel LDAP. Les rôles ne peuvent pas se connecter. Les utilisateurs prennent un rôle qui leur a été assigné pour effectuer des tâches d'administration.	"Procédure de création d'un rôle" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité* "Configuration initiale RBAC (liste des tâches)" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*
`groupadd`(1M) `groupmod`(1M) `groupdel`(1M)	Gère les groupes localement ou dans un référentiel LDAP.	"Ajout d'un groupe" à la page 52

Personnalisation de l'environnement de travail d'un utilisateur

Les informations suivantes sont décrites dans cette section :

Le paramétrage du répertoire personnel d'un utilisateur consiste notamment à fournir des fichiers d'initialisation utilisateur au shell de connexion de l'utilisateur. Un *fichier d'initialisation utilisateur* est un script shell qui définit un environnement de travail d'utilisateur après la connexion de l'utilisateur à un système. En fait, vous pouvez exécuter les mêmes tâches dans un fichier d'initialisation utilisateur que dans un script shell. Toutefois, l'objectif principal d'un fichier d'initialisation utilisateur est de définir les caractéristiques de l'environnement de travail d'un utilisateur, tels que ses chemins de recherche, les variables d'environnement et l'environnement de multifenêtrage. Chaque shell de connexion dispose de son ou ses propres

fichiers d'initialisation utilisateur, répertoriés dans le tableau ci-dessous. Notez que le fichier d'initialisation utilisateur par défaut pour les shells bash et `ksh93` est `/etc/skel/local.profile`.

TABLEAU 1–7 Fichiers d'initialisation utilisateur bash et ksh93

Shell	Fichier d'initialisation utilisateur	Objectif

`bash`	`$HOME/.bash_profile`
	`$HOME/.bash_login`
	`$HOME/.profile`
		Définit l'environnement de l'utilisateur au moment de la connexion.

`ksh93`	`/etc/profile` `$HOME/.profile`	Définit l'environnement de l'utilisateur au moment de la connexion.
	`$ENV`	Définit l'environnement utilisateur au moment de la connexion dans le fichier. Spécifié par la variable d'environnement du shell Korn `ENV`.

Vous pouvez utiliser ces fichiers comme un point de départ, puis les modifiez pour créer un ensemble standard de fichiers qui fournissent l'environnement de travail commun à tous les utilisateurs. Vous pouvez également modifier ces fichiers afin de fournir l'environnement de travail aux différents types d'utilisateurs.

Pour consulter des instructions détaillées sur la façon de créer des ensembles de fichiers d'initialisation pour différents types d'utilisateurs, reportez-vous à la section "Personnalisation des fichiers d'initialisation utilisateur" à la page 46.

Utilisation des fichiers d'initialisation du site

Les fichiers d'initialisation peuvent être personnalisés par l'administrateur et l'utilisateur. Cette tâche importante peut être réalisée avec des fichiers d'initialisation utilisateur centralisés et distribués de manière globale. Ces fichiers sont qualifiés de *fichiers d'initialisation du site*. Les fichiers d'initialisation du site vous permettent d'introduire en continu de nouvelles fonctionnalités dans l'environnement de travail utilisateur, tout en permettant à l'utilisateur de personnaliser son fichier d'initialisation.

Lorsque vous référencez un fichier d'initialisation du site dans un fichier d'initialisation utilisateur, toutes les mises à jour du fichier d'initialisation du site sont automatiquement répercutées lorsque l'utilisateur se connecte au système ou lorsqu'un utilisateur démarre un nouveau shell. Les fichiers d'initialisation du site sont conçus pour vous permettre de distribuer à l'échelle du site les modifications apportées aux environnements de travail des utilisateurs que vous n'aviez pas prévu lorsque vous avez ajouté les utilisateurs.

Vous pouvez personnaliser un fichier d'initialisation du site de la même façon que vous personnalisez un fichier d'initialisation utilisateur. Ces fichiers résident généralement sur un serveur, ou un ensemble de serveurs, et s'affichent comme la première instruction dans un fichier d'initialisation utilisateur. En outre, chaque fichier d'initialisation du site doit être du même type de script shell que le fichier d'initialisation utilisateur qui le référence.

Pour référencer un fichier d'initialisation du site dans un fichier d'initialisation utilisateur bash ou `ksh93`, placez au début du fichier d'initialisation utilisateur une ligne similaire à la ligne suivante :

```
. /net/machine-name/export/site-files/site-init-file
```

Avertissement concernant les références au système local

N'ajoutez pas de références propres au système local dans le fichier d'initialisation utilisateur. En effet, les instructions figurant dans ce fichier doivent être valides, quel que soit le système auquel l'utilisateur se connecte.

Par exemple :

- Pour que le répertoire personnel d'un utilisateur soit disponible n'importe où sur le réseau, faites toujours référence à ce répertoire à l'aide de la variable `$HOME`. Par exemple, utilisez `$HOME/bin` au lieu de `/export/home/` *username*`/bin`. La variable `$HOME` fonctionne lorsque l'utilisateur se connecte à un autre système, et les répertoires personnels sont montés automatiquement.
- Pour accéder aux fichiers d'un disque local, utilisez les noms de chemin d'accès globaux, comme par exemple `/net/`*system-name/directory-name*. N'importe quel répertoire référencé par `/net/`*system-name* peut être automatiquement monté sur n'importe quel système auquel l'utilisateur se connecte, en supposant que le système exécute AutoFS.

Fonctions du shell

Cette version d'Oracle Solaris prend en charge les fonctions et comportements de shell suivants :

- Le shell GNU Bourne-Again (bash) est affecté par défaut au compte d'utilisateur qui est créé lorsque vous installez la version d'Oracle Solaris.
- Le shell standard du système (`bin/sh`) est maintenant Korn Shell 93 (`ksh93`).
- Le shell interactif par défaut (`/usr/bin/bash`) est le shell Bourne-Again (`bash`).
- Les shells bash et `ksh93` prennent en charge l'édition de ligne de commande, ce qui signifie que vous pouvez modifier les commandes avant de les exécuter.

- Vous pouvez afficher le shell par défaut et son chemin d'accès de plusieurs manières.
  - Exécutez les commandes `echo $SHELL` et `which` :

    ```
    $ grep root /etc/passwd
    root:x:0:0:Super-User:/root:/usr/bin/bash

    $ echo $SHELL /usr/bin/bash
    $ which ksh93 /usr/bin/ksh93
    ```

  - Exécutez la commande `pargs` :

    ```
    ~$ pargs -l $$
    /usr/bin/i86/ksh93
    ```

- Le shell `ksh93` comprend également une variable intégrée nommée `.sh.version`, que vous pouvez afficher comme suit :

  ```
  ~$ echo ${.sh.version}
  Version jM 93u 2011-02-08
  ```

- Pour passer à un autre shell, entrez le chemin d'accès du shell que vous souhaitez utiliser.
- Pour quitter un shell, entrez `exit`.

Le tableau ci-dessous décrit les options de shell prises en charge dans Oracle Solaris.

TABLEAU 1–8 Fonctions de shell de base dans la version d'Oracle Solaris

Shell	Chemin	Comments (Commentaires)
Bourne-Again Shell (bash)	`/usr/bin/bash`	Shell par défaut pour les utilisateurs créés par un programme d'installation, ainsi que pour le rôle `root`. Le shell (interactif) par défaut pour les utilisateurs créés avec la commande `useradd` ainsi que pour le rôle `root` est `/usr/bin/bash`. Le chemin d'accès par défaut est `/usr/bin:/usr/sbin`.
Korn shell	`/usr/bin/ksh`	`ksh93` est le shell par défaut dans cette version d'Oracle Solaris.
C shell et C shell amélioré	`/usr/bin/csh` et `/usr/bin/tcsh`	C shell et C shell amélioré
Shell conforme POSIX	`/usr/xpg4/bin/sh`	Shell conforme POSIX
Z shell	`/usr/bin/zsh`	Z shell

Remarque – Le Z shell (`zsh`) et le C shell amélioré(`tsch`) ne sont pas installés sur votre système par défaut. Pour utiliser l'un de ces shells, vous devez d'abord installer les packages logiciels requis.

Historique des shells bash et ksh93

Les shells `bash` et `ksh93` enregistrent un historique de toutes les commandes que vous exécutez. Cet historique est conservé pour chaque utilisateur, ce qui signifie qu'il est préservé d'une session à l'autre et qu'il est représentatif de l'ensemble de vos sessions de connexion.

Par exemple, si vous êtes dans un shell bash, vous pouvez afficher l'historique complet des commandes exécutées, comme suit :

```
$ history
1 ls
2 ls -a
3 pwd
4 whoami
.
.
.
```

Pour afficher un nombre donné de commandes précédentes, incluez un nombre entier dans la commande :

```
$ history 2
12 date
13 history
```

Pour plus d'informations, reportez-vous à la page de manuel `history(1)`

Variables d'environnement des shells bash et ksh93

Les shells bash et `ksh93` stockent des informations sur des variables spéciales constituant pour les shells des *variables d'environnement*. Pour afficher la liste complète des variables d'environnement actuelles pour le shell bash, exécutez la commande `declare` :

```
$ declare
BASH=/usr/bin/bash
BASH_ARGC=()
BASH_ARGV=()
BASH_LINEND=()
BASH_SOuRCE=()
BASH_VERSINFO=([0]=''3'' [1]=''2'' [2]=''25'' [3]=''1''
[4]=''release'' [5]'')
.
.
.
```

Pour le shell `ksh93`, utilisez la commande `set`, qui est l'équivalent de la commande `declare` du shell bash :

```
$ set
  COLUMNS=80
  ENV='$HOME/.kshrc'
  FCEDIT=/bin/ed
  HISTCMD=3
  HZ=''
  IFS=$' \t\n'
  KSH_VERSION=.sh.version
  LANG=C
  LINENO=1
  .
  .
  .
```

Pour imprimer les variables d'environnement de l'un ou l'autre shell, utilisez la commande `echo` ou la commande `printf`. Par exemple :

```
$ echo $SHELL
/usr/bin/bash
$ printf ''$PATH\n''
/usr/bin:/usr/sbin
```

Remarque – Les variables d'environnement ne sont pas conservées entre les sessions. Pour définir des variables d'environnement qui restent cohérentes entre les connexions, vous devez effectuer les modifications correspondantes dans le fichier `.bashrc`.

Un shell peut avoir deux types de variables :

Variables d'environnement	Variables exportées vers tous les processus générés par le shell. La commande `exporter` permet d'exporter une variable. Par exemple : `export VARIABLE=value` Ces paramètres peuvent être affichés à l'aide de la commande `env`. Un sous-ensemble de variables d'environnement, tel que `PATH`, affecte le comportement du shell lui-même.
Variables (locales) de shell	Variables qui affectent uniquement le shell actuel. Dans un fichier d'initialisation utilisateur, vous pouvez personnaliser l'environnement de shell d'un utilisateur en modifiant les valeurs des variables prédéfinies ou en spécifiant des variables supplémentaires.

Le tableau suivant fournit plus de détails sur le shell et les variables d'environnement disponibles dans la version d'Oracle Solaris.

TABLEAU 1–9 Description des variables d'environnement et shell

Variable	Description
CDPATH	Définit une variable utilisée par la commande cd. Si le répertoire cible de la commande cd est spécifié comme un chemin d'accès relatif, la commande cd recherche d'abord le répertoire cible dans le répertoire courant (.). Si la cible est introuvable, les chemins d'accès répertoriés dans la variable CDPATH sont recherchés consécutivement jusqu'à ce que le répertoire cible soit détecté et le changement de répertoire terminé. Si le répertoire cible est introuvable, le répertoire de travail courant est laissé intact. Par exemple, la variable CDPATH est définie sur /home/jean, et deux répertoires existent sous /home/jean, bin et rje. Dans le répertoire /home/jean/bin, lorsque vous tapez cd rje, vous changez les répertoires en /home/jean/rje, même si vous ne spécifiez pas un chemin d'accès complet.
HOME	Définit le chemin d'accès au répertoire personnel de l'utilisateur.
LANG	Définit l'environnement linguistique.
LOGNAME	Définit le nom de l'utilisateur actuellement connecté. La valeur par défaut de LOGNAME est définie automatiquement par le programme de connexion pour le nom d'utilisateur spécifié dans le fichier passwd. Vous devez uniquement vous référez à cette variable, mais pas la réinitialiser.
MAIL	Définit le chemin d'accès à la boîte aux lettres de l'utilisateur.
MANPATH	Définit les hiérarchies de pages de manuel disponibles. **Remarque –** A partir de la version 11 d'Oracle Solaris, la variable d'environnement MANPATH n'est plus requise. La commande man détermine le MANPATH approprié, selon la valeur de la variable d'environnement PATH.
PATH	Indique, dans l'ordre, les répertoires analysés par le shell pour trouver le programme à exécuter lorsque l'utilisateur saisit une commande. Si le répertoire ne se trouve pas dans le chemin de recherche, les utilisateurs doivent entrer le nom de chemin d'accès complet d'une commande. Dans le cadre du processus de connexion, la valeur par défaut PATH est automatiquement définie comme indiqué dans .profile . L'ordre du chemin de recherche est important. Lorsque des commandes identiques figurent à différents emplacements, la première commande détectée avec ce nom est utilisée. Supposons par exemple que PATH est défini dans la syntaxe shell en tant que PATH=/usr/bin:/usr/sbin:$HOME/bin et qu'un fichier nommé sample réside à la fois sous /usr/bin et /home/jean/bin. Si l'utilisateur saisit la commande sample sans indiquer son chemin d'accès complet, la version trouvée dans /usr/bin est utilisée.
PS1	Définit l'invite de shell pour le shell bash ou ksh93.
SHELL	Définit le shell par défaut utilisé par make, vi et d'autres outils.

TABLEAU 1–9 Description des variables d'environnement et shell *(Suite)*

Variable	Description
TERMINFO	Nomme un répertoire lorsqu'une autre base de données terminfo est stockée. Utilisez la variable TERMINFO dans le fichier /etc/profile ou /etc/.login. Pour plus d'informations, reportez-vous à la page de manuel terminfo(4). Lorsque la variable d'environnement TERMINFO est définie, le système vérifie d'abord le chemin d'accès TERMINFO défini par l'utilisateur. Si le système ne trouve pas la définition d'un terminal dans le répertoire TERMINFO défini par l'utilisateur, il effectue une recherche dans le répertoire par défaut, /usr/share/lib/terminfo , pour une définition. Si le système ne trouve pas de définition dans l'un ou l'autre des emplacements, le terminal est qualifié de "terminal idiot".
TERM	Définit le terminal. Cette variable doit être réinitialisée dans le fichier /etc/profile ou le fichier /etc/.login. Lorsque l'utilisateur appelle un éditeur, le système recherche un fichier portant le même nom et qui est défini dans cette variable d'environnement. Le système effectue une recherche dans le répertoire référencé par TERMINFO afin de déterminer les caractéristiques des terminaux.
TZ	Définit le fuseau horaire. Le fuseau horaire est utilisé pour afficher les dates, par exemple, dans la commande ls -l. Si TZ n'est pas défini dans l'environnement utilisateur, le paramètre système est utilisé. Dans le cas contraire, l'heure moyenne de Greenwich est utilisée.

Personnalisation du shell bash

Pour personnaliser le shell bash, ajoutez les informations au fichier .bashrc qui se trouve dans votre répertoire personnel. L'utilisateur initial créé lors de l'installation d'Oracle Solaris dispose d'un fichier .bashrc qui définit les PATH, MANPATH et l'invite de commande. Pour plus d'informations, reportez-vous à la page de manuel bash(1).

Variable d'environnement MANPATH

La variable d'environnement MANPATH indique l'emplacement où la commande man recherche les pages de manuel de référence. La variable d'environnement MANPATH est définie automatiquement en fonction de la valeur PATH de l'utilisateur, mais elle inclut généralement /usr/share/man et usr/gnu/share/man.

Notez que la variable d'environnement MANPATH d'un utilisateur peut être modifiée indépendamment de la variable d'environnement PATH. Un équivalent individuel des emplacements des pages de manuel associées, avec des répertoires dans le $PATH de l'utilisateur, n'est pas nécessaire.

Variable d'environnement PATH

Lorsque l'utilisateur exécute une commande en utilisant le chemin d'accès complet, le shell utilise ce chemin pour trouver la commande. Toutefois, lorsque des utilisateurs n'indiquent qu'un nom de commande, le shell recherche cette commande dans les répertoires, selon l'ordre indiqué par la variable `chemin`. Si la commande est trouvée dans l'un des répertoires, le shell exécute la commande.

Un chemin d'accès par défaut est défini par le système. Cependant, la plupart des utilisateurs le modifient pour ajouter d'autres répertoires de commande. De nombreux problèmes d'utilisateur en matière de configuration de l'environnement et d'accès à la version correcte d'une commande ou d'un outil sont dus à la définition inappropriée des chemins d'accès.

Recommandations relatives à la définition des chemins d'accès

Voici quelques recommandations pour la configuration de variables `PATH` efficaces :

- Si vous devez inclure le répertoire actuel (.) dans le chemin d'accès, il doit être placé en dernier. Inclure le répertoire actuel dans le chemin d'accès constitue un risque de sécurité, car certaines personnes malveillantes peuvent cacher un script ou un fichier exécutable compromis dans le répertoire actuel. Vous pouvez envisager d'utiliser les noms de chemin absolus à la place.
- Conservez le chemin de recherche aussi court que possible. Le shell effectue des recherches dans chaque répertoire du chemin d'accès. Si aucune commande n'est trouvée, de longues recherches peuvent ralentir les performances du système.
- Le chemin de recherche est lu de gauche à droite, de sorte que vous devez placer les répertoires de commandes fréquemment utilisées au début du chemin.
- Assurez-vous que les répertoires ne sont pas dupliqués dans le chemin d'accès.
- Evitez, dans la mesure du possible, d'effectuer des recherches dans des répertoires volumineux. Placez les répertoires volumineux à la fin du chemin.
- Placez les répertoires locaux avant les répertoires montés sur NFS afin de diminuer les risques de "blocage" lorsque le serveur NFS ne répond pas. Cette stratégie permet également de réduire le trafic réseau inutile.

Variables d'environnement linguistique

Les variables d'environnement `LANG` et `LC` indiquent les conventions et conversions propres à l'environnement linguistique pour le shell. Ces conversions et conventions incluent les fuseaux horaires, l'ordre de classement et les formats de date, d'heure, de devise et de chiffres. En outre, vous pouvez utiliser la commande `stty` dans un fichier d'initialisation utilisateur afin d'indiquer si la session de terminal prendra en charge les caractères multioctets.

La variable LANG définit toutes les conversions et conventions possibles pour l'environnement linguistique. Vous pouvez définir différents aspects de la localisation séparément par le biais des variables LC suivantes : LC_COLLATE, LC_CTYPE, LC_MESSAGES, LC_NUMERIC, LC_MONETARY et LC_TIME.

Remarque – Par défaut, Oracle Solaris 11 installe uniquement les environnements linguistiques UTF-8.

Le tableau suivant décrit les valeurs des variables d'environnement pour les environnements linguistiques de base d'Oracle Solaris 11.

TABLEAU 1–10 Valeurs des variables LANG et LC.

Valeur	Environnement linguistique
en_US.UTF-8	Anglais, Etats-Unis (UTF-8)
fr_FR.UTF-8	Français (France) (UTF-8)
de_DE.UTF-8	Allemand, Allemagne (UTF-8)
it_IT.UTF-8	Italien, Italie (UTF-8)
ja_JP.UTF-8	Japonais, Japon (UTF-8)
ko_KR.UTF-8	Coréen, Corée (UTF-8)
pt_BT.UTF-8	Portugais, Brésil (UTF-8)
zh_CN.UTF-8	Chinois simplifié, Chine (UTF-8)
es_ES.UTF-8	Espagnol, Espagne (UTF-8)
zh_TW.UTF-8	Chinois traditionnel, Taïwan (UTF-8)

EXEMPLE 1–1 Définition de l'environnement linguistique à l'aide des variables LANG

Dans un fichier d'initialisation utilisateur Bourne shell ou Korn shell, vous devez ajouter les éléments suivants :

```
LANG=de_DE.ISO8859-1; export LANG


LANG-de_DE.UTF-8; export LANG
```

Autorisations de fichier par défaut (umask)

Lorsque vous créez un fichier ou un répertoire, les autorisations assignées par défaut au fichier ou répertoire sont contrôlées par le *masque utilisateur*. Le masque utilisateur est défini par la commande `umask` dans un fichier d'initialisation utilisateur. Vous pouvez afficher la valeur courante du masque utilisateur en tapant `umask` et en appuyant sur Entrée.

Le masque utilisateur contient les valeurs octales suivantes :

- Le premier chiffre définit les autorisations pour l'utilisateur.
- Le deuxième chiffre définit les autorisations pour le groupe.
- Le troisième chiffre définit les autorisations pour les autres, aussi appelé `world`.

Notez que si le premier chiffre est zéro, il n'est pas affiché. Par exemple, si le masque utilisateur est défini sur 022, le nombre 22 s'affiche.

Pour déterminer la valeur `umask` à définir, soustrayez la valeur des autorisations souhaitées de 666 (pour un fichier) ou 777 (pour un répertoire). Le résultat de cette soustraction correspond à la valeur à utiliser avec la commande `umask`. Par exemple, supposons que vous souhaitez modifier le mode par défaut pour les fichiers et le passer à 644 (`rw-r--r--`). La différence entre 666 et 644 est 022, ce qui correspond à la valeur à utiliser en tant qu'argument de la commande `umask`.

Vous pouvez également déterminer la valeur `umask` que vous voulez définir à l'aide du tableau suivant. Ce tableau indique les autorisations de fichiers et de répertoires qui sont créées pour chacune des valeurs octales de `umask`.

TABLEAU 1–11 Autorisations pour les valeurs `umask`

Valeur octale `umask`	Autorisations de fichier	Autorisations de répertoire
`0`	`rw-`	`rwx`
`1`	`rw-`	`rw-`
`2`	`r--`	`r-x`
`3`	`r--`	`r--`
`4`	`-w-`	`-wx`
`5`	`-w-`	`-w-`
`6`	`--x`	`--x`
`7`	`---` (aucune)	`---` (aucune)

La ligne suivante dans un fichier d'initialisation utilisateur définit les autorisations de fichier par défaut sur `rw-rw-rw-`.

```
umask 000
```

Personnalisation d'un fichier d'initialisation utilisateur

Vous trouverez ci-après un exemple de fichier d'initialisation utilisateur `.profile`. Vous pouvez utiliser ce fichier pour personnaliser vos propres fichiers d'initialisation. Cet exemple utilise des noms et des chemins d'accès système que vous devez modifier pour votre site particulier.

EXEMPLE 1–2 Fichier `.profile`

(Line 1) `PATH=$PATH:$HOME/bin:/usr/local/bin:/usr/gnu/bin:.`
(Line 2) `MAIL=/var/mail/$LOGNAME`
(Line 3) `NNTPSERVER=server1`
(Line 4) `MANPATH=/usr/share/man:/usr/local/man`
(Line 5) `PRINTER=printer1`
(Line 6) `umask 022`
(Line 7) `export PATH MAIL NNTPSERVER MANPATH PRINTER`

1. Définit le chemin de recherche du shell de l'utilisateur.
2. Définit le chemin d'accès au fichier messagerie de l'utilisateur.
3. Définit le serveur de temps/d'horloge de l'utilisateur.
4. Définit le chemin de recherche de l'utilisateur pour les pages de manuel.
5. Définit l'imprimante par défaut de l'utilisateur.
6. Définit les autorisations de création de fichier par défaut de l'utilisateur.
7. Définit les variables d'environnement répertoriées.

◆ ◆ ◆ CHAPITRE 2

Gestion des comptes utilisateur avec l'interface de ligne de commande (tâches)

Ce chapitre fournit des informations de base sur la configuration et la gestion des comptes utilisateur par le biais de l'interface de ligne de commande (CLI).

Pour des informations générales sur la gestion des comptes et environnements utilisateur, reportez-vous au Chapitre 1, “Gestion des comptes et des environnements utilisateur (présentation)”.

Pour plus d'informations sur la gestion des utilisateurs et des rôles dans l'interface graphique du Gestionnaire d'utilisateurs, reportez-vous au Chapitre 3, “Gestion des comptes utilisateur dans l'interface graphique du Gestionnaire d'utilisateurs (tâches)”.

Configuration et gestion des comptes utilisateur dans l'interface de ligne de commande

Les tâches suivantes décrivent la procédure à suivre pour configurer et gérer des comptes utilisateur par le biais de l'interface de ligne de commande.

Configuration et gestion des comptes utilisateur avec l'interface de ligne de commande (liste des tâches)

Tâche	Description	Voir
Collecte d'informations utilisateur	Utilisez un formulaire standard pour rassembler des informations utilisateur et les classer.	“Collecte des informations utilisateur” à la page 45

Tâche	Description	Voir
Personnalisation des fichiers d'initialisation utilisateur	Vous pouvez configurer des fichiers d'initialisation pour offrir des environnements cohérents aux nouveaux utilisateurs.	"Personnalisation des fichiers d'initialisation utilisateur" à la page 46
Modification des paramètres de compte par défaut pour tous les rôles	Modifiez le répertoire personnel par défaut et le répertoire squelette pour tous les rôles.	"Modification des paramètres de compte par défaut pour tous les rôles" à la page 46
Création d'un compte utilisateur	A l'aide des paramètres par défaut du compte que vous configurez, créez un utilisateur local à l'aide de la commande `useradd`.	"Ajout d'un utilisateur" à la page 49
Modification d'un compte utilisateur	Modifiez les informations de connexion d'un utilisateur sur le système.	"Modification d'un utilisateur" à la page 50
Suppression d'un compte utilisateur	Supprimez un compte utilisateur à l'aide de la commande `userdel`.	"Suppression d'un utilisateur" à la page 51
Création puis affectation d'un rôle pour effectuer une tâche d'administration	A l'aide des paramètres de compte par défaut configurés, créez un rôle local pour permettre à l'utilisateur d'exécuter une commande ou une tâche d'administration spécifique.	"Procédure de création d'un rôle" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité* "Procédure d'attribution de rôle" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*
Création d'un groupe	Créez un nouveau groupe par le biais de la commande `groupadd`.	"Ajout d'un groupe" à la page 52
Ajout d'attributs de sécurité à un compte utilisateur	Après avoir configuré un compte utilisateur local, vous pouvez ajouter les attributs de sécurité requis.	"Modification des attributs de sécurité d'un utilisateur" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.
Partage du répertoire personnel d'un utilisateur	Vous devez partager le répertoire personnel de l'utilisateur afin qu'il puisse être monté à distance à partir du système de l'utilisateur.	"Partage de répertoires personnels créés en tant que systèmes de fichiers ZFS" à la page 53

Tâche	Description	Voir
Montage manuel du répertoire personnel d'un utilisateur	En général, vous n'avez pas besoin de monter manuellement les répertoires personnels des utilisateurs qui sont créés en tant que système de fichiers ZFS. Le répertoire personnel est automatiquement monté lors de sa création et il l'est à partir du service de système de fichiers local SMF au moment de l'initialisation.	"Montage manuel du répertoire personnel d'un utilisateur " à la page 54

Collecte des informations utilisateur

Lors de la configuration des comptes utilisateur, vous pouvez créer un formulaire semblable au suivant pour collecter des informations sur les utilisateurs avant de créer leurs comptes.

Elément	Description
Nom d'utilisateur :	
Nom du rôle :	
Profils ou autorisations :	
ID utilisateur :	
Groupe principal :	
Groupes secondaires :	
Commentaire :	
Shell par défaut :	
Statut et vieillissement du mot de passe :	
Nom du chemin d'accès au répertoire personnel :	
Méthode de montage :	
Autorisations sur le répertoire personnel :	
Serveur de courrier :	
Ajouter à ces alias de messagerie :	
Nom du système de bureau :	

▼ Personnalisation des fichiers d'initialisation utilisateur

1 Prenez le rôle `root` ou un rôle disposant du profil de droits User Management.

```
$ su -
Password:
#
```

Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2 Créez un répertoire squelette pour chaque type d'utilisateur.

```
# mkdir /shared-dir/skel/user-type
```

shared-dir Nom d'un répertoire disponible aux autres systèmes sur le réseau

user-type Nom d'un répertoire dans lequel stocker les fichiers d'initialisation pour un type d'utilisateur.

3 Copiez les fichiers d'initialisation utilisateur par défaut dans les répertoires que vous avez créés pour les différents types d'utilisateur.

4 Modifiez les fichiers d'initialisation utilisateur pour chaque type d'utilisateur et personnalisez-les en fonction des besoins de votre site.

La section "Personnalisation de l'environnement de travail d'un utilisateur " à la page 31 décrit en détail les méthodes de personnalisation des fichiers d'initialisation utilisateur.

5 Définissez les autorisations pour les fichiers d'initialisation utilisateur.

```
# chmod 744 /shared-dir/skel/user-type/.*
```

6 Vérifiez que les droits d'accès aux fichiers d'initialisation utilisateur sont corrects.

```
# ls -la /shared-dir/skel/*
```

▼ Modification des paramètres de compte par défaut pour tous les rôles

Dans la procédure suivante, l'administrateur a personnalisé un répertoire `roles`. L'administrateur modifie le répertoire personnel par défaut et le répertoire squelette pour tous les rôles.

1. **Prenez le rôle `root` ou un rôle disposant du profil de droits User Management.**

   Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2. **Créez un répertoire de rôles personnalisés. Par exemple :**

```
# roleadd -D
group=other,1  project=default,3  basedir=/home
skel=/etc/skel  shell=/bin/pfsh  inactive=0
expire=  auths=  profiles=All  limitpriv=
defaultpriv=  lock_after_retries=
```

3. **Modifiez le répertoire personnel par défaut et le répertoire squelette pour tous les rôles. Par exemple :**

```
# roleadd -D -b /export/home -k /etc/skel/roles
# roleadd -D
group=staff,10  project=default,3  basedir=/export/home
skel=/etc/skel/roles  shell=/bin/sh  inactive=0
expire=  auths=  profiles=  roles=  limitpriv=
defaultpriv=  lock_after_retries=
```

   Les utilisations futures de la commande **`roleadd`** créent des répertoires personnels dans `/export/home` et remplissent l'environnement des rôles à partir du répertoire `/etc/skel/roles`.

Instructions relatives à la configuration des comptes utilisateur

Suivez les consignes ci-dessous pour configurer des comptes utilisateur à l'aide de la CLI :

- Dans cette version, les comptes utilisateur sont créés en tant que systèmes de fichiers ZFS Oracle Solaris. En tant qu'administrateur, lorsque vous créez des comptes, vous attribuez également aux utilisateurs leur propre système de fichiers et leur propre jeu de données ZFS. L'exécution des commandes `useradd` et `roleadd` place le répertoire personnel de l'utilisateur sur le système de fichiers `/export/home` en tant que système de fichiers ZFS *individuel*. Par conséquent, les utilisateurs ont la possibilité de sauvegarder leur répertoire personnel, de créer des instantanés ZFS de leur répertoire personnel et de remplacer des fichiers dans leur répertoire personnel actuel à partir des instantanés ZFS qu'ils ont créé.
- Pour configurer des comptes utilisateur, il faut prendre le rôle `root` ou un rôle disposant du profil de droits approprié, comme User Management. Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.
- Lorsque vous créez un compte utilisateur à l'aide de la commande `useradd`, vous devez spécifier l'option `-m` dans la syntaxe. Autrement, un répertoire personnel n'est pas créé pour l'utilisateur.

Par exemple, la commande suivante crée un répertoire personnel pour l'utilisateur `jdoe` :

```
# useradd -m jdoe
```

En revanche, la syntaxe suivante ne crée *pas* de répertoire personnel pour l'utilisateur :

```
# useradd jdoe
```

Remarque – La seule exception à cette règle se présente si vous souhaitez que le module `pam_zfs_key` crée un répertoire personnel chiffré pour l'utilisateur. Dans ce cas, n'ajoutez *pas* l'option `-m` à la commande `useradd`. Reportez-vous aux pages de manuel `pam_zfs_key(5)` et `zfs_encrypt(1M)`.

- La commande `useradd` crée des entrées dans la mappe `auto_home` *uniquement* si l'option `-d` est spécifiée avec `hostname:/pathname`. Dans le cas contraire, le chemin d'accès spécifié est mis à jour en tant que répertoire personnel de l'utilisateur dans la base de données `passwd` et aucune entrée n'est créée dans la mappe `auto_home`. Les répertoires personnels spécifiés dans la mappe de montage automatique `auto_home` sont montés uniquement si le service `autofs` est activé.

  Par exemple, si vous spécifiez l'option `-d` pour créer un utilisateur comme suit, il est créé sans entrée `auto_home`. D'autre part, l'entrée `passwd` spécifie `/export/home/user1` en tant que répertoire personnel de l'utilisateur :

  ```
  # useradd -d /export/home/user1 user1
  ```

  En revanche, si vous ajoutez l'option `-d` pour créer l'utilisateur comme suit, il est créé avec une entrée `auto_home`. D'autre part, la base de données `passwd` contient `/home/user1`, ce qui indique une dépendance au service `autofs` :

  ```
  # useradd -d localhost:/export/home/user1 user1
  ```

- Si le chemin d'accès au répertoire personnel comporte une spécification d'hôte distant (`foobar:/export/home/jdoe`, par exemple), le répertoire personnel de `jdoe` doit être créé sur le système `foobar`. Le chemin par défaut est `localhost:/export/home/`*username*.
- Lorsque ce système de fichiers est un jeu de données ZFS (ce qui est le cas dans Oracle Solaris 11), le répertoire personnel de l'utilisateur est créé sous la forme d'un jeu de données ZFS enfant, où l'autorisation ZFS de prendre des instantanés est déléguée à l'utilisateur. Lorsqu'un nom de chemin d'accès ne correspondant pas à un jeu de données ZFS est précisé, un répertoire standard est créé. Si l'option `-S ldap` est spécifiée, l'entrée de carte `auto_home` est mise à jour sur le serveur LDAP et non sur la carte `auto_home` locale.

▼ Ajout d'un utilisateur

Dans cette version, les comptes utilisateur sont créés en tant que systèmes de fichiers ZFS Oracle Solaris. Chaque répertoire personnel créé à l'aide des commandes `useradd` et `roleadd` place le répertoire personnel de l'utilisateur sur le système de fichiers `/export/home` en tant que système de fichiers ZFS *individuel*.

La commande `useradd` crée des entrées dans la mappe `auto_home` *uniquement* si l'option `-d` est spécifiée avec `hostname:/pathname`. Dans le cas contraire, le chemin d'accès spécifié est mis à jour en tant que répertoire personnel de l'utilisateur dans la base de données `passwd` et aucune entrée n'est créée dans la mappe `auto_home`. Les répertoires personnels spécifiés dans la mappe de montage automatique `auto_home` sont montés uniquement si le service `autofs` est activé.

1 Prenez le rôle `root` ou un rôle disposant du profil de droits User Management.

Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2 Créez un utilisateur local.

Par défaut, l'utilisateur est créé localement. Si vous incluez l'option `-S ldap`, l'utilisateur est créé dans un référentiel LDAP existant.

```
# useradd -d dir -m username
```

`useradd` Crée un compte pour l'utilisateur spécifié.

`-d` Indique l'emplacement du répertoire personnel de l'utilisateur.

Tapez `-d localhost:/export/home/` *username* au lieu de `-d /export/home/` *username* pour forcer l'écriture de l'entrée dans `auto_home`.

`-m` Crée un répertoire personnel local sur le système pour l'utilisateur.

Par exemple, si vous spécifiez l'option `-d` *dir* comme suit, l'utilisateur est créé sans entrée `auto_home`. D'autre part, l'entrée `passwd` spécifie `/export/home/user1` en tant que répertoire personnel de l'utilisateur :

```
# useradd -d /export/home/user1 user1
```

Si vous spécifiez l'option `-d` *dir* comme suit, l'utilisateur est associé à une entrée `auto_home`. D'autre part, la base de données `passwd` contient `/home/user1`, ce qui indique une dépendance au service `autofs` :

```
# useradd -d localhost:/export/home/user1 user1
```

Remarque – La seule exception à cette règle se présente si vous souhaitez que le module `pam_zfs_key` crée un répertoire personnel chiffré pour l'utilisateur. Dans ce cas, n'ajoutez *pas* l'option `-m` à la commande `useradd`. Reportez-vous à la section "Instructions relatives à la configuration des comptes utilisateur" à la page 47.

Pour une description détaillée des tous les arguments et options que vous pouvez spécifier à l'aide de la commande `useradd`, reportez-vous à la page de manuel `useradd(1M)`.

Remarque – Le compte est verrouillé jusqu'à ce que vous affectiez un mot de passe à l'utilisateur.

3 Affectez un mot de passe à l'utilisateur.

```
# passwd username
New password:       Type user password
Re-enter new password:       Retype password
```

Pour plus d'options de commande, reportez-vous aux pages de manuel `useradd(1M)` et `passwd(1)`.

Voir aussi Après avoir créé un utilisateur, vous devrez parfois effectuer d'autres tâches, et notamment ajouter et attribuer des rôles, répertorier et modifier les profils de droits ou encore modifier les propriétés RBAC d'un utilisateur. Pour plus d'informations, reportez-vous aux références suivantes :

- "Procédure de création d'un rôle" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité* et "Procédure d'attribution de rôle" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*
- "Procédure d'affichage de tous les attributs de sécurité définis" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*
- "Création d'un profil de droits" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*
- "Modification des attributs de sécurité d'un utilisateur" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

▼ Modification d'un utilisateur

La commande `usermod` permet de changer la définition de l'identifiant de connexion d'un utilisateur et d'apporter des modifications au système de fichiers dans le cadre de la connexion.

1. **Prenez le rôle `root` ou un rôle disposant du profil de droits User Management.**

   Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2. **Apportez les modifications nécessaires au compte utilisateur.**

   Pour plus d'informations sur les arguments et les options que vous pouvez spécifier avec la commande `usermod`, reportez-vous à la page de manuel `usermod(1M)`.

   Par exemple, pour attribuer un rôle à un utilisateur, il faut taper :

   ```
   # usermod -R role username
   ```

Exemple 2–1 Définition d'une stratégie PAM par utilisateur en modifiant le compte d'un utilisateur

L'exemple suivant illustre la procédure à suivre pour modifier un utilisateur en vue de définir la stratégie PAM. Cette modification spécifie que l'utilisateur `jdoe` doit être authentifié via le protocole Kerberos V5 exclusivement pour les services PAM. Pour plus d'informations, reportez-vous à la page de manuel `pam_user_policy(5)`.

```
# usermod -K pam_policy=krb5_only jdoe
```

Voir aussi Reportez-vous aux références suivantes pour d'autres exemples de modification d'un utilisateur :

- "Procédure d'attribution de rôle" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*
- "Modification des attributs de sécurité d'un utilisateur" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

▼ Suppression d'un utilisateur

1. **Prenez le rôle `root`**

   ```
   $ su -
   Password:
   #
   ```

   Remarque – Cette méthode fonctionne aussi bien lorsque `root` est un compte utilisateur que lorsqu'il est un rôle.

2. **Archivez le répertoire personnel de l'utilisateur.**

3 **Exécutez l'une des commandes suivantes :**

- **Si l'utilisateur dispose d'un répertoire personnel local, supprimez l'utilisateur et le répertoire personnel.**

  `# userdel -r` *username*

  `usesrdel` Supprime le compte de l'utilisateur spécifié.

  `-r` Supprime le compte du système.

  Etant donné que les répertoires personnels sont maintenant des jeux de données ZFS, la méthode recommandée de suppression d'un répertoire personnel local d'un utilisateur supprimé est d'indiquer l'option `-r` avec la commande `userdel`.

- **Autrement, supprimez uniquement l'utilisateur.**

  `# userdel` *username*

  Vous devez supprimer manuellement le répertoire personnel de l'utilisateur sur le serveur distant.

Pour la liste complète des options de commande, reportez-vous à la page de manuel `userdel(1M)`.

Étapes suivantes Un nettoyage supplémentaire peut être nécessaire si l'utilisateur que vous avez supprimé avait des responsabilités d'administration, par exemple la création de tâches `cron`, ou si l'utilisateur dispose de comptes supplémentaires dans des zones non globales.

▼ Ajout d'un groupe

Lorsqu'un administrateur crée un groupe, le système attribue l'autorisation `solaris.group.assign /`*groupname* à cet administrateur, ce qui lui permet d'exercer un contrôle total sur le groupe. Si un autre administrateur disposant de la même autorisation crée un groupe, il contrôle le groupe. Un administrateur qui contrôle un groupe ne peut en aucun cas gérer le groupe de l'autre administrateur. Pour plus d'informations, reportez-vous aux pages de manuel `groupadd`(1M) et `groupmod` (1M).

1 **Prenez le rôle `root` ou un rôle d'administrateur disposant de l'autorisation `solaris.group.manage`.**

Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2 **Répertoriez les groupes existants.**

```
# cat /etc/group
```

3 Créez un nouveau groupe.

```
$ groupadd -g 18 exadata
```

`groupadd` Crée une nouvelle définition de groupe sur le système en ajoutant l'entrée appropriée au fichier `/etc/group`.

`-g` Affecte l'ID de groupe du nouveau groupe.

Pour plus d'informations, reportez-vous à la page de manuel `groupadd(1M)`.

Exemple 2–2 Configuration d'un groupe et d'un utilisateur à l'aide des commandes `groupadd` et `useradd`

L'exemple suivant illustre comment utiliser les commandes `groupadd` et `useradd` pour ajouter le groupe `scutters` et l'utilisateur `scutter1` dans les fichiers du système local.

```
# groupadd -g 102 scutters
# useradd -u 1003 -g 102 -d /export/home/scutter1 -s /bin/csh \
-c "Scutter 1" -m -k /etc/skel scutter1
64 blocks
```

Pour plus d'informations, reportez-vous aux pages de manuel `groupadd(1M)` et `useradd(1M)`.

▼ Partage de répertoires personnels créés en tant que systèmes de fichiers ZFS

Dans cette version d'Oracle Solaris, il est possible de partager un système de fichiers ZFS en définissant la propriété `share.nfs` ou `share.smb`. Vous pouvez également créer un partage de système de fichiers à l'aide de la commande `zfs share`. Par défaut, aucun système de fichiers n'est partagé.

Par défaut, le jeu de données `pool/export/home` est déjà monté sur `/export/home`. La commande `useradd` crée automatiquement les jeux de données par utilisateur en tant qu'enfants de ce jeu de données. En tant qu'administrateur, vous pouvez choisir de créer un nouveau pool pour les répertoires personnels des utilisateurs. La procédure ci-dessous indique les étapes à suivre.

Pour plus d'informations sur le partage et l'annulation du partage des systèmes de fichiers, reportez-vous à la section "Activation et annulation du partage des systèmes de fichiers ZFS" du manuel *Administration d'Oracle Solaris 11.1 : Systèmes de fichiers ZFS*.

1 Prenez le rôle `root`.

Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2 **Créez un pool distinct pour les répertoires personnels des utilisateurs. Par exemple :**

```
# zpool create users mirror c1t1d0 c1t2d0 mirror c2t1d0 c2t2d0
```

3 **Créez un conteneur pour les répertoires personnels. Par exemple :**

```
# zfs create users/home
```

4 **Définissez les propriétés de partage du répertoire personnel. Par exemple, pour créer un partage NFS et définir la propriété `share.nfs` pour `users/home`, tapez :**

```
# zfs set share.nfs=on users/home
```

Dans cette nouvelle syntaxe, chaque système de fichiers contient un paramètre "auto share" créé dès que la propriété `share.nfs` (ou `share.smb`) est définie sur `on` pour ce système de fichiers. La commande précédente partage un système de fichiers nommé `users/home` et tous ses enfants.

5 **Confirmez que les partages de systèmes de fichiers descendants sont également publiés. Par exemple :**

```
# zfs get -r share.nfs users/home
```

L'option `-r` affiche tous les systèmes de fichiers descendants.

Montage manuel du répertoire personnel d'un utilisateur

Les comptes utilisateur créés en tant que systèmes de fichiers ZFS n'ont généralement pas besoin d'être montés manuellement. Avec ZFS, les systèmes de fichiers sont montés automatiquement au moment de leur création, puis montés lors de l'initialisation à partir du service de système de fichiers local SMF.

Lors de la création de comptes utilisateur, assurez-vous que les répertoires personnels sont configurés de la même manière que dans le service de noms, sous `/home/`*nom-utilisateur*. Assurez-vous ensuite que la mappe `auto_home` indique le chemin NFS du répertoire personnel de l'utilisateur. Pour plus d'informations sur les tâches, reportez-vous à la section "Présentation des tâches d'administration Autofs" du manuel *Gestion de systèmes de fichiers réseau dans Oracle Solaris 11.1*.

Si vous avez besoin de monter manuellement le répertoire personnel d'un utilisateur, vous pouvez utiliser la commande `zfs mount`. Par exemple :

```
# zfs mount users/home/alice
```

Remarque – Assurez-vous que le répertoire personnel de l'utilisateur est partagé. Pour plus d'informations, reportez-vous à la section "Partage de répertoires personnels créés en tant que systèmes de fichiers ZFS" à la page 53.

◆ ◆ ◆ CHAPITRE 3

Gestion des comptes utilisateur dans l'interface graphique du Gestionnaire d'utilisateurs (tâches)

Ce chapitre présente les opérations de configuration et de gestion des utilisateurs dans l'interface graphique du Gestionnaire d'utilisateurs Oracle Solaris. Dans l'interface graphique du Gestionnaire d'utilisateurs, vous pouvez effectuer la plupart des tâches réalisables avec l'interface de ligne de commande (et notamment exécuter les fonctions correspondant aux commandes `useradd`, `usermod` et `userdel`). Pour plus d'informations sur le Gestionnaire d'utilisateurs, reportez-vous à l'aide en ligne.

Les informations contenues dans ce chapitre sont répertoriées ci-après :

Pour des informations générales sur la gestion des comptes utilisateur, reportez-vous au Chapitre 1, "Gestion des comptes et des environnements utilisateur (présentation)".

Pour plus d'informations sur la gestion des comptes utilisateur avec l'interface de ligne de commande, reportez-vous au Chapitre 2, "Gestion des comptes utilisateur avec l'interface de ligne de commande (tâches)".

Présentation de l'interface graphique du Gestionnaire d'utilisateurs

Les informations suivantes sont décrites dans cette section :

- "Endossement d'un rôle ou modification des informations d'identification d'un utilisateur" à la page 61

Le Gestionnaire d'utilisateurs repose sur l'architecture Visual Panels et offre une interface incluant des panneaux visuels. Il est possible de gérer à distance les utilisateurs et les rôles par le biais du démon RAD (Remote Administration Daemon). L'interface graphique dépend du module RAD du Gestionnaire d'utilisateurs/de rôles pour effectuer toutes ses opérations. Le module RAD appelle les interfaces de ligne de commande RBAC (contrôle d'accès basé sur les rôles) qui effectuent toutes les fonctions d'administration de l'interface graphique.

Les opérations d'authentification des utilisateurs et d'endossement de rôle sont assurées par l'architecture Visual Panels elle-même et sont accessibles depuis l'ensemble des panneaux, y compris le panneau User Manager (Gestionnaire d'utilisateurs). L'interface graphique du Gestionnaire d'utilisateurs remplace la console de gestion des utilisateurs et des rôles prise en charge dans Oracle Solaris 10. Bien qu'elle ne soit pas tout à fait identique à la console de gestion Solaris, l'interface graphique offre certaines de ses fonctionnalités. Notez que la console de gestion Solaris n'est *pas* prise en charge dans cette version.

Le Gestionnaire d'utilisateurs propose une interface claire et simple d'utilisation. Pour réduire les risques d'erreurs, l'interface graphique présente uniquement des choix valides en fonction des autorisations et des profils de droits accordés à l'utilisateur ou au rôle authentifié. Vous pouvez effectuer les mêmes tâches dans l'interface graphique et avec l'interface de ligne de commande, et notamment exécuter les fonctions correspondant aux commandes `useradd`, `usermod`, `userdel`, `roleadd` et `groupadd`. Pour plus d'informations sur la gestion des utilisateurs et des rôles avec l'interface de ligne de commande, reportez-vous au Chapitre 2, "Gestion des comptes utilisateur avec l'interface de ligne de commande (tâches)".

L'interface graphique du Gestionnaire d'utilisateurs est fournie dans le package IPS `pkg:/system/management/visual-panels/panel-usermgr`.

Démarrage de l'interface graphique du Gestionnaire d'utilisateurs

▼ Démarrage du Gestionnaire d'utilisateurs

1 Prenez le rôle `root` ou connectez-vous en tant qu'utilisateur disposant du profil de droits User Management.

Reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2 **Démarrez le Gestionnaire d'utilisateurs en suivant l'une des méthodes ci-dessous :**

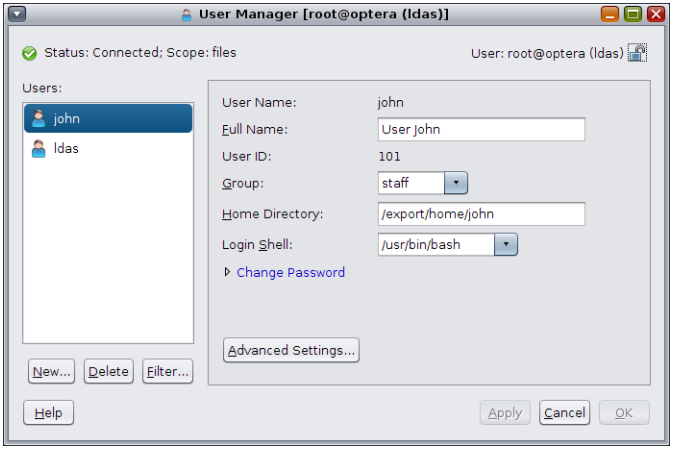
- **Sur le bureau, sélectionnez System (Système) → Administration → User Manager (Gestionnaire d'utilisateurs).**
- **Dans la ligne de commande, tapez :**

```
# vp usermgr &
```

Organisation du panneau User Manager (Gestionnaire d'utilisateurs)

Lorsque vous démarrez l'interface graphique, le panneau principal User Manager (Gestionnaire d'utilisateurs) s'affiche. Le panneau User Manager (Gestionnaire d'utilisateurs) permet d'administrer les utilisateurs et les rôles. Dans la partie gauche du panneau, le champ Status (Statut) indique le statut des services en cours d'exécution sur l'hôte local. Un champ User (Utilisateur) se trouve dans la partie droite du panneau. Ce champ contient les informations d'identification que l'interface graphique du Gestionnaire d'utilisateurs emploie actuellement. Pour modifier les informations d'identification, cliquez sur le bouton représentant un cadenas placé dans la partie droite du panneau. Reportez-vous à la section "Endossement d'un rôle ou modification des informations d'identification d'un utilisateur" à la page 61.

La capture d'écran suivante présente le panneau principal User Manager (Gestionnaire d'utilisateurs).



Le panneau User Manager (Gestionnaire d'utilisateurs) inclut les composants suivants

- La liste des utilisateurs et des rôles vous permet de sélectionner l'entrée que vous souhaitez administrer.
- Les paramètres de base affichent les informations essentielles d'un utilisateur, comme son nom d'utilisateur et son nom complet.

Pour consulter ou modifier les informations d'un utilisateur existant, sélectionnez-le dans la liste affichée. Dès que vous sélectionnez un utilisateur, ses informations s'affichent dans la partie droite du panneau.

Vous pouvez effectuer les opérations suivantes dans le panneau User Manager (Gestionnaire d'utilisateurs) :

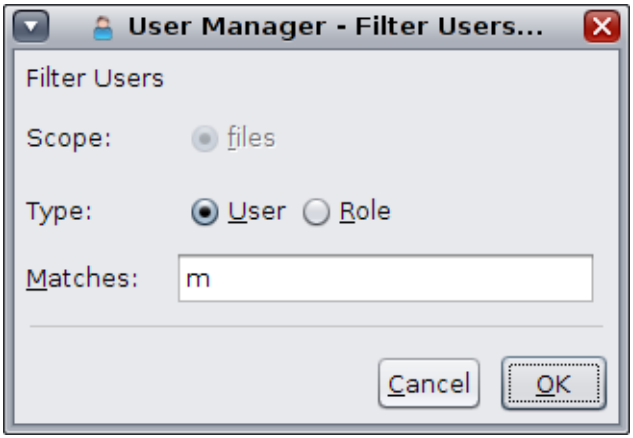
- Créer un utilisateur ou un rôle. Reportez-vous à la section "Ajout d'un utilisateur ou d'un rôle dans le Gestionnaire d'utilisateurs" à la page 62.
- Supprimer un utilisateur ou un rôle existant. Reportez-vous à la section "Suppression d'un utilisateur ou d'un rôle dans l'interface graphique du Gestionnaire d'utilisateurs" à la page 65
- Filtrer les informations d'un utilisateur. Reportez-vous à la section "Sélection du type et de l'étendue du service de noms par défaut" à la page 60.
- Administrer les paramètres avancés d'un utilisateur existant. Reportez-vous à la section "Modification d'un utilisateur ou d'un rôle dans le Gestionnaire d'utilisateurs" à la page 64.

Sélection du type et de l'étendue du service de noms par défaut

Le type et l'étendue du service de noms par défaut de l'interface graphique du Gestionnaire d'utilisateurs sont respectivement `User` (Utilisateur) et `files` (fichiers). Pour administrer l'interface graphique du Gestionnaire d'utilisateurs au sein d'une autre étendue, `ldap` et `roles` (rôles) par exemple, cliquez sur le bouton Filter (Filtrer). Une boîte de dialogue s'ouvre alors, dans laquelle vous pouvez modifier le type ou l'étendue par défaut, ou les deux.

- Les choix de l'option Scope (Etendue) sont `files` (fichiers) et `ldap`.
- Les choix de l'option Type sont `User` (Utilisateur) et `Role` (Rôle). Cliquez sur OK pour enregistrer les changements.

Cliquez sur Cancel (Annuler) pour annuler l'opération.



Remarque – Si le système n'est pas configuré en tant que client `ldap`, seule l'étendue `files` est disponible.

Endossement d'un rôle ou modification des informations d'identification d'un utilisateur

Une personne disposant du profil de droits User Management peut créer de nouveaux utilisateurs, à condition que les attributs avancés de l'utilisateur ou du rôle à créer soient un sous-ensemble de ceux de l'utilisateur qui assure l'administration. Si l'utilisateur chargé de l'administration ne possède pas les autorisations suffisantes, mais un rôle d'administration avec les autorisations suffisantes, il peut jouer ce rôle pour effectuer les opérations d'administration nécessaires en cliquant sur le bouton représentant un cadenas dans le panneau principal User Manager (Gestionnaire d'utilisateurs).

▼ Modification des informations d'identification d'un utilisateur

1 **Démarrez le Gestionnaire d'utilisateurs.**

Reportez-vous à la section "Démarrage du Gestionnaire d'utilisateurs" à la page 58.

2 **Dans le panneau User Manager (Gestionnaire d'utilisateurs), cliquez sur l'icône représentant un cadenas pour ouvrir un sous-menu contenant les options suivantes :**

- Change Role (Changer de rôle)
- Change User (Changer d'utilisateur)
- Administer New Host (Administrer un nouvel hôte)
- Clear History (Effacer l'historique)

3 **Sélectionnez l'option Change Role (Changer de rôle).**

Une boîte de dialogue d'authentification s'ouvre. Cette boîte de dialogue contient un menu déroulant qui répertorie les rôles disponibles pour l'utilisateur spécifié.

4 **Sélectionnez le rôle approprié, puis cliquez sur Log in (Connexion) pour modifier le rôle.**

Après avoir endossé ce rôle, vous pouvez effectuer les tâches d'administration requises.

Ajout, modification et suppression d'utilisateurs et de rôles dans l'interface graphique du Gestionnaire d'utilisateurs

Dans l'interface graphique du Gestionnaire d'utilisateurs, les opérations d'ajout, de modification et de suppression reviennent à exécuter les commandes respectives `useradd`, `usermod` et `userdel`. Pour plus d'informations sur l'ajout d'utilisateurs avec la ligne de commande, reportez-vous au Chapitre 2, “Gestion des comptes utilisateur avec l'interface de ligne de commande (tâches)”.

Les informations suivantes sont décrites dans cette section :

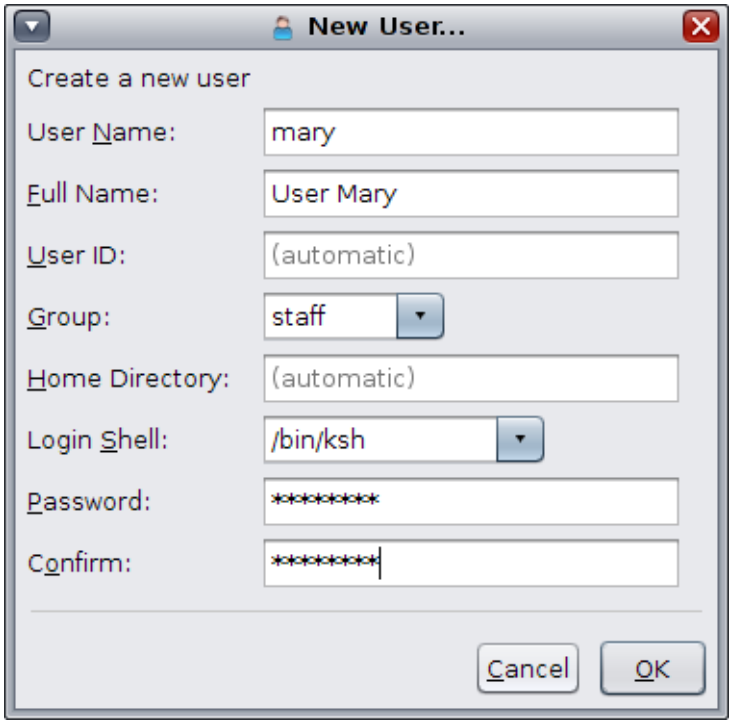
▼ Ajout d'un utilisateur ou d'un rôle dans le Gestionnaire d'utilisateurs

1 **Démarrez le Gestionnaire d'utilisateurs.**

Reportez-vous à la section “Démarrage du Gestionnaire d'utilisateurs” à la page 58.

2 **Pour ajouter un nouvel utilisateur ou un nouveau rôle dans l'étendue du filtre actuellement appliqué par l'interface graphique, cliquez sur le bouton New (Nouveau) dans le panneau principal User Manager (Gestionnaire d'utilisateurs).**

La boîte de dialogue New User (Nouvel utilisateur) s'ouvre.



3 **Dans la boîte de dialogue New User (Nouvel utilisateur), renseignez les champs suivants :**

- Nom d'utilisateur
- Nom complet
- Identifiant utilisateur

  Ce champ est facultatif. Si vous ne fournissez pas cette information, le système définit automatiquement une valeur par défaut.

- Groupe

  Les choix disponibles pour le champ Group (Groupe) varient selon la configuration du système.

- Répertoire personnel

  Ce champ est facultatif. Si vous ne fournissez pas cette information, le système définit automatiquement une valeur par défaut.

Si vous souhaitez que le répertoire personnel de l'utilisateur soit monté automatiquement, faites précéder le chemin d'accès du nom d'hôte ou d'un hôte local. Par exemple : `localhost:/export/home/test1`.

- Shell de connexion

  Les choix disponibles pour le champ Login Shell (Shell de connexion) varient selon la configuration du système.

- Mot de passe

  Attribuez un mot de passe temporaire à l'utilisateur.

- Confirmer

  Confirmez le mot de passe temporaire attribué à l'utilisateur.

Remarque – Il faut impérativement renseigner les champs obligatoires.

---

4 **Pour créer le nouvel utilisateur ou le nouveau rôle, puis l'ajouter à la liste des utilisateurs affichés dans le panneau principal User Manager (Gestionnaire d'utilisateurs), cliquez sur OK.**

Pour annuler l'opération, cliquez sur Cancel (Annuler).

▼ Modification d'un utilisateur ou d'un rôle dans le Gestionnaire d'utilisateurs

1 **Démarrez le Gestionnaire d'utilisateurs.**

Reportez-vous à la section "Démarrage du Gestionnaire d'utilisateurs" à la page 58.

2 **Pour modifier un utilisateur ou un rôle existant, sélectionnez-le dans la liste figurant dans le panneau principal User Manager (Gestionnaire d'utilisateurs).**

Dès que vous sélectionnez un utilisateur, la partie droite du panneau affiche des informations le concernant.

3 **Modifiez tout ou partie des informations relatives à l'utilisateur ou au rôle en question.**

Remarque – Le cas échéant, un indicateur s'affiche en regard des champs modifiés.

---

4 **Cliquez sur Apply (Appliquer) pour enregistrer les modifications apportées.**

5 **(Facultatif) Cliquez sur le bouton Advanced Settings (Paramètres avancés) pour modifier d'autres attributs de sécurité pour l'utilisateur ou le rôle. Reportez-vous à la section "Administration des paramètres avancés dans l'interface graphique du Gestionnaire d'utilisateurs" à la page 65.**

6 **Cliquez sur OK pour enregistrer les modifications et fermer le panneau User Manager (Gestionnaire d'utilisateurs).**

Cliquez sur Cancel (Annuler) pour annuler vos modifications non enregistrées et fermer le panneau.

Suppression d'un utilisateur ou d'un rôle dans l'interface graphique du Gestionnaire d'utilisateurs

Pour supprimer un utilisateur ou un rôle dans l'étendue du filtre actuellement appliqué par l'interface graphique, sélectionnez-le dans le panneau principal User Manager (Gestionnaire d'utilisateurs), puis cliquez sur le bouton de suppression. Pour enregistrer les modifications, cliquez sur OK dans la boîte de dialogue de confirmation qui s'ouvre. Pour annuler l'opération, cliquez sur Cancel (Annuler).

Administration des paramètres avancés dans l'interface graphique du Gestionnaire d'utilisateurs

Les informations suivantes sont décrites dans cette section :

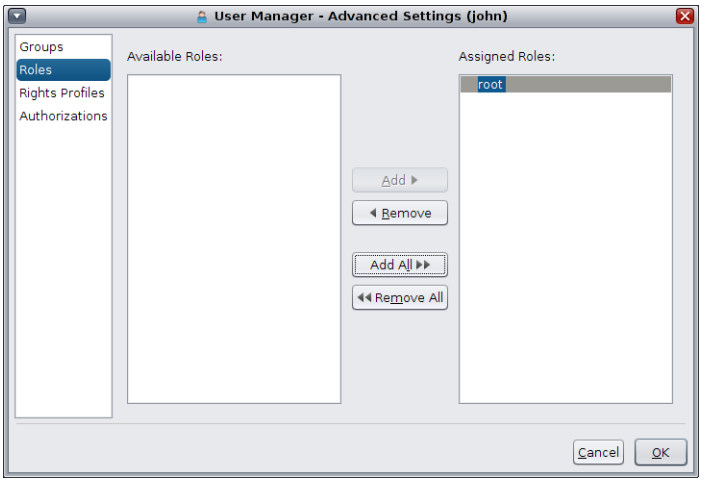
Ouvrez la boîte de dialogue Advanced Settings (Paramètres avancés) du Gestionnaire d'utilisateurs pour associer d'autres attributs de sécurité (comme des profils de droits, des rôles et des autorisations) à un utilisateur.

Pour une présentation des fonctions de sécurité prises en charge par Oracle Solaris, reportez-vous à la Partie I, "Présentation de la sécurité" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*. Pour une présentation détaillée du fonctionnement du contrôle d'accès basé sur les rôles (RBAC) dans cette version, reportez-vous à la Partie III, "Rôles, profils de droits et privilèges" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

Pour administrer les attributs avancés d'un utilisateur ou d'un rôle, sélectionnez ce dernier dans le panneau principal User Manager (Gestionnaire d'utilisateurs), puis cliquez sur le bouton Advanced Settings (Paramètres avancés). Le panneau Advanced Settings (Paramètres avancés)

correspondant à l'utilisateur ou au rôle sélectionné s'affiche. Le nom de l'utilisateur apparaît entre parenthèses dans la partie supérieure du panneau.

La capture d'écran suivante présente le panneau Advanced Settings (Paramètres avancés), qui indique l'attribut de sécurité Roles (Rôles) de l'utilisateur nommé john.



Il est possible de gérer les attributs de sécurité suivants dans le panneau Advanced Settings (Paramètres avancés) :

- Groups (Groupes)
- Roles (Rôles)
- Rights Profiles (Profils de droits)
- Authorizations (Autorisations)

Administration des groupes dans l'interface graphique du Gestionnaire d'utilisateurs

Il faut cliquer sur le bouton Advanced Settings (Paramètres avancés) dans le panneau principal User Manager (Gestionnaire d'utilisateurs) de l'interface graphique pour gérer les groupes.

▼ Administration des groupes

1 Démarrez le Gestionnaire d'utilisateurs.

Reportez-vous à la section "Démarrage du Gestionnaire d'utilisateurs" à la page 58.

2. **Sélectionnez un utilisateur dans le panneau principal User Manager (Gestionnaire d'utilisateurs), puis cliquez sur le bouton Advanced Settings (Paramètres avancés).**

   Le panneau Advanced Settings (Paramètres avancés) s'affiche.

3. **Cliquez sur l'attribut Groups (Groupes) dans la partie gauche du panneau.**

   La liste des groupes disponibles et la liste des groupes auxquels appartient l'utilisateur s'affichent.

   - **Pour intégrer l'utilisateur dans un ou plusieurs groupes, sélectionnez les entrées souhaitées dans la liste Available Groups (Groupes disponibles), puis cliquez sur Add (Ajouter).**

     Le groupe ajouté figure ensuite dans la liste Assigned Groups (Groupes affectés).

   - **Pour supprimer un groupe de la liste Assigned Groups (Groupes affectés), sélectionnez-le puis cliquez sur Remove (Supprimer).**

   - **Pour ajouter ou supprimer l'intégralité des groupes, cliquez sur le bouton Add All (Tout ajouter) ou Remove All (Tout supprimer).**

4. **Cliquez sur OK pour enregistrer les paramètres.**

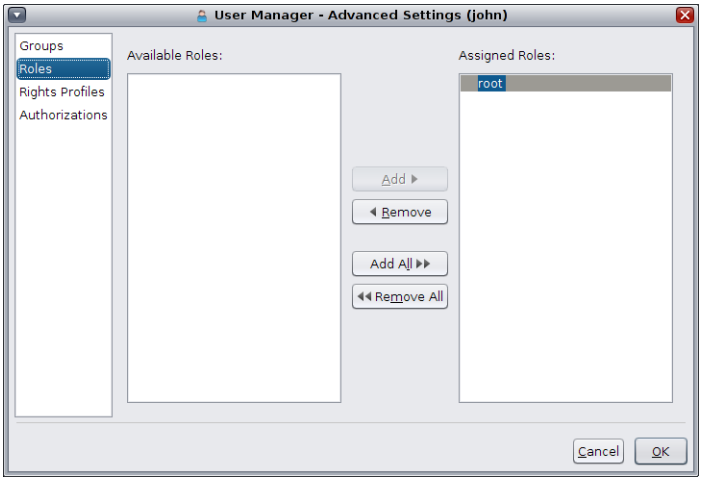
   Les modifications sont appliquées uniquement lorsque vous cliquez sur Apply (Appliquer) ou OK dans le panneau principal User Manager (Gestionnaire d'utilisateurs).

Administration des rôles dans l'interface graphique du Gestionnaire d'utilisateurs

Il faut cliquer sur le bouton Advanced Settings (Paramètres avancés) dans le panneau principal User Manager (Gestionnaire d'utilisateurs) de l'interface graphique pour gérer les rôles.

Remarque – L'attribut Roles (Rôles) est disponible uniquement pour un utilisateur (et non pour un rôle) car les rôles ne peuvent être attribués qu'à des utilisateurs.

La capture d'écran suivante présente le panneau Advanced Settings (Paramètres avancés), qui indique l'attribut de sécurité Roles (Rôles) de l'utilisateur nommé john.



Administration des rôles dans le Gestionnaire d'utilisateurs

1. **Démarrez le Gestionnaire d'utilisateurs.**

   Reportez-vous à la section "Démarrage du Gestionnaire d'utilisateurs" à la page 58.

2. **Sélectionnez un utilisateur dans le panneau principal User Manager (Gestionnaire d'utilisateurs), puis cliquez sur le bouton Advanced Settings (Paramètres avancés).**

   Le panneau Advanced Settings (Paramètres avancés) s'affiche.

3. **Cliquez sur l'attribut Roles (Rôles) dans la partie gauche du panneau.**

   La liste des rôles disponibles et la liste des rôles attribués à l'utilisateur s'affichent.

   - **Pour attribuer un ou plusieurs rôles à l'utilisateur, sélectionnez les entrées souhaitées dans la liste Available Roles (Rôles disponibles), puis cliquez sur Add (Ajouter).**

     Le rôle ajouté figure ensuite dans la liste Assigned Roles (Rôles affectés).

   - **Pour supprimer un rôle de la liste Assigned Roles (Rôles affectés), sélectionnez-le puis cliquez sur Remove (Supprimer).**

   - **Pour ajouter ou supprimer l'intégralité des rôles, cliquez sur le bouton Add All (Tout ajouter) ou Remove All (Tout supprimer).**

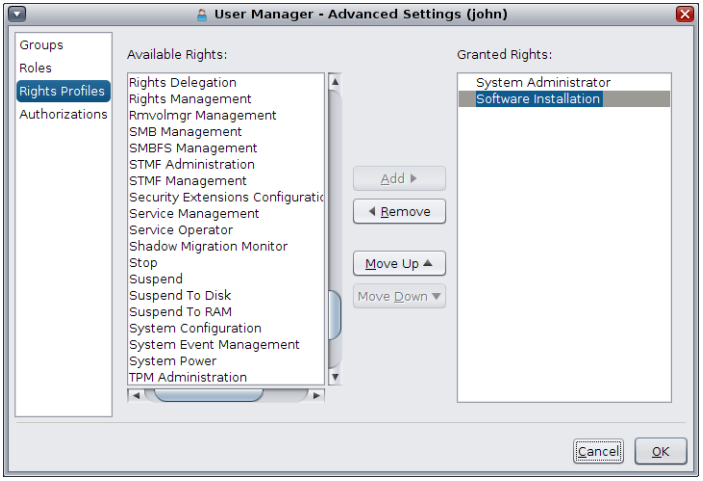
4. **Cliquez sur OK pour enregistrer les paramètres.**

   Les modifications sont appliquées uniquement lorsque vous cliquez sur Apply (Appliquer) ou OK dans le panneau principal User Manager (Gestionnaire d'utilisateurs).

Administration des profils de droits dans l'interface graphique du Gestionnaire d'utilisateurs

Il faut cliquer sur le bouton Advanced Settings (Paramètres avancés) dans le panneau principal User Manager (Gestionnaire d'utilisateurs) de l'interface graphique pour gérer les profils de droits.

La capture d'écran suivante présente le panneau Advanced Settings (Paramètres avancés), qui indique l'attribut de sécurité Rights Profile (Profils de droits) de l'utilisateur nommé john.



Remarque – Les profils de droits sont classés par ordre de priorité. Le cas échéant, cliquez sur les boutons Move Up (Déplacer vers le haut) et Move Down (Déplacer vers le bas) pour modifier l'ordre des profils de droits octroyés à l'utilisateur sélectionné.

▼ Administration des profils de droits dans le Gestionnaire d'utilisateurs

1 **Démarrez le Gestionnaire d'utilisateurs.**

Reportez-vous à la section "Démarrage du Gestionnaire d'utilisateurs" à la page 58.

2 **Sélectionnez un utilisateur dans le panneau principal User Manager (Gestionnaire d'utilisateurs), puis cliquez sur le bouton Advanced Settings (Paramètres avancés).**

Le panneau Advanced Settings (Paramètres avancés) s'affiche.

3 **Cliquez sur l'attribut Rights Profiles (Profils de droits) dans la partie gauche du panneau.**

La liste des profils de droits disponibles et la liste des profils de droits octroyés à l'utilisateur s'affichent.

- **Pour octroyer un ou plusieurs profils de droits à l'utilisateur, sélectionnez les entrées souhaitées dans la liste Available Rights (Droits disponibles), puis cliquez sur Add (Ajouter).**

  Le profil de droits ajouté figure ensuite dans la liste Granted Rights (Droits octroyés).

- **Pour supprimer un profil de droits de la liste Granted Rights (Droits octroyés), sélectionnez-le puis cliquez sur Remove (Supprimer).**

- **Pour ajouter ou supprimer l'intégralité des profils de droits, cliquez sur le bouton Add All (Tout ajouter) ou Remove All (Tout supprimer).**

4 **Cliquez sur OK pour enregistrer les paramètres.**

Les modifications sont appliquées uniquement lorsque vous cliquez sur Apply (Appliquer) ou OK dans le panneau principal User Manager (Gestionnaire d'utilisateurs).

Administration des autorisations dans l'interface graphique du Gestionnaire d'utilisateurs

Des autorisations sont généralement accordées à un utilisateur de façon indirecte par le biais d'un profil de droits. Il est possible de configurer des paramètres pour octroyer une autorisation spécifique à un utilisateur ou un rôle. Certaines autorisations peuvent inclure des attributs supplémentaires, comme un nom d'objet. Par exemple, lorsqu'un administrateur crée le groupe `games`, il reçoit l'autorisation implicite `solaris.group.manage/games`. Les noms d'objets figurent ensuite dans la liste Granted Authorizations (Autorisations octroyées).

▼ Administration des autorisations dans le Gestionnaire d'utilisateurs

1 **Démarrez le Gestionnaire d'utilisateurs.**

Reportez-vous à la section "Démarrage du Gestionnaire d'utilisateurs" à la page 58.

2 **Sélectionnez un utilisateur dans le panneau principal User Manager (Gestionnaire d'utilisateurs), puis cliquez sur le bouton Advanced Settings (Paramètres avancés).**

Le panneau Advanced Settings (Paramètres avancés) s'affiche.

3. **Cliquez sur l'attribut Authorizations (Autorisations) dans la partie gauche du panneau.**

   La liste des autorisations disponibles et la liste des autorisations octroyées à l'utilisateur s'affichent.

   - **Pour attribuer une ou plusieurs autorisations à l'utilisateur, sélectionnez les entrées souhaitées dans la liste Available Authorizations (Autorisations disponibles), puis cliquez sur Add (Ajouter).**

     L'autorisation ajoutée figure ensuite dans la liste Granted Authorizations (Autorisations octroyées).

   - **Pour supprimer une autorisation de la liste Granted Authorizations (Autorisations octroyées), sélectionnez-la puis cliquez sur Remove (Supprimer).**

   - **Pour ajouter ou supprimer l'intégralité des autorisations, cliquez sur le bouton Add All (Tout ajouter) ou Remove All (Tout supprimer).**

4. **Cliquez sur OK pour enregistrer les paramètres.**

   Les modifications sont appliquées uniquement lorsque vous cliquez sur Apply (Appliquer) ou OK dans le panneau principal User Manager (Gestionnaire d'utilisateurs).

Index

L

M

N

P

V