Gestión de las cuentas de usuario y los entornos de usuario en Oracle® Solaris 11.2

Referencia: E53830-02
Septiembre de 2014

ORACLE®

Contenido

Uso de esta documentación

- **Descripción general**: describe la gestión de cuentas de usuario y entornos de usuario.
- **Destinatarios**: administradores del sistema que usan la versión 11 de Oracle Solaris.
- **Conocimientos necesarios**: experiencia en la administración de sistemas UNIX.

Biblioteca de documentación del producto

En la biblioteca de documentación (http://www.oracle.com/pls/topic/lookup?ctx=E56339), se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

Los clientes de Oracle tienen acceso a soporte electrónico por medio de My Oracle Support. Para obtener más información, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o, si tiene alguna discapacidad auditiva, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs.

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Acerca de las cuentas de usuario y los entornos de usuario

En este capítulo, se describe la gestión de cuentas de usuario y entornos de usuario, incluidos los siguientes temas:

Parea obtener información relacionada con la tarea sobre cómo gestionar las cuentas de usuario y los entornos de usuario, consulte el Capítulo 2, Gestión de cuentas de usuario mediante la interfaz de línea de comandos y el Capítulo 3, Gestión de cuentas de usuarios mediante el uso de la interfaz gráfica de usuario de User Manager.

Novedades de la gestión de cuentas de usuario en Oracle Solaris 11.2

En esta sección, se describen las funciones que son nuevas o que cambiaron en esta versión:

Opciones de inicio de sesión ampliadas durante el cierre

Cuando el comando `shutdown`cierra un sistema, el proceso de crea un archivo `/etc/nologin`. Este archivo muestra un mensaje que indica que el sistema se va a cerrar y que no son posibles los inicios de sesión. Como alternativa, un superusuario puede crear y gestionar este archivo `/etc/nologin` por separado.

Este tipo de cierre no bloquea el inicio de sesión del superusuario. A partir de esta versión, los siguientes usuarios adicionales no se bloquean cuando el archivo `nologin` está presente en el sistema:

- Los usuarios asignados con el rol root
- Los usuarios asignados con la autorización `solaris.system.maintenance`

Para obtener más información, consulte las páginas del comando man `nologin`(4) y `shutdown`(1M).

Cambios de seguridad que afectan la gestión de cuentas de usuario

Los administradores del sistema que gestionan las cuentas de usuario debe tener en cuenta que las siguientes funciones de seguridad cambiaron en esta versión:

- Los privilegios específicos extendidos se pueden aplicar a objetos de archivos, números de puerto e ID de usuario. Estos privilegios extendidos reemplazan el conjunto de privilegios que, de lo contrario, están disponibles, excepto para el conjunto básico.

  Para obtener una explicación acerca de los privilegios del usuario, consulte "Ampliación de los privilegios de un usuario o rol" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

  Para obtener instrucciones, consulte el Capítulo 4, "Asignación de derechos a aplicaciones, secuencia de comandos y recursos" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ". Consulte también las páginas del comando man `ppriv`(1) o `privileges`(5).
- Puede definir el derecho `auth_profiles` para que los usuarios deban proporcionar una contraseña antes de ejecutar un comando asignado mediante un perfil de derechos. La contraseña es efectiva por un período de tiempo configurable.

  La palabra clave `AUTH_PROFS_GRANTED` del archivo `policy.conf` establece el requisito de contraseña para ejecutar un comando con privilegios para todos los usuarios de un sistema.

  Para obtener más información, consulte "La ampliación de los derechos de usuario" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ". Consulte también las páginas del comando man `useradd`(1M) y `usermod`(1M).

¿Qué son las cuentas de usuario y los grupos?

Esta sección describe la siguiente información:

- “Directrices para asignar nombres de usuario, ID de usuario e ID de grupo” [17]

Una cuenta de usuario típica incluye la información que un usuario necesita para iniciar sesión y usar un sistema sin tener la contraseña `root` del sistema. Los componentes de cuentas de usuario se describen en “Componentes de cuentas de usuario” [11].

Al configurar una cuenta de usuario, puede agregar el usuario a un grupo de usuarios predefinido. Un uso típico de grupos es configurar permisos de grupo en un archivo y un directorio, lo que permite el acceso sólo a los usuarios que forman parte de ese grupo.

Por ejemplo, puede tener un directorio que contenga archivos confidenciales a los que sólo unos pocos usuarios deberían tener acceso. Puede configurar un grupo denominado `topsecret` que incluya los usuarios que trabajan en el proyecto `topsecret`. Además, puede configurar los archivos `topsecret` con permiso `read` para el grupo `topsecret` para que sólo los usuarios del grupo `topsecret` puedan leer los archivos.

Un tipo especial de cuenta de usuario, denominado *rol*, brinda a los usuarios seleccionados privilegios especiales. Para obtener más información, consulte el Capítulo 1, “Sobre el uso de los derechos para controlar los usuarios y los procesos” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Componentes de cuentas de usuario

En esta sección, se describen los diferentes componentes de una cuenta de usuario.

Nombres de usuario (inicio de sesión)

Los nombres de usuario, también llamados *nombres de inicio de sesión*, permiten a los usuarios acceder a sus propios sistemas y a sistemas remotos que tienen los privilegios de acceso adecuados. Debe seleccionar un nombre de usuario para cada cuenta de usuario que cree.

Considere establecer una manera estándar de asignar nombres de usuario para facilitar su seguimiento. Además, los nombres deben ser fáciles para que los usuarios los recuerden. Un esquema simple para seleccionar un nombre de usuario es usar la inicial del primer nombre y las siete primeras letras del apellido del usuario. Por ejemplo, John Smith se convierte en `jsmith`. Si este esquema da como resultado nombres duplicados, puede utilizar la primera inicial, la inicial del segundo nombre y los seis primeros caracteres del apellido del usuario. Por ejemplo, `John Jay Smith` se convierte en `jjsmith`.

Si este esquema sigue dando como resultando nombres duplicados, tenga en cuenta el siguiente esquema para crear un nombre de usuario:

- Se utiliza la primera inicial, la inicial del segundo nombre y los primeros cinco caracteres del apellido del usuario.
- Se agrega el número 1, 2 o 3, y así sucesivamente hasta tener un nombre único.

Nota - Cada nuevo nombre de usuario debe ser distinto de cualquier alias de correo conocido por el sistema o el dominio NIS. De lo contrario, el correo podría ser entregado al alias en lugar de al usuario real.

Para obtener directrices detalladas sobre la configuración de nombres (inicio de sesión) de usuario, consulte “Directrices para asignar nombres de usuario, ID de usuario e ID de grupo” [17].

Números de ID de usuario

Hay un número de identificación de usuario (UID) asociado con cada nombre de usuario. El número UID identifica el nombre de usuario para cualquier sistema en el que el usuario intenta iniciar la sesión. También lo utilizan los sistemas para identificar los propietarios de los archivos y directorios. Si crea cuentas de usuario para una sola persona en un número de sistemas diferentes, utilice siempre el mismo nombre de usuario y número de ID. De ese modo, el usuario puede mover fácilmente archivos entre sistemas sin problemas de titularidad.

Los números UID deben ser números completos menores o iguales que 2147483647. Los números UID son necesarios para cuentas de usuario normales y cuentas del sistema especiales. La siguiente tabla muestra los números UID que están reservados para las cuentas de usuario y las cuentas del sistema.

TABLA 1-1 Números UID reservados

Números UID	Cuentas de usuario o de inicio de sesión	Descripción
0 – 99	`root`, `daemon`, `bin`, `sys`, etc.	Reservado para ser usado por el sistema operativo
100 – 2147483647	Usuarios comunes	Cuentas con fines generales
60001 y 65534	`nobody` y `nobody4`	Usuarios anónimos NFS
60002	`noaccess`	Usuarios que no son de confianza

No asigne los UID del 0 al 99. Estos UID están reservados para la asignación por parte de Oracle Solaris. Por definición, `root` siempre tiene un UID 0, `daemon` tiene un UID 1 y pseudo usuario `bin` tiene un UID 2. Además, debería ofrecer a inicios de sesión `uucp` e inicios de sesión de pseudo usuario, como `who`, `tty` y `ttytype`, UID bajos para que queden al principio del archivo `passwd`.

Para obtener directrices adicionales sobre la configuración de UID, consulte “Directrices para asignar nombres de usuario, ID de usuario e ID de grupo” [17].

Como con nombres de usuario (inicio de sesión), debe adoptar un esquema para asignar números UID únicos. Algunas compañías asignan números de empleado únicos. A

continuación, los administradores agregan un número al número de empleado para crear un número UID único para cada empleado.

Para minimizar riesgos de seguridad, debería evitar volver a utilizar los UID de cuentas suprimidas. Si debe reutilizar un IUD, elimine la información de la cuenta por completo para que el nuevo usuario no se vea afectado por los atributos definidos para un usuario antiguo. Por ejemplo, puede que se haya incluido a un usuario antiguo en una lista de denegación de impresora. Sin embargo, el acceso denegado a esa impresora podría resultar inapropiado para el nuevo usuario.

Uso de ID de usuario e ID de grupo de gran tamaño

Los UID e ID de grupo (GID) pueden asignarse hasta el valor máximo de un entero firmado o 2147483647.

La siguiente tabla describe limitaciones de UID y GID.

TABLA 1-2 Resumen de limitaciones de UID y GID de gran tamaño

UID o GID	Limitaciones
262144 o superior	Los usuarios que utilizan el comando `cpio` con el formato de archivo predeterminado para copiar un archivo, ven un mensaje de error para cada archivo. Los UID y GID se establecen para `nobody` en el archivo.
2097152 o superior	Los usuarios que utilizan el comando `cpio` con el formato `-H odc` o el comando `pax -x cpio` para copiar archivos ven un mensaje de error devuelto para cada archivo. Los UID y GID se establecen para `nobody` en el archivo.
1000000 o superior	Los usuarios que utilizan el comando `ar` tienen sus UID y GID establecidos en `nobody` en el archivo.
2097152 o superior	Los usuarios que utilizan el comando `tar`, el comando `cpio -H ustar` o el comando `pax -x tar` tienen sus UID y GID establecidos en `nobody`.

Grupos UNIX

Un *grupo* es una recopilación de usuarios que pueden compartir archivos y otros recursos del sistema. Por ejemplo, usuarios que trabajan en el mismo proyecto podrían formarse en un grupo. Un grupo es conocido tradicionalmente como un grupo UNIX.

Cada grupo debe tener un nombre, un número de identificación de grupo (GID) y una lista de nombres de los usuarios que pertenecen a ese grupo. Un número GID identifica el grupo internamente para el sistema.

Los dos tipos de grupos al que un usuario puede pertenecer son los siguientes:

- **Grupo primario:** especifica un grupo que el sistema operativo asigna a archivos creados por los usuarios. Cada usuario debe pertenecer a un grupo primario.

- **Grupos suplementarios:** especifica uno o más grupos a los que también pertenece el usuario. Los usuarios pueden pertenecer a hasta 1024 grupos suplementarios.

Para obtener directrices detalladas sobre la configuración de nombres de grupo, consulte "Directrices para asignar nombres de usuario, ID de usuario e ID de grupo" [17].

En ocasiones, un grupo secundario del usuario no es importante. Por ejemplo, la propiedad de archivos reflejar el grupo primario y no un grupo secundario. Otras aplicaciones, sin embargo, puedan depender de pertenencias a grupos secundarios del usuario. Por ejemplo, un usuario tiene que ser un miembro del grupo `sysadmin` (grupo 14) para utilizar el software Admintool en las versiones anteriores de Oracle Solaris. Sin embargo, no importa si el grupo 14 es el grupo primario actual del usuario.

El comando `groups` enumera la lista de grupos a los que pertenece un usuario. Un usuario puede tener solamente un grupo primario a la vez. Sin embargo, los usuarios pueden cambiar temporalmente su grupo primario a cualquier otro grupo del que el usuario sea miembro mediante el comando `newgrp`.

Al agregar una cuenta de usuario, debe asignar un grupo primario a un usuario o aceptar el grupo predeterminado, `staff` (grupo 10). El grupo primario ya debería existir. Si el grupo primario no existe, especifique el grupo por número GID. Los nombres de usuario no se agregan a grupos primarios ya que la lista podría llegar a ser demasiado larga. Antes de poder asignar usuarios a un nuevo grupo secundario, debe crear el grupo y asignarle un número GID.

Los grupos pueden ser locales para un sistema o gestionados mediante un servicio de nombres. Para simplificar la administración de grupos, debe utilizar un servicio de nombres, como NIS o un servicio de directorio, como LDAP. Estos servicios permiten gestionar de manera centralizada la pertenencia a los grupos.

Contraseñas de usuario

Puede especificar una contraseña para un usuario cuando agrega el usuario. O bien, puede forzar al usuario a que especifique una contraseña cuando inicia sesión por primera vez en el sistema. Si bien los nombres de usuario son de dominio público, las contraseñas deben mantenerse en secreto y sólo deben ser conocidas por los usuarios. Se debe asignar una contraseña a cada cuenta de usuario.

Las contraseñas de usuario deben cumplir con la siguiente sintaxis:

- La longitud de la contraseña es definida por el valor `PASSLENGTH` en el archivo `/etc/default/password`.

  El algoritmo de hash de contraseña predeterminada es `SHA256`. Como resultado, las contraseñas de usuario ya no se limitan a ocho caracteres como en versiones anteriores de Oracle Solaris. La limitación de ocho caracteres sólo se aplica a las contraseñas que utilizan el algoritmo `crypt_unix`(5) anterior, que se ha conservado para la compatibilidad de retroceso con las entradas de archivo `passwd` y los mapas NIS existentes.

Las nuevas contraseñas debe coincidir con las reglas de complejidad dentro del número máximo de caracteres permitidos para el algoritmo de contraseña. Por lo tanto, si utiliza el algoritmo `crypt_unix` y escribe una contraseña de 20 caracteres, la contraseña debe coincidir con las reglas de complejidad en los primeros 8 caracteres. Si el algoritmo de contraseña corresponde a cualquiera de los otros algoritmos, la contraseña debe coincidir con las reglas de complejidad dentro de toda la contraseña que se escribe, que es 20 en este ejemplo.

- Cada contraseña debe cumplir con las restricciones de complejidad especificadas en el archivo `/etc/default/passwd`.
- Cada contraseña no debe ser miembro del diccionario configurado, como se especifica en el archivo `/etc/default/passwd`.
- Las nuevas contraseñas no deben estar incluidas en el historial de contraseñas de un servicio de nombres.

Las reglas de contraseñas se explican en detalle en la página del comando man `passwd`(1).

Para que sus sistemas sean más seguros, los usuarios deberían cambiar sus contraseñas en forma periódica. Para un alto nivel de seguridad, se debe solicitar a los usuarios que cambien sus contraseñas cada seis semanas. Una vez cada tres meses es adecuado para niveles más bajos de seguridad. Los inicios de sesión de administración del sistema (como `root` y `sys`) se deben cambiar mensualmente o siempre que una persona que sabe la contraseña `root` deja la compañía o es reasignada.

Numerosas infracciones de seguridad del equipo implican adivinar una contraseña legítima del usuario. Debe asegurarse de que los usuarios eviten el uso de nombres propios, nombres, nombres de inicio de sesión y otras contraseñas que una persona podría deducir sólo por saber algo sobre el usuario.

Algunas buenas opciones para las contraseñas incluyen lo siguiente:

- Frases (`beammeup`).
- Palabras sin sentido armadas con las primeras letras de cada palabra de una frase. Por ejemplo, `swotrb` para `SomeWhere Over The RainBow`.
- Palabras con números o símbolos sustituidos por letras. Por ejemplo, `sn00py` para `snoopy`.

No utilice estas opciones para las contraseñas:

- Su nombre (escrito hacia delante, hacia atrás o mezclado)
- Nombres de miembros de la familia o mascotas
- Números de licencia de conducir
- Números de teléfono
- Números de seguro social
- Números de empleado
- Palabras relacionadas con un pasatiempo o interés
- Temas estacionales, como Papá Noel en diciembre

- Cualquier palabra en el diccionario

Directorios raíz

El directorio principal es la parte de un sistema de archivos que está asignada a un usuario para almacenar archivos privados. La cantidad de espacio que asigne a un directorio principal depende del tamaño del sistema en el que el directorio está alojado, los tipos de archivo que crea el usuario, el tamaño del archivo y el número de archivos que se crean.

Un directorio principal se puede ubicar en el sistema local del usuario o en un servidor de archivos remoto. En cualquier caso, por convención, el directorio principal debe crearse como `/export/home/`*username*. Para un sitio grande, debería almacenar los directorios principales en un servidor. Utilice un sistema de archivos independiente para cada usuario, por ejemplo, `/export/home/alice` o `/export/home/bob`. Mediante la creación de sistemas de archivos independientes para cada usuario, puede establecer propiedades o atributos según las necesidades de cada usuario.

Independientemente de la ubicación de sus respectivos directorios principales, los usuarios pueden acceder a sus directorios principales mediante un punto de montaje denominado `/home/`*nombre de usuario*. Cuando se usa AutoFS para montar directorios principales, no se le permite crear ningún directorio en el punto de montaje `/home` de ningún sistema. El sistema reconoce el estado especial de `/home` cuando AutoFS está activo. Para obtener más información sobre el montaje automático de los directorios principales, consulte “Administración de autofs” de “Gestión de sistemas de archivos de red en Oracle Solaris 11.2 ”.

Para utilizar un directorio principal en cualquier lugar de la red, siempre debe hacer referencia al directorio principal como `$HOME` y no como `/export/home/`*nombre de usuario*. El último es específico de un equipo. Además, cualquier enlace simbólico creado en el directorio principal de un usuario debe utilizar rutas relativas (por ejemplo, `../../../x/y/x`), para que los enlaces sean válidos, sin importar dónde esté montado el directorio principal.

Para obtener más información sobre cómo se agregan los directorios principales cuando crea cuentas de usuario mediante la interfaz de línea de comandos, consulte “Directrices para la configuración de cuentas de usuario” [40].

Servicios de nombres

Si gestiona cuentas de usuario para un sitio de gran tamaño, es posible que desee tener en cuenta el uso de un servicio de nombres o directorios, como LDAP o NIS. Un servicio de nombres o directorios permite almacenar información de cuenta de usuario de forma centralizada en lugar de almacenar información de cuenta de usuario en cada archivo `/etc` del sistema. Al utilizar un servicio de nombres o directorios para cuentas de usuario, los usuarios pueden moverse de sistema a sistema utilizando la misma cuenta de usuario sin que su información se duplique en cada sistema. Mediante el uso de un servicio de nombres o directorios también garantiza que la información de cuentas de usuario sea coherente.

Entorno de trabajo del usuario

Además de tener un directorio principal para crear y almacenar los archivos, los usuarios necesitan un entorno que les proporcione acceso a las herramientas y los recursos que necesitan para realizar su trabajo. Cuando un usuario inicia sesión en un sistema, el entorno de trabajo del usuario se determina por archivos de inicialización. Estos archivos están definidos por el shell de inicio del usuario, que puede variar, según la versión.

Una buena estrategia para gestionar el entorno de trabajo del usuario es proporcionar archivos de inicialización de usuario personalizados, como `.bash_profile`, `.bash_login`, `.kshrc` o `.profile`, en el directorio raíz del usuario.

Nota - No utilice archivos de inicialización del sistema, como `/etc/profile` o `/etc/.login`, para gestionar el entorno de trabajo del usuario. Estos archivos residen localmente en los sistemas y no se administran de manera centralizada. Por ejemplo, si AutoFS se usa para montar el directorio principal del usuario desde cualquier sistema de la red, tendría que modificar los archivos de inicialización del sistema en cada sistema para garantizar un entorno consistente siempre que un usuario se mueva de un sistema a otro.

Para obtener información detallada acerca de la personalización de archivos de inicialización de usuario para los usuarios, consulte “Acerca del entorno de trabajo del usuario” [26].

Directrices para asignar nombres de usuario, ID de usuario e ID de grupo

Los nombres de usuario, los UID y los GID deben ser únicos dentro de su organización, especialmente si la configuración incluye varios dominios.

Tenga en cuenta las directrices siguientes al crear usuarios o nombres de rol, UID y GID:

- **Nombres de usuario:** deben tener de dos a ocho letras y números. El primer carácter debería ser una letra. Al menos un carácter debería ser una letra en minúscula.

Nota - Aunque los nombres de usuario pueden incluir un punto (.), carácter de subrayado (_) o guión (-), no se recomienda el uso de estos caracteres porque pueden causar problemas con algunos productos de software.

- **Cuentas del sistema**: no utilice ninguno de los nombres de usuario, UID o GID que están contenidos en los archivos predeterminados `/etc/passwd` y `/etc/group`. No utilice UID y GID, 0-99. Estos números están reservados para asignación por parte de Oracle Solaris y no deben ser utilizados por ninguna persona. Tenga en cuenta que esta restricción también se aplica a números que no se incluyan en uso actualmente.

Por ejemplo, `gdm` es el nombre de usuario reservado y el nombre de grupo para el daemon de gestor de visualización GNOME y no debería ser utilizado por otro usuario. Para obtener una lista completa de las entradas predeterminadas `/etc/passwd` y `/etc/group`, consulte la Tabla 1-3, “Entradas de archivo `passwd` predeterminadas” y la Tabla 1-4, “Entradas de archivo `group` predeterminadas”.

Atención - Las cuentas `nobody` y `nobody4` nunca deberían utilizarse para procesos en ejecución. Las dos siguientes cuentas están reservadas para su uso por NFS. El uso de estas cuentas para procesos en ejecución podría provocar riesgos de seguridad inesperados. Los procesos que debe ejecutar como usuario no root deben utilizar las cuentas `daemon` o `noaccess`.

- **Configuración de cuentas del sistema**: la configuración de cuentas del sistema predeterminada no debería cambiarse nunca, tampoco debería cambiarse nunca el shell de inicio de sesión de una cuenta de sistema que está bloqueada. La única excepción a esta regla es la configuración de una contraseña y de parámetros de caducidad de la contraseña para la cuenta `root`.

Nota - El cambio de una contraseña de una cuenta de usuario bloqueada cambia la contraseña, pero ya no desbloquea la cuenta al mismo tiempo. Ahora se requiere un segundo paso para desbloquear la cuenta mediante el comando `passwd -u`.

Dónde se almacena la información de cuentas de usuario y grupos

En esta sección, se incluye la siguiente información:

Según las políticas del sitio, la información de cuentas de usuario y grupos puede almacenarse en los archivos `/etc` del sistema local o en un servicio de nombres o directorios como se indica a continuación:

- La información del servicio de nombres NIS se almacena en mapas.
- La información del servicio de directorios LDAP se almacena en archivos de base de datos indexados.

Nota - Para evitar confusiones, a la ubicación de la información de cuentas de usuario y grupos se la denomina *archivo*, en lugar de *base de datos*, *tabla* o *mapa*.

La mayor parte de la información de cuentas de usuario se almacena en el archivo `passwd`. La información de contraseña se almacena como se indica a continuación:

- En el archivo `passwd` cuando utiliza NIS
- En el archivo `/etc/shadow` cuando utiliza archivos `/etc`
- En el contenedor `people` cuando utiliza LDAP

La caducidad de contraseñas está disponible cuando utiliza LDAP, pero no cuando utiliza NIS.

La información de grupo se almacena en el archivo `group` para NIS. Para LDAP, la información de grupo se almacena en el contenedor `group`.

Campos del archivo `passwd`

Los campos del archivo `passwd` están separados por dos puntos y contienen la siguiente información:

username:*password*:*UID*:*GID*:*comment*:*home-directory*:*login-shell*

Por ejemplo:

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

Para obtener una descripción completa de los campos del archivo `passwd`, consulte la página del comando man `passwd`(1).

Archivo `passwd` predeterminado

El archivo `passwd` contiene entradas para daemons estándar. Los daemons son procesos que se inician al momento del inicio para realizar algunas tareas de todo el sistema, como imprimir, administrar redes o supervisar puertos.

A continuación, se muestra el contenido de un archivo de ejemplo `passwd`.

Nota - Cuando se agregan paquetes al sistema o se eliminan de éste, se crean y se eliminan usuarios y grupos adicionales. Estos cambios en curso se reflejan en el archivo `passwd`. No es necesario que los administradores limpien este archivo.

```
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:/:
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:/:
ikeuser:x:67:12:IKE Admin:/:
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:/:
```

El ejemplo anterior muestra el contenido del archivo de ejemplo `passwd` sin ninguna explicación. La siguiente tabla amplía la información, proporciona una descripción e información sobre el paquete de origen para cada daemon en un archivo `passwd`.

TABLA 1-3 Entradas de archivo `passwd` predeterminadas

Nombre de usuario	ID de usuario	Descripción	Paquete
`root`	`0`	Reservado para la cuenta de superusuario	`system/core-os`
`daemon`	`1`	Daemon de sistema Umbrella asociado con tareas de sistema de rutina	`system/core-os`
`bin`	`2`	Daemon administrativo asociado con binarios del sistema en ejecución para realizar algunas tareas del sistema de rutina	`system/core-os`
`sys`	`3`	Daemon administrativo asociado con el registro del sistema o actualización de archivos en directorios temporales	`system/core-os`
`adm`	`4`	Daemon administrativo asociado con el registro del sistema	`system/core-os`
`lp`	`71`	Reservado para el daemon de impresora de líneas	`system/core-os`
`uucp`	`5`	Asignado al daemon que está asociado con funciones de `uucp`	`system/core-os`
`nuucp`	`9`	Asignado a otro daemon asociado con funciones `uucp`	`system/core-os`

Nombre de usuario	ID de usuario	Descripción	Paquete
dladm	15	Reservado para la administración de enlaces de datos	system/core-os
netadm	16	Reservado para la administración de redes	system/core-os
netcfg	17	Reservado para la administración de configuración de redes	system/core-os
smmsp	25	Asignado al daemon del programa de envío de mensajes Sendmail	system/core-os
gdm	50	Asignado al daemon de gestor de pantallas de GNOME	system/core-os
zfssnap	51	Reservado para las instantáneas automáticas	system/core-os
upnp	52	Reservado para el servidor UPnP	system/core-os
xvm	60	Reservado para el usuario xVM	system/core-os
mysql	70	Reservado para el usuario MySQL	system/core-os
openldap	75	Reservado para el usuario OpenLDAP	library/ldap
webservd	80	Reservado para el acceso WebServer	system/core-os
postgres	90	Reservado para el acceso PostgresSQL	system/core-os
svctag	95	Reservado para el acceso al registro de etiquetas de servicio	system/core-os
unknown	96	Reservado para los usuarios remotos que no se pueden asignar en listas de control de acceso (ACL) de NFSv4	system/core-os
nobody	60001	Reservado para los usuarios de acceso anónimo de NFS	system/core-os
noaccess	60002	Reservado para los usuarios sin acceso	system/core-os
nobody4	65534	Reservado para los usuarios de acceso anónimo de NFS de SunOS 4.x	system/core-os
ikeuser	67	Reservado para acceso de intercambio de claves de internet (IKE).	system/network/ike
ftp	21	Reservado para el acceso de FTP	service/network/ftp
dhcpserv	18	Reservado para usuario de servidor DHCP	service/network/dhcp/isc-dhcp
aiuser	60003	Reservado para usuario AI	system/install/auto-install/auto-install-common
pkg5srv	97	Reservado para el servidor depot pkg(5)	package/pkg

Campos en el archivo `shadow`

El archivo `/etc/shadow` almacena las contraseñas cifradas del usuario y la información relacionada. Los campos del archivo `shadow` están separados por dos puntos y contienen la siguiente información:

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

El algoritmo de hash de contraseña predeterminada es `SHA256`. El hash de contraseña para el usuario es similar al siguiente:

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

Para obtener una descripción completa de los campos del archivo `shadow`, consulte la página del comando man `shadow`(4).

Campos en el archivo `group`

El archivo group es una fuente local de información del grupo. Los campos del archivo `group` están separados por dos puntos y contienen la siguiente información:

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

Por ejemplo:

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

Para obtener una descripción completa de los campos del archivo `group`, consulte la página del comando man `group`(4).

Archivo `group` predeterminado

El archivo `group` predeterminado contiene los siguientes grupos del sistema que admite algunas tareas de todo el sistema, como imprimir, administrar redes o correo electrónico. La mayoría de estos grupos tienen entradas correspondientes en el archivo `passwd`.

```
The following displays the contents of a sample group file.

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:
aiuser::61:
ftp::21
pkg5srv::97:
```

El ejemplo anterior proporciona el contenido del archivo de ejemplo `group` sin ninguna explicación. La siguiente tabla ofrece información adicional sobre cada grupo que aparece en un archivo `group` típico.

TABLA 1-4 Entradas de archivo `group` predeterminadas

Nombre del grupo	ID de grupo	Descripción	pkg(5)
`root`	`0`	Grupo de superusuario	`system/core-os`
`other`	`1`	Grupo opcional	`system/core-os`
`bin`	`2`	Grupo administrativo asociado con binarios del sistema en ejecución	`system/core-os`
`sys`	`3`	Grupo de administración asociado con registro del sistema o directorios temporales	`system/core-os`
`adm`	`4`	Grupo de administración asociado con registro del sistema	`system/core-os`
`uucp`	`5`	Grupo asociado con funciones `uucp`	`system/core-os`
`mail`	`6`	Grupo de correo electrónico	`system/core-os`
`tty`	`7`	Grupo asociado con dispositivos `tty`	`system/core-os`
`lp`	`8`	Grupo de impresora en línea	`system/core-os`
`nuucp`	`9`	Grupo asociado con funciones `uucp`	`system/core-os`
`staff`	`10`	Grupo administrativo general	`system/core-os`
`daemon`	`12`	Grupo asociado con tareas del sistema de rutina	`system/core-os`

Nombre del grupo	ID de grupo	Descripción	pkg(5)
sysadmin	14	Grupo de administración que es útil para los administradores del sistema	system/core-os
smmsp	25	Daemon para programa de envío de mensajes Sendmail	system/core-os
gdm	50	Grupo reservado para el daemon de gestor de visualización GNOME	system/core-os
upnp	52	Grupo reservado para el servidor UPnP	system/core-os
xvm	60	Grupo reservado para el usuario xVM	system/core-os
netadm	65	Grupo reservado para la administración de redes	system/core-os
mysql	70	Grupo reservado para el usuario MySQL	system/core-os
openldap	75	Reservado para el usuario OpenLDAP	library/ openldap
webservd	80	Grupo reservado para acceso WebServer	system/core-os
postgres	90	Grupo reservado para acceso PostgresSQL	system/core-os
slocate	95	Grupo reservado para el acceso a ubicación segura	system/core-os
unknown	96	Grupo reservado para los grupos remotos que no se pueden asignar en listas de control de acceso (ACL) de NFSv4	system/core-os
nobody	60001	Grupo asignado para acceso NFS anónimo	system/core-os
noaccess	60002	Grupo asignado a un usuario o a un proceso que necesita acceder a un sistema a través de alguna aplicación, pero sin realmente registrarse	system/core-os
nogroup	65534	Grupo asignado a un usuario que no es un miembro de un grupo conocido	system/core-os
aiuser	61	Grupo asignado de la instalación automática de autorización	system/ install/auto-install/ auto-install-common
ftp	21	Grupo asignado para el acceso de FTP	system/core-os
pkg5srv	97	Grupo asignado al servidor depot pkg(5)	package/pkg

Comandos para obtener información de cuenta de usuario

En la siguiente tabla, se describen los comandos que pueden utilizar los administradores de sistemas para obtener información acerca de las cuentas de usuario. Esta información se almacena en varios archivos dentro del directorio /etc. Para obtener información de cuenta de usuario, se prefiere el uso de estos comandos antes que el uso del comando cat para ver información similar.

TABLA 1-5 Comandos para obtener información acerca de usuarios

Comando	Descripción	Referencia de página del comando man
`auths`	Muestra y gestiona autorizaciones.	`auths`(1)
`getent`	Muestra una lista de entradas de la base de datos administrativa. La información normalmente proviene de uno o varios de los orígenes especificados para la base de datos `/etc/nsswitch.conf`.	`getent`(1M)
`logins`	Muestra información sobre usuarios, roles e inicios de sesión de sistema. La salida es controlada por las opciones de comando especificadas y puede incluir usuario, rol, inicio de sesión de sistema, interfaz gráfica de usuario, valor de campo de cuenta `passwd`, grupo primario, ID de grupo primario, nombres de grupo múltiples, ID de grupo múltiples, directorio raíz, shell de inicio de sesión y parámetros de vencimiento de contraseña.	`logins`(1M)
`perfiles`	Muestra y permite gestionar perfiles de derechos.	`profiles`(1)
`roles`	Muestra los roles que se han asignado a un usuario.	`roles`(1)
`userattr`	Indica el primer valor que se encuentra para `attribute_name`. Si no se ha especificado un usuario, el usuario se toma del ID del usuario real del proceso. Los nombres de atributos también se definen en las páginas del comando man `user_attr`(4) y `prof_attr`(4). **Nota -** Este comando es nuevo en Oracle Solaris 11.	Example 2–1

Comandos que se utilizan para la gestión de usuarios, roles y grupos

Nota - La GUI de Solaris Management Console y la línea de comandos (CLI) asociada con esta GUI, ya no son compatibles.

Los comandos que se describen en la siguiente tabla están disponibles para la gestión de usuarios, roles y grupos.

TABLA 1-6 Comandos que se utilizan para la gestión de usuarios, roles y grupos

Página del comando man	Descripción	Para obtener información adicional
useradd(1M)	Crea usuarios localmente o en un repositorio LDAP.	Cómo agregar un usuario [44]
usermod(1M)	Cambia propiedades de usuario localmente o en un repositorio LDAP. Si las propiedades de usuario son relevantes para la seguridad, como la asignación de roles, esta tarea podría restringirse al administrador de seguridad o al rol root.	Cómo modificar una cuenta de usuario [45] "Creación de roles" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
userdel(1M)	Suprime un usuario del sistema o del repositorio LDAP. Puede implicar una limpieza adicional, como la eliminación del trabajo cron.	Cómo suprimir un usuario [46]
roleadd(1M) rolemod(1M) roledel(1M)	Gestiona roles localmente o en un repositorio LDAP. Los roles no pueden iniciar sesión. Los usuarios asumen un rol asignado para realizar tareas administrativas.	"Asignación de derechos a usuarios" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
groupadd(1M) groupmod(1M) groupdel(1M)	Gestiona grupos localmente o en un repositorio LDAP.	Cómo agregar un grupo [47]

Acerca del entorno de trabajo del usuario

En esta sección, se describe la siguiente información:

- "Uso de archivos de inicialización de sitio" [27]
- "Cómo evitar referencias de sistema local" [28]
- "Funciones de shell" [28]
- "Historial de shells bash y ksh93" [30]
- "Variables del entorno de shell bash y korn" [31]
- "Personalización del shell Bash" [33]
- "Variable de entorno MANPATH" [33]
- "Variable de entorno PATH" [34]
- "Variables de configuración regional" [34]
- "Permisos de archivo predeterminados (umask)" [35]
- "Personalización de un archivo de inicialización de usuario" [36]

Una parte de la configuración de un directorio principal del usuario es proporcionar archivos de inicialización de usuario para el shell de inicio de sesión del usuario. Un *archivo de inicialización de usuario* es una secuencia de comandos de shell que establece un entorno de

trabajo para un usuario después de que el usuario inicia sesión en un sistema. Básicamente, puede realizar cualquier tarea en un archivo de inicialización de usuario que puede realizar en una secuencia de comandos de shell. Sin embargo, la tarea principal del archivo de inicialización de usuario es definir las características de un entorno de trabajo de usuario, como una ruta de búsqueda, variables de entorno y entorno de ventanas del usuario. Cada shell de inicio de sesión tiene su propio archivo o archivos de inicialización de usuario, que se enumeran en la siguiente tabla. Tenga en cuenta que el archivo de inicialización de usuario predeterminado para los shells `ksh93` y bash es `/etc/skel/local.profile`.

TABLA 1-7 Archivos de inicialización de usuario `ksh93` y bash

Shell	Archivo de inicialización de usuario	Objetivo
`bash`	`$HOME/.bash_profile`	Define el entorno del usuario al iniciar la sesión
	`$HOME/.bash_login`	
	`$HOME/.profile`	
`ksh93`	`/etc/profile`	Define el entorno del usuario al iniciar la sesión
	`$HOME/.profile`	
	`$ENV`	Define el entorno del usuario en el inicio de sesión dentro del archivo y es especificado por la variable de entorno `ENV` del shell Korn

Puede utilizar estos archivos como punto de inicio y luego modificarlos para crear un conjunto de archivos estándar que proporciona un entorno de trabajo común para todos los usuarios. También puede modificar estos archivos para proporcionar el entorno de trabajo para distintos tipos de usuarios.

Para obtener instrucciones paso a paso acerca de cómo crear grupos de archivos de inicialización de usuario para diferentes tipos de usuarios, consulteCómo personalizar los archivos de inicialización de usuario [42].

Uso de archivos de inicialización de sitio

Los archivos de inicialización de sitio pueden ser personalizados por el administrador y por el usuario. Esta importante tarea se puede realizar con archivos de inicialización de usuario centralizados o distribuidos globalmente denominados *archivos de inicialización de sitio*. Los archivos de inicialización de sitio le permiten introducir continuamente nuevas funcionalidades al entorno de trabajo del usuario al tiempo que permiten personalizar el archivo de inicialización del usuario.

Cuando hace referencia a un archivo de inicialización de sitio en un archivo de inicialización de usuario, todas las actualizaciones para el archivo de inicialización de sitio se reflejan

automáticamente cuando el usuario inicia sesión en el sistema o cuando un usuario inicia un nuevo shell. Los archivos de inicialización de sitio permiten distribuir cambios en todo el sitio para entornos de trabajo de los usuarios que no previó al agregar usuarios.

Puede personalizar un archivo de inicialización de sitio de la misma manera que personaliza un archivo de inicialización de usuario. Estos archivos normalmente residen en un servidor o un conjunto de servidores, y aparecen como la primera instrucción en un archivo de inicialización de usuario. También, cada archivo de inicialización de sitio debe ser del mismo tipo de secuencia de comandos de shell que el archivo de inicialización de usuario al que hace referencia.

Para hacer referencia a un archivo de inicialización de sitio en un archivo de inicialización de usuario de shell `ksh93` o bash, coloque una línea al principio del archivo de inicialización de usuario similar a la siguiente línea:

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

Cómo evitar referencias de sistema local

No agregue referencias específicas al sistema local en el archivo de inicialización de usuario. Las instrucciones en un archivo de inicialización de usuario deben ser válidas, independientemente del sistema al que el usuario se conecta.

Por ejemplo:

- Para que un directorio principal del usuario esté disponible en cualquier lugar de la red, siempre haga referencia al directorio principal con la variable `$HOME`. Por ejemplo, use `$HOME/bin` en lugar de `/export/home/`*`username`*`/bin`. La variable `$HOME` funciona cuando el usuario inicia sesión en otro sistema y los directorios principales se montan automáticamente.
- Para acceder a los archivos en un disco local, use nombres de ruta globales, como `/net/`*`system-name/directory-name`*. Cualquier directorio al que se hace referencia por `/net/`*`system-name`* se puede montar automáticamente en cualquier sistema en que el usuario inicie sesión, suponiendo que el sistema ejecuta AutoFS.

Funciones de shell

Esta versión de Oracle Solaris es compatible con las siguientes funciones y comportamiento de shell:

- A la cuenta de usuario que se crea al instalar la versión de Oracle Solaris se le asigna el Bourne-Again Shell (bash) de GNU de manera predeterminada.
- El shell de sistema estándar (`bin/sh`) ahora es el shell Korn 93 (`ksh93`).

- El shell interactivo predeterminado es el shell Bourne-again (`bash`) (`/usr/bin/bash`).
- Tanto el shell bash como el shell `ksh93` cuentan con la función de edición de línea de comandos, lo que significa que se pueden editar los comandos antes de ejecutarlos.
- Puede mostrar la información de ruta y el shell predeterminado de varias maneras:
  - Utilice los comandos `echo $SHELL` y `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
    ```

  - Utilice el comando `pargs`:

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

- El shell `ksh93` también tiene una variable incorporada denominada `.sh.version`, que se puede mostrar de la siguiente manera:

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

- Para cambiar a un shell diferente, escriba la ruta del shell que desea utilizar.
- Para salir de un shell, escriba `exit`.

En la siguiente tabla, se describen las opciones de shell que se admiten en Oracle Solaris.

TABLA 1-8 Funciones de shell básicas en la versión Oracle Solaris

Shell	Ruta	Comentarios
Bourne-Again Shell (bash)	`/usr/bin/bash`	Shell predeterminado para usuarios creados por un instalador, así como el rol `root` El shell (interactivo) predeterminado para usuarios creados con el comando `useradd`, así como el rol `root`, es `/usr/bin/bash`. La ruta predeterminada es `/usr/bin:/usr/sbin`.
Shell Korn	`/usr/bin/ksh`	`ksh93` es el shell predeterminado en esta versión de Oracle Solaris
Shell C y shell C mejorado	`/usr/bin/csh` y `/usr/bin/tcsh`	Shell C y shell C mejorado
Shell compatible con POSIX	`/usr/xpg4/bin/sh`	Shell compatible con POSIX
Shell Z	`/usr/bin/zsh`	Shell Z

Nota - El shell Z (`zsh`) y el shell C mejorado (`tsch`) no se instalan en el sistema de forma predeterminada. Para usar cualquiera de estos shells, primero debe instalar los paquetes de software necesarios.

La tabla siguiente muestra los indicadores de sistema UNIX® predeterminados y el indicador de superusuario de shells que se incluyen en los sistemas operativos Oracle Solaris. Tenga en cuenta que el indicador predeterminado del sistema que se muestra en los ejemplos de comandos varía según la versión de Oracle Solaris.

TABLA 1-9 Indicadores del shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	`$`
Shell Bash, shell Korn y shell Bourne para superusuario	`#`
Shell C	`machine_name%`
Shell C para superusuario	`machine_name#`

Historial de shells bash y `ksh93`

Tanto el shell `bash` como el shell `ksh93` registran un historial de todos los comandos que ejecuta. Este historial se mantiene por usuario, lo que significa que el historial es persistente entre las sesiones de inicio de sesión y es representativo de todas las sesiones de inicio de sesión.

Por ejemplo, si está en un shell bash, puede visualizar el historial completo de los comandos que ha ejecutado, por ejemplo:

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

Para mostrar un número de comandos anteriores, incluya un número entero en el comando:

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

Para obtener más información, consulte la página del comando man `history`(1).

Variables del entorno de shell bash y korn

El shell bash y el shell `ksh93` almacenan información especial de variables que el shell conoce como una *variable de entorno*. Para obtener una lista completa de las variables de entorno actuales del shell bash, utilice el comando `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]''
.
.
.
```

Para el shell `ksh93`, use el comando `set`, que es el comando `declare` equivalente del 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
  .
  .
  .
```

Para imprimir variables de entorno para cualquier shell, utilice el comando `echo` o `printf`. Por ejemplo:

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

Nota - Las variables de entorno no persisten entre sesiones. Para configurar valores de variables de entorno persistentes, establezca los valores en el archivo `.bashrc`.

Un shell puede tener dos tipos de variables:

Variables de entorno	Especifica las variables que se exportan a todos los procesos que son reproducidos por el shell. El comando `export` se utiliza para exportar una variable. Por ejemplo:

`export VARIABLE=value`

Estos valores se pueden visualizar mediante el comando `env`. Un subconjunto de variables de entorno como `PATH`, afecta el comportamiento del shell en sí mismo.

Variables (locales) de shell

Especifica las variables que afectan sólo el shell actual.

En un archivo de inicialización de usuario, puede personalizar el entorno de shell de un usuario cambiando los valores de las variables predefinidas o especificando variables adicionales.

En la siguiente tabla, se proporcionan más detalles acerca de las variables de shell y de entornos disponibles en la versión Oracle Solaris.

TABLA 1-10 Descripciones de variables de shell y de entorno

Variable	Descripción
`CDPATH`	Establece una variable utilizada por el comando `cd`. Si el directorio de destino del comando `cd` se especifica como un nombre de ruta relativa, el comando `cd` primero busca el directorio de destino en el directorio actual (`.`). Si no se encuentra el destino, los nombres de ruta enumerados en la variable `CDPATH` se buscan de manera consecutiva hasta que el directorio de destino se encuentra y el cambio de directorio se completa. Si el directorio de destino no se encuentra, el directorio de trabajo actual se deja sin modificar. Por ejemplo, la variable `CDPATH` se establece en `/home/jean` y existen dos directorios en `/home/jean`, `bin` y `doc`. Si está en el directorio `/home/jean/bin` y escribe `cd doc`, cambia los directorios a `/home/jean/doc`, aunque no especifique una ruta completa.
`HOME`	Establece la ruta para el directorio principal del usuario.
`LANG`	Establece la configuración regional.
`LOGNAME`	Define el nombre del usuario que tiene sesión iniciada actualmente. El valor predeterminado de `LOGNAME` se define automáticamente mediante el programa de inicio de sesión para el nombre de usuario especificado en el archivo `passwd`. Sólo debería ser necesario hacer referencia a esta variable y no reiniciarla.
`MAIL`	Establece la ruta al buzón de correo del usuario.
`MANPATH`	Establece las jerarquías de las páginas del comando man que están disponibles. **Nota -** A partir de Oracle Solaris 11, la variable de entorno `MANPATH` ya no se requiere. El comando `man` determina el comando `MANPATH` según la configuración de variables del entorno de `PATH`.
`PATH`	Especifica, en orden, los directorios que el shell busca para encontrar el programa a ejecutar cuando el usuario escribe un comando. Si el directorio no está en la ruta de búsqueda, los usuarios deben escribir el nombre de ruta completa de un comando. Como parte del proceso de inicio de sesión, la variable de entorno `PATH` predeterminada se define automáticamente y se establece como se especifica en `.profile`. El orden de ruta de búsqueda es importante. Cuando existen comandos idénticos en ubicaciones distintas, se utiliza el primer comando encontrado con ese nombre. Por ejemplo, suponga que `PATH` está definida en la sintaxis del shell como `PATH=/usr/bin:/usr/sbin:$HOME/bin` y un archivo denominado `sample` reside en `/usr/bin` y `/home/`

Variable	Descripción
	jean/bin. Si el usuario escribe el comando sample sin especificar el nombre de ruta completo, se utiliza la versión encontrada en /usr/bin.
PS1	Define el indicador de shell para el shell bash o el shell ksh93.
SHELL	Establece el shell predeterminado utilizado por make, vi y otras herramientas.
TERMINFO	Nombra un directorio donde se almacena una base de datos terminfo alternativa. Utilice la variable TERMINFO en el archivo /etc/profile o /etc/.login. Para obtener más información, consulte la página del comando man terminfo(4). Cuando la variable de entorno TERMINFO se establece, el sistema primero comprueba la ruta TERMINFO definida por el usuario. Si el sistema no encuentra una definición para un terminal en el directorio TERMINFO definido por el usuario, busca el directorio predeterminado, /usr/share/lib/terminfo, para una definición. Si el sistema no encuentra una definición en ninguna ubicación, el terminal se identifica como "ficticio".
TERM	Define el terminal. Esta variable se debe restablecer en el archivo /etc/profile o /etc/.login. Cuando el usuario invoca a un editor, el sistema busca un archivo con el mismo nombre definido en esta variable de entorno. El sistema busca el directorio al que se hace referencia por TERMINFO para determinar las características de terminal.
TZ	Define la zona horaria. La zona horaria se utiliza para mostrar fechas, por ejemplo, en el comando ls -l. Si TZ no se estableció en el entorno del usuario, se utiliza la configuración del sistema. De lo contrario, se utiliza la hora del meridiano de Greenwich.

Personalización del shell Bash

Para personalizar el shell bash, agregue o cambie la información del archivo .bashrc que está situado en el directorio principal. El usuario inicial que se crea al instalar Oracle Solaris tiene un archivo .bashrc que define PATH, MANPATH y el indicador de comandos. Para obtener más información, consulte la página del comando man bash(1).

Variable de entorno MANPATH

La variable de entorno MANPATH especifica dónde el comando man busca páginas del comando man de referencia. MANPATH se establece de manera automática según el valor PATH de un usuario, pero, por lo general, incluye /usr/share/man y usr/gnu/share/man.

Tenga en cuenta que la variable de entorno MANPATH de un usuario se puede modificar, independientemente de la variable de entorno PATH. No es necesario un equivalente uno a uno de las ubicaciones de la página del comando man asociadas, con directorios en la variable de entorno $PATH del usuario.

Variable de entorno PATH

Cuando el usuario ejecuta un comando utilizando la ruta completa, el shell utiliza la ruta para encontrar el comando. Sin embargo, cuando los usuarios especifican sólo un nombre de comando, el shell busca los directorios para el comando en el orden especificado por la variable PATH. Si el comando se encuentra en uno de los directorios, el shell ejecuta el comando.

Una ruta predeterminada está establecida por el sistema. Sin embargo, la mayoría de los usuarios la modifica para agregar otros directorios de comando. Muchos problemas del usuario relacionados con la configuración del entorno y el acceso a la versión correcta de un comando o una herramienta pueden atribuirse a rutas definidas incorrectamente.

Configuración de directrices de ruta

Al configurar las variablesPATH, tenga en cuenta las siguientes directrices:

- Si debe incluir el directorio actual (.) en su ruta, lo debe colocar último. La inclusión del directorio actual en la ruta es un riesgo de seguridad, porque algunas personas maliciosas podrían esconder un archivo ejecutable o una secuencia de comandos comprometido en el directorio actual. Considere el uso de nombres de ruta absolutos en su lugar.
- Mantenga la ruta de búsqueda lo más corta posible. El shell busca cada directorio en la ruta. Si un comando no se encuentra, las búsquedas largas pueden ralentizar el rendimiento del sistema.
- La ruta de búsqueda se lee de izquierda a derecha, por lo que debe colocar directorios para los comandos utilizados habitualmente al principio de la ruta.
- Asegúrese de que los directorios no estén duplicados en la ruta.
- Evite la búsqueda de directorios extensos, si es posible. Coloque directorios extensos al final de la ruta.
- Coloque directorios locales antes de que los directorios montados NFS para disminuir la posibilidad de que el sistema no responda cuando el servidor NFS no responde. Esta estrategia también reduce el tráfico de red innecesario.

Variables de configuración regional

Las variables de entorno LANG y LC especifican las conversiones específicas de configuración regional y las convenciones para el shell. Estas conversiones y convenciones incluyen zonas horarias, pedidos de clasificación y formatos de fechas, hora, moneda y números. Además, puede utilizar el comando stty en un archivo de inicialización de usuario para indicar si la sesión de terminal admitirá caracteres de varios bytes.

La variable LANG establece todas las posibles conversiones y convenciones para la configuración regional dada. Puede establecer diversos aspectos de localización por separado mediante estas variables LC: LC_COLLATE, LC_CTYPE, LC_MESSAGES, LC_NUMERIC, LC_MONETARY y LC_TIME.

Nota - De manera predeterminada, Oracle Solaris 11 sólo instala configuraciones regionales basadas en UTF-8.

En la siguiente tabla, se describen los valores de variables de entorno para las configuraciones regionales principales de Oracle Solaris 11.

TABLA 1-11 Valores para variables de configuración regional

Valor	Configuración regional
`en_US.UTF-8`	Inglés, Estados Unidos (UTF-8)
`fr_FR.UTF-8`	Francés, Francia (UTF-8)
`de_DE.UTF-8`	Alemán, Alemania (UTF-8)
`it_IT.UTF-8`	Italiano, Italia (UTF-8)
`ja_JP.UTF-8`	Japonés, Japón (UTF-8)
`ko_KR.UTF-8`	Coreano, Corea (UTF-8)
`pt_BT.UTF-8`	Portugués, Brasil (UTF-8)
`zh_CN.UTF-8`	Chino simplificado, China (UTF-8)
`es_ES.UTF-8`	Español, España (UTF-8)
`zh_TW.UTF-8`	Chino tradicional, Taiwán (UTF-8)

EJEMPLO 1-1 Definición de la configuración regional

En un archivo de inicialización de usuario de shell Bourne o Korn, debe agregar lo siguiente:

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

Permisos de archivo predeterminados (`umask`)

Cuando crea un archivo o un directorio, los permisos de archivo predeterminados asignados al archivo o el directorio son controlados por la *máscara de usuario*. La máscara de usuario está definida por el comando `umask` en un archivo de inicialización de usuario. Puede mostrar el valor actual de la máscara de usuario si escribe `umask` y presiona la tecla Retorno.

La máscara de usuario contiene los siguientes valores octales:

- El primer dígito define los permisos para el usuario
- El segundo dígito define los permisos para el grupo
- El tercer dígito define los permisos para otros, también denominados `world`

Tenga en cuenta que si el primer dígito es cero, no se muestra. Por ejemplo, si la máscara de usuario se establece en 022, se muestra 22.

Para determinar el valor `umask` que desea definir, reste el valor de los permisos que desee de 666 (para un archivo) o 777 (para un directorio). El resto es el valor que se debe utilizar con el comando `umask`. Por ejemplo, supongamos que desea cambiar el modo predeterminado para los archivos a 644 (`rw-r--r--`). La diferencia entre 666 y 644 es 022, que es el valor que utilizará como un argumento para el comando `umask`.

La tabla siguiente proporciona los valores `umask`. Muestra los permisos de archivo y directorio que se crean para cada uno de los valores octales de `umask`.

TABLA 1-12 Permisos para valores de `umask`

Valor octal de `umask`	Permisos de archivo	Permisos de directorio
`0`	`rw-`	`rwx`
`1`	`rw-`	`rw-`
`2`	`r--`	`r-x`
`3`	`r--`	`r--`
`4`	`-w-`	`-wx`
`5`	`-w-`	`-w-`
`6`	`--x`	`--x`
`7`	`---` (ninguno)	`---` (ninguno)

La siguiente línea en un archivo de inicialización de usuario establece los permisos de archivo predeterminados en `rw-rw-rw-`.

```
umask 000
```

Personalización de un archivo de inicialización de usuario

El siguiente ejemplo muestra un ejemplo del archivo de inicialización de usuario `.profile`. Puede utilizar este archivo de ejemplo como plantilla para personalizar sus propios archivos de inicialización de usuario. En este ejemplo, se utilizan los nombres y las rutas del sistema que tendrá que modificar para su sitio en particular.

EJEMPLO 1-2 Archivo `.profile`

```
PATH=$PATH:$HOME/bin:/usr/local/bin:/usr/gnu/bin:       User's shell serach path
MAIL=/var/mail/$LOGNAME       Path to user's mail file
NNTPSERVER=server1       User's time/clock server
MANPATH=/usr/share/man:/usr/local/man       User's search path for man pages
PRINTER=printer1       User's default printer
```

```
umask 022       User's default file creation permissions
export PATH MAIL NNTPSERVER MANPATH PRINTER      Sets the listed environment variables
```

Gestión de usuarios con el centro de operaciones Oracle Enterprise Manager

Si va a gestionar sistemas operativos físicos y virtuales, servidores y dispositivos de almacenamiento dentro de un centro de datos, en lugar de gestionar solamente sistemas individuales, puede usar las soluciones de gestión disponibles en el centro de operaciones Oracle Enterprise Manager.

Con el centro de operaciones Enterprise Manager puede gestionar usuarios y roles para todo el centro de datos. Puede agregar usuarios locales existentes desde sus sistemas individuales como usuarios del centro de operaciones y puede controlar los activos y las funciones que pueden utilizar estos usuarios.

Para obtener información, consulte http://www.oracle.com/pls/topic/lookup?ctx=oc122.

♦ ♦ ♦ CAPÍTULO 2

Gestión de cuentas de usuario mediante la interfaz de línea de comandos

Este capítulo proporciona información básica para configurar y gestionar cuentas de usuario mediante la interfaz de línea de comandos (CLI).

Para obtener información general sobre la gestión de cuentas de usuario y entornos de usuario, consulte el Capítulo 1, Acerca de las cuentas de usuario y los entornos de usuario.

Para obtener información sobre la gestión de usuarios y roles mediante el uso de la interfaz gráfica de usuario (GUI) de User Manager, consulte el Capítulo 3, Gestión de cuentas de usuarios mediante el uso de la interfaz gráfica de usuario de User Manager.

Mapa de tareas para la configuración y gestión de cuentas de usuario mediante el uso de la interfaz de línea de comandos

Las siguientes tareas describen cómo configurar y gestionar cuentas de usuario mediante la interfaz de línea de comandos (CLI).

Tarea	Descripción	Para obtener instrucciones
Recopilar información de usuario.	Utilice un formulario estándar para recopilar información de usuario a fin de mantenerla organizada.	"Recopilación de información de usuario" [42]
Personalizar los archivos de inicialización de usuario.	Configure archivos de inicialización de usuarios para proporcionar entornos coherentes a los nuevos usuarios.	Cómo personalizar los archivos de inicialización de usuario [42]
Cambiar valores predeterminados de cuentas de todos los roles.	Cambia el directorio principal predeterminado y el directorio de estructura básica de todos los roles.	Cómo cambiar valores predeterminados de cuentas de todos los roles [43]
Crear una cuenta de usuario.	Mediante los valores predeterminados de las cuentas que configura, cree un usuario local con el comando `useradd`.	Cómo agregar un usuario [44]

Tarea	Descripción	Para obtener instrucciones
Modificar una cuenta de usuario.	Modifique la información de inicio de sesión de un usuario en el sistema.	Cómo modificar una cuenta de usuario [45]
Suprimir una cuenta de usuario.	Puede suprimir una cuenta de usuario con el comando `userdel`.	Cómo suprimir un usuario [46]
Crear y, a continuación, asignar un rol para realizar una tarea administrativa.	Mediante los valores predeterminados de las cuentas que configura, cree un rol local, de forma que el usuario pueda realizar una tarea o un comando administrativo específico.	"Creación de roles" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
Crear un grupo.	Para crear un nuevo grupo, utilice el comando `groupadd`.	Cómo agregar un grupo [47]
Agregar atributos de seguridad a una cuenta de usuario.	Después de configurar una cuenta de usuario local, puede agregar los atributos de seguridad necesarios.	"Creación de roles" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 "
Compartir el directorio principal de un usuario.	Debe compartir el directorio raíz de un usuario para que el directorio se pueda montar de manera remota desde el sistema del usuario.	Cómo compartir directorios principales que se crean como sistemas de archivos ZFS [48]
Montar manualmente el directorio principal de un usuario.	Por lo general, no necesita montar de manera manual los directorios principales de usuarios que se crean como un sistema de archivos ZFS. El directorio principal se monta automáticamente cuando se crea y también cuando se inicia desde el servicio del sistema de archivos local SMF.	"Montaje manual del directorio principal de un usuario" [49]

Configuración de cuentas de usuario mediante la interfaz de línea de comandos

En esta sección, se tratan los siguientes temas:

Directrices para la configuración de cuentas de usuario

Tenga en cuenta las siguientes directrices para configurar cuentas de usuario mediante la interfaz de línea de comandos:

- En esta versión, se crean cuentas de usuario como sistemas de archivos ZFS de Oracle Solaris. Como administrador, al crear cuentas de usuario, está concediendo a los usuarios su propio sistema de archivos y su propio conjunto de datos de ZFS. Cada directorio principal creado con los comandos `useradd` y `roleadd` coloca el directorio principal del usuario en el sistema de archivos `/export/home` como un sistema de archivos ZFS *individual*. Como resultado, los usuarios tienen la capacidad de crear copias de seguridad de sus directorios principales, crear instantáneas ZFS de sus directorios principales y reemplazar archivos en su directorio principal actual desde las instantáneas ZFS que han creado.
- Para configurar cuentas de usuario, debe asumir el rol `root` o un rol con el perfil de derechos apropiado, por ejemplo, el perfil de derechos de gestión de usuarios. Consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".
- Al crear una cuenta de usuario con el comando `useradd`, debe especificar la opción `-m` para crear un directorio principal para el usuario.

  Por ejemplo, el siguiente comando creará un directorio raíz para el usuario `jdoe`:

  ```
  # useradd -m jdoe
  ```

  Pero, la siguiente sintaxis *no* creará un directorio raíz para el usuario:

  ```
  # useradd jdoe
  ```

Nota - Si desea que el módulo `pam_zfs_key` cree un directorio principal cifrado para el usuario, *no* especifique la opción `-m` con el comando `useradd`. Consulte las páginas del comando man `pam_zfs_key`(5) y `zfs_encrypt`(1M).

- El comando `useradd` crea entradas en el mapa `auto_home` *sólo* si se especifica la opción `-d` con *hostname*`:`*/pathname*. De lo contrario, el nombre de ruta especificado se actualiza como directorio principal para el usuario en la base de datos `passwd` y no se crea ninguna entrada de mapa `auto_home`. Los directorios raíz que se especifican en el mapa de montador automático `auto_home` sólo se montan si el servicio `autofs` está activado.

  Por ejemplo, si especifica la opción `-d` para crear un usuario como se muestra a continuación, el usuario se crea sin ninguna entrada `auto_home`, y la entrada `passwd` especifica `/export/home/user1` como directorio raíz del usuario:

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

  Si utiliza la opción `-d` para crear el usuario como se muestra a continuación, el usuario tendrá una entrada `auto_home` y la base de datos `passwd` contendrá `/home/user1`, lo que indica una dependencia con el servicio `autofs`:

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

- Si el nombre de ruta del directorio raíz incluye una especificación de host remoto, por ejemplo, `foobar:/export/home/jdoe`, el directorio raíz para `jdoe` se debe crear en el sistema `foobar`. El nombre de ruta predeterminado es `localhost:/export/home/`*username*.
- Cuando un sistema de archivos es un conjunto de datos ZFS, que es el caso de todos los Oracle Solaris 11, el directorio principal del usuario se crea como un conjunto de datos ZFS secundario, con el permiso de ZFS para tomar instantáneas delegado para el usuario. Si se especifica un nombre de ruta que no se corresponde con un conjunto de datos ZFS, se crea un directorio regular. Si se especifica la opción `-S ldap`, se actualiza la entrada de asignación `auto_home` en el servidor LDAP en lugar de la asignación `auto_home`.

Recopilación de información de usuario

Al configurar cuentas de usuario, puede crear un formulario similar al siguiente para recopilar información sobre los usuarios antes de agregar sus cuentas.

Elemento	Descripción
Nombre de usuario	
Nombre del rol	
Perfiles o autorizaciones	
UID	
Grupo principal	
Grupos secundarios	
Comentarios	
Shell predeterminado	
Caducidad y estado de contraseña	
Nombre de ruta de directorio principal	
Método de montaje	
Permisos en directorio principal	
Servidor de correo	
Agregar a estos alias de correo	
Nombre de sistema de escritorio	

▼ Cómo personalizar los archivos de inicialización de usuario

Las siguientes tareas describen cómo configurar archivos de inicialización personalizados para el usuario en su sistema.

1. **Asuma el rol `root` o un rol con perfil de derechos de gestión de usuarios.**

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

Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Cree un directorio de estructura básica para cada tipo de usuario.**

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

shared-dir — El nombre de un directorio que está disponible para otros sistemas en una red.

user-type — El nombre de un directorio para almacenar archivos de inicialización de un tipo de usuario.

3. **Copie los archivos de inicialización de usuario predeterminados en los directorios que creó para los distintos tipos de usuarios.**

4. **Personalice los archivos de inicialización de usuario para cada tipo de usuario.**

Para obtener una descripción detallada de las maneras de personalizar los archivos de inicialización de usuario, consulte “Acerca del entorno de trabajo del usuario” [26].

5. **Establezca los permisos para los archivos de inicialización de usuario.**

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

6. **Verifique que los permisos de los archivos de inicialización de usuario sean correctos.**

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

▼ Cómo cambiar valores predeterminados de cuentas de todos los roles

En el procedimiento siguiente, el administrador ha personalizado un directorio `roles`. El administrador cambia el directorio principal predeterminado y el directorio de estructura básica de todos los roles.

1. **Asuma el rol `root` o un rol con perfil de derechos de gestión de usuarios.**

Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Cree un directorio de roles personalizado.**
   Por ejemplo:

```
# 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. **Cambie el directorio principal predeterminado y el directorio de estructura básica de todos los roles.**
   Por ejemplo:

```
# 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=
```

   Los usos futuros del comando `roleadd` crean directorios principales en `/export/home` y rellenan el entorno de los roles del directorio `/etc/skel/roles`.

Gestión de cuentas de usuario mediante la interfaz de línea de comandos

En esta sección, se tratan los siguientes temas:

▼ Cómo agregar un usuario

1. **Asuma el rol `root` o un rol con perfil de derechos de gestión de usuarios.**
   Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Cree un usuario local.**
   De manera predeterminada, el usuario se crea localmente. Si incluye la opción `-S ldap`, el usuario se crea en un repositorio LDAP existente.

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

`useradd`	Crea una cuenta para el usuario especificado.
`-d`	Especifica la ubicación del directorio raíz del usuario. Utilice `-d localhost:/export/home/`*username* en lugar de `-d /export/home/`*username* para forzar que la entrada se escriba en `auto_home`.
`-m`	Crea un directorio raíz local en el sistema para el usuario.

   Para obtener una descripción detallada de todas las opciones y argumentos que puede especificar con el comando `useradd`, consulte la página del comando man `useradd`(1M).

   Nota - La cuenta está bloqueada hasta que le asigna al usuario una contraseña.

3. **Asigne al usuario una contraseña.**

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

   Para conocer más opciones de comandos, consulte las páginas del comando man `useradd`(1M) y `passwd`(1).

Véase también Después de crear un usuario, es posible que necesite realizar algunas tareas adicionales, incluida la agregación y la asignación de roles a un usuario y la visualización o el cambio de perfiles de derechos de un usuario. Para obtener más información, consulte "Creación de roles" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

▼ Cómo modificar una cuenta de usuario

El comando `usermod` se usa para cambiar la definición de inicio de sesión de un usuario y para realizar los cambios de sistema de archivos relacionados con el inicio de sesión que sean apropiados para el usuario.

1. **Asuma el rol `root` o un rol con perfil de derechos de gestión de usuarios.**
   Consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Modifique la cuenta de usuario según sea necesario.**

Consulte la página del comando man usermod(1M) para obtener información detallada acerca de los argumentos y las opciones que puede especificar con el comando usermod.

Por ejemplo, para agregar un rol a un usuario, escriba:

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

ejemplo 2-1 Configuración de la política de PAM por usuario mediante la modificación de la cuenta del usuario

En el siguiente ejemplo, se muestra cómo modificar un usuario para definir una política de PAM. Esta modificación particular especifica que el usuario jdoe sólo debe estar autenticado con el protocolo Kerberos V5 para todos los servicios PAM. Consulte la página del comando man pam_user_policy(5) para obtener más información.

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

Véase también Para obtener información adicional, consulte “Creación de roles” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

▼ Cómo suprimir un usuario

1. **Asuma el rol de usuario root.**

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

Nota - Este método funciona si root es una cuenta de usuario o un rol.

2. **Archive el directorio principal del usuario.**

3. **Suprima el usuario.**

```
# userdel -r username
```

```
The -r option removes the account from the system.
```

Debido a que los directorios principales del usuario ahora son conjuntos de datos ZFS, el método preferido para eliminar un directorio principal local de un usuario suprimido es especificar la opción -r con el comando userdel.

4. **Si el directorio principal del usuario está en un servidor remoto, suprímalo manualmente.**

```
# userdel username
```

Para obtener una lista completa de opciones de comandos, consulte la página del comando man `userdel`(1M).

Pasos siguientes Es posible que se requiera una limpieza adicional si el usuario que ha suprimido tenía responsabilidades administrativas, por ejemplo, la creación de trabajos `cron`, o si el usuario tenía cuentas adicionales en zonas no globales.

▼ Cómo agregar un grupo

Cuando un administrador crea un grupo, el sistema asigna `solaris.group.assign /`*groupname* para ese administrador, lo que le proporciona control completo sobre ese grupo. Si otro administrador con la misma autorización crea un grupo, éste tiene el control sobre ese grupo. Un administrador que tiene el control de un grupo no puede administrar el grupo del otro administrador. Para obtener más información, consulte las páginas del comando man `groupadd`(1M) y `groupmod`(1M).

1. **Asuma el rol `root` o un rol de administrador con la autorización `solaris.group.manage`.**

   Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Enumere los grupos existentes.**

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

3. **Cree un nuevo grupo.**

   ```
   $ groupadd -g group-id group-name
   ```

`groupadd`	Crea una nueva definición de grupo en el sistema agregando la entrada adecuada al archivo `/etc/group`.
`-g`	Asigna el ID de grupo para el nuevo grupo.

   Para obtener más información, consulte la página del comando man `groupadd`(1M).

ejemplo 2-2 Configuración de un grupo y un usuario con los comandos `groupadd` y `useradd`

En el siguiente ejemplo se muestra cómo utilizar los comandos `groupadd` y `useradd` para agregar el grupo `scutters` y el usuario `scutter1` a los archivos en el sistema 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
```

Para obtener más información, consulte las páginas del comando man `groupadd`(1M) y `useradd`(1M).

Cómo compartir sistemas de archivos ZFS

En esta versión de Oracle Solaris, puede compartir un sistema de archivos ZFS configurando la propiedad `share.nfs` o la propiedad `share.smb`. También puede crear un recurso compartido de sistema de archivos mediante el comando `zfs share`. De manera predeterminada, todos los sistemas de archivos están sin compartir.

De manera predeterminada, el conjunto de datos `pool/export/home` ya está montado en `/export/home`. El comando `useradd` crea automáticamente juegos de datos por usuario como juegos secundarios de este conjunto de datos. Como administrador, puede crear un grupo nuevo para los directorios raíz de usuario.

Para obtener más información sobre el uso compartido o el uso no compartido de sistemas de archivos, consulte “Administración de autofs” de “Gestión de sistemas de archivos de red en Oracle Solaris 11.2 ”.

▼ Cómo compartir directorios principales que se crean como sistemas de archivos ZFS

1. **Asuma el rol de usuario `root`.**

   Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Cree una agrupación separada para los directorios principales del usuario.**

   ```
   # zpool create pool mirror disk 1 disk 2 mirror disk 3 disk 4
   ```

   Por ejemplo:

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

3. **Cree un contenedor para los directorios principales.**

   ```
   # zfs create filesystem
   ```

   Por ejemplo:

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

4. **Defina las propiedades de recursos compartidos para el directorio raíz.**

   Por ejemplo, para crear un recurso compartido de NFS y establecer la propiedad `share.nfs` para `users/home`, escriba:

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

   Al utilizar esta nueva sintaxis, cada sistema de archivos contiene un "recurso compartido automático" que se crea apenas la propiedad `share.nfs` (o la propiedad `share.smb`) se define en `on` para ese sistema de archivos. El comando anterior comparte un sistema de archivos denominado `users/home` y todos sus subordinados.

5. **Confirme que los recursos compartidos de los sistemas de archivos descendentes también se publiquen.**

   Por ejemplo:

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

   La opción `-r` muestra todos los sistemas de archivos descendientes.

Montaje manual del directorio principal de un usuario

Las cuentas de usuario que se crean como sistemas de archivos ZFS no necesitan, normalmente, ser montadas de manera manual. Con ZFS, los sistemas de archivos se montan de manera automática cuando se crean y luego se montan en el momento del inicio desde el servicio del sistema de archivos local SMF.

Al crear cuentas de usuario, asegúrese de que los directorios principales estén establecidos como lo están en el servicio de nombres, en `/home/`*username*. A continuación, asegúrese de que el mapa `auto_home` indique la ruta NFS al directorio principal del usuario. Para obtener más información relacionada con la tarea, consulte “Administración de autofs” de “Gestión de sistemas de archivos de red en Oracle Solaris 11.2 ”.

Si necesita montar manualmente el directorio principal de un usuario, utilice el comando `zfs mount`. Por ejemplo:

```
# zfs mount users/home/jdoe
```

Nota - Asegúrese de que el directorio principal del usuario esté compartido. Para obtener más información, consulte Cómo compartir directorios principales que se crean como sistemas de archivos ZFS [48].

♦ ♦ ♦ CAPÍTULO 3

Gestión de cuentas de usuarios mediante el uso de la interfaz gráfica de usuario de User Manager

En este capítulo, se proporciona una descripción general e información relacionada con tareas para configurar y gestionar usuarios mediante la interfaz gráfica de usuario (GUI) de Solaris User Manager. Puede usar la interfaz gráfica de usuario de User Manager para realizar la mayoría de las tareas que se pueden realizar con los comandos equivalentes, como `useradd`, `usermod` y `userdel`. Para obtener más información sobre la interfaz gráfica de usuario de User Manager, consulte la ayuda en pantalla en la GUI.

En este capítulo, se tratan los siguientes temas:

- “Introducción a la interfaz gráfica de usuario de User Manager” [51]
- “Agregación, modificación y supresión de usuarios y roles mediante la interfaz gráfica de usuario de User Manager” [56]
- “Asignación de atributos avanzados con la interfaz gráfica de usuario de User Manager” [59]

Para obtener información general sobre la gestión de cuentas de usuario, consulte el Capítulo 1, Acerca de las cuentas de usuario y los entornos de usuario.

Para obtener más información sobre la gestión de cuentas de usuario mediante la interfaz de línea de comandos, consulte el Capítulo 2, Gestión de cuentas de usuario mediante la interfaz de línea de comandos.

Introducción a la interfaz gráfica de usuario de User Manager

En esta sección se incluye la siguiente información:

- Cómo iniciar la interfaz gráfica de usuario de User Manager [52]
- “Organización del cuadro de diálogo de User Manager” [52]
- “Filtrado de la información que se muestra en la interfaz gráfica de usuario” [54]

- “Asunción de un rol” [55]

La interfaz gráfica de usuario de User Manager se basa en la estructura Visual Panels y se brinda como una interfaz de Visual Panels. La autenticación de usuarios y la asunción de roles es proporcionada por la estructura Visual Panels y está disponible para todos los paneles, incluida la interfaz gráfica de usuario de User Manager. La interfaz gráfica de usuario de User Manager reemplaza la herramienta User y Roles de Solaris Management Console que se admite en Solaris 10. Aunque no es idéntica a Solaris Management Console, la interfaz gráfica de usuario ofrece algunas de las mismas funciones.

Nota - Solaris Management Console *no* es compatible con esta versión.

La interfaz gráfica de usuario de User Manager presenta una interfaz simple y clara que es fácil de usar. Para minimizar la posibilidad de errores, la interfaz gráfica de usuario sólo presenta las opciones válidas, en función de las autorizaciones y los perfiles de derechos del usuario o rol autenticado.

La interfaz gráfica de usuario de User Manager es proporcionada por el paquete IPS `pkg:/system/management/visual-panels/panel-usermgr`.

▼ Cómo iniciar la interfaz gráfica de usuario de User Manager

1. **Asuma el rol `root` o inicie sesión como usuario con el perfil de derechos de User Management asignado.**
   Consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.
2. **Inicie la interfaz gráfica de usuario de User Manager.**
   - **Escritorio: seleccione Sistema -> Administración -> User manager.**
   - **Línea de comandos:**

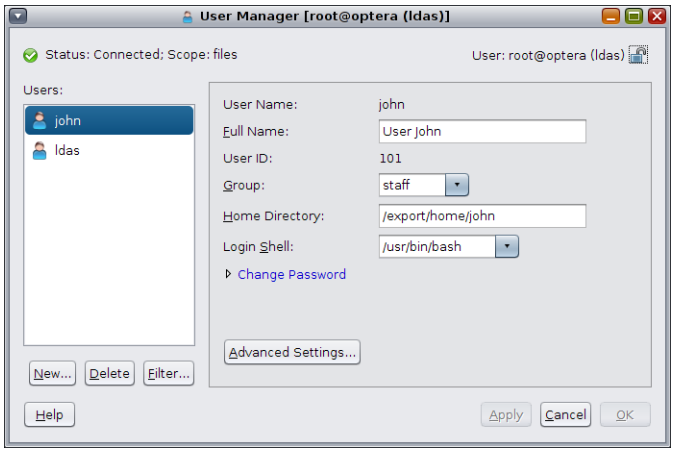
     ```
     # vp usermgr &
     ```

Organización del cuadro de diálogo de User Manager

Cuando inicia la interfaz gráfica de usuario de User Manager, se muestra el cuadro de diálogo de User Manager. El cuadro de diálogo de User Manager se utiliza para administrar usuarios y

roles. En la parte superior izquierda del cuadro de diálogo está el campo Estado, que muestra el estado de los servicios que se están ejecutando actualmente en el host local. En la parte superior derecha del cuadro de diálogo está el campo Usuario, que muestra la credencial que está utilizando actualmente en la interfaz gráfica de usuario de User Manager. Para conocer cómo cambiar las credenciales, consulte “Asunción de un rol” [55].

La siguiente figura muestra el cuadro de diálogo principal de User Manager con el usuario, John, seleccionado.



El cuadro de diálogo de User Manager incluye los siguientes componentes:

- Lista de usuarios y roles: una lista de usuarios que puede seleccionar para administrar.
- Configuración básica: configuración básica de un usuario, como el nombre de usuario y el nombre completo.

Para ver o modificar la información para un usuario existente, seleccione el usuario de la lista de usuarios que se muestra. Después de seleccionar un usuario, la información de ese usuario aparece en el lado derecho del cuadro de diálogo.

Las siguientes acciones están disponibles dentro del cuadro de diálogo de User Manager:

- Crear un usuario o rol nuevo: consulte Cómo agregar un usuario o rol con la interfaz gráfica de usuario de User Manager [56].
- Suprimir un usuario o rol existente: consulte Cómo suprimir un usuario o rol con la interfaz gráfica de usuario de User Manager [58]
- Filtrar la información de un usuario: consulte “Filtrado de la información que se muestra en la interfaz gráfica de usuario” [54].
- Administrar la configuración avanzada de un usuario existente: consulte Cómo modificar un usuario o rol con la interfaz gráfica de usuario de User Manager [58].

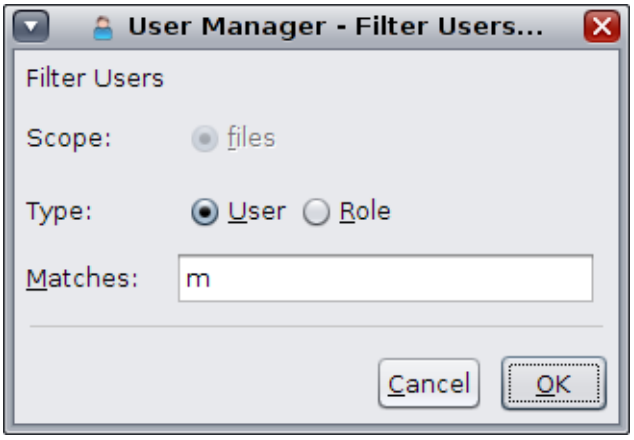
Filtrado de la información que se muestra en la interfaz gráfica de usuario

Puede filtrar la información que se muestra en la interfaz gráfica de usuario de User Manager. Puede elegir mostrar sólo los usuarios o puede elegir mostrar sólo los roles. Además, puede limitar el ámbito para mostrar información de archivo o la información de LDAP si el sistema está configurado como cliente LDAP.

Los valores predeterminados son Usuario y Archivos. Estos valores muestran los usuarios, en lugar de los roles, y muestran información de archivo de los usuarios, en lugar de mostrar las especificaciones de LDAP para un usuario.

En el cuadro de diálogo de filtro, también pude buscar los nombres de usuario o los nombres de rol que coincidan con los criterios de búsqueda que usted introduzca.

En el siguiente cuadro de diálogo, el sistema no está configurado para LDAP, de modo que la opción de ámbito no está disponible. El tipo se filtra para mostrar los usuarios en lugar de los roles. Además, se especifica una búsqueda para encontrar nombres de usuarios que comienzan con "m".



▼ Cómo definir filtros para el ámbito y tipo de servicio de nombres predeterminado

1. **Inicie la interfaz gráfica de usuario de User Manager.**
   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].
2. **Haga clic en el botón Filtro.**

3. **Defina la opción Ámbito para el archivo o, si está disponible, para LDAP.**
4. **Definir la opción Tipo para el usuario o el rol.**
5. **De manera opcional, para filtrar nombres de roles o de usuario específicos, introduzca el texto que desee buscar.**
6. **Haga clic en el botón Aceptar.**

Asunción de un rol

Si tiene un perfil de derechos de User Manager, puede crear nuevos usuarios y nuevos roles, siempre que los atributos avanzados del usuario o rol que se va a crear sean un subconjunto de los de su propia autoridad. Si no dispone de suficiente autorización pero tiene un rol administrativo con suficiente autorización, puede asumir el rol para realizar la administración necesaria haciendo clic en el botón Bloquear en el cuadro de diálogo principal de User Manager, tal como se describe en este procedimiento.

▼ Cómo asumir un rol

1. **Inicie la interfaz gráfica de usuario de User Manager.**

   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].

2. **En el cuadro de diálogo principal de User manager, haga clic en el icono Bloquear junto al nombre de usuario en la sección superior derecha del cuadro de diálogo.**

   Aparece un submenú que contiene las siguientes opciones:

   - Cambiar rol
   - Cambiar usuario
   - Administrar nuevo host
   - Borrar historial

3. **Seleccione la opción para cambiar rol.**

   Se muestra un cuadro de diálogo de autenticación. El cuadro de diálogo de autenticación contiene un menú desplegable que muestra los roles disponibles para usted.

4. **Seleccione el rol adecuado.**
5. **Haga clic en Iniciar sesión para asumir ese rol.**

   Después de asumir el rol, puede realizar las tareas administrativas requeridas.

Agregación, modificación y supresión de usuarios y roles mediante la interfaz gráfica de usuario de User Manager

La agregación, modificación y supresión de los usuarios mediante la interfaz gráfica de usuario de User Manager es equivalente al uso de los comandos `useradd`, `usermod` y `userdel` respectivamente. Para obtener más información sobre cómo agregar usuarios desde la línea de comandos, consulte el Capítulo 2, Gestión de cuentas de usuario mediante la interfaz de línea de comandos.

Esta sección describe la siguiente información:

▼ Cómo agregar un usuario o rol con la interfaz gráfica de usuario de User Manager

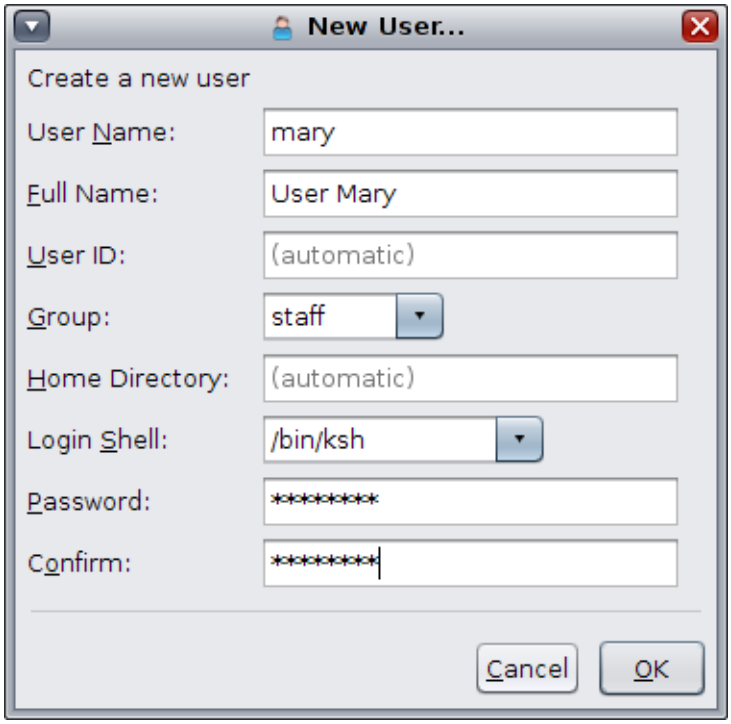
Este procedimiento agrega un nuevo usuario o rol en el ámbito del filtro que está utilizando actualmente la interfaz gráfica de usuario.

1. **Inicie la interfaz gráfica de usuario de User Manager.**

   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].

2. **Haga clic en el botón Nuevo, en el cuadro de diálogo principal de User manager.**

   Se muestra el cuadro de diálogo de nuevo usuario.



3. **Proporcione la información de la cuenta del usuario.**

   - Nombre de usuario
   - Nombre completo
   - ID de usuario: esta información es opcional. Si no se proporciona ninguna información, el sistema le asigna automáticamente un valor predeterminado.
   - Grupo: las opciones disponibles para el campo Grupo varían en función de la configuración del sistema.
   - Directorio principal: esta información es opcional. Si no se proporciona ninguna información, el sistema le asigna automáticamente un valor predeterminado.

     Si desea que el directorio raíz del usuario sea de montaje automático, coloque el nombre de host o el host local delante del nombre de ruta. Por ejemplo, `localhost:/export/home/test1`.
   - Shell de inicio de sesión: las opciones para el campo Shell de inicio de sesión pueden variar en función de la configuración del sistema.
   - Contraseña: asigne una contraseña temporal al usuario.
   - Confirmar: confirme la contraseña temporal que haya asignado al usuario.

4. **Haga clic en el botón Aceptar.**

   El usuario o rol se agrega a la lista de usuarios que se muestra en el cuadro de diálogo principal de User manager, haga clic en Aceptar.

▼ Cómo modificar un usuario o rol con la interfaz gráfica de usuario de User Manager

1. **Inicie la interfaz gráfica de usuario de User Manager.**

   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].

2. **Seleccione el usuario o el rol que desea modificar de la lista que se muestra.**

   Después de seleccionar el usuario, el lado derecho del cuadro de diálogo se rellena con información sobre el usuario actual.

3. **Modifique una parte o la totalidad de la información del usuario o rol actual.**

   Nota - Si se modifica un campo, se muestra un indicador junto al campo.

4. **Haga clic en Apply (Aplicar) para guardar los cambios.**

5. **(Opcional) Haga clic en el botón Advanced Settings (Configuración avanzada) para modificar los atributos de seguridad adicionales para el usuario o rol.**

   Consulte “Asignación de atributos avanzados con la interfaz gráfica de usuario de User Manager” [59].

6. **Haga clic en Aceptar para guardar los cambios y cerrar el cuadro de diálogo.**

▼ Cómo suprimir un usuario o rol con la interfaz gráfica de usuario de User Manager

Este procedimiento suprime un usuario o un rol en el ámbito del filtro que se está utilizando actualmente en la interfaz gráfica de usuario de User Manager.

1. **Seleccione el usuario o el rol en el cuadro de diálogo principal de User manager.**

2. **Haga clic en el botón Suprimir.**

3. **Haga clic en Aceptar en el cuadro de diálogo de confirmación.**

Asignación de atributos avanzados con la interfaz gráfica de usuario de User Manager

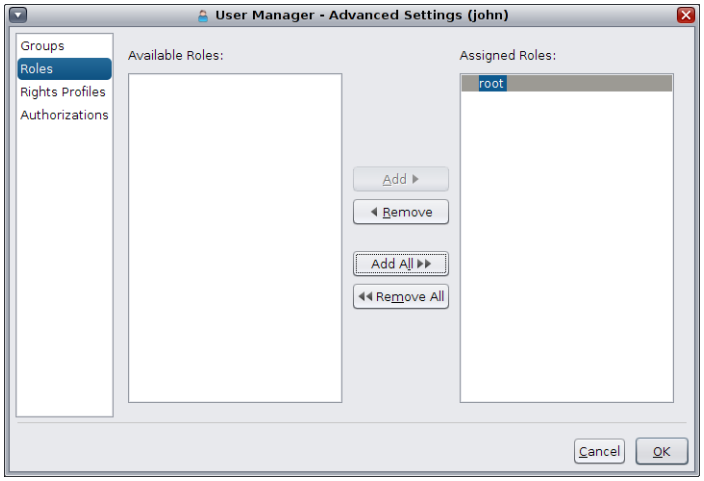
Esta sección describe la siguiente información:

- “Asignación de grupos con la interfaz gráfica de usuario de User Manager” [60]
- “Asignación de roles con la interfaz gráfica de usuario de User Manager” [61]
- “Asignación de perfiles de derechos con la interfaz gráfica de usuario de User Manager” [62]
- “Asignación de autorizaciones con la interfaz gráfica de usuario de User Manager” [64]

Utilice el cuadro de diálogo Advanced Settings (configuración avanzada) de la interfaz gráfica de usuario de User Manager para asignar atributos de seguridad adicionales, por ejemplo, perfiles de derechos, roles y autorizaciones.

Para obtener una descripción general, consulte el Capítulo 1, “Sobre el uso de los derechos para controlar los usuarios y los procesos” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

La siguiente figura muestra el cuadro de diálogo Configuración avanzada con el atributo de seguridad Roles del usuario john seleccionado. El nombre del usuario seleccionado aparece entre paréntesis en la barra de título del cuadro de diálogo.



El cuadro de diálogo de configuración avanzada permite asignar los siguientes atributos de seguridad:

- Grupos
- Roles
- Perfiles de derechos
- Autorizaciones

Asignación de grupos con la interfaz gráfica de usuario de User Manager

Los grupos se asignan mediante la configuración avanzada de la interfaz gráfica de usuario de User Manager.

▼ Cómo asignar grupos

1. **Inicie la interfaz gráfica de usuario de User Manager.**

   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].

2. **Seleccione un usuario en el cuadro de diálogo de User Manager y, luego, haga clic en el botón Configuración avanzada.**

   Se abre el cuadro de diálogo correspondiente.

3. **Haga clic en el atributo Grupos en la parte izquierda del cuadro de diálogo.**

   Se muestra una lista de todos los grupos disponibles y una lista de los grupos a los que pertenece el usuario actual.

   - **Para asignar un grupo (o varios grupos) a un usuario, seleccione el grupo (o los grupos) desde la lista Available Groups (Grupos disponibles) y, luego, haga clic en Add (Agregar).**

     El grupo agregado aparece en la lista Assigned Groups (Grupos asignados).

   - **Para eliminar un grupo de la lista Assigned Groups (Grupos asignados), seleccione el grupo (o los grupos) de la lista y, luego, haga clic en Remove (Eliminar).**

   - **Para agregar o eliminar todos los grupos para el usuario actual, haga clic en Add All (Agregar todos) o Remove All (Eliminar todos).**

4. **Haga clic en OK (Aceptar) para guardar la configuración.**

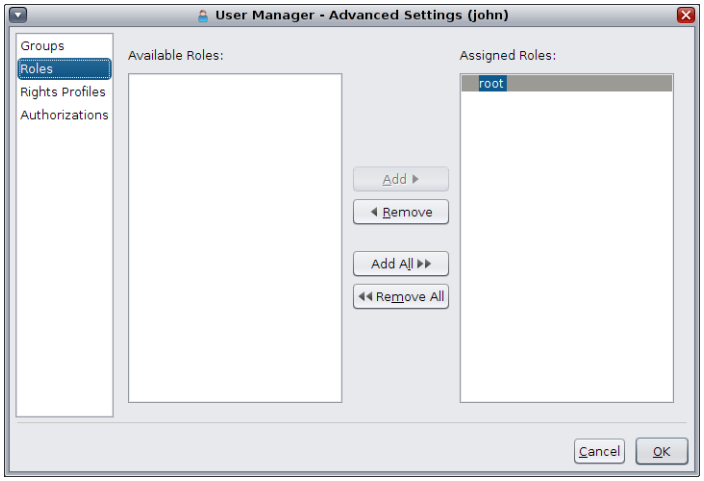
Los cambios no se aplicarán hasta que haga clic en Aceptar o Aplicar en el cuadro de diálogo de User Manager.

Asignación de roles con la interfaz gráfica de usuario de User Manager

Los roles se asignan mediante la configuración avanzada de la interfaz gráfica de usuario de User Manager.

Nota - El atributo Roles está disponible sólo para un usuario, no para un rol, porque los roles sólo se pueden asignar a los usuarios.

La siguiente figura muestra el cuadro de diálogo Configuración avanzada con el atributo de seguridad Roles del usuario john seleccionado.



▼ Cómo asignar roles con la interfaz gráfica de usuario de User Manager

1. **Inicie la interfaz gráfica de usuario de User Manager.**
   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].

2. **Seleccione un usuario en el cuadro de diálogo de User Manager y, luego, haga clic en el botón Configuración avanzada.**

Se abre el cuadro de diálogo correspondiente.

3. **Haga clic en el atributo Roles en la parte izquierda del cuadro de diálogo.**

   Se muestra una lista de los roles disponibles y una lista de los roles que están asignados al usuario actual.

   - **Para asignar un rol (o varios roles) a un usuario, seleccione el rol (o los roles) de la lista de roles disponibles y haga clic en Add (Agregar).**

     El rol agregado se muestra en la lista de roles asignados.

   - **Para eliminar un rol de la lista de roles asignados, seleccione el rol (o los roles) de la lista y, luego, haga clic en Remove (Eliminar).**

   - **Para agregar o eliminar todos los roles para el usuario actual, haga clic en Add All (Agregar todos) o Remove All (Eliminar todos).**

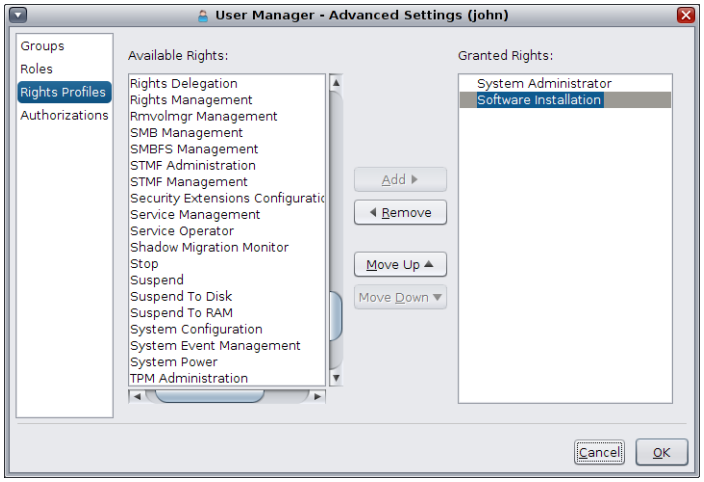
4. **Haga clic en OK (Aceptar) para guardar la configuración.**

   Los cambios no se aplicarán hasta que haga clic en Aceptar o Aplicar en el cuadro de diálogo de User Manager.

Asignación de perfiles de derechos con la interfaz gráfica de usuario de User Manager

Los perfiles de derechos se asignan mediante la configuración avanzada de la interfaz gráfica de usuario de User Manager.

La siguiente figura muestra el cuadro de diálogo Configuración avanzada con el atributo de seguridad Perfil de derechos del usuario john seleccionado.



Nota - La asignación de perfiles de derechos tiene un orden de prioridad. Utilice los botones Mover hacia arriba y Mover hacia abajo para cambiar el orden de los perfiles de derechos que se otorgan al usuario actual.

▼ Cómo administrar perfiles de derechos con la interfaz gráfica de usuario de User Manager

1. **Inicie la interfaz gráfica de usuario de User Manager.**

   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].

2. **Seleccione un usuario en el cuadro de diálogo de User Manager y, luego, haga clic en el botón Configuración avanzada.**

   Se abre el cuadro de diálogo correspondiente.

3. **Haga clic en el atributo Perfil de roles en la parte izquierda del cuadro de diálogo.**

   Se muestra una lista de los perfiles de derechos disponibles y una lista de los perfiles de derechos otorgados al usuario actual.

   - **Para asignar un perfil de derechos (o varios perfiles de derechos) a un usuario, seleccione el perfil de derechos (o los perfiles de derechos) desde la lista de perfiles de derechos disponibles y, luego, haga clic en Add (Agregar).**

     El perfil de derechos agregado se muestra en la lista de perfiles de derechos otorgados.

- **Para eliminar un perfil de derechos de la lista de perfiles de derechos otorgados, seleccione el perfil de derechos (o los perfiles de derechos) y, luego, haga clic en Remove (Eliminar).**
- **Para agregar o eliminar todos los perfiles de derechos para el usuario actual, haga clic en Add All (Agregar todos) o Remove All (Eliminar todos).**

4. **Haga clic en OK (Aceptar) para guardar la configuración.**

   Los cambios no se aplicarán hasta que haga clic en Aceptar o Aplicar en el cuadro de diálogo de User Manager.

Asignación de autorizaciones con la interfaz gráfica de usuario de User Manager

Un usuario normalmente obtiene autorizaciones de manera indirecta mediante un perfil de derechos. La configuración de autorizaciones se puede usar para otorgar una autorización específica a un usuario o rol. Algunas autorizaciones pueden tener atributos adicionales, como un nombre de objeto. Por ejemplo, cuando un administrador crea el grupo `games`, obtiene una autorización implícita: `solaris.group.manage/games`. Los nombres de objeto aparecerán en la lista de autorizaciones otorgadas.

▼ Cómo asignar autorizaciones con la interfaz gráfica de usuario de User Manager

1. **Inicie la interfaz gráfica de usuario de User Manager.**

   Consulte Cómo iniciar la interfaz gráfica de usuario de User Manager [52].

2. **Seleccione un usuario en el cuadro de diálogo de User Manager y, luego, haga clic en el botón Configuración avanzada.**

   Se abre el cuadro de diálogo correspondiente.

3. **Haga clic en el atributo Autorización en la parte izquierda del cuadro de diálogo.**

   Se muestra una lista de las autorizaciones disponibles y una lista de las autorizaciones que se otorgan al usuario actual.

   - **Para asignar una autorización (o varias autorizaciones) para un usuario, seleccione la autorización (o las autorizaciones) de la lista de autorizaciones disponibles y, luego, haga clic en Add (Agregar).**

     La autorización agregada se muestra en la lista de autorizaciones otorgadas.

- **Para eliminar una autorización de la lista de autorizaciones otorgadas, seleccione la autorización (o las autorizaciones) de la lista y, luego, haga clic en Remove (Eliminar).**

- **Para agregar o eliminar todas las autorizaciones para el usuario actual, haga clic en Add All (Agregar todos) o Remove All (Eliminar todos).**

4. **Haga clic en OK (Aceptar) para guardar la configuración.**

   Los cambios no se aplicarán hasta que haga clic en Aceptar o Aplicar en el cuadro de diálogo de User Manager.

Índice

D

E

G

H

I

K

L

M

V