Gestión de las cuentas de usuario y los entornos de usuario en Oracle® Solaris 11.1

Referencia: E36538–01
Octubre de 2012

ORACLE®

130327@25097

Contenido

Prefacio

Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.1 forma parte de un conjunto de documentación que incluye una gran cantidad de información sobre la administración del sistema Oracle Solaris. Esta guía contiene información para los sistemas basados en SPARC y x86.

Este manual asume que ha completado las siguientes tareas:

- Instalar el software Oracle Solaris
- Configurar todo el software de redes que tenga previsto usar

Para Oracle Solaris, se incluyen nuevas funciones que podrían ser interesantes para los administradores del sistema en secciones cuyo título empieza con *Novedades de...* en los capítulos correspondientes.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en *Listas de compatibilidad del sistema operativo Oracle Solaris*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

Para conocer cuáles son los sistemas admitidos, consulte *Listas de compatibilidad del sistema operativo Oracle Solaris*.

Quién debe utilizar este manual

Esta guía está dirigida a los responsables de administrar uno o más sistemas que ejecutan la versión Oracle Solaris. Para utilizar este manual, se debe tener como mínimo entre uno y dos años de experiencia en la administración de sistemas UNIX. Puede resultar útil participar en cursos de formación para administración de sistemas UNIX.

Acceso a 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`.

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

TABLA P–1 Convenciones tipográficas

Tipos de letra	Descripción	Ejemplo
`AaBbCc123`	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo `.login`. Utilice el comando `ls -a` para mostrar todos los archivos. `nombre_sistema% tiene correo.`
`AaBbCc123`	Lo que se escribe, en contraposición con la salida del equipo en pantalla	`nombre_sistema% su` `Contraseña:`
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es `rm` *nombre_archivo*.
AaBbCc123	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la *Guía del usuario*. Una *copia en caché* es aquella que se almacena localmente. *No* guarde el archivo. **Nota**: Algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

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 P–2 Indicadores de 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#`

◆ ◆ ◆ CAPÍTULO 1

Gestión de cuentas de usuario y entornos de usuario (descripción general)

A continuación, se indica la información contenida en este capítulo:

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 (tareas)" y el Capítulo 3, "Gestión de cuentas de usuarios mediante el uso de la interfaz gráfica de usuario de User Manager (tareas)".

Novedades y cambios en la gestión de cuentas de usuario y entornos de usuario

Las siguientes funciones son nuevas o se han cambiado en esta versión:

Cambios de seguridad que afectan la gestión de cuentas de usuario

Las siguientes funciones han cambiado en esta versión:

- Refinamientos de transición de estado para el comando `password`. Este cambio indica qué cuentas de usuario se pueden o no se pueden bloquear. Los cambios principales impactan en las definiciones de las propiedades `LK` y `NL`. Estos cambios son los siguientes:

  `LK` La cuenta está bloqueada. El comando `passwd -l` se ejecutó o la cuenta se bloqueó automáticamente debido a que el número de errores de autenticación alcanzó el número máximo configurado permitido. Consulte las páginas del comando man `policy.conf(4)` y `user_attr(4)`.

  `NL` La cuenta está configurada para la autenticación que no es de UNIX. El comando `passwd -N` se ejecutó. A partir de esta versión, las cuentas en este estado se pueden bloquear mediante la ejecución del comando `passwd -l` y se pueden desbloquear mediante la ejecución del comando `passwd -u`.

- Autorizaciones calificadas. Las autorizaciones pueden calificarse para aplicarse a objetos específicos, como grupos, zonas o nombres de archivos. Consulte "Editor administrativo (pfedit)" en la página 13.
- Se ha vuelto a escribir el comando `profiles` para gestionar perfiles de derechos para ámbitos locales y LDAP. Ya no se admite la edición directa de archivos de control de acceso basado en roles (RBAC).
- En esta versión está disponible la capacidad de definir una política de módulo de autenticación conectable (PAM) por usuario (`pam_policy`) en un perfil de derechos. La política `pam_policy` debe ser un nombre de ruta absoluto a un archivo con formato `pam_conf`(4) o el nombre de un archivo con formato `pam.conf` (4) ubicado en el archivo `/etc/security/pam_policy`. Consulte `pam_user_policy(5)`.

  Además de establecer la política de PAM en un perfil de derechos, también puede establecer directamente `pam_policy` en la entrada `user_attr` del usuario mediante el comando `useradd` o el comando `usermod`. Consulte el Ejemplo 2–1.
- Los usuarios y roles que tienen asignado el perfil de derechos de seguridad de usuario pueden crear nuevas cuentas de usuario, así como delegar algunos de sus derechos a otras cuentas, sin asumir el rol `root`.

Para obtener más información, consulte la Parte III, "Roles, perfiles de derechos y privilegios" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Introducción a la interfaz gráfica de usuario de User Manager

Puede configurar y gestionar usuarios, roles y grupos con la interfaz gráfica de usuario (GUI) de User Manager de Oracle Solaris. La interfaz gráfica de usuario de User Manager está disponible en el escritorio y forma parte del proyecto Visual Panels. En esta versión, la interfaz gráfica de usuario de User Manager sustituye a la interfaz gráfica de usuario de Solaris Management Console. Las tareas que puede realizar con la interfaz gráfica de usuario de User Manager son, en esencia, las mismas que puede realizar mediante la interfaz de línea de comandos, por ejemplo, los comandos `useradd` , `usermod`, `userdel`, `roleadd` , `rolemod`, `roledel`.

Para obtener instrucciones sobre el uso de la interfaz gráfica de usuario de User Manager, consulte el Capítulo 3, "Gestión de cuentas de usuarios mediante el uso de la interfaz gráfica de usuario de User Manager (tareas)" y la ayuda en pantalla.

Editor administrativo (`pfedit`)

Un editor administrativo (`pfedit`) se puede utilizar para editar archivos de sistema en esta versión. Si lo define el administrador del sistema, el valor de este editor es `$EDITOR`. Si el editor no está definido, se utiliza de manera predeterminada el comando `vi`.

Inicie el editor de la siguiente manera:

```
$ pfedit system-filename
```

Para editar archivos de sistema con el comando `pfedit`, usted o su rol deben contar con la autorización `solaris.admin.edit/` *system-filename* para el archivo específico que está editando. Si asigna `auth-sysfilename` a un perfil de derechos existente, simplifica los procedimientos que contienen una combinación de comandos de utilidad de gestión de servicios (SMF) y ediciones de archivos normales. Por ejemplo, si tiene asignada la autorización `solaris.admin.edit/etc/security/audit_warn`, podrá editar el archivo `audit_warn`.

El comando `pfedit` se puede utilizar para editar la mayoría de los archivos de configuración en el directorio `/etc`, sus subdirectorios y, además, los archivos de configuración de aplicaciones, por ejemplo, archivos de GNOME y Firefox. El comando `pfedit` *no* se puede utilizar para editar los archivos de sistema que le otorgan poder a un usuario sobre una franja amplia de un sistema, por ejemplo, el archivo `/etc/security/policy.conf`. Debe tener acceso `root` para editar los archivos de este tipo. Consulte la página del comando man `pfedit`(1M) y el Capítulo 3, "Control de acceso a sistemas (tareas)" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Subdirectorio `/var/user/$USER`

Cada vez que un usuario inicia sesión y se autentica de forma satisfactoria utilizando el módulo `pam_unix_cred`, se crea explícitamente un directorio `/var/user/$USER` si el directorio no existe. Este directorio permite a las aplicaciones almacenar datos persistentes asociados con un usuario determinado en el sistema host. El directorio `/var/user/$USER` se crea en el momento del establecimiento inicial de credenciales y durante una autenticación secundaria cuando se cambian usuarios con los comandos `su`, `ssh` , `rlogin` y `telnet`. El directorio `/var/user/$USER` no requiere ninguna administración. Sin embargo, los usuarios deben tener en cuenta el modo en que se crea el directorio, su función y que está visible en el directorio `/var`.

Cambios en el comando `groupadd`

Un administrador que tenga la autorización `solaris.group.manage` puede crear un grupo. En el momento de la creación del grupo, el sistema asigna `solaris.group.assign` */groupname* al administrador, que le brinda control completo sobre dicho grupo. El administrador entonces puede modificar o suprimir ese grupo según sea necesario. Para obtener más información, consulte las páginas del comando man `groupadd`(1M) y `groupmod` (1M).

Notificación de recuento de inicios de sesión fallidos

Ahora el sistema envía una notificación a los usuarios acerca de los intentos de autenticación fallidos, incluso si la cuenta de usuario no está configurada para forzar inicios de sesión fallidos. Los usuarios que no se pueden autenticar correctamente, verán en pantalla un mensaje similar al siguiente después de la autenticación correcta:

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

Para suprimir las notificaciones de este tipo, cree un archivo `~/.hushlogin`.

¿Qué son las cuentas de usuario y los grupos?

La siguiente información se describe en esta sección:

Una tarea de administración del sistema básica es configurar una cuenta de usuario para cada usuario en un sitio. Una cuenta de usuario típica incluye la información que necesita un usuario

para iniciar sesión y utilizar un sistema, sin tener la contraseña `root` del sistema. Los componentes de cuentas de usuario se describen en "Componentes de cuentas de usuario" en la página 15.

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 de lectura para el grupo `topsecret`. De esta manera, sólo los usuarios del grupo `topsecret` podrán leer los archivos.

Un tipo especial de cuenta de usuario, denominado *rol*, brinda a los usuarios seleccionados privilegios especiales. Para obtener más información, consulte "Control de acceso basado en roles (descripción general)" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Componentes de cuentas de usuario

En las siguientes secciones, se describen varios componentes de una cuenta de usuario.

Nombres de usuario (inicio de sesión)

Los nombres de usuario, también denominados *nombres de inicio de sesión*, permiten a los usuarios acceder a sus propios sistemas y sistemas remotos que tengan los privilegios de acceso apropiados. 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, Ziggy Ignatz sería `zignatz`. 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, `Ziggy Top Ignatz` se convierte en `ztignatz`.

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

- La primera inicial, la inicial del segundo nombre, los primeros cinco caracteres del apellido del usuario
- 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" en la página 22.

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. Y los sistemas utilizan el número UID 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 normales	Cuentas con fines generales
60001 y 65534	`nobody` y `nobody4`	Usuarios anónimos NFS
60002	`noaccess`	Usuarios que no son de confianza

No asigne UID de 0 a 99. Estos UID están reservados para la asignación por 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" en la página 22.

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 UID, "empiece desde 0" para que el nuevo usuario no se vea afectado por conjuntos de atributos de un antiguo usuario. Por ejemplo, a un antiguo usuario se le pudo haber denegado el acceso a una impresora por estar en una lista de denegación de impresora. Sin embargo, ese atributo puede ser inapropiado para el nuevo usuario.

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

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. Y, 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. Y, 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 usuario que pertenecen al 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 el usuario también pertenece. 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" en la página 22.

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 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, un usuario puede cambiar temporalmente el grupo primario del usuario, con el comando `newgrp`, para cualquier otro grupo del que el usuario es miembro.

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 los grupos primarios. Si los nombres de usuario se agregaron a grupos primarios, 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 debe coincidir al menos con el valor identificado por la variable `PASSLENGTH` en el archivo `/etc/passwd`. De manera predeterminada, este valor se define en 6.

  En esta versión, el algoritmo de hash de contraseña predeterminado ha cambiado a `SHA256`. Como resultado, ya no hay una limitación de ocho caracteres para las contraseñas de usuario, como en las 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 con versiones anteriores con las entradas de archivo `passwd` y los mapas NIS existentes.

  El número máximo de caracteres para una contraseña depende del algoritmo, ya sea el algoritmo `crypt_unix` para las contraseñas más antiguas o el algoritmo `SHA256` para las demás. Si el cambio de contraseña es de una contraseña existente y se trata de una contraseña `crypt_unix`, la longitud máxima se establece en 8 caracteres, a menos que el archivo `policy.conf` requiera un cambio de algoritmo de contraseña.

  La nueva contraseña 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`.
- En el caso de las cuentas de usuario en servicios de nombre compatibles con la comprobación de historial de contraseñas, si se define el historial de contraseñas anteriores, las nuevas contraseñas no deben estar incluidas en el historial de contraseñas anteriores.

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

Para hacer que los sistemas del equipo sean más seguros, los usuarios deben modificar sus contraseñas con frecuencia. 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 de los tipos de archivo que crea el usuario, su tamaño 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 raíz, los usuarios pueden acceder a sus directorios raíz mediante un punto de montaje denominado `/home/`*username*. 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 "Descripción general de tareas para administración autofs" de *Gestión de sistemas de archivos de red en Oracle Solaris 11.1*.

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/`*username*. 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" en la página 47.

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 "Personalización de un entorno de trabajo del usuario" en la página 31.

Para obtener información sobre cómo personalizar cuentas de usuario mediante RBAC, consulte "Control de acceso basado en roles (descripción general)" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

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, ya que pueden abarcar 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 son reservados para asignación por 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 y la Tabla 1–4.

  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. Esto incluye el cambio del shell de inicio de sesión de una cuenta del sistema que está actualmente 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

La siguiente información se describe en esta sección:

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 contraseña está disponible cuando utiliza LDAP, pero no NIS.

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

Campos del archivo `passwd`

Los campos en el 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 en el 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.

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

TABLA 1–3 Entradas de archivo `passwd` predeterminadas

Nombre de usuario	Identificador del usuario	Descripción
`root`	`0`	Reservado para la cuenta de superusuario
`daemon`	`1`	Daemon de sistema Umbrella asociado con tareas de sistema de rutina
`bin`	`2`	Daemon administrativo asociado con binarios del sistema en ejecución para realizar algunas tareas del sistema de rutina

TABLA 1–3 Entradas de archivo `passwd` predeterminadas *(Continuación)*

Nombre de usuario	Identificador del usuario	Descripción
`sys`	`3`	Daemon administrativo asociado con el registro del sistema o actualización de archivos en directorios temporales
`adm`	`4`	Daemon administrativo asociado con el registro del sistema
`lp`	`71`	Reservado para el daemon de impresora de líneas
`uucp`	`5`	Asignado al daemon que está asociado con funciones de `uucp`
`nuucp`	`9`	Asignado a otro daemon asociado con funciones `uucp`
`dladm`	`15`	Reservado para la administración de enlaces de datos
`netadm`	`16`	Reservado para la administración de redes
`netcfg`	`17`	Reservado para la administración de configuración de redes
`smmsp`	`25`	Asignado al daemon del programa de envío de mensajes Sendmail
`listen`	`37`	Asignado al daemon de escucha de red
`gdm`	`50`	Asignado al daemon de gestor de pantallas de GNOME
`zfssnap`	`51`	Reservado para las instantáneas automáticas
`upnp`	`52`	Reservado para el servidor UPnP
`xvm`	`60`	Reservado para el usuario xVM
`mysql`	`70`	Reservado para el usuario MySQL
`openldap`	`75`	Reservado para el usuario OpenLDAP
`webservd`	`80`	Reservado para el acceso WebServer
`postgres`	`90`	Reservado para el acceso PostgresSQL
`svctag`	`95`	Reservado para el acceso al registro de etiquetas de servicio
`unknown`	`96`	Reservado para los usuarios remotos que no se pueden asignar en listas de control de acceso (ACL) de NFSv4
`nobody`	`60001`	Reservado para los usuarios de acceso anónimo de NFS
`noaccess`	`60002`	Reservado para los usuarios sin acceso

TABLA 1–3 Entradas de archivo passwd predeterminadas *(Continuación)*

Nombre de usuario	Identificador del usuario	Descripción
nobody4	65534	Reservado para los usuarios de acceso anónimo de NFS de SunOS 4.x
ftp	21	Reservado para el acceso de FTP
dhcpserv	18	Reservado para usuario de servidor DHCP
aiuser	60003	Reservado para usuario AI
pkg5srv	97	Reservado para el servidor depot pkg(5)

Campos en el archivo shadow

Los campos en el 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 en el archivo shadow, consulte la página del comando man shadow(4).

Campos en el archivo group

Los campos en el 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 en el 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. Muchos de estos grupos tienen entradas correspondientes en el archivo `passwd`.

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

TABLA 1–4 Entradas de archivo `group` predeterminadas

Nombre de grupo	ID de grupo	Descripción
`root`	`0`	Grupo de superusuario
`other`	`1`	Grupo opcional
`bin`	`2`	Grupo administrativo asociado con binarios del sistema en ejecución
`sys`	`3`	Grupo de administración asociado con registro del sistema o directorios temporales
`adm`	`4`	Grupo de administración asociado con registro del sistema
`uucp`	`5`	Grupo asociado con funciones `uucp`
`mail`	`6`	Grupo de correo electrónico

TABLA 1–4 Entradas de archivo group predeterminadas *(Continuación)*

Nombre de grupo	ID de grupo	Descripción
tty	7	Grupo asociado con dispositivos tty
lp	8	Grupo de impresora en línea
nuucp	9	Grupo asociado con funciones uucp
staff	10	Grupo administrativo general.
daemon	12	Grupo asociado con tareas del sistema de rutina
sysadmin	14	Grupo de administración que es útil para los administradores del sistema
smmsp	25	Daemon para programa de envío de mensajes Sendmail
gdm	50	Grupo reservado para el daemon de gestor de visualización GNOME
upnp	52	Grupo reservado para el servidor UPnP
xvm	60	Grupo reservado para el usuario xVM
netadm	65	Grupo reservado para la administración de redes
mysql	70	Grupo reservado para el usuario MySQL
openldap	75	Reservado para el usuario OpenLDAP
webservd	80	Grupo reservado para acceso WebServer
postgres	90	Grupo reservado para acceso PostgresSQL
slocate	95	Grupo reservado para el acceso a ubicación segura
unknown	96	Grupo reservado para los grupos remotos que no se pueden asignar en listas de control de acceso (ACL) de NFSv4
nobody	60001	Grupo asignado para acceso NFS anónimo
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
nogroup	65534	Grupo asignado a un usuario que no es un miembro de un grupo conocido
ftp	21	Grupo asignado para el acceso de FTP
pkg5srv	97	Grupo asignado al servidor depot pkg(5)

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 que se pueden utilizar para obtener información acerca de los usuarios

Comando	Descripción	Referencia de página del comando man
`auths`	Muestra y gestiona autorizaciones.	`auths(1)`
`getent`	Obtiene 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)`
`profiles`	Muestra y permite gestionar perfiles de derechos.	`profiles(1)`
`roles`	Muestra los roles que se han asignado a un usuario.	`roles(1)`

TABLA 1–5 Comandos que se pueden utilizar para obtener información acerca de los usuarios *(Continuación)*

Comando	Descripción	Referencia de página del comando man
`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 atributo se definen en `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 – Ya no se admiten la interfaz gráfica de usuario de Solaris Management Console y la interfaz de línea de comandos asociada con esta interfaz gráfica de usuario.

Los siguientes comandos están disponibles para gestionar 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" en la página 49
`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 un usuario" en la página 50 "Cómo cambiar los atributos de seguridad de un usuario" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
`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" en la página 51

TABLA 1–6 Comandos que se utilizan para la gestión de usuarios, roles y grupos *(Continuación)*

Página del comando man	Descripción	Para obtener información adicional
`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.	"Cómo crear un rol" de *Administración de Oracle Solaris 11.1: servicios de seguridad* "Configuración inicial de RBAC (mapa de tareas)" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
`groupadd`(1M) `groupmod`(1M) `groupdel`(1M)	Gestiona grupos localmente o en un repositorio LDAP.	"Cómo agregar un grupo" en la página 52

Personalización de un entorno de trabajo del usuario

La siguiente información se describe en esta sección:

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 sus 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	Finalidad
`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, consulte "Cómo personalizar los archivos de inicialización de usuario" en la página 46.

Uso de archivos de inicialización de sitio

Los administradores y los usuarios pueden personalizar archivos de inicialización de 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 están diseñados para 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.
- Hay varias maneras en las que puede mostrar la información de ruta y el shell predeterminado:
  - 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 de 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.

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 de entorno de shell bash y shell ksh93

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 las variables de entorno que permanecen coherentes entre inicios de sesión, debe realizar los cambios 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 sobre el shell y las variables de entorno que están disponibles en la versión de Oracle Solaris.

TABLA 1–9 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 rje. Si está en el directorio /home/jean/bin y escribe cd rje, cambia los directorios a /home/jean/rje, 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 ha iniciado sesión 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 MANPATH apropiado 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/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.

TABLA 1–9 Descripciones de variables de shell y de entorno *(Continuación)*

Variable	Descripción
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	Establece 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 la información al 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

A continuación se ofrecen algunas instrucciones para configurar variables `PATH` efectivas:

- 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 que los directorios montados NFS para disminuir la probabilidad de "cuelgues" 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 convenciones y conversiones específicas de una región 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 1–10 Valores para variables LANG y LC

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 Configuración regional mediante las variables LANG

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

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

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

Permisos de archivo predeterminados (`umask`)

Cuando crea un archivo o directorio, los permisos de archivo predeterminados asignados a un archivo o directorio están 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`.

También puede determinar el valor `umask` que desea establecer utilizando la siguiente tabla. Esta tabla muestra los permisos de archivo y directorio que se crean para cada uno de los valores octales de `umask`.

TABLA 1–11 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

A continuación, se muestra un ejemplo del archivo de inicialización de usuario `.profile`. Puede utilizar este archivo 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 El archivo `.profile`

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

1. Define la ruta de búsqueda de shell del usuario.
2. Define la ruta al archivo de correo del usuario.
3. Define el servidor de reloj/hora del usuario.
4. Define la ruta de búsqueda del usuario para páginas del comando man.
5. Define la impresora predeterminada del usuario.
6. Establece los permisos de creación de archivo predeterminados del usuario.
7. Establece las variables de entorno enumeradas.

◆ ◆ ◆ CAPÍTULO 2

Gestión de cuentas de usuario mediante la interfaz de línea de comandos (tareas)

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, "Gestión de cuentas de usuario y entornos de usuario (descripción general)".

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 (tareas)".

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

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

Configuración y gestión de cuentas de usuario mediante el uso de la interfaz de línea de comandos (mapa de tareas)

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" en la página 45

Tarea	Descripción	Para obtener instrucciones
Personalizar los archivos de inicialización de usuario.	Puede configurar archivos de inicialización de usuarios para proporcionar entornos coherentes a los nuevos usuarios.	"Cómo personalizar los archivos de inicialización de usuario" en la página 46
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" en la página 46
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" en la página 49
Modificar una cuenta de usuario.	Modifique la información de inicio de sesión de un usuario en el sistema.	"Cómo modificar un usuario" en la página 50
Suprimir una cuenta de usuario.	Puede suprimir una cuenta de usuario con el comando `userdel`.	"Cómo suprimir un usuario" en la página 51
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.	"Cómo crear un rol" de *Administración de Oracle Solaris 11.1: servicios de seguridad* "Cómo asignar un rol" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
Crear un grupo.	Para crear un nuevo grupo, utilice el comando `groupadd`.	"Cómo agregar un grupo" en la página 52
Agregar atributos de seguridad a una cuenta de usuario.	Después de configurar una cuenta de usuario local, puede agregar los atributos de seguridad necesarios.	"Cómo cambiar los atributos de seguridad de un usuario" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
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" en la página 53

Tarea	Descripción	Para obtener instrucciones
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 " en la página 54

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 configurar sus cuentas.

Elemento	Descripción
Nombre de usuario:	
Nombre de rol:	
Perfiles o autorizaciones:	
UID:	
Grupo principal:	
Grupos secundarios:	
Comentario:	
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

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

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

Consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

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 **Edite los archivos de inicialización de usuario para cada tipo de usuario y personalícelos en función de las necesidades del sitio.**

Para obtener una descripción detallada de las maneras de personalizar los archivos de inicialización de usuario, consulte "Personalización de un entorno de trabajo del usuario" en la página 31.

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 "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

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. **Cambia 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`.

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, las cuentas de usuario se crean 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 raíz creado con los comandos `useradd` y `roleadd` coloca el directorio raíz 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 "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.
- Al crear una cuenta de usuario con el comando `useradd`, debe especificar la opción `-m` en la sintaxis del comando. De lo contrario, no se creará un directorio raíz de datos 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 – La única excepción a esta regla es si desea que el módulo `pam_zfs_key` cree un directorio raíz cifrado para el usuario. En este caso, *no* especificaría 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 raíz 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
  ```

  Pero, 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 el sistema de archivos es un conjunto de datos ZFS, como es el caso de todo Oracle Solaris 11, el directorio raíz del usuario se crea como un conjunto de datos ZFS secundario, con el permiso de ZFS para tomar instantáneas delegado al 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`.

▼ Cómo agregar un usuario

En esta versión, las cuentas de usuario se crean como sistemas de archivos ZFS de Oracle Solaris. 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*.

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 raíz 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.

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

Consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

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.

Si especifica la opción `-d` *dir* de la siguiente manera, el usuario se crea sin una entrada `auto_home`, y la entrada `passwd` especifica `/export/home/user1` como el directorio raíz del usuario:

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

Si especifica la opción `-d` *dir* de la siguiente manera, 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
```

Nota – Si desea que el módulo `pam_zfs_key` cree un directorio raíz cifrado para el usuario. En este caso, *no* especifique la opción `-m` con el comando `useradd`. Consulte "Directrices para la configuración de cuentas de usuario" en la página 47.

Para obtener una descripción detallada de todas las opciones y los 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 obtener más información, consulte las páginas del comando man `useradd`(1M) y `passwd`(1).

Véase también Después de crear un usuario, es posible que sea necesario realizar algunas tareas adicionales, incluida la agregación y la asignación de roles a un usuario, la enumeración y el cambio de perfiles de derechos de un usuario y el cambio de las propiedades RBAC de un usuario. Para obtener más información, consulte las siguientes referencias:

- "Cómo crear un rol" de *Administración de Oracle Solaris 11.1: servicios de seguridad* y "Cómo asignar un rol" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
- "Cómo visualizar todos los atributos de seguridad definidos" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
- "Cómo crear un perfil de derechos" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
- "Cómo cambiar los atributos de seguridad de un usuario" de *Administración de Oracle Solaris 11.1: servicios de seguridad*

▼ Cómo modificar un 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 "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

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

   Consulte la página del comando man `usermod(1M)` para obtener detalles sobre 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 `pam_user_policy(5)` para obtener más información.

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

Véase también Consulte las siguientes referencias para obtener ejemplos adicionales de modificación de usuarios:

- "Cómo asignar un rol" de *Administración de Oracle Solaris 11.1: servicios de seguridad*
- "Cómo cambiar los atributos de seguridad de un usuario" de *Administración de Oracle Solaris 11.1: servicios de seguridad*

▼ Cómo suprimir un usuario

1. **Asumir el rol `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 **Ejecute uno de los siguientes comandos:**

- **Si el usuario tiene un directorio principal local, suprima el usuario y el directorio principal.**

  ```
  # userdel -r username
  ```

  `usesrdel` Suprime la cuenta del usuario especificado.

  `-r` Elimina la cuenta del sistema.

  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`.

- **De lo contrario, suprima sólo el usuario.**

  ```
  # userdel username
  ```

  Debe suprimir de forma manual el directorio principal del usuario en el servidor remoto.

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 "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Enumere los grupos existentes.**

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

3 **Crear un nuevo grupo.**

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

`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 ejemplo siguiente 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 directorios principales que se crean como sistemas de archivos ZFS

En esta versión de Oracle Solaris, puede compartir un sistema de archivos ZFS mediante la configuración de 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. El siguiente procedimiento describe estos pasos.

Para obtener más información sobre cómo compartir y dejar de compartir sistemas de archivos, consulte "Cómo compartir y anular la compartición de sistemas de archivos ZFS" de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

1 Asuma el rol de usuario `root`.

Consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Cree una agrupación separada para los directorios principales del usuario. Por ejemplo:

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

3 **Cree un contenedor para los directorios principales. 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 información relacionada con la tarea, consulte "Descripción general de tareas para administración autofs" de *Gestión de sistemas de archivos de red en Oracle Solaris 11.1*.

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

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

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" en la página 53.

◆ ◆ ◆ CAPÍTULO 3

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

En este capítulo, se proporciona una descripción general e información relacionada con tareas para configurar y gestionar usuarios mediante la interfaz gráfica de usuario de Oracle 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 la interfaz de lista de comandos equivalente (`useradd`, `usermod` , `userdel`, etc.). Para obtener más información sobre la interfaz gráfica de usuario de User Manager, consulte la ayuda en pantalla.

A continuación, se indica la información contenida en este capítulo:

Para obtener información general sobre la gestión de cuentas de usuario, consulte el Capítulo 1, "Gestión de cuentas de usuario y entornos de usuario (descripción general)".

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 (tareas)".

Introducción a la interfaz gráfica de usuario de User Manager

La siguiente información se describe en esta sección:

La interfaz gráfica de usuario de User Manager está basada en la estructura Visual Panels y se proporciona como una interfaz de Visual Panels. La gestión remota de usuarios y roles es posible mediante el daemon de administración remota (RAD). La interfaz gráfica de usuario depende del módulo RAD User/Role Manager para realizar todas sus operaciones. El módulo RAD funciona llamando a las interfaces de línea de comandos de control de acceso basado en roles que realizan todas las funciones administrativas de la interfaz gráfica de usuario.

La autenticación de usuarios y la asunción de roles es proporcionada por la estructura Visual Panels y está disponible para todos los paneles, incluido el panel 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 Oracle Solaris 10. Aunque no es idéntica a Solaris Management Console, la interfaz gráfica de usuario ofrece algunas de las mismas funciones. Tenga en cuenta que Solaris Management Console *no* se admite en 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. Las tareas que se pueden realizar con la interfaz gráfica de usuario son las mismas que puede realizar con la interfaz de línea de comandos, por ejemplo, `useradd`, `usermod`, `userdel`, `roleadd`, `groupadd`, etc. Para obtener información sobre la gestión de usuario y roles mediante el uso de la interfaz de línea de comandos, consulte el Capítulo 2, “Gestión de cuentas de usuario mediante la interfaz de línea de comandos (tareas)”.

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

Inicio de la interfaz gráfica de usuario de User Manager

▼ 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 gestión de usuarios asignado.**

   Consulte “Cómo usar los derechos administrativos que tiene asignados” de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Inicie la interfaz gráfica de usuario de User Manager mediante la selección de uno de los siguientes métodos:**

   - **Inicie la interfaz gráfica de usuario de User Manager desde el escritorio; para esto seleccione System (Sistema) → Administration (Administración) → User Manager.**

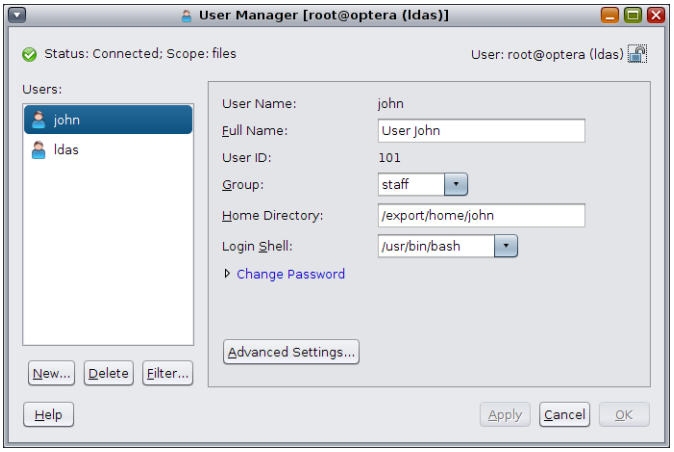
- **Inicie la interfaz gráfica de usuario de User Manager desde la línea de comandos de la siguiente manera:**

  ```
  # vp usermgr &
  ```

Organización del panel de User Manager

Cuando inicia la interfaz gráfica de usuario de User Manager, se muestra el panel principal de User Manager. El panel de User Manager se utiliza para administrar usuarios y roles. En la parte izquierda del panel, hay un campo Status (Estado) que muestra el estado de los servicios que se están ejecutando actualmente en el host local. A la derecha del panel, hay un campo User (Usuario). El campo User (Usuario) muestra la credencial que está siendo usada actualmente por la interfaz gráfica de usuario de User Manager. Para cambiar las credenciales, haga clic en el botón Lock (Bloquear) en el extremo derecho del panel. Consulte "Asunción de un rol o cambio de credenciales de usuario" en la página 59.

En la siguiente figura, se muestra el panel principal de User Manager.



El panel de User Manager incluye los siguientes componentes:

- Lista de usuarios y roles: contiene una lista de usuarios que puede seleccionar para administrar.
- Configuración básica: muestra la 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 panel.

Las siguientes acciones están disponibles desde el panel de User Manager:

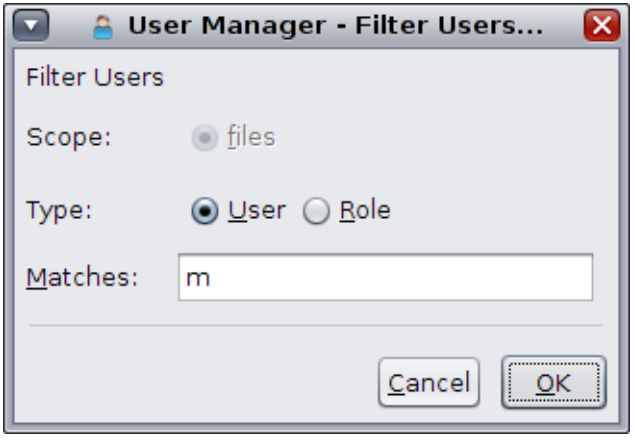
- Crear un usuario o rol nuevo. Consulte "Cómo agregar un usuario o rol con la interfaz gráfica de usuario de User Manager" en la página 60.
- Suprimir un usuario o rol existente. Consulte "Supresión de un usuario o rol con la interfaz gráfica de usuario de User Manager" en la página 63.
- Filtrar la información de un usuario. Consulte "Selección de un ámbito y tipo de servicio de nombre predeterminados" en la página 58.
- Administrar la configuración avanzada de un usuario existente. Consulte "Cómo modificar un usuario o rol con la interfaz gráfica de usuario de User Manager" en la página 62.

Selección de un ámbito y tipo de servicio de nombre predeterminados

El ámbito y el tipo de servicio de nombre predeterminados de la interfaz gráfica de usuario de User Manager son `files` y `User`. Para administrar la interfaz gráfica de usuario de User Manager con un ámbito diferente, por ejemplo `ldap` y `roles`, haga clic en el botón Filter (filtrar). Cuando hace clic en el botón Filter (filtrar), se inicia un cuadro de diálogo que le permite cambiar el ámbito o el tipo predeterminado, o ambos.

- Las opciones para el ámbito son `files` y `ldap`.
- Las opciones para el tipo son `User` y `Role`. Haga clic en OK para guardar los cambios.

Haga clic en Cancel (cancelar) para cancelar la operación.



Nota – Si el sistema no está configurado como cliente `ldap`, sólo está disponible el ámbito `files`.

Asunción de un rol o cambio de credenciales de usuario

Un usuario con el perfil de derechos de gestión de usuarios puede crear nuevos usuarios, siempre que los atributos avanzados del usuario o rol que se vaya a crear sean un subconjunto de los del usuario que realiza la administración. Si el usuario que realiza la administración no tiene suficientes autorizaciones, pero cuenta con un rol administrativo con suficientes autorizaciones, el usuario puede asumir el rol para realizar la administración necesaria si hace clic en el botón Lock (bloquear) en el panel principal de User Manager.

▼ Cómo cambiar las credenciales de un usuario

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

   Consulte "Cómo iniciar la interfaz gráfica de usuario de User Manager" en la página 56.

2. **En el panel principal de User Manager, haga clic en el icono Lock (bloquear) para abrir un submenu 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 el usuario especificado.

4. **Seleccione el rol adecuado y, a continuación, haga clic en Log In (iniciar sesión) para cambiar el 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 (tareas)".

La siguiente información se describe en esta sección:

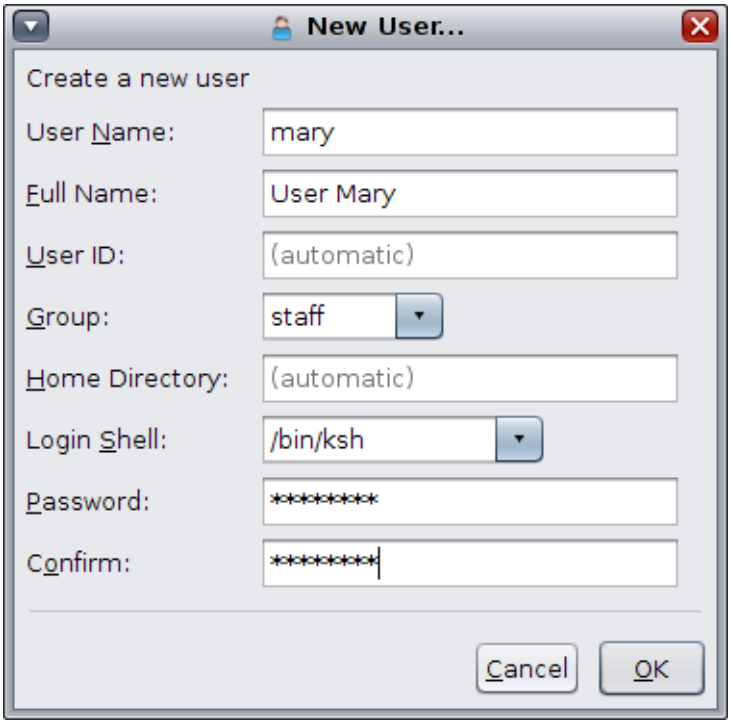
▼ Cómo agregar un usuario o rol con la interfaz gráfica de usuario de User Manager

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

Consulte "Cómo iniciar la interfaz gráfica de usuario de User Manager" en la página 56.

2 **Para agregar un usuario o rol nuevo dentro del ámbito del filtro que está siendo usado actualmente por la interfaz gráfica de usuario, haga clic en el botón New (nuevo) en el panel principal de User Manager.**

Se muestra el cuadro de diálogo de nuevo usuario.



3 **En el cuadro de diálogo de nuevo usuario, complete los siguientes campos:**

- Nombre de usuario
- Full Name (Nombre completo)
- Identificador del usuario

  Este campo es opcional. Si no se proporciona ninguna información, el sistema le asigna automáticamente un valor predeterminado.

- Group (Grupo)

  Las opciones disponibles para el campo de grupo varían en función de la configuración del sistema.

- Home Directory (Directorio raíz)

  Este campo 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`.

- Login Shell (Shell de inicio de sesión)

  Las opciones para el campo de shell de inicio de sesión pueden variar en función de la configuración del sistema.

- Password (Contraseña)

  Asigne una contraseña temporal al usuario.

- Confirm (Confirmar)

  Confirme la contraseña temporal que haya asignado al usuario.

Nota – Debe completar todos los campos, con la excepción de los campos opcionales.

---

4 **Para crear un nuevo usuario o rol y agregar el usuario o rol a la lista de usuarios que se muestra en el panel principal de User Manager, haga clic en OK (Aceptar).**

Para cancelar la operación, haga clic en Cancel (Cancelar).

▼ 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" en la página 56.

2 **Para modificar un usuario o rol existente, en el panel principal de User Manager, seleccione el usuario o el rol que desee modificar de la lista que se muestra.**

Después de seleccionar el usuario, el lado derecho del panel 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 que ha sido modificado.

---

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 "Administración de la configuración avanzada con la interfaz gráfica de usuario de User Manager" en la página 63.**

6 **Haga clic en OK (Aceptar) para guardar los cambios y cerrar el panel de User Manager.**
Haga clic en Cancel (Cancelar) para desechar los cambios sin guardar y cerrar el panel.

Supresión de un usuario o rol con la interfaz gráfica de usuario de User Manager

Para suprimir un usuario o rol dentro del ámbito del filtro que está usando actualmente la interfaz gráfica de usuario de User Manager, seleccione el usuario o rol en el panel principal de User Manager y, luego, haga clic en el botón Delete (Suprimir). Para guardar los cambios, Haga clic en OK (Aceptar) cuando se muestre el cuadro de diálogo de confirmación. Para cancelar la operación, haga clic en Cancel (Cancelar).

Administración de la configuración avanzada con la interfaz gráfica de usuario de User Manager

La siguiente información se describe en esta sección:

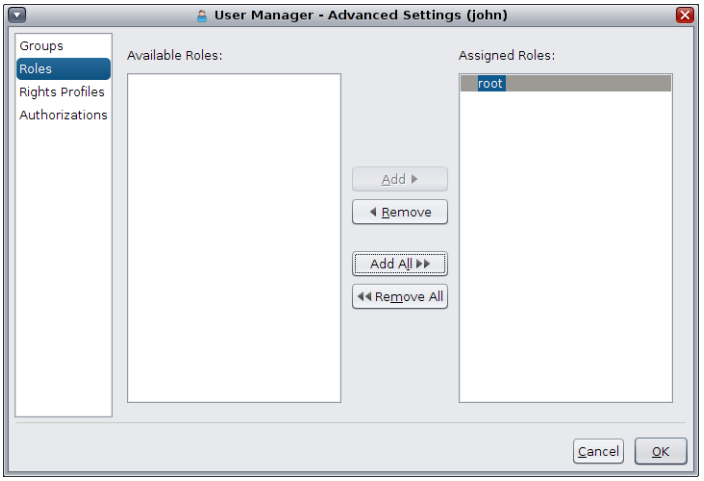
- "Administración de grupos con la interfaz gráfica de usuario de User Manager" en la página 64
- "Administración de roles con la interfaz gráfica de usuario de User Manager" en la página 65
- "Administración de perfiles de derechos con la interfaz gráfica de usuario de User Manager" en la página 67
- "Administración de autorizaciones con la interfaz gráfica de usuario de User Manager" en la página 68

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 de las funciones de seguridad que se admiten en Oracle Solaris, consulte la Parte I, "Descripción general de la seguridad" de *Administración de Oracle Solaris 11.1: servicios de seguridad*. Para obtener una descripción detallada de cómo funciona el control de accesos basado en roles (RBAC) en esta versión, consulte la Parte III, "Roles, perfiles de derechos y privilegios" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Para administrar atributos avanzados para un usuario o rol, seleccione el usuario o rol en el panel principal de User Manager y, luego, haga clic en el botón Advanced Settings (Configuración avanzada). Se muestra el panel de configuración avanzada para el usuario o rol actual. Se muestra el nombre del usuario actual entre paréntesis en la parte superior del panel.

La siguiente figura muestra el panel Advanced Settings (Configuración avanzada) con el atributo de seguridad de roles del usuario john seleccionado.



Los siguientes atributos de seguridad se pueden administrar en el panel Advanced Settings (Configuración avanzada):

- Grupos
- Roles
- Perfiles de derechos
- Autorizaciones

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

Para administrar los grupos, haga clic en el botón Advanced Settings (configuración avanzada) en el cuadro de diálogo principal de User Manager de la interfaz gráfica de usuario de User Manager.

▼ Cómo administrar grupos

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

   Consulte "Cómo iniciar la interfaz gráfica de usuario de User Manager" en la página 56.

2. **Seleccione un usuario en el panel principal de User Manager y, luego, haga clic en el botón Advanced Settings (Configuración avanzada).**

   Se muestra el panel Advanced Settings (Configuración avanzada).

3 **Haga clic en el atributo Groups (Grupos) en la parte izquierda del panel.**

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.**

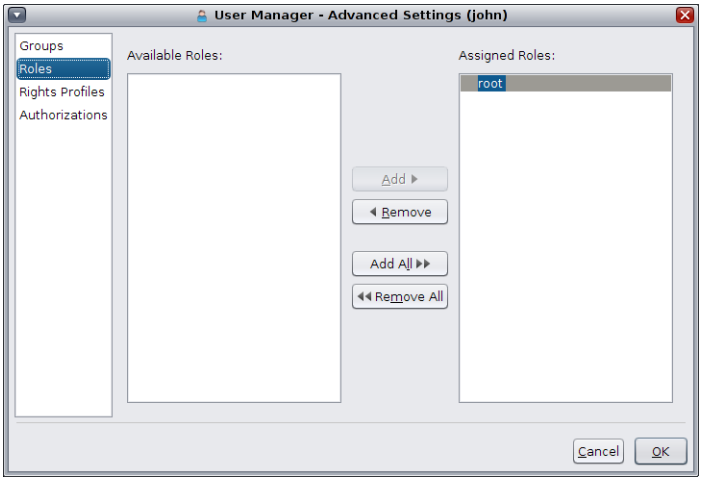
Los cambios no se aplicarán hasta que haga clic en OK (Aceptar) o Apply (Aplicar) en el panel principal de User Manager.

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

Para administrar los roles, haga clic en el botón Advanced Settings (Configuración avanzada), en el cuadro de diálogo principal de User Manager 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 panel Advanced Settings (Configuración avanzada) con el atributo de seguridad de roles del usuario john seleccionado.



▼ Cómo administrar 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" en la página 56.

2 **Seleccione un usuario en el panel principal de User Manager y, luego, haga clic en el botón Advanced Settings (Configuración avanzada).**

Se muestra el panel Advanced Settings (Configuración avanzada).

3 **Haga clic en el atributo Roles, en la parte izquierda del panel.**

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).**

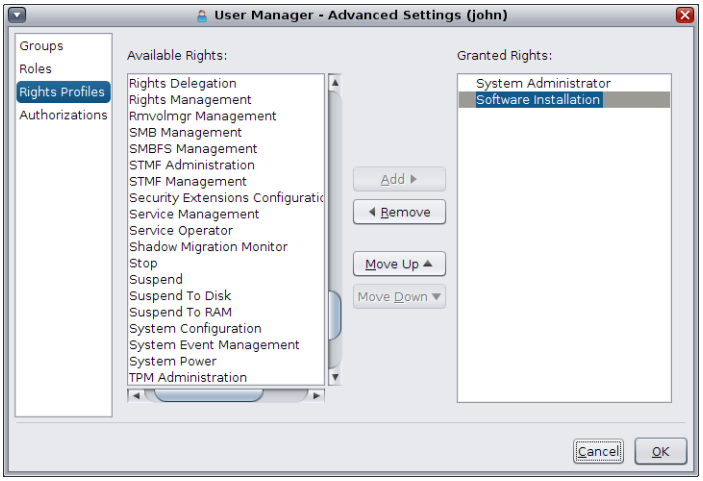
4 **Haga clic en OK (Aceptar) para guardar la configuración.**

Los cambios no se aplicarán hasta que haga clic en OK (Aceptar) o Apply (Aplicar) en el panel principal de User Manager.

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

Para administrar los perfiles de derechos, haga clic en el botón Advanced Settings (Configuración avanzada), en el cuadro de diálogo principal de User Manager de la interfaz gráfica de usuario de User Manager.

La siguiente figura muestra el panel Advanced Settings (Configuración avanzada) con el atributo de seguridad de perfiles de derechos del usuario john seleccionado.



Nota – La asignación de perfiles de derechos tiene un orden de prioridad. Utilice los botones Move Up (Mover arriba) y Move Down (Mover abajo) para cambiar el orden de los perfiles de derechos que se otorgan al usuario actual como desee.

▼ 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" en la página 56.

2 **Seleccione un usuario en el panel principal de User Manager y, luego, haga clic en el botón Advanced Settings (Configuración avanzada).**

Se muestra el panel Advanced Settings (Configuración avanzada).

3 **Haga clic en el atributo Rights Profile (Perfiles de derechos), en la parte izquierda del panel.**

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 OK (Aceptar) o Apply (Aplicar) en el panel principal de User Manager.

Administración 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 administrar 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" en la página 56.

2. **Seleccione un usuario en el panel principal de User Manager y, luego, haga clic en el botón Advanced Settings (Configuración avanzada).**

   Se muestra el panel Advanced Settings (Configuración avanzada).

3. **Haga clic en el atributo Authorization (Autorización) en la parte izquierda del panel.**

   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 OK (Aceptar) o Apply (Aplicar) en el panel principal de User Manager.

Índice

D

E

G

I

M

N