Trabajo con servicios de nombres y directorios en Oracle® Solaris 11.1

Referencia: E36688–01
Octubre de 2012

ORACLE®

130327@25097

Contenido

Lista de tablas

Lista de ejemplos

Prefacio

Trabajo con servicios de nombres y directorios en Oracle Solaris 11.1 describe la configuración y administración de los servicios de nombres y directorios del Sistema operativo Oracle Solaris: DNS, NIS y LDAP. Esta guía forma parte de un conjunto de varios volúmenes que tratan de manera exhaustiva la información de administración del Oracle Solaris.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas admitidos aparecen en las *Oracle Solaris OS: Hardware Compatibility Lists*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

Manuales relacionados

- *Guía de implementación de Oracle Directory Server Enterprise Edition*
- *Guía de administración de Oracle Directory Server Enterprise Edition*
- *DNS and Bind* (DNS y Bind), de Cricket Liu y Paul Albitz, (5.ª edición, O'Reilly, 2006)
- *Comprensión e implementación de servicios de directorios LDAP*, de Timothy A. Howes, Ph.D. y Mark C. Smith

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

Tipo 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	`machine_name%` **`su`** `Password:`
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando para eliminar un archivo es `rm` *filename*.
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

En la tabla siguiente, se muestran los indicadores de sistema UNIX y los indicadores de superusuario para shells que se incluyen en el sistema operativo Oracle Solaris. En los ejemplos de comandos, el indicador de shell indica si el comando debe ser ejecutado por un usuario común o por un usuario con privilegios.

TABLA P–2 Indicadores del shell

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

TABLA P–2 Indicadores del shell *(Continuación)*

Shell	Indicador
Shell C para superusuario	`machine_name#`

PARTE I

Acerca de los servicios de nombres y directorios

Esta parte presenta los servicios de nombres y directorios para el SO Oracle Solaris. También describe cómo configurar los servicios de nombres con la utilidad de gestión de servicios (SMF), de modo que el usuario puede coordinar consultas mediante los distintos servicios de directorios locales y remotos. También explica cómo configurar el servicio de nombre de dominio (DNS), así como los clientes de Active Directory.

◆ ◆ ◆ CAPÍTULO 1

1 Servicios de nombres y directorios (descripción general)

En este capítulo se proporciona una descripción general acerca de los servicios de nombres y directorios incluidos en la versión de Oracle Solaris. También se describen brevemente los servicios de nombres LDAP, DNS y NIS.

En este capítulo, se describen los siguientes temas:

¿Qué es un servicio de nombres?

Un *servicio de nombres* realiza consultas de información almacenada, por ejemplo:

- Nombres de host y direcciones
- Nombres de usuario
- Contraseñas
- Permisos de acceso
- Pertenencia a grupos, mapas de montaje automático, etc.

Esta información está disponible para que los usuarios puedan iniciar una sesión en su host, tener acceso a los recursos y se les concedan los permisos. La información sobre el servicio de nombres se puede almacenar de forma local en diversos formatos de archivos de base de datos, o en un repositorio basado en red central o base de datos.

Sin un servicio de nombres central, cada host tendría que conservar su propia copia de esta información. La información del servicio de nombres se puede almacenar en archivos, mapas o tablas de bases de datos. Si centraliza todos los datos, la administración resulta más fácil.

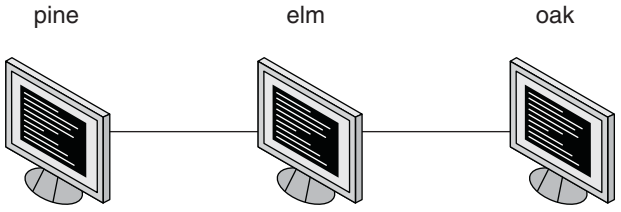
Los servicios de nombres son fundamentales para cualquier red informática. Entre otras funciones, los servicios de nombres proporcionan una funcionalidad que realiza lo siguiente.

- Asocia (*vincula*) nombres con objetos

- Resuelve nombres para objetos
- Elimina vínculos
- Enumera los nombres
- Cambia el nombre de la información

Un servicio de información de la red permite a los sistemas ser identificados por sus nombres comunes en lugar de direcciones numéricas. Esto hace que la comunicación sea más simple, porque los usuarios no tienen que recordar e intentar introducir direcciones numéricas difíciles, como `192.168.0.0`.

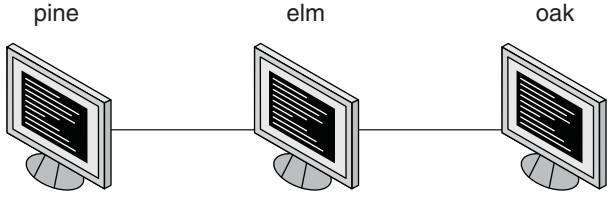
Por ejemplo, veamos una red de tres sistemas que se denominan `pine`, `elm` y `oak`. Antes de que `pine` pueda enviar un mensaje a `elm` u `oak`, `pine` deben conocer sus direcciones de red numéricas. Por esta razón, `pine` conserva un archivo, `/etc/inet/hosts`, que almacena la dirección de red de todos los sistemas de la red, incluida la propia.



`/etc/inet/hosts`

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

Del mismo modo, para que `elm` y `oak` se comuniquen con `pine` o entre sí, los sistemas deben conservar archivos similares.



`/etc/inet/hosts`

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

`/etc/inet/hosts`

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

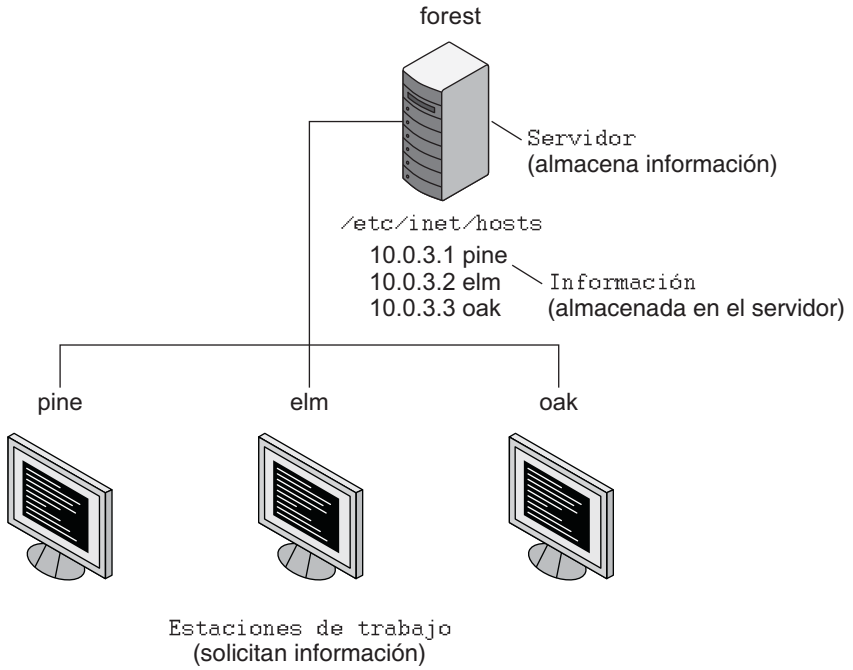
`/etc/inet/hosts`

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

Además de almacenar las direcciones, los sistemas almacenan información de seguridad, datos de correo, información de servicios de red, etc. Debido a que las redes ofrecen más servicios, la lista de información almacenada aumenta. Como resultado, cada sistema debe guardar un conjunto completo de archivos similares a `/etc/inet/hosts`.

Un servicio de información de la red almacena información de red en un servidor, que puede ser consultada por cualquier sistema.

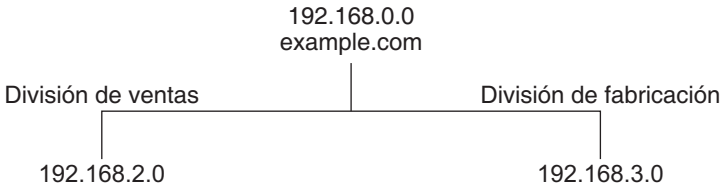
Los sistemas se conocen como *clientes* del servidor. La siguiente figura ilustra la disposición cliente-servidor. Siempre que cambia la información sobre la red, en lugar de actualizar el archivo local de cada cliente, un administrador sólo actualiza la información almacenada por el servicio de información de la red. Esto reduce las posibilidades de error, las inconsistencias entre los clientes y el tamaño de la tarea.



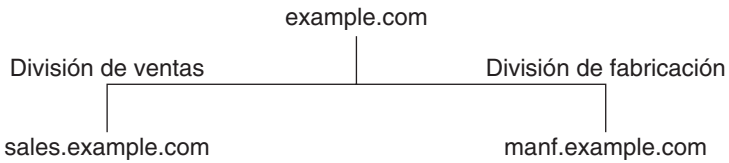
Este acuerdo, de un servidor que proporciona servicios centralizados a los clientes a través de una red, se conoce como *informática para cliente-servidor*.

Aunque el objetivo principal de un servicio de información de la red es centralizar la información, el servicio de información de la red también puede simplificar los nombres de red. Por ejemplo, supongamos que su compañía ha configurado una red que está conectada a Internet. Internet ha asignado la dirección de red `192.168.0.0` y el nombre de dominio

example.com a su red. Su compañía tiene dos divisiones, ventas y fabricación (manf), por lo que su red está dividida en una red principal y una subred de cada división. Cada red tiene su propia dirección.



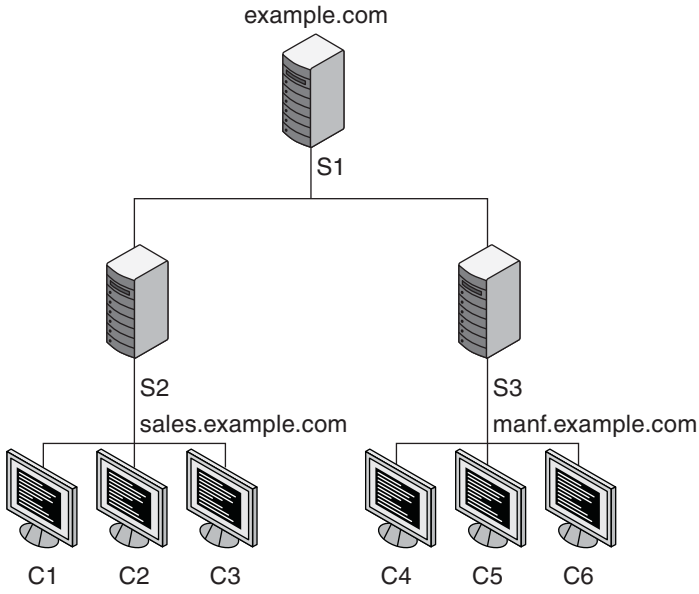
Cada división se podría identificar por su dirección de red, como se muestra en el ejemplo anterior, pero se prefieren los nombres descriptivos que facilitan los servicios de nombres.



En lugar de enviar correo o establecer otras comunicaciones de red para 198.168.0.0, el correo podría ser dirigido a example.com. En lugar de enviar correo a 192.168.2.0 ó 192.168.3.0, el correo podría ser dirigido a sales.example.com o manf.example.com.

Los nombres también son más flexibles que las direcciones físicas. Las redes físicas tienden a permanecer estables, pero la organización de las compañías tiende a cambiar.

Por ejemplo, supongamos que la red example.com es compatible con tres servidores, S1, S2 y S3. Suponga que dos de esos servidores, S2 y S3 admiten clientes.

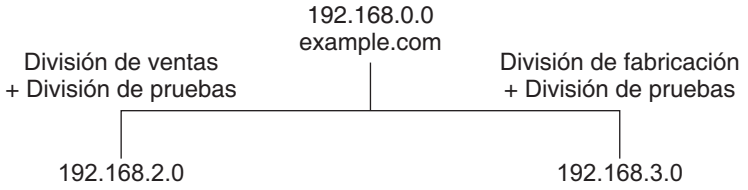


Los clientes `C1`, `C2` y `C3` obtendrían la información de red del servidor `S2`. Los clientes `C4`, `C5` y `C6` obtendrían la información del servidor `S3`. La red resultante se resume en la siguiente tabla. La tabla es una representación generalizada de esa red, pero no se parece a un mapa de información de red real.

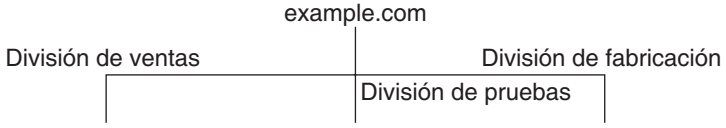
TABLA 1–1 Representación de red example.com

Dirección de red	Nombre de red	Servidor	Clientes
`192.168.1.0`	`example.com`	`S1`	
`192.168.2.0`	`sales.example.com`	`S2`	`C1`, `C2`, `C3`
`192.168.3.0`	`manf.example.com`	`S3`	`C4`, `C5`, `C6`

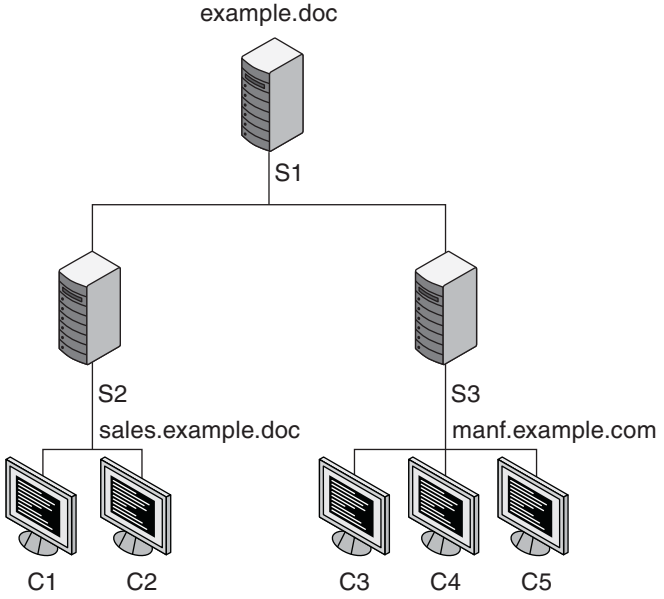
Ahora, supongamos que crea una tercera división, pruebas, que tomó prestados algunos recursos de las otras dos divisiones, pero no creó una tercera subred. La red física ya no es paralela a la estructura corporativa.



El tráfico de la División de pruebas no tiene su propia subred, sino que se puede dividir entre `192.168.2.0` y `192.168.3.0`. Sin embargo, con un servicio de información de la red, el tráfico de la división de pruebas tiene su propia red dedicada.



Por lo tanto, cuando una organización cambia, su servicio de información de la red puede cambiar su asignación, como se muestra aquí.



Ahora, los clientes `C1` y `C2` obtendrían su información del servidor `S2`. `C3`, `C4` y `C5` obtendrían información del servidor `S3`.

Los cambios posteriores de la organización se acomodarán según los cambios en la estructura de información de la red sin reorganizar la estructura de red.

Servicios de nombres de Oracle Solaris

La plataforma de Oracle Solaris proporciona los siguientes servicios de nombres:

- Sistema de nombre de dominio (DNS) (consulte "Descripción del servicio de nombres DNS" en la página 29)
- archivos `/etc`, el sistema de nombres de UNIX original (consulte "Descripción del servicio de nombres de archivos `/etc`" en la página 30)
- Servicio de información de la red (NIS) (consulte "Descripción del servicio de nombres NIS" en la página 30)
- Protocolo ligero de acceso a directorios (LDAP) (consulte Parte III *Configuración y administración de servicios de nombres LDAP*)

La mayoría de las redes modernas usan dos o más de estos servicios combinados. El servicio de nombres que se utiliza para una determinada consulta es coordinada por el cambio de servicio de nombres, que se describe en el Capítulo 2, "Conmutador de servicio de nombres (descripción general)".

Descripción del servicio de nombres DNS

El *sistema de nombre de dominio* (DNS) es una base de datos jerárquica y distribuida, que se implementa en una red TCP/IP. Principalmente se utiliza para buscar direcciones IP para los nombres de host de Internet y los nombres de host para direcciones IP. Los datos se distribuyen a través de la red y se ubican mediante el uso de nombres separados por puntos que se leen de derecha a izquierda. DNS también se utiliza para almacenar otra información de host relacionada con Internet, como información de enrutamiento de intercambio de correo, datos de ubicación y servicios disponibles. La estructura jerárquica de la naturaleza del servicio permite la administración local de dominios locales, a la vez que proporciona cobertura internacional de otros dominios que están conectados a Internet, a una intranet o ambas.

Los clientes de DNS solicitan información acerca del nombre de host de uno o más servidores de nombres y esperan una respuesta. Los servidores DNS responden a solicitudes desde una caché de información cargada de un archivo u otra base de datos de terceros en un DNS maestro, o a través de la red desde un servidor esclavo DNS cooperativo, o desde información almacenada de consultas anteriores. Si no se encuentra una respuesta y el servidor no es responsable por el dominio en cuestión, el servicio buscará de manera recursiva (si se permite), la caché y el nombre de host de otros servidores como respuesta.

Descripción de DNS de multidifusión y detección de servicios

Dos extensiones para el protocolo de DNS son gestionadas por el servicio `svc:network/dns/multicast`. DNS de multidifusión (mDNS) implementa DNS en una red pequeña donde ningún servidor DNS convencional se ha instalado. La detección de servicios DNS (DNS-SD) amplía el DNS de multidifusión para que también proporcione una detección de servicios simple (exploración de red). Para obtener más información, consulte "DNS de multidifusión" en la página 43 and "Detección de servicios DNS de multidifusión" en la página 44.

Precaución – El servicio mDNS usa el nombre de dominio `.local`, de manera que el nombre no se deba utilizar también en DNS para evitar posibles conflictos.

Descripción del servicio de nombres de archivos `/etc`

El sistema de nombres UNIX basado en host original se desarrolló para equipos UNIX autónomos y, posteriormente, se adaptó para el uso en red. Muchos de los antiguos equipos y sistemas operativos UNIX siguen gestionando todos los datos de nombres utilizando sólo los archivos locales. Sin embargo, la gestión de hosts, usuarios y otros datos de nombres mediante archivos locales no es adecuada para redes complejas de gran tamaño. Cada archivo `/etc` se describe en la página del comando man asociada. Por ejemplo, el archivo `/etc/inet/hosts` se describe en la página del comando man `hosts(4)`.

Descripción del servicio de nombres NIS

El *Servicio de información de la red* (NIS) se desarrolló independientemente de DNS. DNS simplifica la comunicación, ya que utiliza nombres de equipo en lugar de direcciones IP numéricas. NIS se centra en facilitar la administración de la red al proporcionar un control centralizado sobre una variedad de información de red. NIS almacena información acerca de la red, nombres y direcciones de equipo, usuarios y servicios de red. Esta recopilación de información de red se conoce como *espacio de nombres NIS*.

La información del espacio de nombres NIS se almacena en mapas NIS. Los mapas NIS están diseñados para reemplazar los archivos `/etc` de UNIX y otros archivos de configuración. Los mapas NIS almacenan mucho más que nombres y direcciones. Como resultado, el espacio de nombres NIS tiene un gran conjunto de mapas. Consulte "Trabajo con mapas NIS" en la página 101 para obtener más información.

NIS utiliza una disposición cliente-servidor que es similar a DNS. Los servidores NIS replicados proporcionan servicios para los clientes NIS. Los servidores principales se denominan servidores *maestros* y, para una mayor confiabilidad, los servidores tienen una copia de

seguridad, o servidores *esclavos*. Ambos servidores maestro y esclavo utilizan el software de recuperación NIS y ambos almacenan mapas NIS. Para obtener más información sobre la arquitectura y administración de NIS, consulte el Capítulo 6, "Instalación y configuración del servicio NIS (tareas)" y el Capítulo 7, "Administración de NIS (tareas)".

Descripción de los servicios de nombres LDAP

El Protocolo ligero de acceso a directorios (LDAP) es el protocolo de red seguro utilizado para acceder a los servidores de directorios para nombres distribuidos y otros servicios de directorio. Este protocolo basado en estándares admite una estructura de base de datos jerárquica. Se puede utilizar el mismo protocolo para proporcionar servicios de nombres que estén en UNIX y en entornos de varias plataformas.

El sistema operativo Oracle Solaris admite LDAP junto con Oracle Directory Server Enterprise Edition (antes Sun Java System Directory Server) y otros servidores de directorios LDAP.

Para obtener más información sobre los servicios de nombres LDAP, consulte el Capítulo 9, "Introducción a los servicios de nombres LDAP (descripción general)".

Para obtener información sobre la transición de NIS a LDAP, consulte el Capítulo 15, "Transición de NIS a LDAP (tareas)".

Para obtener información sobre un inicio de sesión único, como también la configuración y mantenimiento de servicios de autenticación de Kerberos, consulte la Parte VI, "Servicio Kerberos" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Descripción del cambio de servicio de nombres

El cambio de servicio de nombres es un mecanismo para permitir que los clientes realicen búsquedas mediante DNS, LDAP, NIS o fuentes de datos de archivos locales para obtener información de nombres. El conmutador se administra mediante el servicio `svc:/system/name-service/switch`. Para obtener más información, consulte el Capítulo 2, "Conmutador de servicio de nombres (descripción general)".

Servicios de nombres: comparación rápida

	DNS	NIS	LDAP	Archivos
Espacio de nombres	Jerárquico	Plano	Jerárquico	Archivos
Almacenamiento de datos	Archivos/registros de recursos	Mapas de dos columnas	Directorios (variado) Base de datos indexada	Archivos basados en texto

	DNS	NIS	LDAP	Archivos
Servidores	Maestro/esclavo	Maestro/esclavo	Maestro/réplica Varias réplicas maestras	No tiene
Seguridad	DNSSEC, variado	Ninguna (raíz o nada)	Kerberos, TLS, SSL, variado	No tiene
Transporte	TCP/IP	RPC	TCP/IP	E/S de archivo
Escala	Global	LAN	Global	Solo host local
Datos	Host	Todo	Todo	Todo

Nota – DNS es el servicio recomendado para consultas de host o de dirección de red para LDAP y nombres basados en archivos.

◆ ◆ ◆ CAPÍTULO 2

Conmutador de servicio de nombres (descripción general)

En este capítulo, se describe el cambio de servicio de nombres. El cambio de servicio de nombres se utiliza para coordinar el uso de distintos servicios de nombres. En este capítulo, se describen los siguientes temas:

Acerca del cambio de servicio de nombres

El conmutador de servicio de nombres es un servicio de selección configurable que permite al administrador especificar qué origen o servicio de información de nombres va a utilizar para cada tipo de información de la red. Los servicios se denominan bases de datos. El conmutador de servicio de nombres es utilizado por las aplicaciones cliente que llaman a cualquiera de las interfaces `getXbyY()`, como las siguientes.

- `gethostbyname()`
- `getpwuid()`
- `getpwnam()`
- `getaddrinfo()`

Cada sistema cuenta con su propia configuración en un repositorio SMF. Cada propiedad definida en el conmutador de servicio de nombres identifica una base de datos concreta, como un host, una contraseña o un grupo. El valor asignado a cada propiedad muestra uno o más orígenes desde los cuales solicitar la información. A veces, estos valores incluyen indicaciones u opciones. Las indicaciones pueden incluir el número de reintentos para un servicio que se deben efectuar, el tiempo de espera para aplicar o qué hacer si el servicio no funciona correctamente.

Bases de datos y orígenes para el conmutador de servicio de nombres

Las siguientes bases de datos son admitidas por el conmutador de servicio de nombres.

TABLA 2–1 Bases de datos para el conmutador de servicio de nombres

Base de datos de información	Descripción
`alias`	Muestra los alias y las direcciones de correo electrónico.
`auth_attr`	Muestra los nombres y las descripciones de autorización.
`automount`	Muestra información sobre sistemas de archivos remotos que se pueden montar de forma local.
`bootparam`	Muestra información de inicio de clientes sin disco.
`ether`	Muestra las direcciones Ethernet y los nombres de host coincidentes.
`group`	Muestra información acerca de los grupos que se pueden utilizar para compartir el acceso a los archivos.
`host`	Muestra la lista de direcciones IP y los nombres de host coincidentes.
`netgroup`	Muestra información de los sistemas de archivos NFS compartidos.
`netmask`	Muestra máscaras de red utilizadas para implementar subredes IP.
`network`	Muestra el nombre y el número de cada red.
`password`	Muestra información de la cuenta de usuario.
`prof_attr`	Muestra nombres de perfiles de ejecución, descripciones y otros atributos.
`project`	Muestra nombres de proyecto, identificadores únicos y asignaciones de recursos asociadas.
`protocol`	Muestra nombres de protocolo de Internet, números y cualquier otro alias.
`publickey`	Muestra la información de clave pública.
`rpc`	Muestra los nombres y números de programas RPC.
`service`	Muestra el nombre, el puerto y el protocolo para servicios de Internet.
`tnrhdb`	Muestra los atributos de seguridad para un host mediante la función Trusted Extensions de Oracle Solaris.
`tnrhtp`	Muestra plantillas utilizadas por Trusted Extensions.

Además, la propiedad `default` en el conmutador de servicio de nombres define la cadena de origen para cualquier base de datos que no se defina de ningún otro modo. Si la red utiliza los

mismos orígenes para la mayoría de las bases de datos, puede cambiar la propiedad `default` y no definir ninguna propiedad para cada base de datos. Consulte "Cómo cambiar el origen de todas las bases de datos de nombres" en la página 40 para el procedimiento.

Para admitir versiones anteriores, las propiedades `enable_passwd_compat` y `enable_group_compat` se pueden establecer en `true` con el fin de activar el modo `compat` para información de contraseñas y grupos. Este modo proporciona compatibilidad con la sintaxis + o - de estilo antiguo en las bases de datos adecuadas. En la versión actual, esta funcionalidad se ha sustituido por el módulo `pam_list`.

En la siguiente tabla, se describe el tipo de orígenes que pueden aparecer en el conmutador de servicio de nombres para las bases de datos indicadas arriba.

TABLA 2–2 Orígenes de información para el conmutador de servicio de nombres

Orígenes de información	Descripción
`ad`	Identifica las bases de datos almacenadas en un servidor de Active Directory.
`compat`	`compat` se puede utilizar para la información de contraseñas y grupos con el fin de admitir la sintaxis + o - de estilo antiguo en los archivos `/etc/passwd`, `/etc/shadow` y `/etc/group`. Esta funcionalidad se ha sustituido por el módulo `pam_list`.
`dns`	Especifica que la información del host se puede obtener desde el DNS.
`files`	Especifica un archivo almacenado en el directorio `/etc` del cliente, por ejemplo, `/etc/passwd`.
`ldap`	Especifica que las entradas se pueden obtener desde el directorio LDAP.
`mdns`	Especifica información de hosts mediante el DNS de multidifusión (mDNS).
`nis`	Especifica un mapa de datos NIS, por ejemplo, el mapa `hosts`.

Criterios de búsqueda para el conmutador de servicio de nombres

Los siguientes formatos de criterios de búsqueda se pueden usar para seleccionar uno o más orígenes de información y para especificar el orden en el que los orígenes se utilizan.

- **Origen único**: si un tipo de información sólo tiene un origen, como `files`, una rutina de búsqueda que utiliza el conmutador busca la información en ese origen *solamente*. Si la rutina encuentra la información, devuelve el mensaje de estado `success`. Si la rutina no encuentra la información, detiene la búsqueda y devuelve un mensaje de estado diferente. Lo que hace la rutina con el mensaje de estado varía según la rutina.
- **Varios orígenes**: si una base de datos contiene más de un origen para un determinado tipo de información, el conmutador dirige la rutina de búsqueda para buscar en el primer origen enumerado. Si la rutina encuentra la información, devuelve el mensaje de estado `success`. Si la rutina no encuentra la información en el primer origen, intenta encontrarla en el siguiente origen. La rutina busca en todos los orígenes hasta que encuentra la información o hasta que se haya detenido por una especificación `return`. Si se realiza una búsqueda en todos los orígenes enumerados sin encontrar la información, la rutina detiene la búsqueda y devuelve el mensaje de estado `non-success`.

De manera predeterminada, en la Versión Oracle Solaris 11, el primer origen es `files`. Esta configuración impide que el sistema se bloquee si el siguiente origen enumerado no está disponible.

Mensajes de estado para el conmutador de servicio de nombres

Si una rutina encuentra la información, la rutina devuelve un mensaje de estado `success`. Si la rutina no encuentra la información, devuelve uno de los tres mensajes de estado de error posibles. Los posibles mensajes de estado se enumeran en la siguiente tabla.

TABLA 2–3 Mensajes de estado para el conmutador de servicio de nombres

Mensaje de estado	Explicación
`SUCCESS`	La entrada solicitada se encontró en el origen especificado.
`UNAVAIL`	El origen no responde o no está disponible. Es decir, no se puede encontrar ninguno de los orígenes de la base de datos ni se puede acceder a ellos.
`NOTFOUND`	El origen respondió “No existe esa entrada”. En otras palabras, se accedió a la base de datos, pero la información necesaria no se ha encontrado.
`TRYAGAIN`	El origen está ocupado y puede responder la próxima vez. En otras palabras, la base de datos se ha encontrado, pero no ha podido responder a la consulta.

Opciones de acciones de cambio para el conmutador de servicio de nombres

Puede indicar al conmutador de servicio de nombres que responda a los mensajes de estado con una de las dos *acciones* que se muestran en la tabla siguiente.

TABLA 2–4 Respuestas a mensajes de estado del conmutador de servicio de nombres

Acción	Explicación
`return`	Detiene la búsqueda de información.
`continue`	Intenta en el siguiente origen.

Además, para el mensaje de estado `TRYAGAIN`, se pueden definir las siguientes acciones:

- `forever`: permite reintentar en el origen actual de forma indefinida.
- *n*: permite reintentar en el origen actual *n* más veces.

Criterios de búsqueda predeterminados para el conmutador de servicio de nombres

La combinación de opciones de acciones y mensajes de estado del conmutador de servicio de nombres determina qué hace la rutina de búsqueda en cada paso. La combinación de opciones de acciones y mensajes de estado conforman los *criterios de búsqueda*.

Los criterios de búsqueda predeterminados del conmutador son los mismos para cada origen. Esta lista incluye una descripción de varios criterios de búsqueda.

- `SUCCESS=return`. Detiene la búsqueda de información. Continúa con el uso de la información que se ha encontrado.
- `UNAVAIL=continue`. Pasa al siguiente origen del conmutador de servicio de nombres y sigue buscando. Si este origen es el último o el único, devuelve el estado `NOTFOUND`.
- `NOTFOUND=continue`. Pasa al siguiente origen del conmutador de servicio de nombres y sigue buscando. Si este origen es el último o el único, devuelve el estado `NOTFOUND`.
- `TRYAGAIN=continue`. Pasa al siguiente origen del conmutador de servicio de nombres y sigue buscando. Si este origen es el último o el único, devuelve el estado `NOTFOUND`.

Puede cambiar los criterios de búsqueda predeterminados especificando explícitamente cualquier otro criterio con la sintaxis *STATUS=action* indicada en la lista anterior. Por ejemplo, la acción predeterminada para una condición `NOTFOUND` es continuar la búsqueda en el siguiente origen. Los criterios de búsqueda de la base de datos de la red se pueden informar de la siguiente manera:

```
svc:/system/name-service/switch> listprop config/network
config/network  astring            "nis [NOTFOUND=return] files"
```

La entrada `networks: nis [NOTFOUND=return] files` especifica un criterio no predeterminado para el estado `NOTFOUND`. Los criterios no predeterminados están delimitados por corchetes.

En este ejemplo, la rutina de búsqueda se comporta de la siguiente manera:

- Si la base de datos `network` está disponible y contiene la información necesaria, la rutina devuelve un mensaje de estado `SUCCESS`.
- Si la base de datos `network` no está disponible, la rutina devuelve un mensaje de estado `UNAVAIL`. De manera predeterminada, la rutina continúa buscando utilizando los siguientes criterios en la lista.
- Si la base de datos `network` está disponible y se ha encontrado, pero no contiene la información necesaria, la rutina devuelve un mensaje `NOTFOUND`. Sin embargo, en lugar de seguir buscando el siguiente origen, que sería el comportamiento predeterminado, la rutina detiene la búsqueda.
- Si la base de datos `network` está ocupada, la rutina devuelve un mensaje de estado `TRYAGAIN` y, de manera predeterminada, continúa buscando la base de datos `network`.

Nota – Las consultas en el conmutador de servicio de nombres se realizan en el orden en que aparecen los elementos. Sin embargo, las actualizaciones de contraseña se realizan en el orden inverso, a menos que se especifique lo contrario mediante el comando `passwd -r` *repository*. Consulte "Conmutador de servicio de nombres e información de contraseñas" en la página 41 para obtener más información.

¿Qué ocurre si la sintaxis es incorrecta?

Las rutinas de las bibliotecas de clientes contienen entradas predeterminadas compiladas que se utilizan si no se define ninguna propiedad SMF específica o ninguna propiedad SMF `default` en el conmutador de servicio de nombres, o si la propiedad está sintácticamente incorrecta. Habitualmente, los valores predeterminados compilados son sólo "archivos".

auto_home y auto_master

Los criterios de búsqueda del archivo de cambio para los mapas y las tablas `auto_home` y `auto_master` se combinan en una categoría, que se denomina `automount`.

`timezone` y el conmutador de servicio de nombres

La tabla `timezone` no utiliza el conmutador de servicio de nombres, por lo que la tabla no está incluida en la lista de propiedades para el conmutador.

Entradas `keyserv` y publickey en el conmutador de servicio de nombres

Precaución – Debe reiniciar el daemon `keyserv` después de realizar un cambio en el conmutador de servicio de nombres para que los cambios surtan efecto.

El daemon `keyserv` lee las propiedades `publickey` en el conmutador de servicio de nombres sólo cuando se inicia `keyserv`. Si cambia las propiedades del conmutador de servicio de nombres , `keyserv` no registra los cambios hasta que se reinicia el daemon `keyserv` utilizando `svcadm refresh svc:/network/rpc/keyserv:default`. Este comando se debe ejecutar después de que las propiedades se han cambiado y de que el servicio `name-service/switch` se ha refrescado para que los cambios de propiedades se carguen en el repositorio SMF.

Gestión del conmutador de servicio de nombres

Al cambiar el servicio de nombres de una máquina, debe modificar la información del conmutador de servicio de nombres de esa máquina según corresponde. Por ejemplo, si cambia el servicio de nombres de una máquina de files a NIS, debe configurar el conmutador de servicio de nombres para que utilice NIS.

▼ Cómo utilizar un archivo `nsswitch.conf` heredado

1. **Conviértase en administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Copie el archivo `nsswitch.conf` en el nuevo sistema.**

   Asegúrese de nombrar el archivo `/etc/nsswitch.conf`.

3. **Cargue la información del archivo en el repositorio SMF.**

   ```
   # nscfg import -f svc:/system/name-service/switch:default
   ```

4. **Refresque el servicio para el conmutador de servicio de nombres.**

   ```
   # svcadm refresh name-service/switch
   ```

▼ Cómo cambiar el origen de una base de datos

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Cambie la definición de origen de la base de datos seleccionada.**

En este ejemplo, el orden de búsqueda de la base de datos primero es `files` y luego es `nis`.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 **Refresque el servicio para el conmutador de servicio de nombres.**

```
# svcadm refresh name-service/switch
```

▼ Cómo cambiar el origen de todas las bases de datos de nombres

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Cambie la propiedad `config/default`.**

Esta propiedad debe utilizar la definición de origen más común. En este ejemplo, el orden de búsqueda de la base de datos primero es `files` y luego es `nis`.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/default = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 **(Opcional) Cambie las propiedades de bases de datos individuales.**

Utilice este comando para cambiar la definición de origen de cualquier base de datos que no utiliza el orden seleccionado en la propiedad `config/default`.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns nis"
svc:/system/name-service/switch> quit
```

4 **Refresque el servicio para el conmutador de servicio de nombres.**

```
# svcadm refresh name-service/switch
```

DNS y acceso a Internet

El conmutador de servicio de nombres también controla el reenvío DNS para clientes, como se describe en el siguiente capítulo. El reenvío DNS otorga acceso a Internet a los clientes.

Conmutador de servicio de nombres e información de contraseñas

Es posible incluir información de contraseñas y acceder a ella en varios repositorios, como `files` y `nis`. Puede utilizar la propiedad `config/password` en el conmutador de servicio de nombres para establecer el orden de consulta de dicha información.

Precaución – `files` debe ser el primer origen en el conmutador de servicios de nombres para la información de `passwd` a fin de evitar un ataque de denegación de servicio (DoS) en el sistema.

En un entorno NIS, la propiedad `config/password` en el conmutador de servicio de nombres debe mostrar los repositorios en el siguiente orden.

```
config/password  astring            "files nis"
```

Consejo – Si aparece primero `files`, el usuario `root` puede iniciar sesión, en la mayoría de los casos, incluso cuando el sistema encuentra problemas en el servicio de nombres o en la red.

No mantenga varios repositorios *para el mismo usuario*. En la mayoría de los casos, el servicio de nombres consulta y devuelve la primera definición solamente. Las entradas duplicadas normalmente enmascaran problemas de seguridad.

Por ejemplo, si se tiene el mismo usuario en ambos archivos y en el repositorio de la red (según la configuración `config/password` `name-service/switch`), se usa un ID de inicio de sesión sobre el otro. El primer ID coincidente para una máquina determinada se convertirá en el ID utilizado para la sesión de inicio de sesión. Si un ID está en ambos archivos y en el repositorio de la red, y el repositorio de la red se ha desactivado por motivos de seguridad, cualquier máquina en la que reside el ID y a la que se accede antes de que el ID de la red se desactive podría volverse insegura y vulnerable al acceso no deseado e inseguro.

◆ ◆ ◆ CAPÍTULO 3

Gestión de DNS (tareas)

En este capítulo, se proporciona información sobre los servicios de servidores y clientes DNS. Contiene los temas siguientes:

Descripción general del DNS

El DNS, al igual que la mayoría de los protocolos de red, tiene dos partes: un servicio que proporciona respuestas y un cliente que consulta al servicio. En el Sistema operativo Oracle Solaris, el servicio DNS predeterminado es proporcionado por BIND, de Internet Systems Consortium (ISC), y su daemon asociado `named`. El cliente DNS consta de una recopilación de utilidades y bibliotecas.

DNS de multidifusión

El DNS de multidifusión (mDNS) proporciona un sistema de servicio de nombres fácil de configurar y mantener para los sistemas en un enlace local. Todos los dispositivos de red participantes en el mismo enlace local realizan funciones DNS estándar usando el mDNS en lugar de la unidifusión, por lo que no necesitan un servidor DNS de unidifusión. Para los administradores, la principal ventaja del mDNS es que ningún servidor DNS de unidifusión se debe mantener en la red local. No hay necesidad, por ejemplo, de actualizar y mantener nombres de host en archivos con el fin de resolver solicitudes de nombres de host para direcciones IP de sistemas en el enlace local que usan el mDNS.

Detección de servicios DNS de multidifusión

Los servicios de red incluyen impresión, transferencia de archivos, uso compartido de música, servidores para uso compartido de fotografías, documentos y otros archivos, y servicios proporcionados por otros dispositivos locales. La compatibilidad con la detección de servicios DNS en Oracle Solaris incluye una estructura de código abierto y herramientas de Apple inc. para que las aplicaciones puedan anunciar y detectar servicios de red usando el DNS en esta versión de Oracle Solaris.

Para los usuarios, la detección de servicios de red hace que la informática sea más fácil, ya que permite buscar servicios en la red, en lugar de tener que buscarlos de forma manual. Los estándares existentes y el trabajo realizado por otras compañías y grupos garantizan la compatibilidad entre plataformas.

Materiales relacionados sobre el DNS

Para obtener información sobre la administración de DNS y BIND, consulte la siguiente documentación:

- *Manual del administrador de BIND 9* en el sitio web de ISC en http://www.isc.org
- Documentación de notas de migración de BIND 9 en el archivo `/usr/share/doc/bind/migration.txt`
- Listas de las funciones de BIND, errores y defectos conocidos, y vínculos a material adicional en el sitio web de ISC, en http://www.isc.org
- *DNS y BIND (5.° edición)*, por Paul Albitz y Cricket Liu (O'Reilly, 2006)

DNS y la utilidad de gestión de servicios

El daemon del servidor DNS, `named`, se debe gestionar con la utilidad de gestión de servicios (SMF). Para obtener una descripción general de la SMF, consulte el Capítulo 1, "Gestión de servicios (descripción general)" de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M), `svcs`(1) y `svccfg`(1M) para obtener más información.

En la siguiente lista, se ofrece una breve descripción general de la información importante necesaria para utilizar el servicio SMF con el fin de administrar el servicio DNS.

- Para realizar acciones administrativas en este servicio, como la activación, la desactivación o el reinicio, utilice el comando `svcadm`.

Consejo – La desactivación temporal de un servicio mediante la opción `-t` brinda protección para la configuración del servicio. Si el servicio se desactiva con la opción `-t`, los valores originales se restauran en el servicio después de reiniciar. Si el servicio se desactiva sin la opción `-t`, el servicio permanece desactivado después de reiniciar.

- Los identificadores de recursos de gestión de errores (FMRI) para el servicio DNS son `svc:/network/dns/server:`*instance* y `svc:/network/dns/client:`*instance*.
- Puede consultar el estado del servidor y el cliente DNS mediante el comando `svcs`.
  - A continuación, se muestra un ejemplo del comando `svcs` y su salida:

```
# svcs \*dns\*
STATE          STIME    FMRI
disabled       Nov_16   svc:/network/dns/multicast:default
online         Nov_16   svc:/network/dns/server:default
online         Nov_16   svc:/network/dns/client:default
```

  - A continuación, se muestra un ejemplo del comando `svcs -l` y su salida:

```
# svcs -l /network/dns/server
fmri         svc:/network/dns/server:default
name         BIND DNS server
enabled      true
state        online
next_state   none
state_time   Tue Jul 26 19:26:12 2011
logfile      /var/svc/log/network-dns-server:default.log
restarter    svc:/system/svc/restarter:default
contract_id  83
manifest     /lib/svc/manifest/network/dns/server.xml
dependency   require_all/none svc:/system/filesystem/local (online)
dependency   require_any/error svc:/network/loopback (online)
dependency   optional_all/error svc:/network/physical (online)
```

- Si necesita iniciar el servicio DNS con opciones distintas, cambie las propiedades del servicio `svc:/network/dns/server` mediante el comando `svccfg`. Para obtener un ejemplo, consulte "Cómo configurar las opciones del servidor DNS" en la página 47.

Cuando el daemon del servidor DNS, `named`, es gestionado por SMF, el servidor se reinicia automáticamente cuando se produce un evento inesperado que hace que `named` se cierre de forma anormal. Además, usted puede utilizar el comando `svcadm` para reiniciar el servicio. La gestión específica de BIND que está disponible usando el comando `rndc` se puede utilizar de forma simultánea con SMF.

Administración de DNS (tareas)

Las siguientes tareas están documentadas:

▼ Cómo instalar el paquete DNS

Normalmente, el paquete DNS se instala automáticamente con la versión de Oracle Solaris. Si el paquete no se incluye cuando se instala el servidor, utilice el procedimiento siguiente para instalar el paquete.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Instale el paquete DNS.

```
# pkg install pkg:/service/network/dns/bind
```

▼ Cómo configurar un servidor DNS

Nota – No se recomienda la configuración de `named` para especificar un cambio en el directorio raíz. Una opción más segura consiste en crear una zona de Solaris y configurar `named` para que se ejecute en esa zona.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Cree y verifique un archivo de configuración de DNS.

Antes de que empiece el daemon `named`, debe haber un archivo de configuración válido. El archivo se denomina `/etc/named.conf` de manera predeterminada. La configuración de `named`

puede ser muy sencilla. Un archivo vacío proporciona información suficiente para configurar un servidor de sólo caché, suponiendo que se puede acceder a los servidores raíz DNS.

```
# touch /etc/named.conf
# named-checkconf -z /etc/named.conf
```

3 **(Opcional) Cree un archivo de configuración `rndc`.**

Este archivo se utiliza para configurar el acceso de control remoto del servidor DNS.

```
# rndc-confgen -a
wrote key file "/etc/rndc.key"
```

4 **(Opcional) Cambie la información de configuración para el servicio `dns/server`.**

Consulte "Cómo configurar las opciones del servidor DNS" en la página 47.

5 **Inicie el servicio DNS.**

```
# svcadm enable network/dns/server
```

▼ Cómo crear un archivo `rndc.conf`

El archivo `/etc/rndc.conf` se utiliza para configurar el acceso de control remoto del daemon del servidor DNS, `named`, mediante el comando `rndc`. Para crear un archivo predeterminado, utilice el procedimiento siguiente. Consulte la página del comando man `rndc.conf(4)` para obtener más opciones.

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Cree el archivo de configuración `rndc`.**

```
# rndc-confgen -a
wrote key file "/etc/rndc.key
```

3 **Reinicie el servicio DNS.**

```
# svcadm restart dns/server:default
```

▼ Cómo configurar las opciones del servidor DNS

En este procedimiento, se explica cómo seleccionar el protocolo de transporte IPv4 para el tráfico `named`. Consulte la página del comando man `named(1M)`.

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Cambie la información de configuración para el servicio `dns/server`.

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop options/ip_interfaces = "IPv4"
svc:/network/dns/server:default> quit
```

3 Actualice el repositorio SMF y active el servicio DNS.

```
# svcadm refresh network/dns/server
# svcadm enable network/dns/server
```

▼ Cómo ejecutar el servicio DNS como un usuario alternativo

En este procedimiento, se explica cómo asignar a un usuario las autorizaciones correspondientes para gestionar el daemon `named`.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Agregue el usuario al rol adecuado.

```
# usermod -A solaris.smf.manage.bind dnsadmin
```

3 Establezca las propiedades de servicio para el usuario.

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop start/user = dnsadmin
svc:/network/dns/server:default> setprop start/group = dnsadmin
svc:/network/dns/server:default> exit
```

4 Cree un directorio para el nuevo archivo de ID de proceso.

Debido a que sólo `root` tiene acceso de escritura para crear el archivo de ID de proceso predeterminado, `/var/run/named/named.pid`, el daemon `named` debe estar configurado para utilizar un archivo alternativo.

```
# mkdir /var/named/tmp
# chown dnsadmin /var/named/tmp
```

5 Cambie la configuración para utilizar el nuevo directorio.

Agregue las siguientes líneas al archivo `named.conf`:

```
# head /etc/named.conf
options {
directory "/var/named";
pid-file "/var/named/tmp/named.pid";
};
```

6 **Actualice el repositorio SMF y reinicie el servicio DNS.**

```
# svcadm refresh svc:/network/dns/server:default
# svcadm restart svc:/network/dns/server:default
```

▼ Cómo activar un cliente DNS

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Configure el dominio DNS.**

En primer lugar, enumere los dominios de búsqueda y las direcciones IP de los servidores de nombres DNS. A continuación, actualice el repositorio SMF.

```
# svccfg -s network/dns/client
svc:/network/dns/client> setprop config/search = astring: ("example.com" "sales.example.com")
svc:/network/dns/client> setprop config/nameserver = net_address: (192.168.1.10 192.168.1.11)
svc:/network/dns/client> select network/dns/client:default
svc:/network/dns/client:default> refresh
svc:/network/dns/client:default> quit
```

3 **Actualice la información del conmutador de servicio de nombres para utilizar el DNS.**

El primer comando actualiza la información de configuración del DNS en el repositorio SMF.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

4 **Escriba la nueva información en el archivo `/etc/resolv.conf`.**

El archivo `/etc/resolv.conf` todavía se utiliza en algunos procesos, de manera que después de realizar cambios en el repositorio SMF que cambiarían el contenido del archivo, éste se debe volver a crear.

```
# nscfg export svc:/network/dns/client:default
```

5 **Inicie los servicios necesarios para ejecutar el cliente DNS.**

```
# svcadm enable network/dns/client
# svcadm enable system/name-service/switch
```

▼ Cómo solucionar problemas de inicio del servidor DNS

No se tienen que seguir todos estos pasos. Si piensa que ha encontrado el problema en un paso anterior, puede proceder al paso 6 para que el servicio se ejecute correctamente.

1. **Conviértase en administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Compruebe el estado del servicio DNS.**

```
# svcs -x dns/server:default
svc:/network/dns/server:default (BIND DNS server)
 State: online since Tue Oct 18 19:35:00 2011
   See: named(1M)
   See: /var/svc/log/network-dns-server:default.log
Impact: None.
```

3. **Compruebe el archivo de registro del servicio DNS.**

```
# tail /var/svc/log/network-dns-server:default.log
```

4. **Compruebe los mensajes syslog.**

```
# grep named /var/adm/messages
```

5. **Inicie el daemon `named` manualmente.**

   La ejecución de `named` en primer plano hace que todos los registros sean errores estándar para que sea más fácil identificar los problemas.

```
# named -g
```

6. **Después de solucionar el problema, borre el estado de mantenimiento requerido.**

```
# svcadm clear dns/server:default
# svcs dns/server:default
STATE          STIME    FMRI
online         17:59:08 svc:/network/dns/server:default
```

▼ Cómo verificar la configuración del DNS

Al modificar la configuración del DNS, puede verificar la sintaxis del archivo `/etc/named.conf` con el comando `named-checkzone`.

1. **Conviértase en administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Cambie el archivo de configuración, según sea necesario.**

   En este ejemplo, se cambia el directorio predeterminado.

```
# echo 'options {directory "/var/named";};' > /etc/named.conf
```

3 **Verifique el contenido del archivo.**

```
# named-checkconf
/etc/named.conf:1: change directory to '/var/named' failed: file not found

/etc/named.conf:1: parsing failed
```

En este ejemplo, la comprobación falló porque el directorio `/var/named` aún no ha sido creado.

4 **Corrija los errores informados.**

```
# mkdir /var/named
```

5 **Repita los pasos 3 y 4 hasta que no se informe ningún error.**

6 **(Opcional) Para reflejar el cambio en el servicio en ejecución, utilice uno de los siguientes métodos:**

- **Utilice el comando `rndc` para actualizar la configuración con la opción `reload` o `reconfig` en función de los cambios realizados.**
- **Reinicie el servicio `named`.**

  ```
  # svcadm restart svc:/network/dns/server:default
  ```

Administración del DNS de multidifusión

En las siguientes secciones, se explica cómo activar el DNS de multidifusión (mDNS) y la detección de servicios DNS. También se proporcionan ejemplos de cómo anunciar recursos para la detección de servicios DNS.

▼ Cómo activar el mDNS y la detección de servicios DNS

Para que el mDNS y la detección de servicios DNS funcionen, el mDNS se debe desplegar en todos los sistemas que van a participar en el mDNS. El servicio mDNS se utiliza para anunciar la disponibilidad de los servicios proporcionados en el sistema.

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Si es necesario, instale el paquete mDNS.**

```
# pkg install pkg:/service/network/dns/mdns
```

3 Actualice la información del conmutador de servicio de nombres.

Para poder resolver hosts locales, cambie la propiedad `config/host` del servicio `name-service/switch` para incluir `mdns` como origen. Por ejemplo:

```
#  /usr/sbin/svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns mdns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch> quit
```

4 Active el servicio mDNS.

```
# svcadm enable svc:/network/dns/multicast:default
```

La activación del mDNS de esta manera garantiza que los cambios se mantengan luego de las actualizaciones y los reinicios. Para obtener más información, consulte la página del comando man `svcadm`(1M).

5 (Opcional) Si es necesario, compruebe el registro de errores del mDNS.

Compruebe el registro del servicio mDNS, `/var/svc/log/network-dns-multicast:default.log`, en busca de errores o mensajes.

Anuncio de recursos para DNS

Puede utilizar el comando `dns-sd` como herramienta de diagnóstico de red para explorar y detectar servicios, de manera similar a como usaría el comando `ping` o `traceroute`.

El comando `dns-sd` es, más que nada, para uso interactivo, principalmente porque sus argumentos de línea de comandos y su formato de salida pueden cambiar con el paso del tiempo, lo que hace que invocarlo desde una secuencia de comandos de shell sea imprevisible y riesgoso. Además, la naturaleza asíncrona de la detección de servicios DNS (DNS-SD) no se presta a sí misma con facilidad a la programación orientada a la secuencia de comandos.

Para obtener más información, consulte la página del comando man `dns-sd` (1M). Para incorporar el servicio DNS en aplicaciones, consulte la página del comando man `libdns-sd`(3DNS_SD).

A continuación se muestran ejemplos de anuncios de servicios mediante la detección de servicios DNS.

EJEMPLO 3–1 Anuncio de un servicio de impresión

El siguiente comando anuncia la existencia del servicio de impresión LPR en el puerto `515` en un sistema denominado `My Test`, de forma que esté disponible para los clientes de impresión compatibles con DNS-SD:

```
# dns-sd -R "My Test" _printer._tcp. . 515 pdl=application/postscript
```

Para que este registro sea útil, el servicio LPR debe estar disponible en el puerto `515`.

EJEMPLO 3–2 Anuncio de una página web

El siguiente comando anuncia una página web atendida por un servidor HTTP en el puerto `80`, en el sistema `My Test`. La página web aparecerá en la lista Bonjour en Safari y otros clientes web compatibles con DNS-SD.

```
# dns-sd -R "My Test" _http._tcp . 80 path=/path-to-page.html
```

Referencia del DNS

En esta sección, se incluyen tablas de los archivos, los daemons y los comandos que están asociados con el servicio DNS. Además, se incluye una tabla con algunos de los indicadores que se utilizan cuando se crea la versión ISC de BIND.

Archivos DNS

En la siguiente tabla, se describen los archivos asociados con el servicio DNS.

TABLA 3–1 Archivos DNS

Nombre de archivo	Función
`/etc/named.conf`	Proporciona información de configuración para el daemon `named`. Consulte la página del comando man `named.conf(4)` para obtener más información.
`/etc/rndc.conf`	Proporciona información de configuración para el comando `rndc`. Consulte la página del comando man `rndc.conf(4)` para obtener más información.

Comandos y daemons DNS

En la siguiente tabla, se describen los comandos y daemons asociados con el servicio DNS.

TABLA 3–2 Comandos y daemons DNS

Nombre de archivo	Función
`/usr/bin/dns-sd`	Busca o muestra los recursos que utiliza el servicio mDNS. Consulte la página del comando man `dns-sd`(1M) para obtener más información.
`/usr/sbin/dig`	Solicita respuestas de DNS de un servidor DNS. Se utiliza, a menudo, para solucionar problemas. Consulte la página del comando man `dig(1M)` para obtener más información.

TABLA 3–2 Comandos y daemons DNS *(Continuación)*

Nombre de archivo	Función
`/usr/sbin/dnssec-dsfromkey`	Genera un DS RR desde un archivo de claves. Consulte la página del comando man `dnssec-dsfromkey`(1M) para obtener más información.
`/usr/sbin/dnssec-keyfromlabel`	Recupera claves seleccionadas desde dispositivos de cifrado y crea un archivo de claves. Consulte la página del comando man `dnssec-keygen`(1M) para obtener más información.
`/usr/sbin/dnssec-keygen`	Crea claves y archivos de claves para DNS seguros y firmas de transacciones (TSIG). Consulte la página del comando man `dnssec-keygen`(1M) para obtener más información.
`/usr/sbin/dnssec-signzone`	Firma una zona DNS. Consulte la página del comando man `dnssec-signzone`(1M) para obtener más información.
`/usr/sbin/host`	Realiza búsquedas DNS simples y, a menudo, convierte nombres de host en direcciones IP o direcciones IP en nombres de host. Consulte la página del comando man `host`(1M) para obtener más información.
`/usr/sbin/named`	Daemon del servidor DNS, que responde a las solicitudes de información de los clientes. Consulte la página del comando man `named`(1M) para obtener más información.
`/usr/sbin/named-checkconf`	Comprueba la sintaxis del archivo `named.conf`. Consulte la página del comando man `named`(1M) para obtener más información.
`/usr/sbin/named-checkzone`	Comprueba la sintaxis y la integridad de un archivo de zona DNS. Consulte la página del comando man `named-checkzone`(1M) para obtener más información.
`/usr/sbin/named-compilezone`	Convierte un archivo de zona DNS. Consulte la página del comando man `named-compilezone`(1M) para obtener más información.
`/usr/sbin/nscfg`	Utilidad de configuración del servicio de nombres heredada, que permite importar o exportar contenido de `resolv.conf` del repositorio SMF. Consulte la página del comando man `nscfg`(1M) para obtener más información.
`/usr/sbin/nslookup`	Obsoleto: consulta al servidor DNS. En cambio, utilice el comando `dig`.
`/usr/sbin/nsupdate`	Envía solicitudes de actualización de DNS a un servidor DNS. Consulte la página del comando man `nsupdate`(1M) para obtener más información.
`/usr/sbin/rndc`	Proporciona control remoto del daemon del servidor DNS. Consulte la página del comando man `rndc`(1M) para obtener más información.
`/usr/sbin/rndc-confgen`	Genera archivos de configuración para el comando `rndc`. Consulte la página del comando man `rndc-confgen`(1M) para obtener más información.

Indicadores de compilación que se utilizan cuando se crea BIND

Puede ver los indicadores que se utilizaron para compilar BIND mediante el comando `named -V`. En esta tabla, se muestran algunos de los indicadores de compilación que se usaron al crear la versión ISC de BIND para la versión Oracle Solaris 11.

TABLA 3–3 Indicadores de compilación de BIND

Nombre de indicador	Función
`with-openssl`	Crea BIND con compatibilidad de cifrado y capa de conexión segura (SSL), que se necesita para DNSSEC.
`enable-threads`	Activa subprocesos múltiples.
`enable-devpoll`	Utiliza el controlador `/dev/poll` para lograr un sondeo rápido en muchos descriptores de archivos.
`disable-openssl-version-check`	Desactiva la comprobación de versión de OpenSSL debido a que OpenSSL es proporcionado por otra biblioteca dinámica.
`enable-fixed-rrset`	Permite que el registro de recursos fijo establezca el orden, que es necesario para la compatibilidad con versiones anteriores.
`with-pkcs11`	Permite el uso de compatibilidad de hardware de cifrado de OpenSSL.

◆ ◆ ◆ CAPÍTULO 4

Configuración de clientes de Active Directory de Oracle Solaris (tareas)

El módulo de servicio de nombres `nss_ad` proporciona un back-end para los archivos `passwd`, `shadow` y `group`. El módulo `nss_ad` utiliza Active Directory (AD) y su esquema nativo como el servicio de nombres para resolver identificadores y nombres de usuarios y grupos en un bosque AD. Se incluyen los siguientes temas:

Descripción general del módulo de servicio de nombres `nss_ad`

El cliente de Oracle Solaris se debe unir a un dominio AD antes de que se pueda usar cualquier funcionalidad de interoperabilidad, incluido `nss_ad`. La utilidad `kclient` se utiliza para unir el cliente a AD. Durante la operación de unión, `kclient` configura Kerberos v5 en el cliente. A partir de ese momento, `nss_ad` se puede utilizar para resolver solicitudes de servicio de nombres especificando `ad` como origen en el archivo `nsswitch.conf` para las bases de datos compatibles. El módulo `nss_ad` utiliza las credenciales de host para consultar información del servicio de nombres en AD.

El módulo `nss_ad` utiliza los registros del servidor DNS para detectar automáticamente servidores de directorios AD, como controladores de dominio y servidores de catálogos globales. Por lo tanto, el DNS debe estar configurado correctamente en el cliente de Oracle Solaris. El módulo `nss_ad` también utiliza el protocolo v3 de LDAP para acceder a información de nombres desde servidores AD. El esquema de servidor AD no requiere ninguna modificación porque `nss_ad` funciona con el esquema AD nativo.

El módulo `nss_ad` no admite actualmente inicios de sesión de los usuarios de Windows en el sistema Oracle Solaris. Hasta que se admitan dichos inicios de sesión, los usuarios deberán seguir iniciando sesión mediante back-ends tradicionales, como `nis` o `ldap`.

Los servicios idmap y svc:/system/name-service/cache deben estar activados para usar nss_ad. El módulo nss_ad utiliza el servicio idmap para asignar entre identificadores de seguridad (SID) de Windows, identificadores de usuario (UID) de UNIX e identificadores de grupos (GID).

Asegúrese de que todos los nombres de grupos y usuarios de Active Directory estén cualificados con nombres de dominios, como user@domain o group@domain. Por ejemplo, getpwnam(dana) fallará, pero getpwnam(dana@domain) se realizará éxito, siempre que dana sea un usuario de Windows válido en el dominio llamado domain.

Las siguientes reglas adicionales también pertenecen al módulo nss_ad:

- Al igual que AD, nss_ad realiza comparaciones sin distinguir mayúsculas de minúsculas de los nombres de usuarios y grupos.
- Sólo use el módulo nss_ad en configuraciones regionales UTF-8 o en dominios en los que los usuarios y los grupos sólo tienen caracteres ASCII en sus nombres.
- Los SID muy conocidos son un conjunto de SID que identifican usuarios o grupos genéricos en el mundo de Windows. No son específicos del dominio y sus valores permanecen constantes en todos los sistemas operativos Windows. Los nombres de SID muy conocidos están cualificados con la cadena BUILTIN, por ejemplo, Remote Desktop Users@BUILTIN.
- El módulo nss_ad no admite la enumeración. Por lo tanto, las interfaces getpwent() y getgrent(), y los comandos que las usan, como getent passwd y getent group, no pueden recuperar información desde AD.
- El módulo nss_ad actualmente sólo admite los archivos passwd y group. nss_ad no admite otras bases de datos de servicios de nombres que siguen la entrada passwd, como audit_user y user_attr. Si el back-end ad se procesa (en función de la configuración), devuelve el mensaje NOT FOUND (no encontrado) para estas bases de datos.

▼ Cómo configurar el módulo nss_ad

El módulo nss_ad requiere que el cliente de Oracle Solaris use DNS para la resolución de host.

1 Configure el servicio DNS.

Consulte "Cómo activar un cliente DNS" en la página 49 para obtener instrucciones.

Nota – El nombre de dominio AD se debe especificar por medio de la directiva domain o como el primer elemento de la lista especificado por la directiva search.

Si se especifican ambas directivas, la última tiene prioridad. Esto es necesario para que la función de detección automática idmap funcione correctamente.

En el ejemplo siguiente, los comandos dig verifican que el servidor AD se pueda resolver mediante el uso de su nombre y dirección IP.

```
# dig -x 192.168.11.22 +short
myserver.ad.example
# dig myserver.ad.example +short
192.168.11.22
```

2 Agregue dns a la lista de los servicios de nombres para hosts.

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

Nota – Si desea incluir servicios de nombres adicionales, como nis o ldap, para la resolución de host, agréguelos después de dns.

---

3 Verifique que el servicio DNS esté activado y en línea.

Por ejemplo:

```
# svcs svc:/network/dns/client
STATE STIME FMRI
online Oct_14 svc:/network/dns/client:default
```

4 Utilice la utilidad kclient para unir el sistema al dominio AD.

Por ejemplo:

```
# /usr/sbin/kclient -T ms_ad
```

5 Agregue ad a la lista de servicios de nombres de password y group.

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

6 Active el servicio idmap.

```
# svcadm enable idmap
```

7 Actualice el repositorio SMF para el conmutador de servicio de nombres.

```
# svcadm refresh name-service/switch
```

Nota – El módulo nscd, si es necesario, se reinicia automáticamente cada vez que se refresca el conmutador de servicio de nombres.

---

8 **Verifique si puede acceder a información de `user` y `group` desde AD.**

Por ejemplo:

```
# getent passwd 'test_user@example'
test_user@example:x:2154266625:2154266626:test_user::
# getent passwd 2154266625
test_user@example:x:2154266625:2154266626:test_user::
```

Actualizaciones de contraseñas

En la página del comando man `passwd(4)`, se incluye una lista de los formatos válidos para la propiedad `config/passwd` en el conmutador de servicio de nombres. Se admite la agregación de `ad` a estas configuraciones. Sin embargo, no se admite el cambio de contraseñas de usuario de AD mediante el comando `passwd`. Si se encuentra en la entrada `passwd` durante una actualización de contraseña, `ad` se omite. Utilice el comando `kpasswd` para actualizar las contraseñas de usuario de AD.

El orden de búsqueda `ad` se puede agregar a entradas `password` y `group` válidas existentes en el conmutador de servicio de nombres. Por ejemplo:

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

Cómo el módulo de servicio de nombres `nss_ad` recupera datos desde AD

En la siguiente sección, se describe el modo en que el módulo `nss_ad` resuelve las solicitudes del servicio de nombres para archivos `passwd`, `shadow` y `group` mediante la recuperación de datos correspondientes desde AD.

Recuperación de información de `passwd`

En la sintaxis siguiente, se muestra el formato correcto de una entrada de `passwd`:

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

Consulte la página del comando man `passwd(4)` para obtener más información.

El módulo `nss_ad` recupera información de `passwd` desde AD de la siguiente forma:

- *username*: el campo usa el valor del atributo AD `samAccountName` y está calificado por el nombre de dominio en el cual reside el objeto, por ejemplo, `terryb@example.com`.

- *password*: el campo usa el valor de x porque la contraseña de usuario no está disponible en el objeto AD.
- *uid*: el campo usa el SID del usuario de Windows del atributo AD objectSID, que se asigna al UID mediante el servicio idmap.
- *gid*: el campo usa el SID del grupo primario del usuario de Windows, que se asigna al GID mediante el servicio idmap. El SID del grupo se obtiene agregando el valor del atributo AD primaryGroupIDal SID del dominio. Para los usuarios en AD, el atributo primaryGroupID es un atributo opcional, por lo que es posible que no exista. Si el atributo no existe, nss_ad usa la utilidad de asignación diagonal idmap para asignar el SID del usuario desde el atributo objectSID.
- *gecos*: el valor del atributo AD CN.
- *home-directory*: el valor del atributo AD homeDirectory si existe un valor. De lo contrario, este campo se deja vacío.
- *login-shell*: el campo se deja vacío porque no hay un atributo de shell de inicio de sesión en el esquema AD nativo.

Recuperación de información de shadow

En la sintaxis siguiente, se muestra el formato correcto de una entrada de shadow:

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

Consulte la página del comando man shadow(4) para obtener más información.

El módulo nss_ad recupera información de shadow desde AD de la siguiente forma:

- *username*: el campo usa el valor del atributo AD samAccountName y está calificado por el nombre de dominio en el cual reside el objeto, por ejemplo, terryb@example.com.
- *password*: el campo usa el valor de *NP* porque la contraseña de usuario no está disponible en el objeto AD.

El resto de campos de shadow se dejan vacíos porque no son relevantes con AD y Kerberos v5.

Recuperación de información de group

En la sintaxis siguiente, se muestra el formato correcto de una entrada de group:

groupname:*password*:*gid*:*user-list*

Consulte la página del comando man group(4) para obtener más información.

El módulo nss_ad recupera información desde AD de la siguiente forma:

- *groupname*: el campo usa el valor del atributo AD `samAccountName` y está calificado por el nombre de dominio en el cual reside el objeto, por ejemplo, `admins@example`.
- *password*: el campo se deja vacío porque los grupos de Windows no tienen contraseñas.
- *gid*: el campo usa el SID del grupo de Windows del atributo AD `objectSID`, que se asigna al GID mediante el servicio `idmap`.
- *user-list*: el campo se deja vacío.

PARTE II

Configuración y administración de NIS

Esta parte proporciona una descripción general del servicio de nombres del Servicio de información de la red (NIS), y la configuración, la administración y la resolución de problemas de NIS dentro de SO Oracle Solaris.

◆ ◆ ◆ CAPÍTULO 5

Servicio de información de red (descripción general)

Este capítulo ofrece una descripción general del Servicio de información de la red (NIS).

NIS es un servicio de nombres distribuido. Es un mecanismo para identificar y localizar objetos y recursos de red. Proporciona un método de almacenamiento y recuperación uniforme para la información de toda la red en forma de protocolo de transporte y independiente de los medios.

En este capítulo, se tratan los siguientes temas:

Introducción a NIS

Mediante la ejecución de NIS, el administrador del sistema puede distribuir bases de datos administrativas, denominadas *mapas*, entre una serie de servidores (*maestro* y *esclavos*). El administrador puede actualizar las bases de datos desde una ubicación centralizada de manera automática y confiable para asegurarse de que todos los clientes compartan la misma información del servicio de nombres de forma coherente y en toda la red.

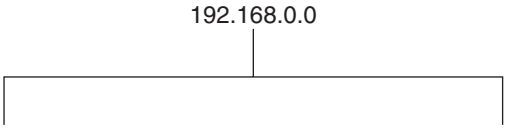
NIS se desarrolló independientemente de DNS y tiene un enfoque ligeramente distinto. Mientras que DNS trata de facilitar la comunicación con el uso de nombres de equipos en lugar de direcciones IP numéricas, NIS se centra en facilitar la administración de la red mediante un control centralizado sobre distintos tipos de información de red. NIS almacena información no sólo sobre los nombres y las direcciones del equipo, sino también sobre los usuarios, la red y los servicios de red. Esta recopilación de *información* de red se conoce como el *espacio de nombres* NIS.

Nota – En algunos contextos, los nombres de *equipo* se conocen como nombres de *host* o nombres de *máquina*. Aquí se utiliza *máquina*, pero algunos nombres de mapas de datos NIS o mensajes de pantalla podrían utilizar *host* o *máquina*.

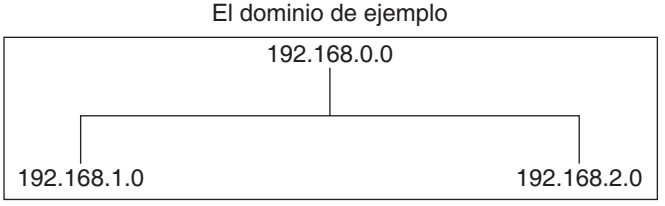
Arquitectura de NIS

NIS utiliza una disposición cliente-servidor. Los servidores NIS proporcionan servicios a los clientes NIS. El servidor principal se denomina servidor *maestro* y, por motivos de seguridad, puede tener varios servidores de reserva o servidores *esclavos*. Tanto el servidor maestro como los servidores esclavos utilizan el software de recuperación de información NIS y almacenan mapas de datos NIS.

NIS utiliza dominios para organizar los equipos, los usuarios y las redes en su espacio de nombres. Sin embargo, no utiliza una jerarquía de dominios. Un espacio de nombres NIS es plano.



Por lo tanto, esta red física se organizará en un dominio NIS.



Un dominio NIS no se puede conectar directamente a Internet usando sólo NIS. Sin embargo, las organizaciones que desean utilizar NIS y también estar conectadas a Internet puede combinar NIS con DNS. Puede utilizar NIS para gestionar toda la información local y usar DNS para consultas de host de Internet. NIS también proporciona un servicio de reenvío que reenvía las consultas de host al DNS si no se puede encontrar la información en un mapa de datos NIS. El sistema Oracle Solaris también permite configurar el conmutador de servicio de nombres de modo que las solicitudes de consulta de hosts se puedan dirigir de las siguientes formas:

- Para acceder únicamente al DNS.

- Para acceder al DNS, pero si un host no se encuentra en el DNS, se accede al NIS.
- Para acceder al NIS, pero si un host no se encuentra en el NIS, se accede al DNS.

Para una máxima interoperabilidad, DNS es el servicio recomendado para consultas de host. Consulte Capítulo 2, “Conmutador de servicio de nombres (descripción general)” para obtener más información.

Tipos de máquina NIS

Hay tres tipos de equipos NIS.

- Servidor maestro
- Servidores esclavos
- Clientes de servidores NIS

Cualquier equipo puede ser un cliente NIS, pero sólo los equipos con discos deben ser servidores NIS, ya saean maestros o esclavos. Los servidores también son clientes, normalmente de sí mismos.

Servidores NIS

Los servidores NIS tienen dos variedades, maestro y esclavo. El equipo designado como servidor maestro contiene el conjunto de mapas que el administrador del sistema crea y actualiza según sea necesario. Cada dominio NIS debe tener un solo servidor maestro que puede propagar actualizaciones NIS con la menor degradación de rendimiento.

Puede designar servidores NIS adicionales en el dominio como servidores esclavos. Un servidor esclavo tiene una copia completa del conjunto maestro de mapas NIS. Siempre que los mapas del servidor maestro están actualizados, las actualizaciones se propagan entre los servidores esclavos. Los servidores esclavos pueden manejar el desbordamiento de solicitudes del servidor maestro, por lo que se minimizarán los errores del tipo “servidor no disponible”.

Normalmente, el administrador del sistema designa un servidor maestro para todos los mapas NIS. Sin embargo, ya que cada mapa NIS tiene el nombre de equipo del servidor maestro codificado dentro de él, puede designar servidores diferentes para actuar como servidores maestro y esclavos para diferentes mapas. Para evitar confusiones, designe un único servidor como maestro para todos los mapas que se crean en un solo dominio. Los ejemplos de este capítulo suponen que un servidor es el maestro para todos los mapas del dominio.

Clientes NIS

Los clientes NIS ejecutan los procesos que solicitan datos de mapas en los servidores. Los clientes no hacen distinciones entre servidores maestro y esclavos, ya que todos los servidores NIS deberían tener la misma información.

Nota – El sistema operativo Oracle Solaris no admite una configuración en la que un cliente NIS y un cliente LDAP nativo coexisten en el mismo sistema cliente.

Elementos NIS

El servicio de nombres NIS se compone de los siguientes elementos:

- Dominios (consulte "Dominio NIS" en la página 68)
- Daemons (consulte "Daemons NIS" en la página 68)
- Comandos (consulte "Comandos NIS" en la página 69)
- Mapas (consulte "Mapas de datos NIS" en la página 70)

Dominio NIS

Un *dominio* NIS es una recopilación de hosts que comparten un conjunto común de mapas de datos NIS. Cada dominio tiene un nombre de dominio, y cada máquina que comparte el conjunto común de mapas pertenece a ese dominio.

Los dominios NIS y los dominios DNS no son necesariamente los mismos. En algunos entornos, los dominios NIS se definen según los diseños administrativos de la subred de la red de toda la empresa. Los nombres y dominios DNS son definidos por las jerarquías y los estándares de nombres de DNS de Internet. Los dos sistemas de nombres de dominio podrían o no estar configurados para que coincidan idénticamente. El nombre de dominio para los dos servicios se controla por separado y se puede configurar de forma diferente.

Cualquier host puede pertenecer a un dominio determinado, siempre que haya un servidor para los mapas de ese dominio en la misma red o subred. Las consultas de dominio NIS utilizan llamadas de procedimiento remoto (RPC). Por lo tanto, NIS requiere que todos los clientes y todas las máquinas del servidor que proporcionan servicios directos a esos clientes se encuentren en la misma subred accesible. No es extraño tener cada subred administrativa gestionada como un dominio NIS separado (distinto de un dominio DNS de toda la empresa), pero usando bases de datos comunes gestionadas desde una máquina maestra común. El nombre de dominio NIS y toda la información de configuración NIS compartida son gestionados por el servicio SMF `svc:/network/nis/domain`.

Daemons NIS

El servicio NIS es proporcionado por los daemons que se muestran en la siguiente tabla. El servicio NIS es gestionado por SMF. Las acciones administrativas de este servicio, como la activación, la desactivación o el reinicio, pueden realizarse con el comando `svcadm`. Para obtener una descripción general de la SMF, consulte el Capítulo 1, "Gestión de servicios

(descripción general)" de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M) y `svcs`(1) para obtener más información.

TABLA 5–1 Daemons NIS

Daemon	Función
`nscd`	Un servicio cliente que proporciona una caché para la mayoría de las solicitudes de servicios de nombres, gestionado por el servicio `svc:/system/name-service/cache`.
`rpc.yppasswdd`	El daemon de actualización de contraseña NIS gestionado por el servicio `svc:/network/nis/passwd`.
	Nota – El daemon `rpc.yppasswdd` considera que todos los shells que comienzan con una `r` están restringidos. Por ejemplo, si se encuentra en `/bin/rksh`, no puede cambiar de ese shell a otro shell. Si tiene un shell que comienza con `r` pero no debe estar restringido, consulte el Capítulo 8, "Resolución de problemas de NIS" para la resolución del problema.
`rpc.ypupdated`	Un daemon que modifica otros mapas, como `publickey`, y es gestionado por el servicio `svc:/network/nis/update`.
`ypbind`	El proceso de enlace gestionado por el servicio `svc:/network/nis/client`.
`ypserv`	El proceso de servidor gestionado por el servicio `svc:/network/nis/server`.
`ypxfrd`	Un daemon de transferencia de mapas de alta velocidad gestionado por el servicio `svc:/network/nis/xfr`.

Comandos NIS

El servicio NIS es admitido por varios comandos, que se describen en la siguiente tabla.

TABLA 5–2 Resumen de comandos NIS

Comando	Descripción
`make`	Actualiza mapas de datos NIS leyendo `/var/yp/Makefile` (cuando el comando se ejecuta en el directorio `/var/yp`). Puede utilizar `make` para actualizar todos los mapas basados en los archivos de entrada o para actualizar mapas individuales. En la página del comando man `ypmake`(1M), se describe la funcionalidad de `make` para NIS.
`makedbm`	Toma un archivo de entrada y lo convierte en los archivos `dbm.dir` y `dbm.pag`. NIS usa archivos `dbm` válidos como mapas. Usted también puede utilizar `makedbm -u` para desmontar un mapa y poder ver los pares clave-valor que incluye.
`ypcat`	Muestra el contenido de un mapa NIS.

TABLA 5–2 Resumen de comandos NIS *(Continuación)*

Comando	Descripción
`ypinit`	Crea automáticamente mapas para un servidor NIS desde los archivos de entrada. También se utiliza para construir el archivo inicial `/var/yp/binding/`*domain*`/ypservers` en los clientes. Utilice `ypinit`para configurar el servidor maestro NIS y los servidores esclavos NIS por primera vez.
`ypmatch`	Imprime el valor para uno o varias claves especificadas en un mapa NIS. No puede especificar qué versión del mapa del servidor NIS está viendo.
`yppoll`	Indica qué versión de un mapa de datos NIS se está ejecutando en el servidor que se especifica. También muestra el servidor maestro para el mapa.
`yppush`	Copia una nueva versión de un mapa NIS desde el servidor NIS maestro a sus esclavos. Ejecute el comando `yppush` en el servidor maestro NIS.
`ypset`	Indica a un proceso `ypbind` que se enlace a un servidor NIS. Este comando no es para el uso ocasional y no se aconseja su uso por temas de seguridad. Consulte las páginas del comando man `ypset`(1M) y `ypbind`(1M) para obtener información sobre las opciones `ypset` y `ypsetme` del proceso `ypbind`.
`ypwhich`	Muestra qué servidor NIS utiliza un cliente en este momento para servicios NIS. Si se invoca con la opción `-m` *mapname*, este comando muestra qué servidor NIS es el maestro de cada mapa. Si sólo se utiliza `-m`, el comando muestra los nombres de todos los mapas disponibles y sus respectivos servidores maestros.
`ypxfr`	Extrae un mapa de datos NIS de un servidor remoto y lo coloca en el directorio local `/var/yp/`*domain* usando NIS como el medio de transporte. Puede ejecutar `ypxfr` de forma interactiva o periódica desde un archivo `crontab`. También se es llamado por `ypserv` para iniciar una transferencia.

Mapas de datos NIS

La información de mapas de datos NIS se almacena en formato ndbm. En las páginas del comando man `ypfiles`(4) y `ndbm`(3C), se explica el formato del archivo de mapa.

Los mapas de datos NIS amplían el acceso a los archivos de datos `/etc` de UNIX y a otros archivos de configuración, como `passwd`, `shadow` y `group`, de modo que se puedan compartir los mismos datos entre una red de sistemas. El uso compartido de estos archivos simplifica las actualizaciones administrativas y la gestión de esos archivos de datos. NIS se puede desplegar con un mínimo esfuerzo. Sin embargo, las grandes empresas, en especial las que tienen requisitos de seguridad, deben contemplar la posibilidad de usar servicios de nombres LDAP en su lugar. En una red que ejecutan NIS, el servidor NIS maestro para cada dominio NIS mantiene un conjunto de mapas NIS para otros equipos en el dominio para consulta. Los servidores NIS esclavos también mantienen duplicados de los mapas del servidor maestro. Los equipos cliente NIS pueden obtener información de espacio de nombres de servidores maestros o esclavos.

Los mapas de datos NIS son esencialmente tablas de dos columnas. Una columna es la *clave* y la otra columna es la información relacionada con la clave. NIS busca información para un en la las claves. Parte de la información se almacena en varios mapas, porque cada mapa utiliza una clave distinta. Por ejemplo, los nombres y las direcciones de equipos se almacenan en dos mapas: `hosts.byname` y `hosts.byaddr`. Cuando un servidor tiene una nombre de equipo y necesita encontrar su dirección, busca en el mapa `hosts.byname`. Cuando tiene la dirección y necesita encontrar el nombre, busca en el mapa `hosts.byaddr`.

Un archivo NIS `Makefile` se almacena en el directorio `/var/yp` de máquinas designadas como servidor NIS en el momento de la instalación. La ejecución de `make` en ese directorio hace que `makedbm` cree o modifique los mapas de datos NIS predeterminados de los archivos de entrada.

Nota – Siempre cree mapas en el servidor maestro, ya que los mapas creados en un servidor esclavo no se transfieren automáticamente al servidor maestro.

Mapas de datos NIS predeterminados

En el sistema Oracle Solaris, se proporciona un conjunto predeterminado de mapas de datos NIS. Puede que desee utilizar todos estos mapas o sólo algunos de ellos. NIS también puede utilizar los mapas que usted cree o agregue al instalar otros productos de software.

Los mapas predeterminados para un dominio NIS se encuentran en el directorio `/var/yp/`*domain–name* de cada servidor. Por ejemplo, los mapas que pertenecen al dominio `test.com` se encuentran en el directorio `/var/yp/test.com` de cada servidor.

En la siguiente tabla, se describen los mapas de datos NIS predeterminados y se muestra el nombre del archivo de origen de cada mapa.

TABLA 5–3 Descripciones de mapas de datos NIS

Nombre de mapa	Archivo de origen correspondiente	Descripción
`audit_user`	`audit_user`	Contiene datos de preselección de auditoría de usuarios.
`auth_attr`	`auth_attr`	Contiene nombres de autorización y descripciones.
`bootparams`	`bootparams`	Contiene nombres de ruta de los archivos que necesitan los clientes durante el inicio: root, swap y posiblemente otros.
`ethers.byaddr`	`ethers`	Contiene los nombres de equipo y las direcciones Ethernet. La dirección Ethernet es la clave en el mapa.

TABLA 5–3 Descripciones de mapas de datos NIS *(Continuación)*

Nombre de mapa	Archivo de origen correspondiente	Descripción
`ethers.byname`	`ethers`	Es lo mismo que `ethers.byaddr`, excepto que la clave es nombre del equipo en lugar de la dirección Ethernet.
`exec_attr`	`exec_attr`	Perfil contiene atributos de ejecución de perfil.
`group.bygid`	`group`	Contiene información de seguridad de grupo con ID de grupo como clave.
`group.byname`	`group`	Contiene información de seguridad de grupo con nombre de grupo como clave.
`hosts.byaddr`	`hosts`	Contiene el nombre del equipo y la dirección IP, con dirección IP como clave.
`hosts.byname`	`hosts`	Contiene el nombre del equipo y la dirección IP, con el nombre del equipo (host) como clave.
`mail.aliases`	`aliases`	Contiene alias y direcciones de correo, con alias como clave.
`mail.byaddr`	`aliases`	Contiene dirección de correo y alias, con dirección de correo como clave.
`netgroup.byhost`	`netgroup`	Contiene el nombre de grupo, el nombre de usuario y el nombre del equipo.
`netgroup.byuser`	`netgroup`	Es lo mismo que `netgroup.byhost`, excepto que clave es el nombre de usuario.
`netgroup`	`netgroup`	Es lo mismo que `netgroup.byhost`, excepto que clave es nombre de grupo.
`netid.byname`	`passwd`, `hosts` `group`	Se utiliza para autenticación estilo UNIX. Contiene el nombre del equipo y la dirección de correo (incluido el nombre del dominio). Si hay un archivo `netid` disponible es consultado, además de los datos disponibles a través de los otros archivos.
`publickey.byname`	`publickey`	Contiene la base de datos de claves públicas que utiliza la RPC segura.
`netmasks.byaddr`	`netmasks`	Contiene la máscara de red que se utilizará con el envío de IP, con la dirección como clave.
`networks.byaddr`	`networks`	Contiene los nombres de redes conocidas por el sistema y sus direcciones IP, con la dirección como clave.

TABLA 5–3 Descripciones de mapas de datos NIS *(Continuación)*

Nombre de mapa	Archivo de origen correspondiente	Descripción
`networks.byname`	`networks`	Es lo mismo que `networks.byaddr`, excepto que la clave es el nombre de red.
`passwd.adjunct.byname`	`passwd` y `shadow`	Contiene información de auditoría y la información de contraseña oculta para clientes C2.
`passwd.byname`	`passwd` y `shadow`	Contiene información de contraseña con nombre de usuario como clave.
`passwd.byuid`	`passwd` y `shadow`	Es lo mismo que `passwd.byname`, excepto que la clave es el ID de usuario.
`prof_attr`	`prof_attr`	Contiene los atributos para la ejecución de perfiles.
`protocols.byname`	`protocols`	Contiene los protocolos de red conocidos para la red.
`protocols.bynumber`	`protocols`	Es lo mismo que `protocolos.byname`, excepto que la clave es el número de protocolo.
`rpc.bynumber`	`rpc`	Contiene el número del programa y el nombre de RPC conocidos en el sistema. La clave es el número RPC de programa.
`services.byname`	`services`	Muestra los servicios de Internet conocidos para la red. La clave es el puerto o el protocolo.
`services.byservice`	`services`	Muestra los servicios de Internet conocidos para la red. La clave es nombre de servicio.
`user_attr`	`user_attr`	Contiene los atributos ampliados para usuarios y roles.
`ypservers`	N/A	Muestra los servidores NIS conocidos por la red.

El mapa `ageing.byname` contiene la información que utiliza el daemon `yppasswdd` para leer y escribir información sobre la caducidad de la contraseña en el árbol de información de directorios (DIT) cuando se implementa la transición de NIS a LDAP. Si no se utiliza la fecha de la contraseña, puede quitarse el comentario del archivo de asignación. Para obtener más información sobre la transición de NIS a LDAP, consulte el Capítulo 15, “Transición de NIS a LDAP (tareas)”.

Uso de mapas de datos NIS

NIS hace que las actualizaciones de bases de datos de red sean mucho más sencillas que con el sistema de archivos `/etc`. Ya no tiene que cambiar los archivos administrativos `/etc` en cada máquina cada vez que modifica el entorno de red.

Sin embargo, NIS no proporciona ninguna seguridad adicional que la que proporcionan los archivos `/etc`. Si se requiere seguridad adicional, como restringir el acceso a las bases de datos de red, enviar los resultados de las búsquedas por la red mediante SSL o usar funciones más avanzadas, como, por ejemplo, búsquedas protegidas por Kerberos, los servicios de nombres LDAP se deben usar en su lugar.

Por ejemplo, cuando se agrega un nuevo usuario a una red en la que se ejecuta NIS, sólo tiene que actualizar el archivo de entrada en el servidor maestro y ejecutar el comando `make`. Este comando actualiza automáticamente los mapas `passwd.byname` y `passwd.byuid`. Estos mapas se transfieren a los servidores esclavos y se vuelven disponibles para todas las máquinas cliente del dominio y sus programas. Cuando una aplicación o máquina cliente solicita información utilizando el nombre de usuario o el UID, el servidor NIS consulta el mapa `passwd.byname` o `passwd.byuid`, según corresponda, y envía la información solicitada al cliente.

Puede utilizar el comando `ypcat` para visualizar los valores en un mapa. El formato básico de `ypcat` es el siguiente.

```
% ypcat mapname
```

Donde *mapname* es el nombre del mapa que desea examinar o su *apodo*. Si un mapa se compone únicamente de claves, como en el caso de `ypservers`, utilice `ypcat -k`. De lo contrario, `ypcat` imprime líneas en blanco. En la página del comando man `ypcat(1)`, se describen más opciones para `ypcat`.

Puede usar el comando `ypwhich` para determinar qué servidor es el servidor maestro de un mapa particular. Escriba lo siguiente.

```
% ypwhich -m mapname
```

Donde *mapname* es el nombre o el apodo del mapa cuyo maestro que desea buscar. `ypwhich` responde mostrando el nombre del servidor maestro. Para obtener más información, consulte la página del comando man `ypwhich(1)`.

Apodos de mapas de datos NIS

Los *apodos* son alias para los nombres completos de mapas. Para obtener una lista de apodos de mapas disponibles, como `passwd` para `passwd.byname` tipo `ypcat -x` o `ypwhich -x`.

Los apodos se almacenan en el archivo `/var/yp/nicknames`, que contiene el apodo de un mapa seguido del nombre especificado completo para el mapa, separado por un espacio. Esta lista se puede modificar o se le pueden agregar elementos. Actualmente, hay un límite de 500 apodos.

Enlace NIS

Los clientes NIS se conectan a un servidor NIS mediante el proceso de enlace. Este proceso es compatible con los servicios `svc:/network/nis/client` y `svc:/network/nis/domain`. Estos servicios deben estar activados para que cualquier servicio NIS funcione. El servicio `svc:/network/nis/client` puede funcionar en uno de estos dos modos: lista de servidores o difusión.

- Lista de servidores: en el modo de lista de servidores, el proceso `ypbind` consulta al servicio `svc:/network/nis/domain` los nombres de todos los servidores NIS del dominio. El proceso `ypbind` se vincula sólo con servidores en este archivo.

  Se pueden agregar servidores NIS mediante el comando `svccfg`. Se agregan a la propiedad `config/ypservers` en el servicio `svc:/network/nis/domain`. Cada valor de propiedad representa un servidor NIS determinado.

  Además, cualquier nombre de servidor que se especifica en el servicio `svc:/network/nis/domain` debe contener una entrada en el archivo `/etc/inet/hosts` para que el enlace NIS funcione.
- Difusión: el proceso `ypbind` también puede usar una difusión RPC para iniciar un enlace. Debido a que las difusiones son sólo eventos de la subred local que no se enrutan más allá, debe haber, al menos, un servidor (maestro o esclavo) en la misma subred que el cliente. Los servidores pueden existir en diferentes subredes, ya que la propagación de los mapas funciona a través de los límites de la subred. En un entorno de subred, un método más común es hacer que el enrutador de subred sea un servidor NIS. Esto permite al servidor de dominio servir a los clientes de cualquier interfaz de subred.

  El modo de difusión es, por lo general, el modo de operación recomendado. El modo de difusión no requiere que se especifiquen entradas de host adicionales (o que se realicen cambios en `/etc/inet/hosts`).

Normalmente, una vez que un cliente se enlaza a un servidor, permanece enlazado a ese servidor hasta que sucede algo que lo hace cambiar. Por ejemplo, si un servidor queda fuera de servicio, los clientes a los que servía se vincularán a nuevos servidores.

Para determinar qué servidor NIS está actualmente proporcionando servicio a un cliente específico, utilice el siguiente comando.

```
% ypwhich machinename
```

Donde *machinename* es el nombre del cliente. Si no se menciona ningún nombre de máquina, el comando `ypwhich` lo define de manera predeterminada como la máquina local (es decir, la máquina en la que se ejecuta el comando).

Modo de lista de servidores

El proceso de vinculación en el modo de servidor-lista funciona de la siguiente manera:

1. Cualquier programa que se ejecuta en la máquina cliente NIS y que necesita información proporcionada por un mapa de datos NIS, le pregunta a `ypbind` el nombre de un servidor.
2. El daemon `ypbind` busca en el archivo `/var/yp/binding/`*domainname*`/ypservers` una lista de servidores NIS para el dominio.
3. El daemon `ypbind` inicia el enlace con el primer servidor de la lista. Si el servidor no responde, `ypbind` intenta con el segundo, y así sucesivamente hasta que encuentra un servidor o agota la lista.
4. El daemon `ypbind` indica al proceso del cliente con qué servidor comunicarse. Luego el cliente envía la solicitud directamente al servidor.
5. El daemon `ypserv` en el servidor NIS maneja la solicitud consultando el mapa correspondiente.
6. El daemon `ypserv` envía la información solicitada de vuelta al cliente.

Modo de difusión

El proceso de vinculación de modo de emisión funciona de la siguiente manera:

1. El daemon `ypbind` se debe iniciar con la opción de difusión establecida (`broadcast`).
2. El daemon `ypbind` emite una difusión de RPC en busca de un servidor NIS.

Nota – Para poder admitir esos clientes, es necesario tener un servidor NIS de cada subred que requiera servicio NIS.

---

3. El daemon `ypbind` inicia el enlace con el primer servidor que responde a la difusión.
4. El daemon `ypbind` indica al proceso del cliente con qué servidor comunicarse. Luego el cliente envía la solicitud directamente al servidor.
5. El daemon `ypserv` en el servidor NIS maneja la solicitud consultando el mapa correspondiente.
6. El daemon `ypserv` envía la información solicitada de vuelta al cliente.

◆ ◆ ◆ CAPÍTULO 6

Instalación y configuración del servicio NIS (tareas)

En este capítulo, se describen la instalación y la configuración iniciales del Servicio de información de la red (NIS).

Nota – En algunos contextos, los nombres de *equipo* se denominan nombres de *host* o nombres de *equipo*. Aquí se utiliza "máquina", pero algunos nombres de mapas de datos NIS o mensajes de pantalla podrían utilizar *host* o *máquina*.

En este capítulo, se tratan los siguientes temas:

Configuración del mapa de tareas de NIS

Tarea	Descripción	Para obtener instrucciones
Preparar archivos de origen para la conversión.	Permite eliminar los archivos `/etc` locales antes de crear los mapas de datos NIS a partir de ellos.	"Cómo preparar los archivos de origen para la conversión" en la página 82
Configurar el servidor maestro.	Permite crear un servidor maestro, que es el origen primario de la información NIS.	"Cómo configurar el servidor maestro" en la página 85

Tarea	Descripción	Para obtener instrucciones
Iniciar NIS en el servidor maestro.	Permite iniciar proporcionando información NIS desde un servidor NIS.	"Inicio y detención de servicios NIS en un servidor NIS" en la página 87
Configurar servidores esclavos.	Permite crear un servidor esclavo, que es un origen secundario de información NIS.	"Cómo configurar un servidor esclavo" en la página 90
Configurar un cliente NIS.	Permite a los clientes utilizar información NIS.	"Administración de clientes NIS" en la página 93

Antes de empezar a configurar NIS

Antes de configurar su espacio de nombres NIS, debe realizar lo siguiente.

- Planifique su dominio NIS. Consulte "Planificación del dominio NIS" en la página 80 para obtener más información.
- Instale información sobre el conmutador de servicio de nombres correctamente configurada en todas las máquinas que usarán NIS. Consulte Capítulo 2, "Conmutador de servicio de nombres (descripción general)" para obtener más información.

NIS y la utilidad de gestión de servicios

El servicio NIS es gestionado por la utilidad de gestión de servicios. Para obtener una descripción general de la SMF, consulte el Capítulo 1, "Gestión de servicios (descripción general)" de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M) y `svcs`(1) para obtener más información.

En la siguiente lista, se ofrece una breve descripción general de la información importante necesaria para utilizar el servicio SMF con el fin de administrar NIS.

- Las acciones administrativas de este servicio, como la activación, la desactivación o el reinicio, pueden realizarse con el comando `svcadm`. Sin embargo, `ypstart` e `ypstop` también se pueden utilizar desde la línea de comandos para iniciar o detener NIS. Consulte las páginas del comando man `ypstart`(1M) y `ypstop`(1M) para obtener más información.

  Consejo – La desactivación temporal de un servicio mediante la opción `-t` proporciona protección para la configuración del servicio. Si el servicio se desactiva con la opción `-t`, los valores originales se restaurarán para el servicio tras un reinicio. Si el servicio se desactiva sin `-t`, permanecerá desactivado después de reiniciar.

- Los identificadores de recursos de gestión de errores (FMRI) NIS son los siguientes:
  - `svc:/network/nis/server` para el servidor NIS.

- `svc:/network/nis/client` para el cliente NIS.
- `svc:/network/nis/domain` para el nombre de dominio.

- Puede consultar el estado del servicio NIS con el comando `svcs`.
  - A continuación, se muestran ejemplos del comando `svcs` y su salida:

```
$ svcs network/nis/server
STATE        STIME    FMRI
online       Jan_10   svc:/network/nis/server:default
```

```
$ svcs \*nis\*
STATE          STIME    FMRI
online         Oct_09   svc:/network/nis/domain:default
online         Oct_09   svc:/network/nis/client:default
```

  - A continuación, se muestra un ejemplo del comando `svcs -l` y su salida:

```
$ svcs -l /network/nis/client
fmri         svc:/network/nis/client:default
name         NIS (YP) client
enabled      true
state        online
next_state   none
state_time   Tue Aug 23 19:23:28 2011
logfile      /var/svc/log/network-nis-client:default.log
restarter    svc:/system/svc/restarter:default
contract_id  88
manifest     /lib/svc/manifest/network/nis/client.xml
manifest     /lib/svc/manifest/network/network-location.xml
manifest     /lib/svc/manifest/system/name-service/upgrade.xml
manifest     /lib/svc/manifest/milestone/config.xml
dependency   require_all/none svc:/system/filesystem/minimal (online)
dependency   require_all/restart svc:/network/rpc/bind (online)
dependency   require_all/restart svc:/network/nis/domain (online)
dependency   optional_all/none svc:/network/nis/server (absent)
dependency   optional_all/none svc:/network/location:default (online)
dependency   optional_all/none svc:/system/name-service/upgrade (online)
dependency   optional_all/none svc:/milestone/config (online)
dependency   optional_all/none svc:/system/manifest-import (online)
dependency   require_all/none svc:/milestone/unconfig (online)
```

  - Puede usar la utilidad `svccfg` para obtener información más detallada sobre un servicio. Consulte la página del comando man `svccfg(1M)`.

  - Puede comprobar la presencia de un daemon mediante el comando `ps`.

```
$ ps -ef |grep ypbind
daemon 100813   1   0   Aug 23 ?     0:00 /usr/lib/netsvc/yp/ypbind -broadcast
```

Planificación del dominio NIS

Antes de configurar los equipos como servidores o clientes NIS, debe planificar el dominio de NIS.

Decida qué equipos estarán en el dominio NIS. Un dominio NIS no tiene que reflejar su dominio DNS. Un dominio DNS puede tener más de un dominio NIS, y su dominio DNS puede tener máquinas que están fuera del dominio NIS.

Un nombre de dominio NIS puede tener 256 caracteres. Una buena práctica es limitar los nombres de dominio a no más de 32 caracteres. Los nombres de dominio NIS distinguen entre mayúsculas y minúsculas. Para mayor comodidad, puede elegir su nombre de dominio de Internet como base para el nombre de dominio NIS. Tenga en cuenta que los usuarios pueden confundirse si el nombre de dominio NIS incluye mayúsculas, pero el nombre de dominio DNS no. Por ejemplo, si su nombre de dominio de Internet es `example.com`, también puede nombrar el dominio NIS `example.com`. Si desea dividir `example.com` en dos dominios NIS, por ejemplo, uno para el departamento de ventas y otro para el departamento de fabricación, puede nombrar un dominio `sales.example.com` y el otro dominio `manf.example.com`.

Nota – La combinación y la administración de dominios NIS divididos puede ser una tarea muy difícil, por lo que debe asegurarse de que hay un buen motivo para dividir un dominio NIS.

Para que una máquina pueda usar servicios NIS, se deben configurar el nombre de dominio NIS y el nombre de máquina correctos. El nombre de una máquina se define con el comando `hostname`. El nombre de dominio de una máquina se define con el comando `domainname`. Los comandos `hostname` y `domainname` se pueden usar para mostrar el nombre de la máquina y el nombre de dominio NIS.

Identificación de los servidores y clientes NIS

Seleccione un equipo para que sea el servidor maestro. Decida qué máquinas serán servidores esclavos.

Decida qué equipos serán clientes NIS. Normalmente, todas las máquinas del dominio NIS se configuran para que sean clientes NIS, aunque esto no es necesario.

Preparación del servidor maestro

En las siguientes secciones se describe cómo preparar los archivos de origen y los archivos `passwd` para el servidor maestro.

Directorio de archivos de origen

Los archivos de origen están normalmente en el directorio `/etc` del servidor maestro. Sin embargo, no se recomienda dejarlos en `/etc` porque el contenido de los mapas es el mismo que el contenido de los archivos locales en el servidor maestro. Se trata de un problema especial para los archivos `passwd` y `shadow`, ya que todos los usuarios tienen acceso a los mapas del servidor maestro y la contraseña `root` se pasaría a todos los clientes NIS mediante el mapa `passwd`. Consulte "Seguridad de espacio de nombres y archivos `passwd`" en la página 81 para obtener más información.

Sin embargo, si coloca los archivos de origen en otro directorio, debe modificar `Makefile` en `/var/yp` cambiando la línea `DIR=/etc` a `DIR=/`*su elección* donde *su elección* es el nombre del directorio que utilizará para almacenar los archivos de origen. Esto le permite tratar los archivos locales en el servidor como si fueran los de un cliente. Se recomienda guardar primero una copia del archivo `Makefile` original.

Además, los mapas de datos NIS `audit_user`, `auth_attr`, `exec_attr` y `prof_attr` se deben crear desde un directorio que no sea el predeterminado. Modifique `/var/yp/Makefile` cambiando `RBACDIR` =*/etc/security* a *RBACDIR=/your-choice*.

Seguridad de espacio de nombres y archivos `passwd`

Por motivos de seguridad, los archivos que se utilizan para crear los mapas de contraseña NIS no deben contener una entrada para `root`, a fin de impedir el acceso no autorizado a root. Por lo tanto, los mapas de contraseña no deben crearse a partir de archivos ubicados en el directorio `/etc` del servidor maestro. Los archivos de contraseña utilizados para crear los mapas de contraseña deben tener la entrada `root` eliminada y deben estar en un directorio que puede protegerse contra accesos no autorizados.

Por ejemplo, los archivos de entrada de contraseña del servidor maestro se deben almacenar en un directorio, como `/var/yp`, o cualquier directorio de su elección, siempre que el archivo en sí no sea un enlace a otro archivo y su ubicación sea especifíca en `Makefile`. La opción de directorio correcta se define automáticamente según la configuración especificada en `Makefile`.

Precaución – Asegúrese de que el archivo `passwd` en el directorio especificado por `PWDDIR` no contenga una entrada para `root`.

Si los archivos de origen se encuentran en un directorio diferente de `/etc`, debe modificar la macro de contraseña `PWDIR` en `/var/yp/Makefile` para hacer referencia al directorio en el que residen los archivos `passwd` y `shadow`. Cambie la línea `PWDIR=/etc` a `PWDIR=/` *your-choice*, donde *your-choice* es el nombre del directorio que utilizará para almacenar los archivos de origen de mapa `passwd`.

▼ Cómo preparar los archivos de origen para la conversión

En este procedimiento, se explica cómo preparar los archivos de origen para la conversión a mapas de datos NIS.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Compruebe los archivos de origen en el servidor maestro para asegurarse de que reflejen su sistema.

Revise los siguientes archivos:

- `audit_user`
- `auth_attr`
- `auto.home` o `auto_home`
- `auto.master` o `auto_master`
- `bootparams`
- `ethers`
- `exec_attr`
- `group`
- `hosts`
- `ipnodes`
- `netgroup`
- `netmasks`
- `networks`
- `passwd`
- `protocols`
- `rpc`
- `service`
- `shadow`
- `user_attr`

3 Copie todos estos archivos de origen, excepto `passwd` y `shadow`, en el directorio de origen que seleccione.

El directorio de origen es definido en `/var/yp/Makefile` por la macro `DIR`.

4 **Copie los archivos `passwd` y `shadow` en el directorio de origen de contraseña que ha seleccionado.**

El directorio de origen de contraseña es definido en Makefile por la macro `PWDIR`.

5 **Copie los archivos `audit_user`, `auth_attr`, `exec_attr` y `prof_attr` en el directorio de origen RBAC que ha seleccionado.**

El directorio de origen RBAC es definido en `/var/yp/Makefile` por la macro `RBACDIR`. Si lo desea, puede fusionar el contenido de los archivos en el directorio `/etc/security/auth_attr.d` en una copia del archivo `auth_attr` antes de copiarlo. Del mismo modo, puede combinar los archivos en los directorios `exec_attr.d` y `prof_attr.d` con `exec_attr` y `prof_attr` si lo desea.

Precaución – Debido a que será necesario volver a fusionar estos archivos cada vez que el sistema se actualice, mantenga los archivos locales separados de los archivos de la versión en los directorios `/etc/security/*.d`.

6 **Compruebe el archivo `/etc/mail/aliases`.**

A diferencia de otros archivos de origen, el archivo `/etc/mail/aliases` no se puede mover a otro directorio. Este archivo debe residir en el directorio `/etc/mail`. Consulte la página del comando man `aliases(4)` para obtener más información.

Nota – Puede agregar un archivo de alias de correo específico de NIS. Para ello, coloque la entrada `ALIASES = /etc/mail/aliases` en `/var/yp/Makefile` en otra ubicación. Cuando ejecuta el comando `make`, la entrada `ALIASES` crea un mapa `mail.aliases`. El servicio `sendmail` utiliza este mapa además del archivo `/etc/mail/alias` cuando el archivo `/etc/nsswitch.conf` tiene como objetivo `nis` además de `files`. Consulte "Modificación y uso de `/var/yp/Makefile`" en la página 104.

7 **Elimine todos los comentarios y otras líneas extrañas y la información de los archivos de origen.**

Estas operaciones se pueden realizar mediante una secuencia de comandos `sed` o `awk`, o con un editor de texto. `/var/yp/Makefile` realiza algunas limpiezas de archivos automáticamente, pero se recomienda examinar y limpiar manualmente estos archivos antes de ejecutar el comando `make`.

8 **Asegúrese de que los datos de todos los archivos de origen estén en el formato correcto.**

Los datos del archivo de origen deben estar en el formato correcto para ese archivo en particular. Revise las páginas del comando man de los distintos archivos para asegurarse de que cada archivo se encuentre en el formato correcto.

Preparación de /var/yp/Makefile

Después de comprobar los archivos de origen y copiarlos en el directorio de archivos de origen, debe convertir esos archivos de origen en los mapas de formato ndbm que usa el servicio NIS. Esta operación es realizada de forma automática para cada usuario por ypinit al llamarlo en el servidor maestro, como se explica en "Cómo configurar el servidor maestro" en la página 85.

La secuencia de comandos ypinit llama al programa make, que usa /var/yp/Makefile. Una copia predeterminada del archivo se proporciona en el directorio /var/yp y contiene los comandos necesarios para transformar los archivos de origen en los mapas de formato ndbm deseados.

Puede utilizar el archivo Makefile predeterminado tal cual o modificarlo. Si modifica el archivo Makefile predeterminado, primero asegúrese de copiar y almacenar el archivo Makefile predeterminado original en caso de necesitarlo en otra ocasión. Es posible que necesite realizar una o más de las siguientes modificaciones en Makefile:

- *Mapas no predeterminados*

  Si ha creado sus propios archivos de origen no predeterminados y desea convertirlos en mapas de datos NIS, debe agregar esos archivos de origen en Makefile.

- *Valor de* DIR

  Si desea que Makefile para utilizar los archivos de origen almacenados en algún directorio que no sea /etc, como se explica en "Directorio de archivos de origen" en la página 81, debe cambiar el valor de DIR en Makefile al directorio que desea utilizar. Cuando modifique este valor en Makefile, no deje sangría en la línea.

- *Valor de* PWDIR

  Si desea que Makefile utilice los archivos de origen passwd, shadow y adjunct que están almacenados en un directorio que no sea /etc, debe cambiar el valor de PWDIR en el Makefile al directorio que desea utilizar. Cuando modifique este valor en Makefile, no deje sangría en la línea.

- *Valor de* RBACDIR

  Si desea que Makefile utilice los archivos de origen audit_user, auth_attr, exec_attr y prof_attr que se almacenan en un directorio que no sea /etc, debe cambiar el valor de RBACDIR en Makefile al directorio que desea utilizar. Cuando modifique este valor en Makefile, no deje sangría en la línea.

- *Solucionador de nombre de dominio*

  Si desea que el servidor NIS utilice el solucionador de nombres de dominio para las máquinas que no están en el dominio actual, comente la línea B= del archivo Makefile y quite el comentario (active) de la línea B=-b.

La función de `Makefile` es crear los mapas de datos NIS adecuados para cada una de las bases de datos mostradas en `all`. Después de pasar por `makedbm`, los datos se recopilan en dos archivos, `mapname.dir` y `mapname.pag`. Ambos archivos están en el directorio `/var/yp/`*domainname* del servidor maestro.

El archivo `Makefile` crea mapas `passwd` a partir de los archivos `/PWDIR/passwd`, `/PWDIR/shadow` y `/PWDIR/security/passwd.adjunct`, según corresponde.

Cómo instalar el paquete de servidor maestro NIS

Por lo general, el paquete de servidor maestro NIS se instala cuando corresponde con la versión de Oracle Solaris. Si el paquete no se incluye cuando se instala el sistema, utilice el procedimiento siguiente para instalar el paquete.

1. **Conviértase en administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Instale el paquete de servidor maestro NIS.**

   ```
   # pkg install pkg:/service/network/nis
   ```

Cómo configurar el servidor maestro

La secuencia de comandos `ypinit` configura el servidor maestro, los servidores esclavos y los clientes para que utilicen NIS. También inicialmente ejecuta el comando `make` para crear los mapas en el servidor maestro.

Para utilizar el comando `ypinit` con el fin de crear un nuevo conjunto de mapas de datos NIS en el servidor maestro, lleve a cabo el siguiente procedimiento.

1. **Conviértase en administrador en el servidor maestro NIS.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Edite el archivo `/etc/inet/hosts`.**

   Agregue el nombre de host y la dirección IP de cada servidor NIS. Use el siguiente formato: *IPaddress FQDN-hostname aliases*.

   Por ejemplo:

   ```
   129.0.0.1    master.example.com master
   129.0.0.2    slave1.example.com slave1
   129.0.0.3    slave2.example.com slave2
   ```

3 Cree nuevos mapas en el servidor maestro.

```
# /usr/sbin/ypinit -m
```

4 Escriba los nombres de los servidores NIS.

Cuando `ypinit` solicita una lista de otras máquinas para convertirlos en servidores esclavos NIS, escriba el nombre del servidor en el que está trabajando, junto con los nombres de los servidores esclavos NIS especificados en el archivo `/etc/inet/hosts`.

5 Verifique que el nombre de dominio NIS esté definido.

```
# domainname
example.com
```

6 Escriba y para que se detenga el proceso si se produce un error no fatal.

Cuando `ypinit` pregunta si se desea que el procedimiento termine ante el primer error no fatal o que continúe a pesar de los errores no fatales, escriba **y**. Cuando selecciona **y**, `ypinit` se cierra al encontrar el primer problema. Puede solucionar el problema y reiniciar `ypinit`. Esto se recomienda si está ejecutando `ypinit` por primera vez. Si prefiere continuar, puede intentar corregir manualmente todos los problemas que se producen y, luego, reiniciar `ypinit`.

Nota – Un error no fatal se puede producir cuando alguno de los archivos de mapa no están presentes. Esto no es un error que afecta la funcionalidad de NIS. Es posible que necesite agregar mapas manualmente si no se han creado de forma automática. Consulte "Mapas de datos NIS predeterminados" en la página 71 para obtener una descripción de todos los mapas NIS predeterminados.

---

7 Elija si los archivos de origen se deben suprimir.

El comando `ypinit` pregunta si los archivos existentes en el directorio `/var/yp/`*domain-name* se pueden destruir. Este mensaje sólo se muestra si NIS se ha instalado previamente. Normalmente se elige suprimir los archivos de origen si se desea eliminar los archivos de una instalación anterior.

8 Una vez que el comando `ypinit` crea la lista de servidores, invoca el comando `make`.

Este programa utiliza las instrucciones que se incluyen en `Makefile` (ya sea el archivo predeterminado o el archivo modificado) ubicado en `/var/yp`. El comando `make` elimina el resto de las líneas con comentario de los archivos que usted ha indicado. También funciona con `makedbm` en los archivos, creando los mapas correspondientes y estableciendo el nombre del servidor maestro para cada mapa.

Si los mapas transferidos por `Makefile` corresponden a un dominio que no es el devuelto por el comando `domainname` en el servidor maestro, puede asegurarse de que sean transferidos al dominio correcto iniciando `make` en la secuencia de comandos de shell `ypinit` con una identificación adecuada de la variable `DOM`, como aparece a continuación:

```
# make DOM=domain-name  passwd
```

Este comando transfiere el mapa `passwd` al dominio deseado, en lugar del dominio al que pertenece el maestro.

9 **Si es necesario, realice cambios en el conmutador de servicio de nombres.**

Consulte "Gestión del conmutador de servicio de nombres" en la página 39.

▼ Cómo admitir varios dominios NIS en un servidor maestro

Por lo general, un servidor maestro NIS sólo admite un dominio NIS. Sin embargo, si utiliza un servidor maestro para admitir varios dominios, debe modificar levemente los pasos, como se describe en "Cómo configurar el servidor maestro" en la página 85, al configurar el servidor para atender los dominios adicionales.

1 **Conviértase en administrador en el servidor maestro NIS.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Cambie el nombre de dominio NIS.**

```
# domainname sales.example.com
```

3 **Cree los archivos NIS.**

```
# make DOM=sales.example.com
```

Inicio y detención de servicios NIS en un servidor NIS

Ahora que ya están creados los mapas en los servidores maestros, puede iniciar los daemons NIS en el servidor maestro y comenzar el servicio. Al activar el servicio NIS, los daemons `ypserv` y `ypbind` se inician en el servidor. Cuando un cliente solicita información al servidor, `ypserv` es el daemon que responde a las solicitudes de información de clientes después de buscarlos en los mapas de datos NIS. Los daemons `ypserv` y `ypbind` son administrados como una unidad.

A continuación, se muestran los tres métodos mediante los que el servicio NIS se puede iniciar o detener en un servidor:

- El servicio SMF inicia automáticamente el servicio NIS durante el proceso de inicio si el servicio NIS se activó con anterioridad.
- El uso de los comandos `svcadm enable` *fmri* y `svcadm disable` *fmri* es el método manual preferido.

- Los comandos `ypstart` y `ypstop` proporcionan otro método manual, aunque el comando `svcadm` es el preferido para que usted pueda utilizar SMF con el fin de administrar el servicio NIS.

Inicio automático del servicio NIS

Cuando el servicio `svc:/network/nis/server` se activa, el daemon `ypserv` se inicia automáticamente en el inicio. Consulte "Cómo configurar el servidor maestro" en la página 85 para obtener más información.

▼ Cómo activar los servicios del servidor NIS manualmente

Cuando se utiliza el comando `svcadm`, el nombre de instancia sólo es necesario si está ejecutando más de una instancia del servicio. Para obtener más información, consulte "NIS y la utilidad de gestión de servicios" en la página 78 o la página del comando man `svcadm`(1M).

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Inicie los servicios necesarios del servidor NIS.

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/server
```

Nota – El servicio NIS también se puede activar utilizando el comando `ypstart`, aunque se prefiere el comando `svcadm`.

▼ Cómo desactivar los servicios del servidor NIS

Cuando se utiliza el comando `svcadm`, un nombre de instancia específico sólo es necesario si está ejecutando más de una instancia del servicio. Para obtener más información, consulte "NIS y la utilidad de gestión de servicios" en la página 78 o la página del comando man `svcadm`(1M).

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Desactive los servicios necesarios del servidor NIS.

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/server
```

Nota – El servicio NIS también se puede desactivar con el comando `ypstop`.

▼ Cómo refrescar el servicio del servidor NIS

En este procedimiento, se explica cómo refrescar los servicios del servidor NIS tras un cambio de configuración realizado.

Cuando se utiliza el comando `svcadm`, un nombre de instancia específico sólo es necesario si está ejecutando más de una instancia del servicio. Para obtener más información, consulte "NIS y la utilidad de gestión de servicios" en la página 78 o la página del comando man `svcadm`(1M).

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Refresque los servicios necesarios del servidor NIS.**

```
# svcadm refresh network/nis/domain
# svcadm refresh network/nis/server
```

Configuración de servidores NIS esclavos

Su red puede tener uno o más servidores esclavos. Tener servidores esclavos garantiza la continuidad de los servicios NIS cuando el servidor maestro no está disponible.

Preparación de un servidor esclavo

Antes de ejecutar el comando `ypinit` para crear los servidores esclavos, primero asegúrese de que el servicio `svc:/network/nis/domain` se haya configurado.

Nota – Los nombres de dominio NIS distinguen entre mayúsculas y minúsculas, aunque los nombres de dominio DNS no.

Asegúrese de que la red funcione correctamente antes de configurar un servidor esclavo NIS. En concreto, asegúrese de que pueda utilizar el comando `sshd` para enviar archivos desde el servidor maestro NIS hasta los servidores esclavos NIS.

▼ Cómo configurar un servidor esclavo

En el siguiente procedimiento, se explica cómo configurar un servidor esclavo. Repita este procedimiento para cada máquina que desea configurar como servidor esclavo NIS.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Edite el archivo `/etc/inet/hosts`.

Agregue el nombre y la dirección IP de cada uno de los demás servidores NIS. Use el siguiente formato: *IPaddress FQDN-hostname aliases*.

Por ejemplo:

```
129.0.0.1    master.example.com master
129.0.0.2    slave1.example.com slave1
129.0.0.3    slave2.example.com slave2
```

3 Cambie el directorio a `/var/yp` en el servidor esclavo.

Nota – Primero debe configurar el nuevo servidor esclavo como cliente NIS para que pueda obtener los mapas de datos NIS del servidor maestro por primera vez. Consulte "Administración de clientes NIS" en la página 93 para obtener más información.

---

4 Inicialice el servidor esclavo como cliente NIS.

```
# /usr/sbin/ypinit -c
```

El comando `ypinit` comando le solicita una lista de servidores NIS. Primero escriba el nombre del servidor esclavo local en el que está trabajando y, a continuación, escriba el nombre del servidor maestro, seguido por los nombres de los demás servidores esclavos NIS en el dominio. Para los demás servidores esclavos, siga el orden del más próximo físicamente al más lejano en términos de red.

5 Determine si se están ejecutando los servicios de clientes y, a continuación, inicie o reinicie los servicios según sea necesario.

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
online         20:32:56  svc:/network/nis/client:default
```

Si los servicios se muestran con el estado `online` (en línea), NIS se está ejecutando. Si el estado del servicio es `disabled` (desactivado), NIS no se está ejecutando.

a. Si los servicios de clientes se están ejecutando, reinícielos.

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. Si los servicios de clientes no se están ejecutando, inícielos.

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

6 Determine si el servidor maestro NIS se está ejecutando y, a continuación, inicie o reinicie el servicio según sea necesario.

```
# svcs network/nis/server
STATE          STIME     FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. Si el servidor maestro NIS se está ejecutando, reinicie el servicio.

```
# svcadm restart network/nis/server
```

b. Si el servidor maestro NIS no se está ejecutando, inicie el servicio.

```
# svcadm enable network/nis/server
```

7 Inicialice esta máquina como servidor esclavo.

```
# /usr/sbin/ypinit -s master
```

Donde *master* es el nombre de la máquina del servidor maestro NIS existente.

▼ Cómo iniciar NIS en un servidor esclavo

En el siguiente procedimiento, se explica cómo iniciar NIS en un servidor esclavo.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Reinicie el servicio de cliente e inicie todos los procesos del servidor NIS.

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
# svcadm enable network/nis/server
```

▼ Cómo agregar un nuevo servidor esclavo

Una vez que NIS se está ejecutando, es posible que tenga que crear un servidor esclavo NIS que no se haya incluido en la lista inicial proporcionada al comando `ypinit`. Utilice este procedimiento para agregar un nuevo servidor esclavo NIS.

1 Conviértase en administrador en el servidor maestro NIS.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Cambie al directorio de dominios NIS.

```
# cd /var/yp/domainname
```

3 Desensamble el archivo `ypservers`.

```
# makedbm -u ypservers >/tmp/temp_file
```

El comando `makedbm` convierte `ypservers` del formato `ndbm` a un archivo ASCII temporal `/tmp/temp_file`.

4 Edite el archivo `/tmp/temp_file`.

Agregue el nombre del nuevo servidor esclavo a la lista de servidores. A continuación, guarde y cierre el archivo.

5 Ejecute el comando `makedbm` con `temp_file` como el archivo de entrada e `ypservers` como el archivo de salida.

```
# makedbm /tmp/temp_file ypservers
```

El comando `makedbm` convierte `ypservers` nuevamente al formato `ndbm`.

6 Verifique que el mapa `ypservers` sea correcto.

Debido a que no hay ningún archivo ASCII para `ypservers`, escriba lo siguiente en el servidor esclavo:

```
slave3# makedbm -u ypservers
```

El comando `makedbm` muestra cada entrada en `ypservers` en la pantalla.

Nota – Si un nombre de equipo no está en `ypservers`, no recibirá las actualizaciones en los archivos de mapa porque `yppush` consulta este mapa para obtener la lista de servidores esclavos.

---

7 Conviértase en administrador en el nuevo servidor esclavo NIS.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

8 Verifique que el nombre de dominio NIS esté definido.

```
# domainname
example.com
```

9 Configure el nuevo directorio de dominio de servidor NIS esclavo.

Copie el conjunto de mapas de datos NIS del servidor maestro y, a continuación, inicie el cliente NIS. Al ejecutar el comando `ypinit`, siga los indicadores y enumere los servidores NIS en el orden de preferencia.

```
slave3# cd /var/yp
slave3# ypinit -c
```

10 Inicialice este equipo como esclavo.

```
slave3# /usr/sbin/ypinit -s ypmaster
```

Donde *ypmaster* es el nombre del equipo del servidor NIS maestro existente.

11 Detenga el equipo que se ejecuta como cliente NIS.

```
slave3# svcadm disable network/nis/client
```

12 Determine si se están ejecutando los servicios de clientes y, a continuación, inicie o reinicie los servicios según sea necesario.

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
online         20:32:56  svc:/network/nis/client:default
```

Si los servicios se muestran con el estado `online` (en línea), NIS se está ejecutando. Si el estado del servicio es `disabled` (desactivado), NIS no se está ejecutando.

a. Si los servicios de clientes se están ejecutando, reinícielos.

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. Si los servicios de clientes no se están ejecutando, inícielos.

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

13 Determine si el servidor NIS se está ejecutando y, a continuación, inicie o reinicie el servicio según sea necesario.

```
# svcs network/nis/server
STATE          STIME     FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. Si el servidor NIS se está ejecutando, reinicie el servicio.

```
slave3# svcadm restart network/nis/server
```

b. Si el servidor NIS no se está ejecutando, inicie el servicio.

```
slave3# svcadm enable network/nis/server
```

Administración de clientes NIS

En esta sección, se explican los dos métodos para configurar una máquina cliente con el fin de usar NIS como su servicio de nombres.

Nota – El sistema operativo Oracle Solaris no admite una configuración en la que un cliente NIS y un cliente LDAP nativo coexisten en la misma máquina cliente.

- **Modo de emisión**: método preferido para configurar una máquina cliente con el fin de usar NIS. Consulte "Cómo configurar un cliente NIS en modo de emisión" en la página 94 para obtener instrucciones.
- **Método de lista de servidores**: otro método para configurar una máquina cliente usando el comando `ypinit` con el fin de especificar los servidores. Consulte "Cómo configurar un cliente NIS usando servidores NIS específicos" en la página 94 para obtener instrucciones.

▼ Cómo configurar un cliente NIS en modo de emisión

Éste es el método preferido para establecer un cliente NIS.

Al iniciar el servicio `nis/client`, el servicio ejecuta el comando `ypbind`, que busca un servidor NIS en la subred local. Si se encuentra una subred, `ypbind` se enlaza a ella. Esta búsqueda se denomina *emisión*. Si no hay ningún servidor NIS en la subred local del cliente, `ypbind` no puede realizar el enlace y la máquina cliente no puede obtener datos de espacios de nombres del servicio NIS. Consulte "Cómo configurar un cliente NIS usando servidores NIS específicos" en la página 94 para obtener instrucciones.

1. **Conviértase en administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Establezca el nombre de dominio NIS.**

   ```
   # domainname example.com
   ```

3. **Si es necesario, realice cambios en el conmutador de servicio de nombres.**

   Consulte "Gestión del conmutador de servicio de nombres" en la página 39.

4. **Inicie los servicios de clientes NIS.**

   ```
   # svcadm enable network/nis/domain
   # svcadm enable network/nis/client
   ```

▼ Cómo configurar un cliente NIS usando servidores NIS específicos

Antes de empezar En el siguiente procedimiento, se requiere que los nombres de hosts que se introducen en el paso 3 puedan ser resueltos por el DNS. Si no utiliza un DNS o introduce un nombre de host en

lugar de una dirección IP, asegúrese de agregar una entrada apropiada para cada servidor NIS en el archivo `/etc/hosts` del cliente. Para obtener más información, consulte la página del comando man `ypinit(1M)`.

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Establezca el nombre de dominio NIS.**

```
# domainname example.com
# svcadm enable network/nis/domain
```

3 **Ejecute la secuencia de comandos de configuración de cliente.**

```
# ypinit -c
```

Se le solicita que nombre los servidores NIS desde donde el cliente obtiene la información del servicio de nombres. Puede enumerar el servidor maestro y todos los servidores esclavos que desee. Los servidores que enumera se pueden ubicar en cualquier lugar del dominio. Se recomienda primero enumerar los servidores más cercanos (con respecto a la red) a la máquina que los que están más distantes de la red.

▼ Desactivación de los servicios de clientes NIS

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Desactive los servicios de clientes NIS.**

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/client
```

◆ ◆ ◆ CAPÍTULO 7

Administración de NIS (tareas)

En este capítulo, se describe cómo administrar NIS. Contiene los temas siguientes:

Nota – El servicio NIS es gestionado por la utilidad de gestión de servicios. Las acciones administrativas de este servicio, como la activación, la desactivación o el reinicio, pueden realizarse con el comando `svcadm`. Consulte "NIS y la utilidad de gestión de servicios" en la página 78 para obtener más información sobre el uso de SMF con NIS. Para obtener una descripción general de la SMF, consulte el Capítulo 1, "Gestión de servicios (descripción general)" de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M) y `svcs`(1) para obtener más información.

Los servicios NIS también se pueden iniciar y detener utilizando los comandos `ypstart` y `ypstop`. Consulte las páginas del comando man `ypstart`(1M) y `ypstop`(1M) para obtener más información.

Archivos de contraseña y seguridad del espacio de nombres

Por motivos de seguridad, siga estas directrices.

- Es mejor limitar el acceso a los mapas NIS en el servidor maestro.
- Los archivos que se usan para crear los mapas de datos NIS de contraseñas no deben contener una entrada para `root` a fin de proteger el acceso no autorizado. Para lograrlo, los archivos de contraseña que se utilizan para crear los mapas de contraseñas no deben tener la entrada `root` y deben estar en un directorio diferente del directorio `/etc` del servidor maestro. Este directorio debe estar protegido contra accesos no autorizados.

Por ejemplo, los archivos de entrada de contraseña del servidor maestro se pueden almacenar en un directorio, como `/var/yp` o en cualquier directorio que desee, siempre que el archivo en sí no sea un enlace a otro archivo especificado en Makefile. Al usar la utilidad de gestión de servicios o la secuencia de comandos `ypstart` para iniciar el servicio NIS, la opción de directorio correcta se define según la configuración especificada en `Makefile`.

Nota – Además del formato de archivo `passwd` de la versión Solaris 1 más antigua, esta implementación de NIS acepta los formatos de archivos `passwd` y `shadow` de la versión Solaris 2 como entrada para crear los mapas de datos NIS de contraseñas.

Administración de usuarios NIS

En esta sección, se incluye información sobre la configuración de contraseñas de usuario, la agregación de nuevos usuarios a un dominio NIS y la asignación de usuarios a `netgroups`.

▼ Cómo agregar un nuevo usuario NIS a un dominio NIS

1 **Conviértase en administrador en el servidor maestro NIS.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Cree el nuevo ID de inicio de sesión del usuario con el comando `useradd`.**

```
# useradd userID
```

Donde *userID* es el ID de inicio de sesión del nuevo usuario. Este comando crea entradas en los archivos `/etc/passwd` y `/etc/shadow` en el servidor maestro NIS.

3 **Cree la nueva contraseña inicial del usuario.**

Para crear una contraseña inicial que el nuevo usuario puede usar para iniciar sesión, ejecute el comando `passwd`.

```
# passwd userID
```

Donde *userID* es el ID de inicio de sesión del nuevo usuario. Se le pedirá la contraseña para asignar a este usuario.

Este paso es necesario porque la entrada de la contraseña creada por el comando `useradd` está bloqueada, lo que significa que el nuevo usuario no puede iniciar sesión. Especificando una contraseña inicial, se desbloquea la entrada.

4 **Copie la nueva entrada en los archivos de entrada de mapa `passwd` del servidor maestro.**

Los archivos de origen de mapa del servidor maestro deben estar en un directorio distinto de `/etc`. Copie y pegue las nuevas líneas de los archivos `/etc/passwd` y `/etc/shadow` a los archivos

de entrada de mapa `passwd` en el servidor. Consulte "Archivos de contraseña y seguridad del espacio de nombres" en la página 97 para obtener información adicional.

Por ejemplo, si agregó el nuevo usuario `brown`, la línea de `/etc/passwd` que copiaría en el archivo de entrada `passwd` debería ser como la que se indica a continuación.

```
brown:x:123:10:User brown:/home/brown:/bin/csh:
```

La línea para `brown` que copiaría de `/etc/shadow` tendría que ser de la siguiente manera:

```
brown:$5$YiFpYWXb$6jJkG/gKdfkKtlTbemORnbeH.qsvO9MwBD3ulTihq9B:6445::::::
```

5 Asegúrese de que `Makefile` especifique correctamente el directorio en el que reside el archivo de entrada de contraseña.

6 Suprima las entradas del nuevo usuario de los archivos de entrada `/etc/passwd` y `/etc/shadow`.

Por motivos de seguridad, no guarde entradas de usuario en los archivos `/etc/passwd` y `/etc/shadow` del servidor maestro NIS Después de copiar las entradas para el nuevo usuario en los archivos de origen de mapa NIS que se almacenan en algún otro directorio, use el comando `userdel` del servidor maestro para suprimir el nuevo usuario.

Por ejemplo, para suprimir el nuevo usuario `brown` desde los archivos `/etc` del servidor maestro, debería introducir lo siguiente.

```
# userdel brown
```

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

7 Actualice los mapas de datos NIS `passwd`.

Después de actualizar el archivo de entrada `passwd` en el servidor maestro, actualice los mapas `passwd` ejecutando `make` en el directorio que contiene el archivo de origen.

```
# userdel brown
# cd /var/yp
# make passwd
```

8 Indique al nuevo usuario la contraseña inicial que le ha asignado o su ID de inicio de sesión.

Después de iniciar sesión, el nuevo usuario puede ejecutar `passwd` en cualquier momento para establecer una contraseña diferente.

Configuración de contraseñas de usuario

Los usuarios ejecutan `passwd` para cambiar sus contraseñas.

% **`passwd`** *username*

Para que los usuarios puedan cambiar sus contraseñas, debe iniciar el daemon `rpc.yppasswdd` en el servidor maestro para actualizar el archivo de contraseñas.

El daemon `rpc.yppasswdd` se inicia automáticamente en el servidor maestro. Tenga en cuenta que cuando la opción `-m` se proporciona para `rpc.yppasswdd`, el comando `make` se ejecuta en `/var/yp` inmediatamente después de una modificación del archivo. Si desea evitar que el comando `make` se ejecute cada vez que el archivo `passwd` se cambia, elimine la opción `-m` del comando `rpc.yppasswd` en la secuencia de comandos `ypstart` y controle la transferencia de los mapas `passwd` por medio del archivo `crontab`.

Grupos de red NIS

Los grupos de red NIS son grupos (conjuntos) de usuarios o equipos que usted define con fines administrativos. Por ejemplo, puede crear grupos de red que realicen las siguientes acciones.

- Definir un conjunto de usuarios que pueden acceder a una equipo específico.
- Definir un conjunto de equipos cliente NFS que obtengan acceso a algunos archivos de sistema específicos.
- Definir un conjunto de usuarios que vayan a tener privilegios de administrador en todos los equipos en un determinado dominio NIS.

A cada grupo de red se le asigna un nombre de grupo de red. Los grupos de red no establecen directamente permisos o derechos de acceso. En cambio, los nombres de grupo de red se usan en otros mapas NIS donde normalmente se utiliza un nombre de usuario o nombre de equipo. Por ejemplo, imagine que ha creado un grupo de red de los administradores de red denominado `netadmins`. Para otorgar a todos los miembros del grupo de red `netadmins` acceso a una máquina determinada, sólo tiene que agregar una entrada `netadmin` al archivo `/etc/passwd` de esa máquina. Los nombres del grupo de red pueden también agregarse al archivo `/etc/netgroup` y propagarse al mapa `netgroup` de NIS. Consulte la página del comando man `netgroup(4)` para obtener más información sobre el uso de grupos de red.

En una red que utiliza NIS, el archivo de entrada `netgroup` en el servidor maestro NIS se utiliza para generar tres mapas: `netgroup`, `netgroup.byuser` y `netgroup.byhost`. El mapa `netgroups` contiene la información básica en el archivo de entrada `netgroup`. Los otros dos mapas de datos NIS contienen información en un formato que acelera las consultas de información de grupo de red, por la máquina o el nombre de usuario.

Las entradas en el archivo de entrada `netgroup` tienen el siguiente formato: *name ID*, donde *name* es el nombre que se proporciona a un grupo de red y *ID* identifica una máquina o un usuario que pertenece al grupo de red. Puede especificar tantos ID (miembros) a un grupo de red como desee, separados por comas. Por ejemplo, para crear un grupo de red con tres miembros, la entrada del archivo de entrada `netgroup` estaría en el siguiente formato: *name ID*, *ID*, *ID*. Los ID de los miembros en la entrada de un archivo de entrada `netgroup` tienen el siguiente formato.

```
([-|machine], [-|user], [domain])
```

Donde *machine* es el nombre de máquina, *user* es el ID de usuario y *domain* es el dominio NIS de la máquina o el usuario. El elemento *dominio* es opcional y sólo se debe usar para identificar equipos o usuarios en otro dominio NIS. Se requieren los elementos *machine* y *user* de la entrada de cada miembro, pero se utiliza un guión (`-`) para denotar un valor nulo. No es necesaria ninguna relación entre los elementos equipo y usuario en una entrada.

Los siguientes son dos ejemplos de entradas de archivo de entrada `netgroup`, y cada uno crea un grupo de red denominado `admins` que está compuesto por los usuarios `hauri` y `juanita`, que están en el dominio remoto `sales` y las máquinas `altair` y `sirius`.

```
admins (altair, hauri), (sirius,juanita,sales)
admins (altair,-), (sirius,-), (-,hauri), (-,juanita,sales)
```

Algunos programas utilizan los mapas de datos NIS de grupo de red para la verificación de permisos durante el inicio de sesión, el montaje remoto, el inicio de sesión remoto y la creación de shell remoto. Estos programas incluyen `mountd` y `login`. El comando `login` consulta los mapas de grupo de red para ver las clasificaciones de usuario, si encuentra nombres de grupo de red en la base de datos `passwd`. El daemon `mountd` consulta los mapas de grupo de red para clasificaciones de máquinas si encuentra nombres de grupo de red en el archivo `/etc/dfs/dfstab`. De hecho, cualquier programa que utiliza la interfaz `ruserok` comprueba los mapas de grupo de red para clasificaciones de máquinas y usuarios si detecta nombres de grupo de red en el archivo `/etc/hosts.equiv` o `.rhosts`.

Si agrega un nuevo usuario o equipo NIS a la red, asegúrese de agregarlos a los grupos de red del archivo de entrada`netgroup`. A continuación, utilice los comandos `make` y `yppush` para crear mapas de grupo de red y enviarlos a todos los servidores NIS. Consulte la página del comando man `netgroup(4)` para obtener más información sobre el uso de grupos de red y la sintaxis del archivo de entrada de grupo de red.

Trabajo con mapas NIS

Esta sección contiene la siguiente información.

Obtención de información de mapa

Los usuarios pueden obtener información desde y sobre los mapas en cualquier momento utilizando los comandos `ypcat`, `ypwhich` y `ypmatch`. En los ejemplos que siguen, *mapname* se refiere al nombre oficial de un mapa y a su apodo (si tiene).

Para mostrar todos los valores de un mapa, escriba lo siguiente:

```
% ypcat mapname
```

Para mostrar las claves y los valores (si hay alguno) de un mapa, escriba lo siguiente:

```
% ypcat -k mapname
```

Para mostrar todos los apodos de mapas, escriba cualquiera de los siguientes comandos:

```
% ypcat -x
% ypmatch -x
% ypwhich -x
```

Para mostrar todos los mapas disponibles y sus servidores maestros, escriba lo siguiente:

```
% ypwhich -m
```

Para mostrar el servidor maestro de un mapa determinado, escriba lo siguiente:

```
% ypwhich -m mapname
```

Para que coincida una clave con una entrada en un mapa, escriba lo siguiente:

```
% ypmatch key mapname
```

Si el elemento que está buscando no es una clave en un mapa, escriba lo siguiente:

```
% ypcat mapname | grep item
```

Donde *artículo* es la información que está buscando. Para obtener información sobre otros dominios, utilice la opción `-d domainname` de estos comandos.

Si la máquina que solicita información para un dominio que no es el predeterminado no tiene un enlace para el dominio solicitado, `ypbind` consulta el archivo `/var/yp/binding/`*domainname*`/ypservers` para obtener una lista de servidores para ese dominio. Si este archivo no existe, emite una emisión RPC para un servidor. En este caso, debe haber un servidor para el dominio solicitado en la misma subred que el que equipo solicitante.

Cambio del servidor maestro de un mapa

Para cambiar el servidor maestro de un mapa seleccionado, primero tiene que crear el mapa en el nuevo servidor maestro NIS. Debido a que el nombre del servidor maestro antiguo se produce como par clave-valor en el mapa existente (este par es insertado automáticamente por `makedbm`), no es suficiente copiar el mapa en el nuevo servidor maestro o transferir una copia al nuevo servidor maestro con `ypxfr`. Tiene que volver a asociar la clave con el nuevo nombre de servidor maestro. Si el mapa tiene un archivo de origen ASCII, deberá copiar este archivo en el nuevo maestro.

▼ Cómo cambiar el servidor maestro de un mapa

1. **Conviértase en administrador en el servidor maestro NIS.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Cambie los directorios.**

   ```
   newmaster# cd /var/yp
   ```

3. **El archivo `/var/yp/Makefile` debe tener una entrada para el nuevo mapa antes de especificar el mapa que se va a realizar.**

   Si no es así, edite el archivo `Makefile` ahora. Para este ejemplo, agregue una entrada para un mapa llamado `sites.byname`.

4. **Para actualizar o volver a crear el mapa, escriba lo siguiente:**

   ```
   newmaster# make sites.byname
   ```

5. **Si el servidor maestro antiguo sigue siendo un servidor NIS, inicie sesión de manera remota (`ssh`) en el servidor maestro antiguo y edite `/var/yp/Makefile`.**

   Asegúrese de comentar la sección del `Makefile` que creó el mapa `sites.byname` para que ya no se cree allí.

6. **Si `sites.byname` sólo existe como un archivo `ndbm`, vuelva a crearlo en el nuevo servidor maestro.**

   En primer lugar, desmonte una copia del archivo `sites.byname` mediante el comando `ypcat`. Después ejecute la versión desmontada mediante `makedbm`.

   ```
   newmaster# cd /var/yp
   newmaster# ypcat sites.byname | makedbm domain/sites.byname
   ```

   Después de crear el mapa en el nuevo servidor maestro, debe enviar una copia del nuevo mapa a los demás servidores esclavos. No use `yppush`, porque los demás servidores esclavos intentarán obtener copias nuevas del servidor maestro antiguo, en lugar del nuevo. Un método típico para eludir esto es transferir una copia del mapa del nuevo maestro al maestro antiguo. Para ello, conviértase en superusuario o asuma un rol equivalente, en el servidor maestro y escriba lo siguiente.

   ```
   oldmaster# /usr/lib/netsvc/yp/ypxfr -h newmaster sites.byname
   ```

   Ahora es seguro ejecutar `yppush`. Los demás servidores esclavos todavía creen que el maestro antiguo es el maestro actual e intentarán obtener la versión actual del mapa del servidor maestro antiguo. Cuando los clientes hacen esto, obtienen un nuevo mapa, que da nombre al nuevo maestro como maestro actual.

   Si este método falla, puede iniciar sesión como usuario root en cada servidor NIS y ejecutar el comando `ypxfr` como se muestra a continuación.

Modificación de archivos de configuración

NIS analiza de forma inteligente los archivos de configuración. Aunque esto hace que la administración de NIS sea más fácil, también hace que el comportamiento de NIS sea más sensible a los cambios en la configuración y los archivos de configuración.

Utilice los procedimientos de esta sección cuando realice cualquiera de las siguientes opciones:

- `/var/yp/Makefile` para agregar o suprimir los mapas admitidos.
- Agregar o suprimir `$PWDIR/security/passwd.adjunct` para permitir o denegar la seguridad C2 (`$PWDIR` está definido en `/var/yp/Makefile`).

▼ Cómo modificar archivos de configuración

Tenga en cuenta lo siguiente.

- Al suprimir un mapa o archivo de origen de un servidor NIS maestro no se borran automáticamente los archivos correspondientes de los servidores esclavos. Debe suprimir mapas y archivos de origen de servidores esclavos a mano.
- Los nuevos mapas no se transfieren automáticamente a servidores esclavos existentes. Debe ejecutar `ypxfr` desde los servidores esclavos.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Detenga el servidor NIS.

```
# svcadm disable network/nis/server
```

3 Realice los cambios necesarios en los archivos.

4 Inicie el servidor NIS.

```
# svcadm enable network/nis/server
```

Modificación y uso de `/var/yp/Makefile`

Puede modificar `Makefile` que se proporcionan de manera predeterminada en `/var/yp` para que se ajuste a sus necesidades. Puede agregar o suprimir mapas, y puede cambiar los nombres de algunos de los directorios.

Consejo – Conserve una copia del original sin modificaciones de `Makefile` para futura referencia.

Trabajo con `Makefile`

Para agregar un nuevo mapa de datos NIS, debe obtener copias de los archivos `ndbm` para el mapa en el directorio `/var/yp/`*domainname* de cada uno de los servidores NIS del dominio. Esto normalmente lo realiza `Makefile` por usted. Después de decidir qué servidor NIS es el maestro del mapa, modifique `Makefile` en el servidor maestro para que pueda reconstruir el mapa adecuadamente. Distintos servidores pueden ser los maestros de diferentes mapas, pero en la mayoría de los casos, esto lleva a la confusión. Intente configurar un solo servidor como maestro de todos los mapas.

Normalmente un archivo de texto legible por el usuario se filtra a través de `awk`, `sed` o `grep` para que pueda realizar entradas en `makedbm`. Consulte el `Makefile` predeterminado, para obtener ejemplos. Consulte `make(1S)` para obtener información general sobre el comando `make`.

Utilice los mecanismos que ya tiene en `Makefile` al decidir cómo crear dependencias que `make` reconocerá. Tenga en cuenta que `make` es muy sensible a la presencia o ausencia de tabulaciones al principio de líneas dentro de las reglas de dependencia. Una tabulación faltante puede invalidar una entrada que, de lo contrario, estaría bien construida.

La agregación de una entrada a `Makefile` incluye lo siguiente.

- Agregar el nombre de la base de datos a la regla `all`.
- Escribir la regla `time`.
- Agregar la regla para la base de datos.

Por ejemplo, para que `Makefile` funcione en archivos de entrada del montador automático, tendría que agregar los mapas `auto_direct.time` y `auto_home.time` a la base de datos NIS.

Para agregar estos mapas a la base de datos NIS, es necesario modificar `Makefile`.

Cambio de macros/variables de `Makefile`

Puede cambiar la configuración de las variables definidas en la parte superior de `Makefile` cambiando el valor a la derecha del signo igual (=). Por ejemplo, si no desea utilizar los archivos ubicados en `/etc` como entrada para los mapas, sino que prefiere utilizar los archivos ubicados en otro directorio, como, por ejemplo, `/var/etc/domainname`, debe cambiar `DIR` de `DIR=/etc` a `DIR=/var/etc/`*domainname*. También debe cambiar `PWDIR` de `PWDIR=/etc` a `PWDIR=/var/etc/`*domainname*.

Las variables son las siguientes:

- *DIR*= El directorio que contiene todos los archivos de entrada NIS, excepto `passwd` y `shadow`. El valor predeterminado es `/etc`. Debido a que no es una buena práctica utilizar los archivos en el directorio `/etc` del servidor maestro como archivos de entrada NIS, debe cambiar este valor.
- *PWDIR*= El directorio que contiene los archivos de entrada NIS `passwd` y `shadow`. Debido a que no es una buena práctica utilizar los archivos en el directorio `/etc` del servidor maestro como archivos de entrada NIS, debe cambiar este valor.

- *DOM*= El nombre de dominio NIS. El valor predeterminado de `DOM` se puede establecer utilizando el comando `domainname`.

Modificación de entradas de `Makefile`

El siguiente procedimiento describe cómo suprimir y eliminar bases de datos desde `Makefile`.

▼ Cómo modificar `/var/yp/Makefile` para usar bases de datos específicas

Este procedimiento requiere que ya se haya configurado un servidor maestro NIS.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Modifique la línea que comienza con la palabra `all` agregando los nombres de la base de datos que desea agregar:

```
all: passwd group hosts ethers networks rpc services protocols \
    netgroup bootparams aliases netid netmasks \
    audit_user auth_attr exec_attr prof_attr \
  auto_direct auto_home auto_direct.time auto_home.time
```

El orden de las entradas no es relevante, pero el espacio en blanco al principio de las líneas de continuación deben una tabulación, no espacios.

3 Agregue las siguientes líneas al final de `Makefile`:

```
auto_direct: auto_direct.time
auto_home: auto_home.time
```

4 Agregue una entrada para `auto_direct.time` en la mitad del archivo.

```
auto_direct.time: $(DIR)/auto_direct
 @(while read L; do echo $$L; done < $(DIR)/auto_direct
 $(CHKPIPE)) | \ (sed -e "/^#/d" -e "s/#.*$$//" -e "/^ *$$/d"
 $(CHKPIPE)) | \ $(MAKEDBM) - $(YPDBDIR)/$(DOM)/auto_direct;
 @touch auto_direct.time;
 @echo "updated auto_direct";
 @if [ ! $(NOPUSH) ]; then $(YPPUSH) auto_direct; fi
 @if [ ! $(NOPUSH) ]; then echo "pushed auto_direct"; fi
```

Donde

- `CHKPIPE` se asegura de que las operaciones a la izquierda de la conducción (`|`) se completen con éxito antes de conducir los resultados a próximos comandos. Si las operaciones a la izquierda de la conducción no se realizan correctamente, el proceso se terminará con un mensaje `NIS make terminated`.
- `NOPUSH` evita que `makefile` llame a `yppush` para transferir el nuevo mapa a los servidores esclavos. Si `NOPUSH` no está definido, el envío se realiza automáticamente.

El bucle `while` al principio está diseñado para eliminar las líneas extendidas con barra diagonal inversa en el archivo de entrada. La secuencia de comandos `sed` elimina comentarios y líneas vacías.

Siga el mismo procedimiento para todos los demás mapas del montador automático, como `auto_home`, o cualquier otro mapa no predeterminado.

5 Ejecute el comando `make`.

```
# make mapname
```

Donde *mapname* es el nombre del mapa que desea crear.

▼ Cómo modificar `Makefile` para suprimir bases de datos

Si no desea que `Makefile` produzca mapas para una base de datos específica, edite `Makefile` como se indica a continuación.

1 Suprima el nombre de la base de datos de la regla `all`.

2 Suprima o realice un comentario en la regla de la base de datos que desea suprimir.

Por ejemplo, para suprimir la base de datos `hosts`, se debe eliminar la entrada `hosts.time`.

3 Elimine la regla de tiempo.

Por ejemplo, para suprimir la base de datos `hosts`, se debe eliminar la entrada `hosts:hosts.time`.

4 Elimine el mapa del servidor maestro y de los servidores esclavos.

Actualización y modificación de mapas existentes

Después de instalar NIS, es posible que descubra que algunos mapas requieren actualizaciones frecuentes mientras que otras nunca necesitan cambiar. Por ejemplo, el mapa de datos `passwd.byname` puede cambiar con frecuencia en una red grande de la empresa, mientras que el mapa `auto_master` cambia un poco o nada.

Como se menciona en "Mapas de datos NIS predeterminados" en la página 71, la ubicación predeterminada de los mapas de datos NIS predeterminados es el servidor maestro en `/var/yp/`*domainname*, donde *domainname* es el nombre del dominio NIS. Cuando necesite actualizar un mapa, puede utilizar uno de los dos procedimientos de actualización, en función de si es o no un mapa predeterminado.

- Un mapa predeterminado es un mapa en el conjunto predeterminado creado por el comando `ypinit` desde las bases de datos de la red.
- Los mapas no predeterminados pueden ser cualquiera de los siguientes:

- Mapas que se incluyen con una aplicación adquirida de un proveedor.
- Mapas creados específicamente para su sitio.
- Mapas creados a partir de un archivo que no sea de texto.

Las siguientes secciones explican cómo utilizar varias herramientas de actualización. En la práctica, se podría decidir sólo usarlas si agrega mapas no predeterminados o cambia el conjunto de servidores NIS después de que el sistema ya está activo y en ejecución.

▼ Cómo actualizar mapas proporcionados con el conjunto predeterminado

Utilice el siguiente procedimiento para actualizar mapas que se suministran con el conjunto predeterminado.

1 Conviértase en administrador en el servidor maestro NIS.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Edite el archivo de origen del mapa que desea cambiar.

El archivo puede residir en `/etc` o en otro directorio de su elección.

3 Ejecute el comando `make`.

```
# cd /var/yp
# make mapname
```

El comando `make` actualiza el mapa de acuerdo con los cambios que ha realizado en su archivo correspondiente. También propaga los cambios entre los demás servidores.

Mantenimiento de mapas actualizados

En las siguientes secciones se describen procedimientos adicionales después de haber completado la actualización de los mapas que se proporcionan con el conjunto predeterminado.

Propagación de un mapa NIS

Después de que se cambia un mapa, el archivo `Makefile` usa `yppush` para propagar un nuevo mapa a los servidores esclavos (a menos que `NOPUSH` esté definido en `Makefile`). Esto se realiza al informar al daemon `ypserv` y enviar un mapa de solicitud de transferencia. Luego el daemon `ypserv` en el esclavo inicia un proceso `ypxfr`, que, a su vez, se pone en contacto con el daemon `ypxfrd` en el servidor maestro. Se realizan algunas comprobaciones básicas (por ejemplo, ¿cambió realmente el mapa?), y, a continuación, el mapa se transfiere. `ypxfr` en el esclavo envía una respuesta al proceso `yppush` indicando si la transferencia se completó con éxito.

Nota – El procedimiento anterior *no* funcionará para los nuevos mapas que aún no existen en los servidores esclavos. Deben enviarse nuevos mapas a los servidores esclavos ejecutando `ypxfr` los esclavos.

En ocasiones, los mapas no se pueden propagar, y usted debe usar `ypxfr` manualmente para enviar información de nuevos mapas. Puede elegir utilizar `ypxfr` de dos maneras diferentes: periódicamente mediante el archivo `root crontab` o interactivamente en la línea de comandos. Estos métodos se discuten en las siguientes secciones.

Uso del comando `cron` para transferencias de mapas

Loa mapas tienen distintas frecuencias de cambio. Por ejemplo, es posible que algunos mapas no cambien durante meses en un tiempo, como sucede con `protocols.byname` entre los mapas predeterminados y `auto_master` entre los mapas no predeterminados. Sin embargo, `passwd.byname` puede cambiar varias veces al día. La programación de transferencia de mapas mediante el uso del comando `crontab` le permite definir tiempos de propagación específicos para mapas individuales.

Para ejecutar periódicamente `ypxfr` a una frecuencia adecuada para el mapa, el archivo root `crontab` en cada servidor esclavo debe contener las entradas `ypxfr` adecuadas. `ypxfr` se pone en contacto con el servidor maestro y transfiere el mapa sólo si la copia del servidor maestro es más reciente que la copia local.

Nota – Si su servidor maestro ejecuta `rpc.yppasswdd` con la opción predeterminada `-m`, cada vez que alguien cambia su contraseña `yp`, el daemon `passwd` ejecuta `make`, que vuelve a crear los mapas `passwd`.

Uso de secuencias de comandos de shell con `cron` y `ypxfr`

Como alternativa para crear entradas `crontab` separadas para cada mapa, puede ser preferible hacer que el comando raíz `crontab` ejecute una secuencia de comandos shell que actualice periódicamente todos los mapas. Las secuencias de muestra de comandos de shell de actualización de mapas están en el directorio `/usr/lib/netsvc/yp`. Los nombres de secuencia de comandos son `ypxfr_1perday`, `ypxfr_1perhour` y `ypxfr_2perday`. Puede modificar o sustituir estas secuencias de comandos de shell para que se ajusten a los requisitos de su sitio. En el ejemplo siguiente, se muestra la secuencia de comandos de shell `ypxfr_1perday` predeterminada.

EJEMPLO 7–1 Secuencia de comandos de shell ypxfr_1perday

```
#! /bin/sh
#
# ypxfr_1perday.sh - Do daily yp map check/updates
PATH=/bin:/usr/bin:/usr/lib/netsvc/yp:$PATH
```

EJEMPLO 7–1 Secuencia de comandos de shell ypxfr_1perday *(Continuación)*

```
export PATH
# set -xv
ypxfr group.byname
ypxfr group.bygid
ypxfr protocols.byname
ypxfr protocols.bynumber
ypxfr networks.byname
ypxfr networks.byaddr
ypxfr services.byname
ypxfr ypservers
```

Esta secuencia de comandos de shell actualiza los mapas una vez al día si se ejecuta el archivo root `crontab` diariamente. También puede tener secuencias de comandos que actualizan mapas una vez por semana, una vez por mes, una vez por hora y así sucesivamente. Sin embargo, tenga en cuenta la reducción del rendimiento que implica la propagación frecuente de los mapas. Para obtener más información, consulte la página del comando man `crontab(1)`.

Ejecute las mismas secuencias de comandos de shell como `root` en cada servidor esclavo configurado para el dominio NIS. Modifique el momento exacto de ejecución de un servidor a otro para evitar retrasar el servidor maestro.

Si desea transferir el mapa de un determinado servidor esclavo, utilice la opción `-h` *machine* de `ypxfr` dentro de la secuencia de comandos de shell. Ésta es la sintaxis de los comandos que se colocan en la secuencia de comandos.

```
# /usr/lib/netsvc/yp/ypxfr -h machine [ -c ] mapname
```

Donde *equipo* es el nombre del servidor con los mapas que desea transferir y *mapname* es el nombre del mapa solicitado. Si utiliza la opción `-h` sin especificar un equipo, `ypxfr` intenta obtener el mapa del servidor maestro. Si `ypserv` no es se está ejecutando localmente en el momento que se ejecuta `ypxfr`, debe utilizar el indicador `-c`, de modo que `ypxfr` no envíe una solicitud de mapa actual sin cifrar a `ypserver` local.

Puede utilizar la opción `-s` *dominio* para transferir mapas desde otro dominio a su dominio local. Estos mapas deben ser los mismos en todos los dominios. Por ejemplo, dos dominios pueden compartir los mismos mapas `services.byname` y `services.byaddr`. Si desea obtener más control, también puede utilizar `rcp` o `rsync` para transferir archivos entre dominios.

Invocación directa del comando `ypxfr`

El segundo método de invocación del comando `ypxfr` es ejecutarlo como un comando. Normalmente, esto se realiza en situaciones excepcionales, por ejemplo, cuando se configura un servidor NIS temporal para crear un entorno de prueba o cuando se intenta ajustar rápidamente un servidor NIS que ha estado fuera de servicio según los demás servidores.

Registro de la actividad de ypxfr

Los intentos de transferencia y los resultados de ypxfr se pueden capturar en un archivo de registro. Si existe un archivo llamado /var/yp/ypxfr.log, los resultados se agregan a éste. No se intenta limitar el tamaño del archivo de registro. Para evitar que crezca indefinidamente, vacíelo de vez en cuando escribiendo lo siguiente.

```
# cd /var/yp
# cp ypxfr.log ypxfr.log.old
# cat /dev/null > /var/yp/ypxfr.log
```

Puede hacer que crontab ejecute esos comandos una vez por semana. Para desactivar el registro, elimine el archivo de registro.

Modificación de mapas no predeterminados

Para actualizar un mapa no predeterminado, debe hacer lo siguiente:

1. Crear o editar su archivo de texto correspondiente.
2. Crear (o volver a crear) la actualización nueva o actualizada. Existen dos formas de crear un mapa.
   - Utilice Makefile. Makefile es el método preferido para crear un mapa no predeterminado. Si el mapa tiene una entrada en Makefile, ejecute make *name*, donde *name* es el nombre del mapa que desea crear. Si el mapa no tiene una entrada Makefile, intente crear una siguiendo las instrucciones que se indican en "Modificación y uso de /var/yp/Makefile" en la página 104.
   - Use el programa /usr/sbin/makedbm. En la página del comando man makedbm(1M), se describe completamente este comando.

Uso del comando makedbm para modificar un mapa no predeterminado

Hay dos métodos diferentes para utilizar makedbm con el fin de modificar mapas si no dispone de un archivo de entrada:

- Redirija el resultado de makedbm -u a un archivo temporal, modifique el archivo y, a continuación, utilice el archivo modificado como entrada de makedbm.
- Haga que la salida de makedbm -u se opere en una canalización que se alimenta en makedbm. Esto es adecuado si se puede actualizar el mapa desmontado con un anexo awk, sed o cat.

Creación de nuevos mapas a partir de archivos de texto

Suponga que un archivo de texto `/var/yp/mymap.asc` se ha creado con un editor o una secuencia de comandos del shell en el maestro. Desea crear un mapa de datos NIS a partir de este archivo y guardarlo en el subdirectorio *home-domain*. Para ello, escriba lo siguiente en el servidor maestro.

```
# cd /var/yp
# makedbm mymap.asc home-domain/mymap
```

El mapa *mymap* ahora existe en el servidor maestro del directorio *home-domain*. Para distribuir el nuevo mapa a servidores esclavos, ejecute `ypxfr`.

Agregación de entradas a un mapa basado en archivo

La agregación de entradas a `mymap` es simple. En primer lugar, debe modificar el archivo de texto `/var/yp/`*mymap*`.asc`. Si modifica los archivos dbm reales sin modificar el archivo de texto correspondiente, se pierden las modificaciones. A continuación, ejecute `makedbm` como se mostró anteriormente.

Creación de mapas a partir de la entrada estándar

Cuando no hay ningún archivo de texto original, cree el mapa de datos NIS con el teclado escribiendo la entrada en `makedbm`, como se muestra a continuación (termine con Control+D).

```
ypmaster# cd /var/yp
ypmaster# makedbm home-domain/mymap key1 value1  key2 value2  key3 value3
```

Modificación de mapas realizados a partir de la entrada estándar

Si más tarde necesita modificar el mapa, puede utilizar `makedbm` para desmontar el mapa y crear un archivo intermedio de texto temporal. Para desmontar el mapa y crear un archivo temporal, escriba lo siguiente.

```
% cd /var/yp
% makedbm -u homedomain/mymap > mymap.temp
```

El archivo temporal resultante *mymap*`.temp` tiene una entrada por línea. Puede editar este archivo según sea necesario, con cualquier editor de texto.

Para actualizar el mapa, proporcione el nombre del archivo temporal modificado a `makedbm` escribiendo lo siguiente:

```
% makedbm mymap.temp homedomain/mymap
% rm mymap.temp
```

A continuación, propague el mapa a los servidores esclavos convirtiéndose en `root` y escribiendo lo siguiente.

```
# yppush mymap
```

En los párrafos anteriores, se explica cómo usar `makedbm` para crear mapas. Sin embargo, casi todo lo que realmente tiene que hacer se puede llevar a cabo mediante el comando `ypinit` y `/var/yp/Makefile`, a menos que agregue mapas no predeterminados a la base de datos o cambie el conjunto de servidores NIS una vez que el sistema ya está activo y en ejecución.

Ya sea que use `Makefile` en `/var/yp` o algún otro procedimiento, el objetivo es el mismo. Como resultado final, debe haber un nuevo par de archivos dbm formados correctamente en el directorio de mapas del servidor maestro.

Trabajo con servidores NIS

Los procedimientos siguientes muestran cómo modificar la configuración NIS mediante el enlace a un servidor NIS específico, la configuración del nombre de dominio NIS, el reenvío de consultas de host al DNS y la desactivación de los servicios NIS.

Vínculo a un servidor NIS específico

Utilice los siguientes pasos para vincular con un servidor NIS que especifique. Para obtener más información, consulte las páginas del comando man `ypinit(1M)`, `ypstart(1M)` y `svcadm(1M)`.

1. Agregue el nombre de host del servidor NIS y la dirección IP al archivo `/etc/hosts`.
2. Verifique que el nombre de dominio NIS esté definido.

   ```
   # domainname
   example.com
   ```
3. Solicite el nombre de host del servidor NIS.

   ```
   # /usr/sbin/ypinit -c
   Server name:      Type the NIS server host name
   ```
4. Reinicie los servicios NIS mediante uno de los siguientes pasos:
   - Para que los servicios se mantengan en todos los reinicios, ejecute el comando `svcadm`.

     ```
     # svcadm enable svc:/network/nis/client
     ```
   - Para que los servicios se mantengan sólo hasta que reinicie, ejecute los comandos `ypstop` y `ypstart`.

     ```
     # /usr/lib/netsvc/yp/ypstop
     # /usr/lib/netsvc/yp/ypstart
     ```

▼ Cómo establecer un nombre de dominio NIS de una máquina

Para cambiar el nombre de dominio NIS de una máquina, realice el siguiente procedimiento.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Defina el nombre de dominio NIS.

```
# domainname research.example.com
```

3 Actualice y ejecute los servicios de nombres de dominio.

```
# svccfg -s nis/domain:default refresh
# svcadm enable nis/domain
```

4 Configure la máquina como cliente NIS, servidor esclavo o servidor maestro.

Consulte Capítulo 6, "Instalación y configuración del servicio NIS (tareas)" para obtener más información.

▼ Cómo configurar la consulta de dirección y nombre de host de la máquina mediante NIS y DNS

Normalmente, los clientes NIS se configuran con el archivo `nsswitch.conf` para utilizar sólo NIS para las consultas de dirección y nombre de la máquina. Si este tipo de consulta falla, un servidor NIS puede reenviar estas consultas a DNS.

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Agregue la clave `YP_INTERDOMAIN`.

Los dos archivos de mapa, `hosts.byname` y `hosts.byaddr`, deben incluir la clave `YP_INTERDOMAIN`. Para probar esta clave, edite `/var/yp/Makefile` y modifique las líneas siguientes.

```
#B=-b
B=

a


B=-b
#B=
```

`makedbm` se iniciará con el indicador `-b` cuando crea los mapas, y la clave `YP_INTERDOMAIN` clave se insertará en los archivos `ndbm`.

3 Ejecute el comando `make` para recrear los mapas.

```
# make hosts
```

4 Compruebe que los servidores de nombres DNS estén definidos correctamente.

El siguiente comando enumera todas las direcciones IP de los servidores de nombres DNS:

```
# svcprop -p config/nameserver network/dns/client
```

5 Para activar el reenvío DNS, reinicie cada servidor.

```
# svcadm restart network/nis/server:instance
```

En esta implementación de NIS, el daemon `ypserv` se inicia automáticamente con la opción `-d` para reenviar solicitudes al DNS.

Desactivación de los servicios NIS

Si el daemon `ypserv` en el servidor maestro NIS está desactivado, ya no puede actualizar ninguno de los mapas de datos NIS.

- Para desactivar NIS en un cliente, escriba lo siguiente:

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/client
```

- Para desactivar NIS en un servidor maestro o esclavo determinado, escriba lo siguiente en el servidor:

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/server
```

◆ ◆ ◆ CAPÍTULO 8

Resolución de problemas de NIS

En este capítulo, se explica cómo resolver los problemas que encontrados en redes que ejecutan NIS. Trata los problemas que se encuentran tanto en servidores como en clientes NIS.

Antes de intentar depurar un servidor o cliente NIS, consulte Capítulo 5, "Servicio de información de red (descripción general)", donde se explica el entorno NIS. Luego, en esta sección, busque el subtítulo que mejor describa su problema.

Nota – El servicio NIS es gestionado por la utilidad de gestión de servicios. Las acciones administrativas de este servicio, como la activación, la desactivación o el reinicio, pueden realizarse con el comando `svcadm`. Consulte "NIS y la utilidad de gestión de servicios" en la página 78 para obtener más información sobre el uso de SMF con NIS. Para obtener una descripción general de la SMF, consulte el Capítulo 1, "Gestión de servicios (descripción general)" de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M) y `svcs`(1) para obtener más información.

Los servicios NIS también se pueden iniciar y detener utilizando los comandos `ypstart` y `ypstop`. Consulte las páginas del comando man `ypstart`(1M) y `ypstop`(1M) para obtener más información.

Problemas de enlace NIS

Síntomas de problemas de enlace NIS

Los síntomas comunes de problemas de vinculación de NIS son los siguientes.

- Mensajes que indican que `ypbind` no puede encontrar un servidor o no puede comunicarse con un servidor.
- Mensajes que indican que el servidor no responde

- Mensajes que indican que NIS no está disponible
- Los comandos de un cliente tienen dificultadas en el modo de fondo o funcionan mucho más lento que lo habitual
- Los comandos en un cliente se bloquean. A veces, los comandos se bloquean aunque el sistema parezca estar bien en general y puede ejecutar nuevos comandos.
- Los comandos de un cliente colapsan con mensajes extraños o sin mensajes

Problemas de NIS que afectan a un cliente

Si sólo uno o dos clientes experimentan síntomas que indican dificultades en el vínculo de NIS, los problemas probablemente estén en esos clientes. Si muchos clientes NIS no se pueden vincular correctamente, el problema probablemente exista en uno o más de los servidores NIS. Consulte "Problemas de NIS que afectan a muchos clientes" en la página 121.

`ypbind` no se ejecuta en el cliente

Un cliente presenta problemas, pero otros clientes en la misma subred funcionan con normalidad. En el cliente que tiene el problema, ejecute `ls -l` en un directorio, como `/usr`, que contiene los archivos que pertenecen a muchos usuarios, incluidos algunos que no están en el archivo `/etc/passwd` del cliente. Si la pantalla que aparece enumera propietarios de archivos que no están en el `/etc/passwd` local como números, en lugar de nombres, esto indica que servicio NIS no funciona en el cliente.

Estos síntomas generalmente significan que el proceso `ypbind` del cliente no se está ejecutando. Verifique si se están ejecutando los servicios del cliente NIS.

```
client# svcs \*nis\*
STATE          STIME    FMRI
disabled       Sep_01   svc:/network/nis/domain:default
disabled       Sep_01   svc:/network/nis/client:default
```

Si los servicios están en estado `disabled` (desactivado), inicie sesión como `root` o asuma un rol equivalente, e inicie el servicio del cliente NIS.

```
client# svcadm enable network/nis/domain
client# svcadm enable network/nis/client
```

Falta el nombre de dominio o es incorrecto

Un cliente tiene problemas, los otros clientes funcionan normalmente, pero `ypbind` se está ejecutando en el cliente con el problema. El cliente puede tener un dominio mal configurado.

En el cliente, ejecute el comando `domainname` para ver qué nombre de dominio está definido.

```
client7# domainname
example.com
```

Compare la salida con el nombre de dominio real en `/var/yp` en el servidor maestro NIS. El dominio NIS real se muestra como un subdirectorio en el directorio `/var/yp`.

```
client7# ls -l /var/yp
-rwxr-xr-x 1 root Makefile
drwxr-xr-x 2 root binding
drwx------ 2 root example.com
```

Si el nombre de dominio devuelto ejecutando `domainname` en una máquina no es el mismo que el nombre de dominio del servidor enumerado como directorio en `/var/yp`, el nombre de dominio especificado en el archivo `/etc/defaultdomain` de la máquina es incorrecto. Restablezca el nombre de dominio NIS como se muestra en "Cómo establecer un nombre de dominio NIS de una máquina" en la página 114.

Nota – El nombre de dominio NIS distingue entre mayúsculas y minúsculas.

Cliente no vinculado a servidor

Si el nombre de dominio está configurado correctamente, `ypbind` se está ejecutando y los comandos aún se bloquean, asegúrese de que el cliente esté enlazado a un servidor ejecutando el comando `ypwhich`. Si acaba de iniciar `ypbind`, ejecute `ypwhich` varias veces (por lo general, la primera vez informa que el dominio no está enlazado y la segunda vez se realiza con éxito normalmente).

No hay ningún servidor disponible

Si su nombre de dominio está definido correctamente, `ypbind` se está ejecutando y recibe mensajes que indican que el cliente no puede comunicarse con un servidor, esto podría indicar diferentes problemas:

- ¿El cliente tiene un archivo `/var/yp/binding/`*domainname*`/ypservers` que contiene una lista de servidores con los cuales realizar el enlace? Si no, ejecute `ypinit -c` y especifique el orden de preferencia de los servidores a los que se debe vincular el cliente.
- Si el cliente tiene un archivo `/var/yp/binding/`*domainname*`/ypservers`, ¿hay suficientes servidores enumerados si uno o dos dejan de estar disponibles? Si no es así, agregue servidores adicionales a la lista ejecutando `ypinit -c`.
- ¿Los servidores NIS seleccionados tienen entradas en el archivo `/etc/inet/hosts`? Para ver los servidores NIS seleccionados, utilice el comando `svcprop -p config/ypservers nis/domain`. Si estos hosts no están en el archivo `/etc/inet/hosts` local, agregue los servidores a los mapas de datos NIS `hosts` y vuelva a crear los mapas mediante la ejecución del comando `ypinit -c` o `ypinit -s` como se describe en "Trabajo con mapas NIS" en la página 101.
- ¿El conmutador de servicio de nombres está configurado para comprobar el archivo `hosts` local de la máquina además de NIS? Consulte el Capítulo 2, "Conmutador de servicio de nombres (descripción general)" para obtener más información sobre el conmutador.

- ¿El conmutador de servicio de nombres está configurado para comprobar `files` primero para `services` y `rpc`? Consulte Capítulo 2, "Conmutador de servicio de nombres (descripción general)" para obtener más información sobre el conmutador.

Las pantallas de `ypwhich` son incoherentes

Al usar `ypwhich` varias veces en el mismo cliente, la pantalla que aparece varía porque el servidor NIS cambia. Esto es normal. El vínculo del cliente NIS al servidor NIS cambia con el tiempo, cuando la red o los servidores NIS están ocupados. Siempre que sea posible, el red pasa a ser estable en un punto en que todos los clientes obtienen un tiempo de respuesta aceptable de los servidores NIS. Siempre que el equipo cliente tenga servicio NIS, no importa el lugar de donde proviene el servicio. Por ejemplo, un equipo servidor NIS puede obtener sus propios servicios NIS de otro servidor NIS de la red.

Cuando la vinculación de servidor no es posible

En casos extremos en que no es posible la vinculación del servidor local, el uso del comando `ypset` puede permitir temporalmente la vinculación a otro servidor, si está disponible, en otra red o subred. Sin embargo, para poder utilizar la opción `-ypset`, `ypbind` se debe iniciar con la opción `-ypset` o con la opción `-ypsetme`. Para obtener más información, consulte la página del comando man `ypbind(1M)`.

```
# /usr/lib/netsvc/yp/ypbind -ypset
```

Para ver otro método, consulte "Vínculo a un servidor NIS específico" en la página 113.

Precaución – Por motivos de seguridad, el uso de las opciones `-ypset` y `-ypsetme` no se recomienda. Utilice estas opciones sólo para la depuración en circunstancias controladas. El uso de las opciones `-ypset` y `-ypsetme` puede causar brechas de seguridad graves, ya que, aunque los daemons se están ejecutando, cualquier persona puede alterar los enlaces del servidor y provocar problemas a otros usuarios y permitir el acceso no autorizado a datos confidenciales. Si debe iniciar el daemon `ypbind` con estas opciones, después de solucionar el problema, debe finalizar el proceso `ypbind` y volver a iniciarlo sin estas opciones.

Para reiniciar el daemon `ypbind`, utilice la SMF de la siguiente forma:

```
# svcadm enable -r svc:/network/nis/client:default
```

`ypbind` se bloquea

Si el daemon `ypbind` falla casi inmediatamente cada vez que se inicia, busque un problema en el registro del servicio `svc:/network/nis/client:default`. Compruebe la presencia del daemon `rpcbind` escribiendo lo siguiente:

```
% ps -e |grep rpcbind
```

Si `rpcbind` no está presente, no se mantiene activo o se comporta de manera extraña, compruebe el archivo del registro `svc:/network/rpc/bind:default`. Para obtener más información, consulte las páginas del comando man `rpcbind`(1M) y `rpcinfo`(1M).

Es posible que pueda comunicarse con `rpcbind` en el cliente con el problema desde un equipo que funcione con normalidad. Desde la máquina en funcionamiento, escriba lo siguiente:

```
% rpcinfo client
```

Si `rpcbind` en la máquina con el problema es aceptable, `rpcinfo` genera la siguiente salida:

```
    program    version    netid    address    service    owner
...
    100007    3    udp6       ::.191.161          ypbind     1
    100007    3    tcp6       ::.135.200          ypbind     1
    100007    3    udp        0.0.0.0.240.221     ypbind     1
    100007    2    udp        0.0.0.0.240.221     ypbind     1
    100007    1    udp        0.0.0.0.240.221     ypbind     1
    100007    3    tcp        0.0.0.0.250.107     ypbind     1
    100007    2    tcp        0.0.0.0.250.107     ypbind     1
    100007    1    tcp        0.0.0.0.250.107     ypbind     1
    100007    3    ticlts     2\000\000\000       ypbind     1
    100007    2    ticlts     2\000\000\000       ypbind     1
    100007    3    ticotsord  9\000\000\000       ypbind     1
    100007    2    ticotsord  9\000\000\000       ypbind     1
    100007    3    ticots     @\000\000\000       ypbind     1
...
```

El equipo tendrá diferentes resultados. Si las direcciones no se muestran, `ypbind` ha podido registrar sus servicios. Reinicie el equipo y ejecute `rpcinfo` de nuevo. Si hay procesos de `ypbind` y cambian cada vez que se intenta reiniciar el servicio NIS, reinicie el sistema, aunque el daemon `rpcbind` se esté ejecutando.

Problemas de NIS que afectan a muchos clientes

Si sólo uno o dos clientes experimentan síntomas que indican dificultades en el vínculo de NIS, los problemas probablemente estén en esos clientes. Consulte “Problemas de NIS que afectan a un cliente” en la página 118. Si muchos clientes NIS no se pueden vincular correctamente, el problema probablemente exista en uno o más de los servidores NIS.

rpc.yppasswdd considera restringido a un shell no restringido que empieza con r

1. Cree `/etc/default/yppasswdd` que contenga una cadena especial:"`check_restricted_shell_name=1`".
2. Si se marca la cadena "`check_restricted_shell_name=1`", no ocurre la comprobación de la 'r'.

No se puede acceder a la red o los servidores

NIS se puede bloquear si la red o los servidores NIS están tan sobrecargados que el daemon `ypserv` no puede recibir una respuesta para el proceso `ypbind` del cliente antes de que se supere el tiempo de espera. NIS también puede bloquearse si se produce un fallo en la red.

En estas circunstancias, cada cliente de la red experimenta el mismo problema o problemas similares. En la mayoría de los casos, la situación es temporal. Los mensajes normalmente desaparecen cuando el servidor NIS se reinicia y reinicia `ypserv`, cuando la carga de los servidores NIS o la red disminuye, o cuando la red reanuda las operaciones normales.

Funcionamiento incorrecto del servidor

Asegúrese de que los servidores estén activos y en ejecución. Si no está físicamente cerca los servidores, utilice el comando `ping`.

Daemons NIS no en ejecución

Si los servidores están activos y en ejecución, intente encontrar una equipo cliente que se comporte normalmente, y ejecute el comando `ypwhich`. Si `ypwhich` no responde, ciérrelo. A continuación, inicie sesión como `root` en el servidor NIS y compruebe si el proceso NIS se está ejecutando escribiendo lo siguiente:

```
# ptree |grep ypbind
100759 /usr/lib/netsvc/yp/ypbind -broadcast
        527360 grep yp
```

Si ni el daemon `ypserv` (servidor NIS) ni el daemon ypbind (cliente NIS) se están ejecutando, reinícielos escribiendo lo siguiente:

```
# svcadm restart network/nis/client
```

Si tanto el proceso `ypserv` como el proceso `ypbind` se están ejecutando en el servidor NIS, ejecute el comando `ypwhich`. Si el comando no responde, el daemon `ypserv` probablemente se bloqueó y se debe reiniciar. Mientras está conectado como `root` en el servidor, reinicie el servicio NIS escribiendo lo siguiente:

```
# svcadm restart network/nis/server
```

Los servidores tienen versiones diferentes de un mapa NIS

Debido a que NIS propaga mapas entre los servidores, ocasionalmente puede encontrar diferentes versiones del mismo mapa en distintos servidores NIS de la red. Esta diferencia en versiones es normal y es aceptable si las diferencias no duran más de un breve período.

La causa más común de la diferencia de mapas es cuando se impide la propagación normal de los mapas. Por ejemplo, un servidor NIS o un enrutador entre servidores NIS está fuera de servicio. Cuando todos los servidores NIS y los enrutadores entre ellos se están ejecutando, `ypxfr` se debe realizar correctamente.

Si los servidores y los enrutadores funcionan correctamente, compruebe lo siguiente:

- Compruebe la salida del registro de `ypxfr`. Consulte "Registro de la salida de `ypxfr`" en la página 123.
- Compruebe el archivo de registro `svc:/network/nis/xfr:default` para ver si hay errores.
- Compruebe los archivos de control. Consulte "Revise el archivo `crontab` y la secuencia de comandos de shell`ypxfr`" en la página 123.
- Compruebe el mapa `ypservers` en el servidor maestro. Consulte "Compruebe el mapa `ypservers`" en la página 124.

Registro de la salida de ypxfr

Si un determinado servidor esclavo tiene problemas al actualizar mapas, inicie sesión en ese servidor y ejecute el comando `ypxfr` de forma interactiva. Si el comando falla, indica por qué ha fallado, y usted puede solucionar el problema. Si el comando tiene éxito, pero usted sospecha que ha fallado en algún momento, cree un archivo de registro para activar el registro de mensajes. Para crear un archivo de registro, introduzca lo siguiente en el servidor esclavo.

```
ypslave# cd /var/yp
ypslave# touch ypxfr.log
```

Esto crea un archivo `ypxfr.log` que guarda todos los resultados de `ypxfr`.

El resultado es similar al resultado que `ypxfr` muestra cuando se ejecuta de manera interactiva, pero cada línea del archivo de registro tiene una marca de hora y fecha. Es posible que vea un orden poco común en los indicadores de fecha y hora. Esto es correcto, ya que los indicadores de fecha y hora le indican cuándo `ypxfr` se comenzó a ejecutar. Si se ejecutan copias de `ypxfr` simultáneamente, pero demoran diferentes cantidades de tiempo, podrían escribir su línea de estado de resumen en los archivos de registro en un orden diferente del que se invocaron. Cualquier patrón de fallas intermitentes aparece en el registro.

Nota – Cuando ha solucionado el problema, desactive el registro eliminando el archivo de registro. Si olvida eliminarlo, continúa creciendo sin límite.

Revise el archivo crontab y la secuencia de comandos de shellypxfr

Inspeccione el archivo `root crontab` y compruebe la secuencia de comandos de shell de `ypxfr` que invoca. Los errores tipográficos de estos archivos puede provocar problemas de propagación. Las fallas al hacer referencia a una secuencia de comandos de shell dentro del archivo `/var/spool/cron/crontabs/root`, o las fallas para hacer referencia a un mapa dentro de cualquier secuencia de comandos de shell también puede causar errores.

Compruebe el mapa ypservers

Además, asegúrese de que el servidor NIS esclavo esté enumerado en el mapa `ypservers` del servidor maestro del dominio. Si no es así, el servidor esclavo sigue funcionando perfectamente como servidor, pero `yppush` no propaga cambios de mapas para el servidor esclavo.

Solución provisional para actualizar mapas en un servidor esclavo roto

Si el problema del servidor NIS esclavo no es claro, puede realizar una solución provisional al depurar el problema mediante el comando `scp` o `ssh` para copiar una versión reciente del mapa incoherente desde cualquier servidor NIS en perfectas condiciones. En el siguiente ejemplo, se muestra cómo transferir el mapa con el problema.

```
ypslave# scp ypmaster:/var/yp/mydomain/map.\* /var/yp/mydomain
```

El carácter * no se ha incluido en la línea de comandos, por lo que se ampliará en `ypmaster`, en lugar de localmente en `ypslave`.

`ypserv` se bloquea

Cuando el proceso de `ypserv` se bloquea casi inmediatamente y no se mantiene activo ni siquiera con activaciones repetidas, el proceso de depuración es prácticamente idéntico al que se describe en "ypbind se bloquea" en la página 120. En primer lugar, ejecute el siguiente comando para ver los errores que aparecen:

```
# svcs -vx nis/server
```

Compruebe la existencia del daemon `rpcbind` de la siguiente forma:

```
# ptree |grep rpcbind
```

Reiniciar el servidor si no encuentra el daemon. De lo contrario, si el daemon se está ejecutando, escriba lo siguiente y busque una salida similar:

```
% rpcinfo -p ypserver

% program     vers     proto     port     service
100000    4    tcp    111    portmapper
100000    3    tcp    111    portmapper
100068    2    udp    32813    cmsd
...
100007    1    tcp    34900    ypbind
100004    2    udp    731    ypserv
100004    1    udp    731    ypserv
100004    1    tcp    732    ypserv
100004    2    tcp    32772    ypserv
```

Es posible que su equipo tenga diferentes números de puerto. Las cuatro entradas que representan el proceso `ypserv` son las siguientes:

```
100004     2     udp     731     ypserv
100004     1     udp     731     ypserv
100004     1     tcp     732     ypserv
100004     2     tcp     32772     ypserv
```

Si no hay entradas e `ypserv` es no puede registrar sus servicios con `rpcbind`, reinicie el equipo. Si existen entradas, anule el registro del servicio de `rpcbind` antes de reiniciar `ypserv`. Para anular el registro del servicio de `rpcbind`, en el servidor, escriba lo siguiente.

```
# rpcinfo -d number 1
# rpcinfo -d number 2
```

Donde *number* es el número de ID indicado por `rpcinfo` (`100004`, en el ejemplo anterior).

PARTE III

Servicios de nombres LDAP

Esta parte ofrece una descripción general sobre los servicios de nombres LDAP. Además, incluye la configuración, la administración y la resolución de problemas de servicios de nombres LDAP en SO Oracle Solaris, con un enfoque en el uso de Oracle Directory Server Enterprise Edition.

◆ ◆ ◆ CAPÍTULO 9

Introducción a los servicios de nombres LDAP (descripción general)

En los capítulos sobre LDAP, se describe cómo configurar un cliente de servicios de nombres LDAP para trabajar con Oracle Directory Server Enterprise Edition (antes Sun Java System Directory Server). Sin embargo, mientras que utilizar Oracle Directory Server Enterprise Edition es recomendable, no es obligatorio. En el Capítulo 14, “Servicio de nombres LDAP (Referencia)”, se incluye una breve descripción de los requisitos genéricos del servidor de directorios.

Nota – Un servidor de directorios no es necesariamente un servidor LDAP. Sin embargo, en el contexto de estos capítulos, el término "servidor de directorios" es sinónimo de "servidor LDAP".

En este capítulo, se tratan los temas siguientes:

Suposiciones de destinatarios

Los capítulos de los servicios de nombres LDAP están escritos para los administradores del sistema que ya tienen conocimientos básicos de LDAP. A continuación, se presenta un lista parcial de conceptos con los que debe estar muy familiarizado. De lo contrario, es posible que tenga dificultades al utilizar esta guía para implementar los servicios de nombres LDAP en el sistema Oracle Solaris.

- Modelo de información LDAP (entradas, clases de objeto, atributos, tipos, valores)
- Modelo de nombres LDAP (estructura de árbol de información de directorios [DIT])
- Modelo funcional LDAP (parámetros de búsqueda: objeto de base [DN], ámbito, límite de tamaño, límite de tiempo, filtros [índices de navegación para Oracle Directory Server Enterprise Edition], lista de atributos)
- Modelo de seguridad LDAP (métodos de autenticación, modelos de control de acceso)
- Planificación general y diseño de un servicio de directorios LDAP, incluido cómo planificar los datos y cómo diseñar DIT, la topología, la replicación y la seguridad

Lectura en segundo plano sugerida

Para obtener más información sobre cualquiera de las conceptos anteriores o estudiar LDAP y la implementación de servicios de directorio en general, consulte las siguientes fuentes:

- *Guía de implementación de Oracle Directory Server Enterprise Edition*

  En esta guía se ofrece una base para planificar su directorio, incluido el diseño del directorio, el diseño del esquema, el árbol de directorios, la topología, la replicación y la seguridad. El último capítulo proporciona ejemplos de situaciones de implementación para ayudarle a planificar tanto implementaciones sencillas de menor escala como implementaciones complejas a nivel mundial.
- *Guía de administración de Oracle Directory Server Enterprise Edition*

Requisitos previos adicionales

Si necesita instalar Oracle Directory Server Enterprise Edition, consulte la *Guía de instalación* para obtener la versión de Oracle Directory Server Enterprise Edition que está utilizando.

Servicios de nombres LDAP comparados con otros servicios de nombres

Consulte "Servicios de nombres: comparación rápida" en la página 31 para obtener una comparación de los servicios de nombres DNS, NIS y LDAP.

Ventajas de servicios de nombres LDAP

- LDAP le permite consolidar la información, sustituir bases de datos específicas de la aplicación y, así, reducir el número de bases de datos que se deben gestionar.
- LDAP permite que diferentes servicios de nombres compartan los datos.
- LDAP proporciona un repositorio central para los datos.
- LDAP permite la sincronización de datos más frecuente entre los maestros y las réplicas.
- LDAP es compatible con varias plataformas y varios proveedores.

Restricciones de servicios de nombres LDAP

A continuación, se muestran algunas restricciones relacionadas con los servicios de nombres LDAP:

- Un servidor LDAP actualmente no se admite como su propio cliente.
- La configuración y la gestión de servicios de nombres LDAP son más complejas y exigen una cuidadosa planificación.
- Un cliente NIS y un cliente LDAP nativo no pueden coexistir en la misma máquina cliente.

Nota – Un servidor de directorios (un servidor LDAP) *no puede* ser su propio cliente. Es decir, no es posible configurar el equipo que está ejecutando el software del servidor de directorios para convertirlo en cliente de los servicios de nombres LDAP.

Configuración de servicios de nombres LDAP (mapa de tareas)

Tarea	Para obtener instrucciones
Planificar el modelo de red.	"Planificación del modelo de red LDAP" en la página 160
Planificar el árbol de información de directorios.	Capítulo 10, "Requisitos de planificación para servicios de nombres LDAP (tareas)"

Tarea	Para obtener instrucciones
Configurar servidores de réplica.	"Servidores LDAP y de réplica" en la página 162
Planificar el modelo de seguridad.	"Planificación del modelo de seguridad LDAP" en la página 163
Seleccionar perfiles de cliente y valores de atributo predeterminados.	"Planificación de perfiles de cliente y valores de atributo predeterminados para LDAP" en la página 165
Planificar cómo completar los datos.	"Planificación para completar los datos de LDAP" en la página 165
Configurar Oracle Directory Server Enterprise Edition antes de usarlo con los servicios de nombres LDAP.	*Oracle Directory Server Enterprise Edition*
Configurar Oracle Directory Server Enterprise Edition para usarlo con los clientes del servicio de nombres LDAP.	Capítulo 11, "Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP (tareas)"
Inicializar un cliente LDAP.	"Inicialización de un cliente LDAP" en la página 189
Inicializar un cliente mediante los perfiles.	"Cómo inicializar un cliente LDAP mediante perfiles" en la página 190
Inicializar un cliente manualmente.	"Cómo inicializar un cliente LDAP manualmente" en la página 194
Cancelar la inicialización de un cliente.	"Cómo cancelar la inicialización de un cliente LDAP" en la página 195
Utilizar los descriptores de búsqueda de servicios para modificar perfiles de cliente.	"Uso de descriptores de búsqueda de servicios para modificar el acceso de cliente a distintos servicios" en la página 173
Recuperar la información del servicio de nombres.	"Recuperación de información de servicios de nombres LDAP" en la página 199
Personalizar un entorno de cliente.	"Personalización del entorno de cliente LDAP" en la página 200

Formato de intercambio de datos LDAP

El formato de intercambio de datos LDAP (LDIF) se utiliza como un formato común de intercambio basado en texto entre varias herramientas LDAP, como `ldapadd` y `ldapmodify`. LDIF se describe completamente en LDIF RFC 2849. A continuación, se incluyen dos ejemplos de salida LDIF creada por el comando `ldapadd`. Utilice `ldaplist(1)` con la opción `-l` para visualizar la siguiente información.

```
% ldaplist -l hosts myhost
hosts

dn: cn=myhost+ipHostNumber=7.7.7.115,ou=Hosts,dc=mydc,dc=mycom,dc=com
cn: myhost
iphostnumber: 7.7.7.115
objectclass: top
objectclass: device
objectclass: ipHost
description: host 1 - floor 1 - Lab a - building b
% ldaplist -l passwd user1
passwd

dn: uid=user1,ou=People,dc=mydc,dc=mycom,dc=com
uid: user1
cn: user1
userpassword: {crypt}duTx91g7PoNzE
uidnumber: 199995
gidnumber: 20
gecos: Joe Smith [New York]
homedirectory: /home/user1
loginshell: /bin/csh
objectclass: top
objectclass: shadowAccount
objectclass: account
objectclass: posixAccount
```

Uso de nombres de dominio completo con LDAP

Si LDAP se utiliza para resolver nombres de host, un cliente LDAP siempre devuelve un nombre de dominio completo (FQDN) para un nombre de host. FQDN LDAP es similar al nombre de dominio completo (FQDN) devuelto por DNS. Por ejemplo, suponga que su nombre de dominio es el siguiente:

```
west.example.net
```

`gethostbyname()` y `getnameinfo()` devuelven la versión del nombre de dominio completo al buscar el nombre de host *servidor*:

```
server.west.example.net
```

Árbol de información de directorios predeterminado

De manera predeterminada, los clientes LDAP acceden a la información asumiendo que el árbol de información de directorios (DIT) tiene una estructura específica. Para cada dominio admitido por el servidor LDAP, hay un subárbol con una estructura definida. Esta estructura predeterminada, sin embargo, se puede modificar al especificar descriptores de búsqueda de servicios (SSD). Para un dominio determinado, el DIT predeterminado tendrá un contenedor base que mantiene un número de contenedores conocidos que poseen las entradas para un tipo de información específico. Consulte la siguiente tabla para ver los nombres de estos subárboles. Esta información se puede encontrar en RFC 2307 y otros.

TABLA 9–1 Ubicaciones predeterminadas de DIT

Contenedor predeterminado	Tipo de información
`ou=Ethers`	bootparams, ethers
`ou=Group`	group
`ou=Hosts`	hosts, ipnodes, publickey para hosts
`ou=Aliases`	aliases
`ou=Netgroup`	netgroup
`ou=Networks`	networks, netmasks
`ou=People`	passwd, shadow, user_attr, audit_user, publickey para usuarios
`ou=Protocols`	protocols
`ou=Rpc`	rpc
`ou=Services`	services
`ou=SolarisAuthAttr`	auth_attr
`ou=SolarisProfAttr`	prof_attr, exec_attr
`ou=projects`	project
`automountMap=auto_*`	auto_*

Esquema LDAP predeterminado

Los esquemas son definiciones que describen qué tipos de información se pueden almacenar como entradas de un directorio LDAP. Es posible que se deba ampliar el esquema del servidor de directorios para admitir clientes del servicio de nombres LDAP. En el Capítulo 14, “Servicio de nombres LDAP (Referencia)”, se incluye información detallada sobre esquemas específicos de IETF y Oracle Solaris. También se puede acceder a las distintas RFC desde el sitio web de IETF `http://www.ietf.org`.

Descriptores de búsqueda de servicios y asignación de esquemas

Nota – Si utiliza asignación de esquemas, debe hacerlo con un mucho cuidado y de forma coherente. Asegúrese de que la sintaxis del atributo asignado sea coherente con el atributo al que está asignado. En otras palabras, asegúrese de que los atributos de un solo valor se asignen a atributos de un solo valor, que las sintaxis del atributo estén en el acuerdo, y que las clases de objeto asignado tengan los atributos obligatorios correctos (posiblemente asignados).

Como se indicó anteriormente, los servicios de nombres LDAP esperan, de manera predeterminada, que la estructura del DIT tenga una cierta forma. Si lo desea, puede indicar al servicio de nombres LDAP que busque en ubicaciones que no sean las ubicaciones predeterminadas en el DIT mediante descriptores de búsqueda de servicios (SSD). Además, puede especificar que se utilicen diferentes atributos y clases de objeto en lugar de los especificados por el esquema predeterminado. Para obtener una lista de los filtros predeterminados, consulte "Filtros predeterminados utilizados por los servicios de nombres LDAP" en la página 230.

Descripción de SSD

El atributo `serviceSearchDescriptor` define de qué manera y en qué lugar el cliente del servicio de nombres LDAP debe buscar información para un servicio concreto. El atributo `serviceSearchDescriptor` contiene un nombre de servicio, seguido por uno o más triples de filtro, alcance, base separados por punto y coma. Estos triples se utilizan para definir búsquedas sólo para el servicio específico y se buscan en orden. Si hay varios triples de filtros, alcance, base definidos para un servicio determinado, cuando ese servicio busque una entrada en particular, buscará en cada base con el alcance y el filtro especificado.

Nota – La ubicación predeterminada no se busca para un servicio (base de datos) con el SSD, a menos que se incluya en el SSD. Habrá un comportamiento imprevisible si se determinan varios SSD para un servicio.

En el ejemplo siguiente, el cliente del servicio de nombres LDAP realiza una búsqueda de un nivel en `ou=west,dc=example,dc=com` seguida de una búsqueda de un nivel en `ou=east,dc=example,dc=com` para el servicio `passwd`. Si desea buscar los datos de `passwd` para el `username` de un usuario, el filtro LDAP predeterminado `(&(objectClass=posixAccount)(uid=username))` se utiliza para cada `BaseDN`.

```
serviceSearchDescriptor: passwd:ou=west,dc=example,dc=com;ou=east,
dc=example,dc=com
```

En el ejemplo siguiente, el cliente del servicio de nombres LDAP realiza una búsqueda de subárbol en `ou=west,dc=example,dc=com` para el servicio `passwd`. Si desea buscar los datos de `passwd` para el `username` de un usuario, el subárbol `ou=west,dc=example,dc=com` se busca con el filtro LDAP `(&(fulltimeEmployee=TRUE)(uid=username))`.

```
serviceSearchDescriptor: passwd:ou=west,dc=example,
dc=com?sub?fulltimeEmployee=TRUE
```

También es posible asociar varios contenedores con un tipo de servicio determinado. En el siguiente ejemplo, el descriptor de búsqueda de servicio especifica la búsqueda para las entradas de contraseña en tres contenedores.

```
ou=myuser,dc=example,dc=com
ou=newuser,dc=example,dc=com
ou=extuser,dc=example,dc=com
```

Tenga en cuenta que un carácter ' ,' en el ejemplo implica que el `defaultSearchBase` está agregado en la base relativa de SSD.

```
defaultSearchBase: dc=example,dc=com
serviceSearchDescriptor: \
passwd:ou=myuser,;ou=newuser,;ou=extuser,dc=example,dc=com
```

Atributos attributeMap

El servicio de nombres LDAP permite que uno o más nombres de atributo se vuelvan a asignar para cualquiera de sus servicios. El cliente LDAP utiliza los atributos conocidos que se describen en el Capítulo 14, “Servicio de nombres LDAP (Referencia)”. Si asigna un atributo, debe asegurarse de que tenga el mismo significado y sintaxis que el atributo original. Tenga en cuenta que la asignación del atributo `userPassword` puede causar problemas.

Hay un par de motivos por los que puede que desee utilizar asignaciones de esquemas.

- Desea asignar atributos en un servidor de directorios existente.
- Si tiene nombres de usuario que sólo difieren en las mayúsculas y minúsculas, debe asignar el atributo `uid`, que no tiene en cuenta las mayúsculas y las minúsculas, en lugar de un atributo que distingue entre mayúsculas y minúsculas.

El formato para este atributo es `service:attribute-name=mapped-attribute-name` .

Si desea asignar más de un atributo para un servicio determinado, puede definir varios atributos `attributeMap`.

En el siguiente ejemplo, los atributos `employeeName` y `home` se utilizarán siempre que los atributos `uid` y `homeDirectory` se utilicen para el servicio `passwd`.

```
attributeMap: passwd:uid=employeeName
attributeMap: passwd:homeDirectory=home
```

Existe un caso especial donde puede asignar el atributo `gecos` del servicio `passwd` a varios atributos. A continuación, se muestra un ejemplo.

```
attributeMap: gecos=cn sn title
```

Esto asigna los valores de `gecos` a una lista separada por espacios de los valores de los atributos `cn`, `sn` y `title`.

Atributo objectclassMap

El servicio de nombres LDAP permite que las clases de objetos se vuelvan a asignar para cualquiera de sus servicios. Si desea asignar más de una clase de objeto a un servicio determinado, puede definir varios atributos `objectclassMap`. En el siguiente ejemplo, la clase de objeto `myUnixAccount` se utiliza cuando se usa la clase de objeto `posixAccount`.

```
objectclassMap: passwd:posixAccount=myUnixAccount
```

Perfiles de cliente LDAP

Para simplificar la configuración del cliente y evitar tener que volver a introducir la misma información para todos los clientes, cree un único perfil de cliente en el servidor de directorios. De esta manera, un solo perfil define la configuración para todos los clientes configurados para utilizarlo. Cualquier modificación posterior para los atributos del perfil se propaga a los clientes en un tipo definido por el intervalo de actualización.

La información de configuración especificada en los perfiles del cliente LDAP se importa automáticamente en el repositorio SMF cuando se inicia el servicio `svc:/network/ldap/client`.

Los perfiles de clientes se deben almacenar en una ubicación conocida en el servidor LDAP. El DN raíz para el dominio especificado debe tener una clase de objeto de `nisDomainObject` y un atributo `nisDomain` que contiene el dominio del cliente. Todos los perfiles se encuentran en el contenedor `ou=profile` relacionado con este contenedor. Estos perfiles se deben poder leer en forma anónima.

Atributos de perfil de cliente LDAP

En la siguiente tabla, se muestran los atributos de perfil del cliente LDAP, que se pueden definir automáticamente al ejecutar `idsconfig`. Consulte "Cómo inicializar un cliente LDAP manualmente" en la página 194 y la página del comando man `idsconfig(1M)` para obtener información sobre cómo definir manualmente un perfil de cliente.

TABLA 9–2 Atributos de perfil de cliente LDAP

Atributo	Descripción
`cn`	Nombre del perfil. El atributo no tiene un valor predeterminado. El valor debe ser especificado.
`preferredServerList`	Las direcciones de host de los servidores preferidos es una lista separada por espacios de las direcciones del servidor. (No utiliza nombres de host). Los servidores de esta lista se prueban en orden *antes* que los de `defaultServerList` hasta que se realiza una conexión correcta. Esto no tiene valor predeterminado. Se debe especificar al menos un servidor en `preferredServerList` o `defaultServerList`.
`defaultServerList`	Las direcciones de host de los servidores predeterminados es una lista separada por espacios de las direcciones del servidor. (No utiliza nombres de host). Después de que se prueban los servidores de `preferredServerlist`, se prueban los servidores predeterminados de la subred del cliente, seguidos por los servidores predeterminados restantes, hasta que se realiza una conexión. Se debe especificar al menos un servidor en `preferredServerList` o `defaultServerList`. Los servidores de esta lista se prueban sólo después de los de la lista de servidores preferidos. Este atributo no tiene valor predeterminado.
`defaultSearchBase`	DN relativo en el que se localizan los contenedores conocidos. No hay valor predeterminado para este valor. Sin embargo, se puede cambiar por un determinado servicio por el atributo `serviceSearchDescriptor`.
`defaultSearchScope`	Define el ámbito de una base de datos de búsqueda de un cliente. Se puede sustituir por el atributo `serviceSearchDescriptor`. Los valores posibles son `one` o `sub`. El valor predeterminado es el nivel de búsqueda `one`.
`authenticationMethod`	Identifica el método de autenticación utilizado por el cliente. No hay valor predeterminado (anónimo). Consulte "Selección de métodos de autenticación para el servicio de nombres LDAP" en la página 146 para obtener más información.
`credentialLevel`	Identifica el tipo de credenciales que el cliente debe utilizar para autenticar. Las opciones son `anonymous`, `proxy` o `self` (también conocida como per-user). El valor predeterminado es `anonymous`.
`serviceSearchDescriptor`	Define cómo y dónde el cliente debe buscar una base de datos de nombres, por ejemplo, si el cliente debe buscar en uno o más puntos en el DIT. De manera predeterminada, no hay SSD predefinidos.
`serviceAuthenticationMethod`	Método de autenticación utilizado por un cliente para el servicio especificado. De manera predeterminada, no hay métodos de autenticación de servicios definidos. Si un servicio no tiene `serviceAuthenticationMethod` definido, se establecerá como predeterminado para el valor de `authenticationMethod`.

TABLA 9–2 Atributos de perfil de cliente LDAP *(Continuación)*

Atributo	Descripción
`attributeMap`	Asignaciones de atributo utilizadas por el cliente. De manera predeterminada, `attributeMap` no está definido.
`objectclassMap`	Asignaciones de clase de objeto utilizadas por el cliente. `objectclassmap` está definido como predeterminado.
`searchTimeLimit`	Tiempo máximo [en segundos] que el cliente debe permitir para realizar la búsqueda antes de un intervalo. Esto no afecta al tiempo que el servidor LDAP permitirá para que se complete la búsqueda. El valor predeterminado es `30` segundos.
`bindTimeLimit`	Tiempo máximo, en segundos, que el cliente debe permitir para vincular con un servidor antes de un intervalo. El valor predeterminado es de `30` segundos.
`followReferrals`	Especifica si un cliente debe seguir una referencia de LDAP. Los valores posibles son `TRUE` o `FALSE`. El valor predeterminado es `TRUE`.
`profileTTL`	Tiempo entre actualizaciones del perfil de cliente del servidor LDAP por `ldap_cachemgr(1M)`. El valor predeterminado es `43200` segundos o 12 horas. Si tiene un valor de 0, el perfil nunca se actualizará.

Atributos locales del cliente LDAP

En la siguiente tabla, se muestran los atributos del cliente LDAP que se puede definir de forma local por medio del comando `ldapclient`. Consulte la página del comando man `ldapclient(1M)` para obtener más información.

TABLA 9–3 Atributos locales del cliente LDAP

Atributo	Descripción
`adminDN`	Especifica el nombre distintivo del administrador la entrada para la credencial de administración. Si el valor del conmutador `enableShadowUpdate` es `true` en el sistema cliente, y `credentialLevel` tiene un valor diferente de `self`, entonces se debe especificar `adminDN`.
`adminPassword`	Especifica la contraseña de la entrada del administrador para la credencial de administración. Si el valor del conmutador `enableShadowUpdate` es `true` en el sistema cliente, y `credentialLevel` tiene un valor diferente de `self`, entonces se debe especificar `adminPassword`.
`domainName`	Especifica el nombre de dominio del cliente (que se convierte en el dominio predeterminado para el sistema cliente). Este atributo no tiene un valor predeterminado y se debe especificar.

TABLA 9–3 Atributos locales del cliente LDAP *(Continuación)*

Atributo	Descripción
`proxyDN`	Nombre distintivo de proxy. Si el sistema cliente se configura con `credentialLevel` de `proxy`, `proxyDN` se debe especificar.
`proxyPassword`	Contraseña del proxy. Si el sistema cliente se configura con `credentialLevel` de proxy, `proxyPassword` se debe especificar.
`certificatePath`	Directorio del sistema de archivos local que contiene las bases de datos de certificados. Si un sistema de cliente se configura con `authenticationMethod` o `serviceAuthenticationMethod` mediante TLS, se utiliza este atributo. El valor predeterminado es `/var/ldap`.

Nota – Si el `BaseDN` de un SSD *contiene una coma final*, se trata como un valor relativo del `defaultSearchBase`. Los valores del `defaultSearchBase` se agregan al `BaseDN` antes de realizar una búsqueda.

Daemon ldap_cachemgr

`ldap_cachemgr` es un daemon que se ejecuta en equipos cliente LDAP. El servicio `svc:/network/ldap/client` gestiona el daemon `ldap_cachemgr`, por lo que el servicio debe estar activado para que el daemon se ejecute correctamente. El daemon realiza las siguientes funciones clave.

- Obtiene acceso a los datos de configuración ejecutándose como `root`.
- Actualiza la configuración de cliente almacenada en los perfiles del servidor y extrae estos datos de los clientes.
- Mantiene una lista ordenada de servidores LDAP activos para utilizar.
- Mejora la eficacia de la consulta al tomar algunas solicitudes de consulta comunes realizadas por varios clientes.
- Mejora la eficacia de consultas de host.
- Si el conmutador `enableShadowUpdate` está establecido en `true`, obtiene acceso a la credencial del administrador configurada y realiza actualizaciones de los datos `shadow`.

Nota – `ldap_cachemgr` se debe estar ejecutando en todo momento para los servicios de nombres LDAP para trabajar.

Consulte la página del comando man `ldap_cachemgr(1M)` para obtener más información.

Modelo de seguridad de servicios de nombres LDAP

Los servicios de nombres LDAP pueden utilizar el repositorio LDAP de dos formas diferentes. Una es como una fuente del servicio de nombres y el servicio de autenticación. La otra es estrictamente como la fuente de datos de nombres. En esta sección, se tratan los conceptos de identidad de clientes, los métodos de autenticación, los módulos `pam_ldap` y `pam_unix_*`, y la gestión de cuentas cuando el repositorio LDAP se utiliza como un servicio de nombres y un servicio de autenticación. En esta sección, también se trata el uso de los servicios de nombres LDAP junto con el entorno de Kerberos (Parte VI, "Servicio Kerberos" de *Administración de Oracle Solaris 11.1: servicios de seguridad*) y los módulos `pam_krb5`(5).

Nota – Antes, si se activaba la gestión de cuentas `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación en cualquier momento que iniciaran sesión en el sistema. Por lo tanto, los inicios de sesión que no se basan en contraseña realizados con herramientas, como `ssh`, fallarán.

Realice la gestión de cuentas y recupere el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios como el usuario que inicia sesión. El nuevo control en el servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8` , que está activado de manera predeterminada.

Para cambiar este control por otro que no sea el predeterminado, agregue las instrucciones de control de acceso (ACI) en el servidor de directorios:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

Nota – Si utiliza Kerberos como sistema de autenticación y lo integra con el sistema de nombres LDAP, podrá para admitir un entorno de inicio de sesión único (SSO) en la compañía mediante Kerberos. También podrá utilizar el mismo sistema de identidad al realizar una consulta en los datos de nombres LDAP por usuario o por host.

Para acceder a la información del repositorio LDAP, los clientes pueden establecer primero la identidad con el servidor de directorios. Esta identidad puede ser anónima o como un host o usuario que es reconocido por el servidor LDAP. En función de la identidad del cliente y la información de control de acceso (ACI) del servidor, el servidor LDAP permitirá que el cliente

lea información del directorio. Para obtener más información sobre ACI, consulte la *Guía de administración* para la versión de Oracle Directory Server Enterprise Edition que está utilizando.

Si la identidad se basa en el host de donde proviene la solicitud, esto indica que está utilizando la autenticación proxy. Una vez que el host se autentica, todos los usuarios en ese host obtienen acceso. Si la identidad se basa en el usuario, esto indica que utiliza la autenticación per-user. Cada usuario en un host debe estar autenticado para obtener acceso.

Si el cliente se conecta de otra forma que no sea anónimo para cualquier solicitud determinada, el cliente debe demostrar su identidad en el servidor mediante un método de autenticación compatible con el cliente y el servidor. Una vez que el cliente estableció su identidad, puede realizar las distintas las solicitudes de LDAP.

Al iniciar sesión en un sistema, el servicio PAM puede utilizar información de la máquina local, del servicio LDAP, de un servidor Kerberos o de una combinación de los tres para decidir si el intento de inicio de sesión se realizará correctamente. Cuando se utiliza el módulo `pam_kerb`, la decisión de permitir el acceso es determinada por el servidor Kerberos. Cuando se utiliza el módulo `pam_ldap`, la mitad de la decisión debe proceder del servidor LDAP y la otra mitad proviene del host local. Con información del host local, utilizando los módulos `pam_unix_*`, la decisión se realiza de forma local.

Al utilizar `pam_ldap` para iniciar sesión mediante el servicio LDAP, hay una diferencia en cómo acceden al directorio el servicio de nombres y el servicio de autenticación (`pam_ldap`). El servicio de nombres lee las distintas entradas y sus atributos del directorio según una identidad predefinida. El servicio de autenticación establece si el usuario introdujo la contraseña correcta mediante el nombre y la contraseña del usuario para autenticarse en el servidor LDAP. Consulte la página del comando man `pam_ldap(5)` para obtener más información sobre el servicio de autenticación.

Cuando se usa Kerberos para realizar la autenticación y cuando la autenticación en servicios de nombres LDAP también está activada (como se requiere para el modo por usuario), Kerberos puede proporcionar funciones duales. Kerberos se autentica en el servidor y la identidad Kerberos para el principal (usuario o un host) se utiliza para autenticarse en el directorio. En este modo, la misma identidad de usuario que se utiliza para autenticarse en el sistema, también se utiliza para autenticarse en el directorio para consultas y actualizaciones. Los administradores pueden utilizar información de control de acceso (ACI) en el directorio para limitar los resultados fuera del servicio de nombres, si lo desean.

Seguridad de la capa de transporte

La seguridad de la capa de transporte (TLS) se puede utilizar para proteger la comunicación entre un cliente LDAP y el servidor de directorios, y proporciona privacidad e integridad de los datos. El protocolo TLS es un superconjunto del protocolo Capa de sockets seguros (SSL). Los servicios de nombres LDAP admiten conexiones TLS. Tenga en cuenta que con SSL agrega carga en el servidor de directorios y el cliente.

Deberá configurar el servidor de directorios para SSL. Para obtener más información sobre la configuración de Oracle Directory Server Enterprise Edition para SSL, consulte la Guía de administración para la versión de Oracle Directory Server Enterprise Edition para que está utilizando. También deberá configurar el cliente LDAP para SSL.

Si utiliza TLS, las bases de datos de seguridad necesarias deben estar instaladas. En concreto, se necesitan el certificado y los archivos clave de la base de datos. Por ejemplo, si utiliza un formato de base de datos más antiguo desde Netscape Communicator, dos archivos, `cert7.db` y `key3.db`, son necesarios. O si utiliza un nuevo formato de base de datos desde Mozilla, tres archivos `cert8.db`, `key3.db` y `secmod.db`, son necesarios. El archivo `cert7.db` o el archivo `cert8.db` contienen certificados de confianza. El archivo `key3.db` contiene las claves del cliente. Incluso si el servicio de nombres LDAP no utiliza las claves del cliente, este archivo debe estar presente. El archivo `secmod.db` contiene el los módulos de seguridad, como el módulo `PKCS#11`. Este archivo no es necesario si se utiliza el formato antiguo.

Para obtener más información, consulte "Configuración de seguridad TLS" en la página 196.

Asignación de niveles de credencial de cliente

Los clientes de servicios de nombres LDAP se autentican en el servidor LDAP de acuerdo con el nivel de credencial de un cliente. Los clientes LDAP pueden tener varios niveles asignados para autenticarse en un servidor de directorios.

- `anonymous`
- `proxy`
- `proxy anonymous`
- `self` (denominado per-user en este documento)

Nivel de credencial anonymous de LDAP

Si utiliza el acceso `anonymous`, sólo puede acceder a los datos que están disponibles para todos. En modo anonymous, no se realiza una operación LDAP BIND. También debe tener en cuenta las consecuencias en la seguridad. El acceso `anonymous` a determinadas partes del directorio implica que cualquier usuario con acceso al directorio tiene acceso de lectura. Si utiliza un nivel de credencial `anonymous`, debe permitir acceso de lectura a todas las entradas y los atributos de nombres LDAP.

Precaución – Nunca se debe permitir la escritura `anonymous` en un directorio, ya que cualquiera puede cambiar información en el DIT al que tiene acceso de escritura, incluidas las contraseñas de otros usuarios o su propia identidad.

Nota – Oracle Directory Server Enterprise Edition le permite restringir el acceso basándose en direcciones IP, un nombre DNS, un método de autenticación, y la hora del día. Es posible que desee limitar el acceso con más restricciones. Para obtener más información, consulte "Gestión de control de acceso" en la *Guía de administración* para la versión de Oracle Directory Server Enterprise Edition que está utilizando.

Nivel de credencial proxy de LDAP

El cliente se autentica o se enlaza con un único conjunto compartido de credenciales de enlace LDAP, también conocido como cuenta proxy. Esta cuenta proxy puede ser cualquier entrada que puede vincularse al directorio. Esta cuenta proxy necesita acceso suficiente para realizar las funciones del servicio de nombres en el servidor LDAP. La cuenta proxy es un recurso compartido por sistema. Es decir, cada usuario que ha iniciado sesión en un sistema mediante acceso proxy, incluido el usuario root, ve los mismos resultados que todos los demás usuarios de ese sistema. Necesita configurar `proxyDN` y `proxyPassword` en cada cliente utilizando el nivel de credencial `proxy`. La contraseña cifrada `proxyPassword` se almacena localmente en el cliente. Puede configurar distintos proxies para los diferentes grupos de clientes. Por ejemplo, puede configurar un proxy para todos los clientes de ventas para acceder a los directorios a los que puede acceder toda la compañía y los de ventas, al mismo tiempo que evita que los clientes de ventas accedan a directorios de recursos humanos con información de nómina. O, en los casos más extremos, puede asignar diferentes proxies a cada cliente o asignar un solo proxy para todos los clientes. Una implementación LDAP típica probablemente estará entre los dos extremos. Tenga en cuenta las opciones cuidadosamente. Muy pocos agentes proxy pueden limitar la capacidad para controlar el acceso del usuario a los recursos. Sin embargo, tener demasiados proxy complican la configuración y el mantenimiento del sistema. Necesita otorgar los derechos apropiados para el usuario de proxy, según el entorno. Consulte "Almacenamiento de credenciales de clientes LDAP" en la página 146 para obtener información acerca de cómo determinar el método de autenticación más adecuado para su configuración.

Si se cambia la contraseña para un usuario de proxy, debe actualizarla en cada cliente que utiliza ese usuario proxy. Si utiliza caducidad de las contraseñas en cuentas LDAP, asegúrese de desactivar la opción para usuarios proxy.

Nota – Tenga en cuenta que el nivel de credencial de proxy se aplica a todos los usuarios y los procesos de cualquier sistema determinado. Si dos usuarios necesitan utilizar diferentes políticas de nombres, deben utilizar diferentes equipos o deben utilizar el modelo de autenticación por usuario.

Además, si los clientes utilizan una credencial `proxy` para autenticarse, el `proxyDN` debe tener el mismo `proxyPassword` en todos los servidores.

Nivel de credencial proxy anonymous de LDAP

`proxy anonymous` es una entrada de varios valores, ya que tiene más de un valor de credenciales definido. Un cliente asignado al nivel `proxy anonymous` intentará primero autenticarse con su identidad proxy. Si el cliente no puede autenticarse como usuario de proxy por algún motivo (bloqueo de usuario, contraseña caducada, por ejemplo) utilizará el acceso anónimo. Esto podría resultar en un nivel de servicio diferente, según cómo está configurado el directorio.

Autenticación per-user de LDAP

La autenticación por usuario (self) utiliza la identidad de Kerberos (principal) para realizar una consulta por cada usuario o cada sistema al autenticarse en el servidor de directorios. Con autenticación por usuario, el administrador del sistema puede utilizar la instrucción de control de acceso (ACI), las listas de control de acceso (ACL), los roles, los grupos u otros mecanismos de control de acceso al directorio para otorgar o denegar el acceso a los datos del servicio de nombres de usuarios o sistemas específicos.

Nota – Al configurar el modo por usuario, el valor de configuración para activar este modo es "self", lo que indica el modo por usuario.

Para utilizar el modelo de autenticación por usuario, debe implementarse el servicio de inicio de sesión único de Kerberos. Además, uno o más servidores de directorios utilizados en la implementación deben admitir SASL y el mecanismo de autenticación SASL/GSSAPI. Debido a que Kerberos espera utilizar archivos y DNS para consultas de nombre de host, en lugar de LDAP, debe implementar DNS en este entorno. Además, para usar autenticación por usuario, `nscd` debe estar activado. El daemon `nscd` no es un componente opcional en esta configuración.

Conmutador enableShadowUpdate

Si el conmutador `enableShadowUpdate` está establecido en `true` en el cliente, las credenciales de administrador se utilizarán para actualizar los datos shadow. Los datos shadow se almacenan en la clase de objeto `shadowAccount`, en el servidor de directorios. Las credenciales de administrador son definidas por los valores de los atributos `adminDN` y `adminPassword`, como se describe en "Atributos locales del cliente LDAP" en la página 139. Estas credenciales de administración no se utilizan para ningún otro fin.

Las credenciales de administración tienen propiedades similares a las credenciales `Proxy`. La excepción es que para las credenciales de administración, el usuario debe tener todos los privilegios para la zona o tener un UID eficaz de `root` para leer o actualizar los datos shadow. Las credenciales de administración se pueden asignar a cualquier entrada que se puede vincular al directorio. Sin embargo, *no* utilice la misma identidad del gestor de directorios (`cn=Directory Manager`) del servidor LDAP.

Esta entrada con credenciales de administración debe tener acceso suficiente para leer y escribir los datos shadow en el directorio. Debido a que la entrada es un recurso compartido por sistema, los atributos `adminDN` y `adminPassword`, se deben configurar en cada cliente. La

contraseña cifrada `adminPassword` se almacena localmente en el cliente. La contraseña utiliza los mismos métodos de autenticación que se han configurado para el cliente. Las credenciales de administración son usadas por todos los usuarios y los procesos de un sistema determinado para leer y actualizar datos shadow.

Almacenamiento de credenciales de clientes LDAP

Si configura un cliente para que use una identidad proxy, el cliente guarda la información del proxy en el servicio `svc:/network/ldap/client`. La implementación LDAP actual no almacena credenciales proxy en el perfil de un cliente. Las credenciales proxy establecidas mediante `ldapclient` durante la inicialización se almacenan en el repositorio SMF. Esto tiene como resultado una mejor seguridad en la información de DN de proxy y contraseña. Consulte el Capítulo 12, “Configuración de clientes LDAP (tareas)” para obtener información sobre la configuración de perfiles de cliente.

De modo similar, si configura un cliente para activar las actualizaciones de datos shadow, y el nivel de credencial del cliente no es `self`, el cliente guarda la información en el servicio `svc:/network/ldap/client`.

Si configura un cliente utilice autenticación por usuario, la identidad Kerberos y la información de ticket Kerberos para cada principal (cada usuario o host) se utilizan durante la autenticación. En este entorno el servidor de directorios asigna el principal de Kerberos para un DN y la credenciales de Kerberos se utilizan para autenticar a ese DN. El servidor de directorios puede, entonces, utilizar sus mecanismos de instrucción de control de acceso (ACI) para permitir o denegar el acceso a los datos del servicio de nombres. En esta situación, el ticket de información Kerberos se utiliza para autenticarse en el servidor de directorios y el sistema no almacena autenticación DN o las contraseñas en el sistema. Por consiguiente, en este tipo de configuración, no es necesario que especifique los atributos `adminDN` y `adminPassword` cuando el cliente se inicializa con el comando `ldapclient`.

Selección de métodos de autenticación para el servicio de nombres LDAP

Al asignar el nivel de credencial `proxy` o `proxy-anonymous` a un cliente, también tiene que seleccionar un método para que el proxy se autentique en el servidor de directorios. De manera predeterminada, el método de autenticación es `none`, que implica el acceso anónimo. El método de autenticación también es posible que tenga una opción de seguridad de transporte asociada.

El método de autenticación, como el nivel de credencial, puede tener varios valores. Por ejemplo, en el perfil de cliente puede especificar que el cliente primero intente vincular con el método`simple` protegido por TLS. Si no funciona, el cliente deberá intentar vincular con el método `sasl/digest-MD5`. El `authenticationMethod` sería `tls:simple;sasl/digest-MD5`.

Los servicios de nombres LDAP admiten algunos mecanismos de Autenticación sencilla y capa de seguridad (SASL). Estos mecanismos permiten un intercambio de contraseña seguro sin necesidad de TLS. Sin embargo, estos mecanismos no proporcionan integridad de los datos o privacidad. Consulte la RFC 2222, para obtener información sobre SASL.

Los siguientes mecanismos de autenticación son compatibles.

- `none`

  El cliente no se autentica en el directorio. Es equivalente al nivel de credencial `anonymous`.

- `simple`

  Si el sistema cliente utiliza el método de autenticación `simple`, vincula con el servidor enviando la contraseña de usuario sin cifrar. La contraseña está, por lo tanto, sujeta a ser vista a menos que la sesión esté protegida por IPsec. Las ventajas principales de utilizar el método de autenticación `simple` son que todos los servidores de directorios lo admiten y que es fácil de configurar.

- `sasl/digest-MD5`

  La contraseña de cliente está protegida durante la autenticación, pero la sesión no está cifrada. Algunos servidores de directorios, incluidos Oracle Directory Server Enterprise Edition, también admiten el método de autenticación `sasl/digest-MD5`. La principal ventaja de `digest-MD5` es que la contraseña no se transmite sin cifrar durante la autenticación y, por lo tanto, es más seguro que el método de autenticación `simple`. Consulte la RFC 2831 para obtener información sobre `digest-MD5`. `digest-MD5` se considera una mejora de `cram-MD5` por su seguridad mejorada.

  Cuando se utiliza `sasl/digest-MD5`, la autenticación es segura, pero la sesión no está protegida.

  Nota – Si está utilizando Oracle Directory Server Enterprise Edition, la contraseña *se debe almacenar sin cifrar* en el directorio.

- `sasl/cram-MD5`

  En este caso, la sesión LDAP no está cifrada, pero la contraseña del cliente está protegida durante la autenticación, ya que se realiza mediante `sasl/cram-MD5`. Este método de autenticación está obsoleto y no debe usarse.

- `sasl/GSSAPI`

  Este método de autenticación se utiliza junto con el modo de credencial self para activar las consultas por usuario. Un nscd por usuario asignado para poder utilizar las credenciales del cliente se vincula con el servidor de directorios usando el método sasl/GSSAPI y las credenciales de cliente de Kerberos. El acceso se puede controlar en el servidor de directorios por usuario.

- `tls:simple`

El cliente se vincula mediante el método `simple` y la sesión está cifrada. La contraseña está protegida.

- `tls:sasl/cram-MD5`

  La sesión LDAP está cifrada y el cliente se autentica con el servidor de directorios mediante `sasl/cram-MD5`.

- `tls:sasl/digest-MD5`

  La sesión LDAP está cifrada y el cliente se autentica con el servidor de directorios mediante `sasl/digest-MD5`.

Precaución – Oracle Directory Server Enterprise Edition requiere que las contraseñas se almacenen sin cifrar para utilizar `digest-MD5`. Si el método de autenticación está definido en `sasl/digest-MD5` o `tls:sasl/digest-MD5`, las contraseñas para el usuario proxy deberán almacenarse sin cifrar. Tenga especial cuidado en que el atributo `userPassword` tenga la ACI adecuada si está almacenado sin cifrar, de modo que no se pueda leer.

La siguiente tabla resume los diferentes métodos de autenticación y sus respectivas características.

TABLA 9–4 Métodos de autenticación

	Enlace	Transferencia de contraseña	Contraseña en Oracle Directory Server Enterprise Edition	Sesión
`none`	No	N/A	N/A	Sin cifrado
`simple`	Sí	Sin cifrar	Cualquiera	Sin cifrado
`sasl/digest-MD5`	Sí	Cifrado	Sin cifrar	Sin cifrado
`sasl/cram-MD5`	Sí	Cifrado	N/A	Sin cifrado
`sasl/GSSAPI`	Sí	Kerberos	Kerberos	Cifrado
`tls:simple`	Sí	Cifrado	Cualquiera	Cifrado
`tls:sasl/cram-MD5`	Sí	Cifrado	N/A	Cifrado
`tls:sasl/digest-MD5`	Sí	Cifrado	Sin cifrar	Cifrado

Especificación de métodos de autenticación para servicios específicos en LDAP

El método de autenticación se puede especificar para un servicio determinado en el atributo `serviceAuthenticationMethod`. Los siguientes servicios permiten la selección del método de autenticación:

- `passwd-cmd`

  Este servicio es utilizado por `passwd(1)` para cambiar la contraseña de inicio de sesión y los atributos de contraseña.

- `keyserv`

  Este servicio es utilizado por las utilidades `chkey(1)` y `newkey(1M)` para crear y cambiar el par de claves Diffie-Hellman de un usuario.

- `pam_ldap`

  Este servicio se utiliza para autenticar usuarios con `pam_ldap(5)`.

  `pam_ldap` admite la gestión de cuentas.

Nota – Si el servicio no tiene un `serviceAuthenticationMethod` definido, se establecerá el valor del atributo `authenticationMethod` de manera predeterminada.

Nota – En modo per-user, "Módulo de servicio Kerberos" en la página 151 (pam Kerberos) se utiliza como el servicio de autenticación. `ServiceAuthenticationMethod` no es necesario en este modo de operación.

Nota – Si el conmutador `enableShadowUpdate` está establecido en `true`, el daemon `ldap_cachemgr` se enlaza al servidor LDAP mediante el método de autenticación definido en el parámetro `serviceAuthenticationMethod` de `passwd-cmd` si el método está definido. De lo contrario, se utiliza `authenticationMethod`. El daemon no usará el método de autenticación `none`.

El siguiente ejemplo muestra una sección de un perfil de cliente en el que los usuarios utilizarán sasl/digest-MD5 para autenticarse en el servidor de directorios, pero utilizarán una sesión de SSL para modificar su contraseña.

```
serviceAuthenticationMethod=pam_ldap:sasl/digest-MD5
serviceAuthenticationMethod=passwd-cmd:tls:simple
```

Métodos de autenticación conectables

Mediante la estructura PAM, puede elegir entre varios servicios de autenticación, incluidos los módulos `pam_unix_*`, `pam_krb5` y `pam_ldap_*`.

Si se utiliza el método de autenticación por usuario, `pam_krb5`, el servicio de autenticación más fuerte de los tres mencionados más arriba, debe estar activado. Consulte `pam_krb5(5)` y *Administración de Oracle Solaris 11.1: servicios de seguridad*.

El sistema de autenticación pam_krb5 se puede utilizar incluso si la autenticación por usuario no está activada. Si se utilizan los niveles de credencial de proxy o anonymous para acceder a los datos del servidor de directorios, entonces, no es posible restringir el acceso a los datos del directorio por usuario.

Debido a su mayor flexibilidad, la compatibilidad con métodos de autenticación más seguros y la capacidad para usar la gestión de cuentas, el uso del módulo pam_ldap es preferible al uso de los módulos pam_unix_* cuando se utilizan los métodos de autenticación anonymous o proxy.

Módulos de servicio pam_unix_*

Si no ha cambiado el archivo /etc/pam.conf, la autenticación UNIX está activada de manera predeterminada.

Nota – El módulo pam_unix se ha eliminado y ya no es compatible con la versión Oracle Solaris. Un conjunto de otros módulos de servicios proporciona una funcionalidad mayor o equivalente. Por lo tanto, en esta guía, pam_unix hace referencia a la funcionalidad equivalente, no al módulo pam_unix en sí.

A continuación, se muestra una lista de los módulos que proporcionan el equivalente al módulo pam_unix original.

pam_authtok_check(5)
pam_authtok_get(5)
pam_authtok_store(5)
pam_dhkeys(5)
pam_passwd_auth(5)
pam_unix_account(5)
pam_unix_auth(5)
pam_unix_cred(5)
pam_unix_session(5)

Los módulos pam_unix_* siguen el modelo tradicional de autenticación UNIX, como se describe en la siguiente lista.

1. El cliente recupera la contraseña cifrada del usuario del servicio de nombres.
2. Se le pedirá al usuario la contraseña de usuario.
3. La contraseña de usuario está cifrada.
4. El cliente compara las dos contraseñas cifradas para determinar si el usuario debe autenticarse.

Adicionalmente, hay dos restricciones cuando se usan los módulos pam_unix_*.

- La contraseña se debe almacenar en formato UNIX `crypt` y no con otros métodos de cifrado, incluido sin cifrar.
- El atributo `userPassword` debe ser legible por el servicio de nombres.

  Por ejemplo, si define el nivel de credencial en `anonymous`, todos los usuarios deben poder leer el atributo `userPassword`. De manera similar, si define el nivel de credencial en `proxy`, el usuario proxy debe poder leer el atributo `userPassword`.

Nota – La autenticación UNIX no es compatible con el método de autenticación `sasl digest-MD5`, ya que Oracle Directory Server Enterprise Edition requiere que las contraseñas se almacenen sin cifrar para utilizar `digest-MD5`. La autenticación UNIX requiere que la contraseña se almacene en formato `crypt`.

Nota – El módulo `pam_unix_account` admite la gestión de cuentas cuando el conmutador `enableShadowUpdate` está establecido en `true`. Los controles para una cuenta de usuario LDAP remota se aplican del mismo modo que se aplican los controles a una cuenta de usuario local que se define en los archivos `passwd` y `shadow`. En el modo `enableShadowUpdate`, para la cuenta LDAP, el sistema actualiza y utiliza los datos shadow del servidor LDAP para la caducidad de la contraseña y el bloqueo de cuenta. Por supuesto que los datos shadow de la cuenta local sólo se aplican al sistema de cliente local, mientras que los datos shadow de una cuenta de usuario LDAP se aplica a al usuario en todos los sistemas cliente.

Comprobación del historial de la contraseña sólo se admite para el cliente local, no para una cuenta de usuario LDAP.

Módulo de servicio Kerberos

Consulte la página del comando man `pam_krb5`(5) y *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Módulo de servicio LDAP

Al implementar la autenticación LDAP, el usuario se enlaza al servidor LDAP mediante el método de autenticación definido en el parámetro `serviceAuthenticationMethod` de `pam_ldap` si existe uno. De lo contrario, se utiliza `authenticationMethod`.

Si `pam_ldap` puede vincularse al servidor con la identidad del usuario y contraseña proporcionados, autentifica al usuario.

Nota – Antes, si se activaba la gestión de cuentas `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación en cualquier momento que iniciaran sesión en el sistema. Por lo tanto, los inicios de sesión que no se basan en contraseña realizados con herramientas, como `ssh`, fallarán.

Realice la gestión de cuentas y recupere el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios como el usuario que inicia sesión. El nuevo control en el servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8` , que está activado de manera predeterminada.

Para cambiar este control por otro que no sea el predeterminado, agregue las instrucciones de control de acceso (ACI) en el servidor de directorios:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

`pam_ldap` no lee el atributo `userPassword`. Por lo tanto, no es necesario otorgar acceso para leer el atributo `userPassword`, a menos que haya otros clientes que utilicen la autenticación UNIX. Además, `pam_ldap` no admite el método de autenticación `none`. Por lo tanto, debe definir los atributos `serviceAuthenticationMethod` o `authenticationMethod` para que los clientes puedan usar `pam_ldap`. Consulte la página del comando man `pam_ldap(5)` para obtener más información.

Precaución – Si se utiliza el método de autenticación `simple`, el atributo `userPassword` puede ser leído en la transferencia por terceros.

En la tabla siguiente, se resumen las diferencias principales entre los mecanismos de autenticación.

TABLA 9–5 Comportamiento de autenticación en LDAP

Evento	pam_unix_*	pam_ldap	pam_krb5
Contraseña enviada	Utiliza el método de autenticación de servicio `passwd`	Utiliza el método de autenticación de servicio `passwd`	Utiliza el inicio de sesión único de Kerberos en tecnología, no las contraseñas

TABLA 9–5 Comportamiento de autenticación en LDAP *(Continuación)*

Evento	pam_unix_*	pam_ldap	pam_krb5
Nueva contraseña enviada	Cifrada	Sin cifrado (a menos que utilice TLS)	Utiliza Kerberos, no se transmiten contraseñas
Nueva contraseña almacenada	Formato `crypt`	Esquema de almacenamiento de contraseñas definido en Oracle Directory Server Enterprise Edition	Las contraseñas son gestionadas por Kerberos
¿Requiere lectura de contraseña?	Sí	No	No
Compatibilidad `sasl/digest-MD5` después de cambiar la contraseña	No. Contraseña no está almacenada en `clear`. El usuario no puede autenticarse.	Sí. Siempre que esquema de almacenamiento predeterminado se establezca en `clear`, el usuario puede autenticarse.	No. Se utiliza `sasl/GSSAPI`. No se transfieren contraseñas a través y no hay contraseñas para almacenar en el servidor de directorios, excepto cuando se utiliza un kdc de Kerberos que gestiona su base de datos de contraseñas en el servidor de directorios LDAP.
¿Política de contraseñas admitida?	Sí. `enableShadowUpdate` debe estar establecido en `true`.	Sí, si se ha configurado esta opción.	Consulte `pam_krb5(5)`, Módulo de gestión de cuentas de Kerberos V5.

PAM y cambio de contraseñas

Utilice el comando `passwd` para cambiar una contraseña. Si el conmutador `enableShadowUpdate` no está establecido en `true`, el atributo `userPassword` debe poder ser escrito por el usuario. Si el conmutador `enableShadowUpdate` se establece en `true`, las credenciales de administración debe poder actualizar el atributo `userPassword`. Recuerde que el `serviceAuthenticationMethod` para `passwd-cmd` sustituye el `authenticationMethod` de esta operación. En función del método de autenticación que se utiliza, la contraseña actual se puede transmitir sin cifrar.

En el caso de la autenticación UNIX, el nuevo atributo `userPassword` se cifra usando el formato `crypt` de UNIX y se etiqueta antes de ser escrito en LDAP. Por lo tanto, la nueva contraseña se cifra en la transferencia, independientemente del método de autenticación utilizado para vincular con el servidor. Consulte la página del comando man `pam_authtok_store(5)` para obtener más información.

Si el conmutador `enableShadowUpdate` está establecido en `true`, los módulos `pam_unix_*` también actualizan la información shadow relacionada cuando se cambia la contraseña de

usuario. Los módulos `pam_unix_*` actualizan los mismos campos `shadow` en los archivos `shadow` locales que los módulos actualizan cuando se cambia la contraseña de usuario local.

`pam_ldap` ya no admite la actualización de la contraseña. El `pam_authtok_store` con la opción `server_policy` ahora reemplaza la capacidad de actualización de contraseña de `pam_ldap`. Al utilizar `pam_authtok_store`, la nueva contraseña se envía al servidor LDAP sin cifrar. Por lo tanto, para garantizar la privacidad, utilice TLS. Si TLS no se utiliza, la nueva `userPassword` puede ser espiada. Si establece una contraseña sin etiqueta con Oracle Directory Server Enterprise Edition, el software cifra la contraseña mediante el atributo `passwordStorageScheme`. Para obtener más información acerca de `passwordStorageScheme`, consulte la sección sobre la gestión de cuentas de usuario en la *Guía de administración* para la versión de Oracle Directory Server Enterprise Edition que está utilizando.

Nota – Debe tener en cuenta los siguientes problemas de configuración al establecer el atributo `passwordStorageScheme`. Si un NIS u otro cliente que usan la autenticación UNIX están utilizando LDAP como repositorio, `passwordStorageScheme` debe ser `crypt`. Además, si se usa la autenticación LDAP con `sasl/digest-MD5` con Oracle Directory Server Enterprise Edition, `passwordStorageScheme` se debe establecer en clear.

Gestión de cuentas de LDAP

Si selecciona `pam_krb5` como su sistema de gestión de cuenta y contraseña, el entorno Kerberos gestionará todas la cuentas, las contraseñas, el bloqueo de cuentas y otros detalles de gestión de cuentas. Consulte la página del comando man `pam_krb5(5)` y *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Si no utiliza `pam_krb5`, los servicios de nombres LDAP se pueden configurar para aprovechar el soporte de la directiva de bloqueo de contraseña y cuenta en Oracle Directory Server Enterprise Edition. Puede configurar `pam_ldap(5)` para admitir la gestión de cuentas de usuario. `passwd(1)` aplica reglas de sintaxis de contraseña establecidas por la política de contraseñas de Oracle Directory Server Enterprise Edition cuando se utiliza con la configuración de PAM adecuada.

Las siguientes funciones de gestión de cuentas se admiten mediante `pam_ldap(5)`. Estas funciones dependen de la configuración de la directiva de bloqueo de contraseña y cuenta de Oracle Directory Server Enterprise Edition. Puede activar las funciones que desee.

- Notificación de fecha de la contraseña y caducidad

  Los usuarios deben cambiar sus contraseñas en función de la programación. Una contraseña caduca si no se cambia en el tiempo configurado. Una contraseña caducada hace que la autenticación del usuario falle.

  Los usuarios ven un mensaje de advertencia siempre que inician sesión en el período de advertencia de caducidad. El mensaje especifica el número de días u horas que faltan para que caduque la contraseña.

- Comprobación de la sintaxis de la contraseña

  Las nuevas contraseñas deben cumplir con los requisitos de longitud mínima de la contraseña. Además, una contraseña no puede coincidir con el valor de los atributos `uid`, `cn`, `sn` o `mail` en la entrada de directorio del usuario.

- Comprobación de contraseñas en el historial

  Los usuarios no pueden reutilizar las contraseñas. Si un usuario intenta cambiar la contraseña por otra que se utilizó previamente, `passwd(1)` falla. Los administradores de LDAP pueden configurar la cantidad de contraseñas que se mantienen en la lista de historial del servidor.

- Bloqueo de cuenta de usuario

  Es posible bloquear una cuenta de usuario después de una determinada cantidad de fallas de autenticación repetidas. Un usuario también puede estar bloqueado si un administrador inactiva su cuenta. La autenticación seguirá fallando hasta que pase el tiempo de bloqueo de la cuenta o que el administrador vuelva a activarla.

Nota – Las funciones anteriores de gestión de cuentas sólo funcionan con Oracle Directory Server Enterprise Edition. Para obtener información sobre la configuración de la contraseña y la directiva de bloqueo de cuenta en el servidor, consulte el capítulo "Gestión de cuentas de usuario" en la Guía de administración para la versión de Oracle Directory Server Enterprise Edition que está utilizando. Consulte también “Ejemplo de archivo `pam_conf` que utiliza el módulo para gestión de cuentas `pam_ldap`” en la página 210. No active la gestión de cuentas para las cuentas `proxy`.

Antes de configurar la contraseña y la política de bloqueo de cuentas en Oracle Directory Server Enterprise Edition, asegúrese de que todos los hosts utilicen el cliente LDAP “más reciente” con la gestión de cuentas `pam_ldap`.

Además, asegúrese de que los clientes tengan un archivo `pam.conf(4)` configurado adecuadamente. De lo contrario, los servicios de nombres LDAP no funcionarán si caduca la contraseña `proxy` o de usuario.

Nota – Antes, si se activaba la gestión de cuentas `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación en cualquier momento que iniciaran sesión en el sistema. Por lo tanto, los inicios de sesión que no se basan en contraseña realizados con herramientas, como `ssh`, fallarán.

Realice la gestión de cuentas y recupere el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios como el usuario que inicia sesión. El nuevo control en el servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8` , que está activado de manera predeterminada.

Para cambiar este control por otro que no sea el predeterminado, agregue las instrucciones de control de acceso (ACI) en el servidor de directorios:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

Gestión de cuentas de LDAP con los módulos pam_unix_*

Si el conmutador `enableShadowUpdate` está establecido en `true` en el cliente, la funcionalidad de gestión de cuentas disponible para cuentas locales también está disponible para cuentas LDAP. La funcionalidad incluye la fecha de la contraseña, el vencimiento y la notificación de la cuenta, el inicio de sesión fallido del bloqueo de cuenta, etc. Además, ahora las opciones `-dluNfnwx` para el comando `passwd` se admiten en LDAP. Por lo tanto, todas las funciones del comando `passwd` y los módulos `pam_unix_*` en el servicio de nombres de los archivos se pueden usar en el servicio de nombres LDAP. El conmutador `enableShadowUpdate` ofrece una manera de implementar la gestión de cuentas de forma coherente para usuarios que están definidos en los archivos y en el ámbito LDAP.

Para evitar que los usuarios modifiquen sus propios datos de gestión de cuentas y, por lo tanto, eludan la directiva de contraseñas, el servidor LDAP está configurado para impedir al usuario el acceso de escritura a sus propios datos shadow en el servidor. Un administrador con credenciales de administración realiza las actualizaciones de datos shadow para un sistema cliente. Una configuración de ese tipo, sin embargo, entra en conflicto con el módulo `pam_ldap`, que requiere que las contraseñas puedan ser modificadas por los usuarios. Por lo tanto, la gestión de cuentas de `pam_ldap` y los módulos `pam_unix_*` son incompatibles.

Precaución – No utilice los módulos `pam_ldap` y los módulos `pam_unix_*` en el mismo dominio de nombres LDAP. Todos los clientes utilizan el módulo `pam_ldap` o todos los clientes utilizan los módulos `pam_unix_*`. Esta limitación podría indicar que usted necesita un servidor LDAP dedicado. Por ejemplo, una aplicación web o de correo electrónico puede esperar que los usuarios cambien sus propias contraseñas en el servidor LDAP.

La implementación de `enableShadowUpdate` también requiere que la credencial de administrador (`adminDN` y `adminPassword`) se almacene localmente en cada cliente. Esta información se almacena en el servicio `svc:/network/ldap/client`.

A diferencia de cuando se usa `pam_ldap` para la gestión de cuentas, el uso de los módulos `pam_unix_*` para la gestión de cuentas no requiere un cambio en el archivo `/etc/pam.conf`. El archivo `/etc/pam.conf` predeterminado es suficiente.

◆ ◆ ◆ CAPÍTULO 10

Requisitos de planificación para servicios de nombres LDAP (tareas)

En este capítulo se trata la planificación de alto nivel que debe hacer antes de comenzar los procesos de instalación y configuración del servidor y el cliente.

En este capítulo se tratan los siguientes temas.

Descripción general de la planificación de LDAP

El perfil de cliente LDAP es una recopilación de información de la configuración que un cliente LDAP utiliza para acceder a la información de los servicios de nombres LDAP sobre el servidor LDAP admitido. En este capítulo se trata la planificación de los distintos aspectos de los servicios de nombres LDAP. Estos aspectos incluyen el modelo de red, el árbol de información de directorios, el modelo de seguridad, los valores predeterminados de los distintos atributos de perfil y, por último, la preparación para completar los datos.

Planificación del modelo de red LDAP

Por cuestiones de disponibilidad y rendimiento, cada subred de toda la red de la compañía debe tener su propio servidor LDAP para servir a todos los clientes LDAP de la subred. Sólo uno de los servidores debe ser un servidor maestro LDAP. El resto podrían ser todas réplicas del servidor maestro.

Para planificar la configuración de red, tenga en cuenta cuántos servidores están disponibles, cómo un cliente podría llegar a los servidores, y en qué orden se debe acceder a los servidores. Si hay uno por subred, puede utilizar el atributo `defaultServerList` para mostrar una lista de todos los servidores y que el cliente LDAP ordene y manipule el orden de acceso. Si es necesario acceder a los servidores en un orden determinado debido a motivos de velocidad o gestión de datos, debe utilizar el atributo `preferredServerList` para definir el orden fijo de acceso a los servidores. `defaultServerList` trata todos los servidores de la lista por igual, mientras que los servidores de `preferredServerList` están en orden de prioridad, donde el primer servidor de la lista es el mejor servidor que se va a utilizar. La principal diferencia es que cuando se utiliza `preferredServerList`, el servidor disponible con la prioridad más alta se usa en otro servidor disponible de menor prioridad. En caso de que un servidor con la prioridad más alta esté disponible, la máquina cliente se desconecta del servidor con prioridad más baja. Cuando se utiliza `defaultServerList`, todos los servidores tienen la misma prioridad, y un servidor en línea no reemplaza a un servidor existente. Ambas listas se pueden utilizar en una configuración. Tenga en cuenta que posiblemente no desee colocar el servidor maestro en ninguna de estas listas para reducir la carga en el servidor maestro.

Además, puede encontrar tres atributos más que puede valer la pena tener en cuenta al planificar la configuración del servidor y la red. El atributo `bindTimeLimit` se puede utilizar para definir el valor de tiempo de espera para una solicitud de conexión TCP. El atributo `searchTimeLimit` se puede utilizar para definir el valor de tiempo de espera para una operación de búsqueda LDAP. El atributo `profileTTL` se puede utilizar para controlar la frecuencia con la que el cliente LDAP debe descargar su perfil de los servidores. Para una red lenta o inestable, los atributos `bindTimeLimit` y `searchTimeLimit` pueden necesitar un valor más alto que los predeterminados. Para las pruebas realizadas en las primeras etapas de la implementación, es posible que desee reducir el valor del atributo `profileTTL` para que los clientes incorporen los frecuentes cambios realizados en el perfil almacenado en los servidores LDAP.

Planificación del árbol de información de directorios

Los servicios de nombres LDAP tienen un árbol de información de directorios (DIT) predeterminado y un esquema asociado predeterminado. Por ejemplo, el contenedor `ou=people` contiene información de la cuenta de usuario, la contraseña y shadow. El contenedor `ou=hosts` contiene información acerca de los sistemas de la red. Cada entrada del contenedor `ou=people` sería de `objectclass` `posixAccount` y `shadowAccount`.

El DIT predeterminado es una estructura de directorios bien diseñada y basada en estándares abiertos. Para obtener más información, consulte RFC 2307bis y RFC 4876. El DIT

predeterminado suele ser suficiente para la mayoría de las necesidades de los servicios de nombres y se recomienda su uso sin necesidad de ninguna modificación. Si decide utilizar el DIT predeterminado, lo único que necesita decidir es desde qué nodo (DN de base) en el árbol de directorios se buscará la información de los servicios de nombres para un dominio determinado. Este nodo se especifica con el atributo `defaultSearchBase`. Además, es posible que desee establecer el atributo `defaultSearchScope` para indicar a los clientes el ámbito de consulta en el que se deben realizar las consulta de un servicio de nombres. ¿Es sólo buscar un nivel bajo el DN (uno) o todo el subárbol bajo el DN (sub)?

Hay veces, sin embargo, que más flexibilidad es necesaria para que el servicio de nombres LDAP funcione con un DIT existente o controle un DIT más complicado con los datos del servicio de nombres esparcidos por el árbol de directorios. Por ejemplo, puede haber entradas de cuenta de usuario en diferentes partes del árbol. Los atributos `serviceSearchDescriptor`, `attributeMap` y `objectclassMap` en el perfil del cliente están diseñados para gestionar estas situaciones.

Un descriptor de búsqueda de servicios puede utilizarse para ignorar la base de búsqueda predeterminada, el ámbito de búsqueda y el filtro de búsqueda de un servicio en particular. Consulte "Descriptores de búsqueda de servicios y asignación de esquemas" en la página 135.

Los atributos `attributeMap` y `objectclassMap` proporcionan una forma de asignación de esquemas. Hacen posible que los servicios de nombres LDAP trabajen con un DIT existente. Puede asignar la clase de objeto `posixAccount` a una clase de objeto existente, `myAccount`, por ejemplo. Puede asignar un atributo en la clase de objeto `posixAccount` a un atributo en la clase de objeto `myAccount`.

Varios servidores de directorios

Varios servidores LDAP pueden servir a un DIT. Por ejemplo, algunos subárboles de DIT residen en otros servidores LDAP. En ese caso, un servidor LDAP puede derivar al cliente LDAP a un servidor diferente para obtener los datos del servicio de nombres que conoce pero no está en su base de datos. Si planifica este tipo de configuración de DIT, debe establecer el atributo del perfil de cliente `followReferrals` para indicarle al servicio de nombres LDAP que siga las referencias del servidor para continuar las consultas del servicio de nombres. Sin embargo, es mejor que todos los datos del servicio de nombres de un dominio residan en un solo servidor de directorios, si es posible.

Las referencias pueden ser útiles si desea que los clientes accedan a las réplicas de sólo lectura la mayor parte del tiempo y sigan las referencias a un servidor maestro de lectura/escritura sólo cuando sea necesario. De esta forma, el servidor maestro no se sobrecarga con solicitudes que pueden controlar las réplicas.

Uso compartido de los datos con otras aplicaciones

Para hacer un mejor uso de LDAP, debe tener una única entrada de LDAP para cada entrada lógica. Por ejemplo, para un usuario, usted no sólo puede tener información de páginas blancas de la compañía, sino que también puede tener información de cuentas y posiblemente datos específicos de aplicaciones. Dado que `posixAccount` y `shadowAccount` son clases de objeto auxiliares, se pueden agregar a cualquier entrada del directorio. Esta opción necesita una cuidadosa planificación, configuración y administración.

Selección del sufijo del directorio

Consulte la documentación de Oracle Directory Server Enterprise Edition para obtener información acerca de cómo elegir un sufijo de directorio adecuado.

Servidores LDAP y de réplica

Hay tres diferentes estrategias para emplear al configurar servidores de réplica.

- Replicación de maestro único
- Replicación de maestro flotante
- Replicación de varios maestros

Maestro único

Con la replicación de maestro único, sólo un servidor maestro de una red de partición o no particionada determinada conserva las copias de las entradas de directorio que se pueden escribir. Cualquier servidor de réplica tiene copias de sólo lectura de las entradas de directorio. Mientras que las réplicas y los maestros pueden realizar operaciones de búsqueda, comparación y vinculación, sólo el servidor maestro puede realizar operaciones de escritura.

La desventaja potencial para la estrategia de la replicación de maestro único es que el servidor maestro es un único punto de fallo. Si el servidor maestro no funciona, ninguna de las réplicas puede procesar las operaciones de escritura.

Maestro flotante

La estrategia del maestro flotante es similar a la estrategia de maestro único ya que sólo hay un servidor maestro con capacidades de escritura en un momento determinado para una red particionada o no particionada. Sin embargo, al implementar la estrategia del maestro flotante, cuando el servidor maestro no funciona, una réplica se transforma automáticamente en un servidor maestro por medio de un algoritmo.

Una desventaja posible de la estrategia de replicación del maestro flotante es que, si la red pasa a ser particionada y las réplicas de cada partición se convierten en maestros, el proceso de conciliación de los nuevos maestros puede ser muy complicado al volver a ingresar a la red.

Varios maestros

Con la replicación de varios maestros, hay varios servidores maestros con sus propias copias de lectura y escritura de los datos de las entradas de directorio. Mientras que la estrategia de varios maestros elimina el problema de tener un único punto de fallo, se pueden presentar conflictos de actualización entre los servidores. En otras palabras, si el atributo de una entrada se modifica alrededor de la misma hora en dos maestros, puede presentarse una política de resolución de conflictos de actualización, como "el último escritor gana".

Para obtener información sobre el modo de configurar servidores de réplica, consulte la *Guía de administración* para la versión de Oracle Directory Server Enterprise Edition que esté utilizando. En general, para las implementaciones empresariales a gran escala, la replicación de varios maestros es la opción recomendada.

Planificación del modelo de seguridad LDAP

Para planificar el modelo de seguridad, primero, debe tener en cuenta la identidad que el cliente LDAP debe utilizar para hablar con el servidor LDAP. Por ejemplo, debe decidir si desea una solución de inicio de sesión único para toda la empresa, sin contraseñas que se envíen por transferencia, o la transferencia cifrada de datos y la posibilidad de acceder a los resultados de datos de control desde servidor de directorios de cada usuario. También se debe decidir si desea una autenticación más segura para proteger la contraseña del usuario durante la transferencia o si se debe cifrar la sesión entre el cliente LDAP y el servidor LDAP para proteger los datos de LDAP transmitidos.

Los atributos `credentialLevel` y `authenticationMethod` en el perfil se utilizan para esto. Existen cuatro posibles niveles de credenciales para `credentialLevel`: `anonymous`, `proxy`, `proxy anonymous` y `self`. Consulte “Modelo de seguridad de servicios de nombres LDAP” en la página 141 para obtener información más detallada de los conceptos de seguridad del servicio de nombres LDAP.

Nota – Antes, si se activaba la gestión de cuentas `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación en cualquier momento que iniciaran sesión en el sistema. Por lo tanto, los inicios de sesión que no se basan en contraseña realizados con herramientas, como `ssh`, fallarán.

Realice la gestión de cuentas y recupere el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios como el usuario que inicia sesión. El nuevo control en el servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8` , que está activado de manera predeterminada.

Para cambiar este control por otro que no sea el predeterminado, agregue las instrucciones de control de acceso (ACI) en el servidor de directorios:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

Nota – Si activa `pam_krb5` y Kerberos como una solución de inicio de sesión único para toda la empresa, puede diseñar un sistema en el que sólo sean necesarias las contraseñas de inicio de sesión al principio de una sesión. Consulte *Administración de Oracle Solaris 11.1: servicios de seguridad* para obtener más información. Si activa Kerberos, por lo general, también deberá activar DNS. Consulte los capítulos sobre DNS en este manual para obtener más información.

Las principales decisiones que hay que tomar al planificar el modelo de seguridad son las siguientes.

- ¿Utilizará Kerberos y la autenticación por usuario?
- ¿Qué nivel de credencial y qué métodos de autenticación utilizarán los clientes LDAP?
- ¿Utilizará TLS?
- ¿Necesita tener compatibilidad con versiones anteriores de NIS? En otras palabras, ¿los clientes utilizan el módulo `pam_unix_*` o `pam_ldap`?
- ¿Cuál será la configuración del atributo `passwordStorageScheme` de los servidores?
- ¿Cómo configurará la información de control de acceso?

  Para obtener más información sobre ACI, consulte la *Guía de administración* para la versión de Oracle Directory Server Enterprise Edition que está utilizando.

- ¿Los clientes utilizan el módulo `pam_unix_*` o `pam_ldap` para realizar la gestión de cuentas de LDAP?

Planificación de perfiles de cliente y valores de atributo predeterminados para LDAP

Una vez realizados los pasos de planificación anteriores (modelo de red, DIT, y modelo de seguridad), debe tener una idea de los valores para los siguientes atributos de perfil.

- `cn`
- `defaultServerList`
- `preferredServerList`
- `bindTimeLimit`
- `searchTimeLimit`
- `profileTTL`
- `defaultSearchBase`
- `defaultSearchScope`
- `serviceSearchDescriptor`
- `attributeMap`
- `objectclassMap`
- `followReferrals`
- `credentialLevel`
- `authenticationMethod`
- `serviceCredentialLevel`
- `serviceAuthenticationMethod`

De los atributos anteriores, sólo `cn`, `defaultServerList` y `defaultSearchBase` son necesarios. No tienen valores predeterminados. El resto son opcionales y algunos tienen valores predeterminados.

Consulte Capítulo 12, “Configuración de clientes LDAP (tareas)” para obtener más información sobre la configuración de los clientes LDAP.

Planificación para completar los datos de LDAP

Rellenar el servidor LDAP con datos, después de que el servidor LDAP se ha configurado con el DIT adecuado y el esquema. Utilice la nueva herramienta `ldapaddent`. Esta herramienta creará entradas en contenedores LDAP desde sus correspondientes archivos `/etc`. Se puede utilizar para rellenar los contenedores con los siguientes tipos de datos: `aliases`, `auto_*`, `bootparams`, `ethers`, `group`, `hosts` (incluidas las direcciones IPv6), `netgroup`, `netmasks`, `redes`, `passwd`, `sombra`, `protocolos`, las `claves: publickey`, `rpc` y `servicios`. Además, se pueden agregar los archivos relacionados con RBAC: `/etc/user_attr`, `/etc/security/auth_attr`, `/etc/security/prof_attr` y `/etc/security/exec_attr`.

De manera predeterminada, `ldapaddent` lee desde la entrada estándar y agrega esos datos al contenedor LDAP asociado con la base de datos especificada en la línea de comandos. Pero un archivo de entrada del que se deben leer los datos puede ser especificado usando la opción `-f`.

Dado que las entradas se almacenan en el directorio según la configuración del cliente, el cliente debe estar configurado para utilizar el servicios de nombres LDAP.

Para obtener un mejor rendimiento, cargue las bases de datos en este orden:

1. Base de datos `passwd` seguida de la base de datos `shadow`
2. Base de datos `networks` seguida de la base de datos `netmasks`
3. Base de datos `bootparams` seguida de la base de datos `ethers`

Tenga en cuenta que, al agregar entradas del montador automático, el nombre de la base de datos tiene el formato de `auto_*` (por ejemplo, `auto_home`).

Si tiene archivos `/etc` de diferentes hosts para agregar al servidor LDAP, puede fusionarlos en el mismo archivo `/etc` y luego utilizar el comando `ldapaddent` en un host para agregar los archivos, o ejecutar el comando `ldapaddent` en los distintos hosts uno por uno, con la expectativa de que cada host ya esté configurado como cliente LDAP.

Si los datos de su servicio de nombres ya se encuentran en un servidor NIS y desea mover los datos al servidor LDAP para los servicios de nombres LDAP, utilice el comando `ypcat` para volcar los mapas de datos NIS a los archivos. Luego, ejecute el comando `ldapaddent` en estos archivos para agregar los datos al servidor LDAP.

El siguiente procedimiento presupone que las tablas se van a extraer de un cliente `yp`.

▼ Cómo rellenar un servidor con entradas host mediante el comando `ldapaddent`

1 Asegúrese de que Oracle Directory Server Enterprise Edition se haya configurado mediante el comando `idsconfig`.

2 En un máquina de cliente, conviértase en superusuario o asuma un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte el Capítulo 9, “Uso del control de acceso basado en roles (tareas)” de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

3 Convierta el equipo en un cliente LDAP.

```
# ldapclient init -a profileName=new -a domainName=west.example.com 192.168.0.1
```

4 Rellene el servidor con los datos.

```
# ldapaddent -D “cn=directory manager” -f /etc/hosts hosts
```

Se le pedirá que introduzca una contraseña.

En este ejemplo, el comando `ldapaddent` usa el método de autenticación que se ha configurado en el perfil nuevo. Si selecciona la simple, la contraseña se enviará sin cifrar. Para obtener más información, consulte la página del comando man `ldapaddent(1M)`.

En modo autónomo, el comando debe ser similar al siguiente:

```
# ldapaddent -h 192.168.0.1 -N new -M west.example.com -a simple-D “cn=directory manager” -f /etc/hosts hosts
```

◆ ◆ ◆ CAPÍTULO 11

Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP (tareas)

En este capítulo, se describe cómo configurar Oracle Directory Server Enterprise Edition para admitir una red de clientes de servicios de nombres LDAP. La información es específica de Oracle Directory Server Enterprise Edition. Para obtener información acerca de la instalación y configuración del servidor de directorios, consulte la documentación de Oracle Directory Server Enterprise Edition.

Nota – Antes de configurar Oracle Directory Server Enterprise Edition para trabajar con clientes LDAP, debe haber realizado todos los procedimientos descritos en la documentación de instalación y configuración que se incluye con Oracle Directory Server Enterprise Edition.

Nota – Un servidor de directorios (un servidor LDAP) *no puede* ser su propio cliente.

En este capítulo se tratan los siguientes temas.

Configuración de Oracle Directory Server Enterprise Edition con el comando idsconfig

Creación de una lista de comprobación según la instalación del servidor

Durante el proceso de instalación del servidor, tiene que definir variables cruciales con las cuales debe crear una lista de comprobación similar a la que se muestra a continuación antes de ejecutar idsconfig. Puede utilizar la lista de comprobación en blanco proporcionada en "Listas de comprobación en blanco para configuración de LDAP " en la página 207.

Nota – La información que se incluye a continuación funcionará como base para todos los ejemplos que siguen en los capítulos relacionados con LDAP. El dominio de ejemplo es de una compañía hipotética, Ejemplo, Inc. con tiendas en todo el país. Los ejemplos se ocuparán de la división de la costa oeste, con el nombre de dominio west.example.com.

TABLA 11–1 Variables del servidor definidas para la red example.com

Variable	Definición para la red de ejemplo
Número de puerto en el que una instancia del servidor de directorios está instalada	389 (predeterminado)
Nombre del servidor	myserver (desde el nombre de dominio completo (FQDN) myserver.west.example.com o el nombre de host 192.168.0.1)
Servidores de réplica (IPnumber: número de puerto)	192.168.0.2 [para myreplica.west.example.com]
Gestor de directorios	cn=directory manager (predeterminado)
Nombre de dominio al que se prestará servicio	west.example.com
Tiempo máximo (en segundos) para procesar las solicitudes de clientes antes de que se agote el tiempo de espera	1
Número máximo de entradas devueltas por cada solicitud de búsqueda	1

Nota – Si utiliza nombres de host al definir `defaultServerList` o `preferredServerList`, *debe* asegurarse de que no se utiliza LDAP para las consultas de host. Esto significa que `ldap` no se debe configurar en la propiedad `config/host` del servicio `svc:/network/name-service/switch`.

TABLA 11–2 Variables de perfil de cliente definidas para la red example.com

Variable	Definición para la red de ejemplo
Nombre de perfil (el nombre predeterminado es default)	`WestUserProfile`
Lista de servidores (de manera predeterminada, la subred local)	`192.168.0.1`
Lista de servidores preferidos (en el orden en que se deben probar los servidores, primero, segundo, etc.)	`none`
Ámbito de búsqueda (número de niveles inferiores en el árbol de directorios; 'One', predeterminado, o 'Sub')	`one` (predeterminado)
Credenciales utilizadas para acceder al servidor; El valor predeterminado es `anonymous`.	`proxy`
¿Seguir las referencias? (un puntero hacia otro servidor si el servidor principal no está disponible). El valor predeterminado es `no`.	`Y`
Límite de tiempo de búsqueda (el valor predeterminado es 30 segundos) para esperar a que el servidor devuelva información.	`default`
Límite de tiempo de vínculo (el valor predeterminado es 10 segundos) para ponerse en contacto con el servidor.	`default`
Valor predeterminado del método de autenticación: `none`	`simple`

Nota – Los perfiles de cliente se definen por dominio. Al menos un perfil debe estar definido para un dominio determinado.

Índices de atributos

El comando `idsconfig` indexa la siguiente lista de atributos para un mejor rendimiento:

```
membernisnetgroup    pres,eq,sub
nisnetgrouptriple    pres,eq,sub
ipHostNumber         pres,eq,sub
uidNumber            pres,eq
gidNumber            pres,eq
```

```
ipNetworkNumber      pres,eq
automountkey         pres,eq
oncRpcNumber         pres,eq
```

Definiciones de esquema

idsconfig(1M) agrega automáticamente las definiciones de esquema necesarias. A menos que tenga mucha experiencia en administración LDAP, no modifique manualmente el esquema del servidor. Consulte el Capítulo 14, "Servicio de nombres LDAP (Referencia)" para obtener una lista ampliada de esquemas utilizados por el servicio de nombres LDAP.

Uso de índices de exploración

La funcionalidad de índice de exploración de Oracle Directory Server Enterprise Edition, también conocida como vista de lista virtual (VLV), ofrece al cliente una forma de ver un grupo selecto o un número de entradas de una lista muy larga, con lo cual el proceso de búsqueda demora menos tiempo para cada cliente. Los índices de exploración proporcionan parámetros de búsqueda predefinidos y optimizados con los que el cliente del servicio de nombres LDAP puede acceder a información específica desde los distintos servicios más rápidamente. Tenga en cuenta que si no crea índices de exploración, los clientes no tendrán acceso a todas las entradas de un tipo determinado si se exceden los límites del servidor. Por ejemplo, si hay 5.000 entradas de contraseña, pero el tamaño límite de 1.000 entradas está activado, 4.000 entradas no se devolverán durante algunas operaciones de consulta. A menudo, esto puede generar fallos de inicio de sesión y otros fallos graves en las máquinas cliente.

Los índices VLV se configuran en el servidor de directorios y el usuario de proxy tiene acceso de lectura a estos índices.

Antes de configurar los índices de navegación en Oracle Directory Server Enterprise Edition, tenga en cuenta el costo de rendimiento asociado con estos índices. Para obtener más información, consulte la *Guía de administración* para la versión de Oracle Directory Server Enterprise Edition que está utilizando.

idsconfig crea entradas para varios índices VLV. Consulte la página del comando man idsconfig(1M) para obtener más información. Consulte la salida del comando idsconfig para determinar las entradas VLV creadas por idsconfig. Consulte "Ejemplo de configuración de idsconfig" en la página 175 para ver un ejemplo de la salida de idsconfig.

Uso de descriptores de búsqueda de servicios para modificar el acceso de cliente a distintos servicios

Un descriptor de búsqueda de servicios (SSD) cambia la solicitud de búsqueda predeterminada de una operación determinada en LDAP a una búsqueda que se defina. Los SSD son particularmente útiles si, por ejemplo, utiliza LDAP con definiciones de contenedor personalizadas u otro sistema operativo, y ahora está en la transición a la última versión de Oracle Solaris. Con SSD, puede configurar los servicios de nombres LDAP sin tener que cambiar la base de datos y los datos LDAP existentes.

Configuración de SSD con el comando idsconfig

Suponga que su predecesor en Ejemplo, Inc. tenía LDAP configurado y almacenaba los usuarios en el contenedor `ou=Users`. Está actualizando a la última versión de Oracle Solaris. Por definición, un cliente LDAP asume que las entradas de usuario se almacenan en el contenedor `ou=People`. Por lo tanto, cuando se trata de búsquedas en el servicio `passwd`, el cliente LDAP buscará el nivel `ou=people` del DIT y no encontrará los valores correctos.

Una solución trabajosa para el problema mencionado arriba sería sobrescribir por completo el árbol de información de directorios (DIT) de Ejemplo, Inc. existente y volver a escribir todas las aplicaciones existentes en la red de Ejemplo, Inc. para que sean compatibles con el nuevo servicio de nombres LDAP. Una segunda solución, pero mucho más preferible, sería utilizar un SSD que le indique a un cliente LDAP que busque información del usuario en un contenedor `ou=Users`, en lugar de buscar en el contenedor `ou=people` predeterminado.

Debe definir el SSD necesario durante la configuración de Oracle Directory Server Enterprise Edition usando `idsconfig`. La línea indicadora aparece de la siguiente manera.

```
Do you wish to setup Service Search Descriptors (y/n/h? y
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] a
Enter the service id: passwd
Enter the base: service ou=user,dc=west,dc=example,dc=com
Enter the scope: one[default]
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's
```

```
  Q  Exit menu
Enter menu choice: [Quit] p

Current Service Search Descriptors:
===================================
Passwd:ou=Users,ou=west,ou=example,ou=com?

Hit return to continue.

  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] q
```

Ejecución del comando `idsconfig`

Nota – No necesita derechos especiales para ejecutar `idsconfig`, ni tampoco necesita ser cliente del servicio de nombres LDAP. Recuerde crear una lista de comprobación como se menciona en "Creación de una lista de comprobación según la instalación del servidor" en la página 170 al prepararse para ejecutar `idsconfig`. No tiene que ejecutar `idsconfig` desde un servidor o un cliente de servicio de nombres LDAP. Puede ejecutar `idsconfig` desde cualquier máquina de Oracle Solaris en la red.

Precaución – `idsconfig` envía la contraseña del gestor de directorio sin cifrar. Si no desea que esto suceda, debe ejecutar `idsconfig` en el mismo servidor de directorios, no en un cliente.

▼ Cómo configurar Oracle Directory Server Enterprise Edition con el comando idsconfig

1. **Asegúrese de que el Oracle Directory Server Enterprise Edition de destino esté activo y en ejecución.**

2. **Ejecute el comando `idsconfig`.**

   ```
   # /usr/lib/ldap/idsconfig
   ```

Consulte el Ejemplo 11–1 para obtener un ejemplo de ejecución de idsconfig usando las definiciones enumeradas en las listas de comprobación de clientes y servidores al comienzo de este capítulo en "Creación de una lista de comprobación según la instalación del servidor" en la página 170.

3 Responda las preguntas cuando se le solicite.

Tenga en cuenta que 'no' [n] es el valor de entrada predeterminado del usuario. Si necesita aclaración sobre alguna pregunta determinada, escriba

h

y aparecerá un breve párrafo de ayuda.

Después de que idsconfig haya completado la configuración del directorio, debe ejecutar los comandos especificados en el servidor antes de que la configuración del servidor esté completa y lista para servir a los clientes.

Ejemplo de configuración de idsconfig

Esta sección proporciona un ejemplo de una configuración básica de idsconfig que utiliza muchos de los valores predeterminados. El método más complicado para modificar perfiles de cliente es crear SSD. Para obtener un análisis detallado, consulte "Uso de descriptores de búsqueda de servicios para modificar el acceso de cliente a distintos servicios" en la página 173.

Los datos entre corchetes después de un indicador muestran el valor predeterminado para ese indicador. Para aceptar el valor predeterminado, presione la tecla de retorno.

Nota – Los parámetros que se dejan en blanco en la pantalla de resumen no se configuran.

Después de que idsconfig haya completado la configuración del directorio, debe ejecutar los comandos especificados en el servidor antes de que la configuración del servidor esté completa y lista para servir a los clientes.

EJEMPLO 11–1 Ejecución del comando idsconfig para la red de Ejemplo, Inc

En el siguiente ejemplo, la utilidad idsconfig se ejecuta inmediatamente después de crear una instancia de servidor en el servidor LDAP.

```
# usr/lib/ldap/idsconfig
It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
```

EJEMPLO 11–1 Ejecución del comando idsconfig para la red de Ejemplo, Inc *(Continuación)*

```
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  No valid suffixes were found for Base DN dc=west,dc=example,dc=com
Enter suffix to be created (b=back/h=help): [dc=west,dc=example,dc=com]
Enter ldbm database name (b=back/h=help): [west]
  sasl/GSSAPI is not supported by this LDAP server
Enter the profile name (h=help): [default] WestUserProfile
Default server list (h=help): [192.168.0.1]
Preferred server list (h=help):
Choose desired search scope (one, sub, h=help):  [one]
The following are the supported credential levels:
  1  anonymous
  2  proxy
  3  proxy anonymous
  4  self
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
  1  none
  2  simple
  3  sasl/DIGEST-MD5
  4  tls:simple
  5  tls:sasl/DIGEST-MD5
  6  sasl/GSSAPI
Choose Authentication Method (h=help): [1] 2


Current authenticationMethod: simple
Do you want to add another Authentication Method? n
Do you want the clients to follow referrals (y/n/h)? [n]
Do you want to modify the server timelimit value (y/n/h)? [n] y
Enter the time limit for DSEE (current=3600): [-1]
Do you want to modify the server sizelimit value (y/n/h)? [n] y
Enter the size limit for DSEE (current=2000): [-1]
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n]
Client search time limit in seconds (h=help): [30]
Profile Time To Live in seconds (h=help): [43200]
Bind time limit in seconds (h=help): [10]
Do you want to enable shadow update (y/n/h)? [n]
Do you wish to setup Service Search Descriptors (y/n/h)? [n]

              Summary of Configuration

  1  Domain to serve              : west.example.com
  2  Base DN to setup             : dc=west,dc=example,dc=com
        Suffix to create          : dc=west,dc=example,dc=com
        Database to create        : west
  3  Profile name to create       : WestUserProfile
  4  Default Server List          : 192.168.0.1
  5  Preferred Server List        :
```

EJEMPLO 11–1 Ejecución del comando idsconfig para la red de Ejemplo, Inc *(Continuación)*

```
 6  Default Search Scope          : one
 7  Credential Level              : proxy
 8  Authentication Method         : simple
 9  Enable Follow Referrals       : FALSE
10  DSEE Time Limit                : -1
11  DSEE Size Limit                : -1
12  Enable crypt password storage : TRUE
13  Service Auth Method pam_ldap  :
14  Service Auth Method keyserv   :
15  Service Auth Method passwd-cmd:
16  Search Time Limit             : 30
17  Profile Time to Live          : 43200
18  Bind Limit                    : 10
19  Enable shadow update          : FALSE
20  Service Search Descriptors Menu

Enter config value to change: (1-20 0=commit changes) [0]
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for proxyagent:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y

 1. Changed timelimit to -1 in cn=config.
 2. Changed sizelimit to -1 in cn=config.
 3. Changed passwordstoragescheme to "crypt" in cn=config.
 4. Schema attributes have been updated.
 5. Schema objectclass definitions have been added.
 6. Database west successfully created.
 7. Suffix dc=west,dc=example,dc=com successfully created.
 8. NisDomainObject added to dc=west,dc=example,dc=com.
 9. Top level "ou" containers complete.
10. automount maps: auto_home auto_direct auto_master auto_shared processed.
11. ACI for dc=west,dc=example,dc=com modified to disable self modify.
12. Add of VLV Access Control Information (ACI).
13. Proxy Agent cn=proxyagent,ou=profile,dc=west,dc=example,dc=com added.
14. Give cn=proxyagent,ou=profile,dc=west,dc=example,dc=com read permission
    for password.
15. Generated client profile and loaded on server.
16. Processing eq,pres indexes:
    uidNumber (eq,pres)   Finished indexing.
    ipNetworkNumber (eq,pres)   Finished indexing.
    gidnumber (eq,pres)   Finished indexing.
    oncrpcnumber (eq,pres)   Finished indexing.
    automountKey (eq,pres)   Finished indexing.
17. Processing eq,pres,sub indexes:
    ipHostNumber (eq,pres,sub)   Finished indexing.
    membernisnetgroup (eq,pres,sub)   Finished indexing.
    nisnetgrouptriple (eq,pres,sub)   Finished indexing.
18. Processing VLV indexes:
    west.example.com.getgrent vlv_index   Entry created
    west.example.com.gethostent vlv_index   Entry created
    west.example.com.getnetent vlv_index   Entry created
    west.example.com.getpwent vlv_index   Entry created
    west.example.com.getrpcent vlv_index   Entry created
```

EJEMPLO 11–1 Ejecución del comando idsconfig para la red de Ejemplo, Inc *(Continuación)*

```
      west.example.com.getspent vlv_index   Entry created
      west.example.com.getauhoent vlv_index   Entry created
      west.example.com.getsoluent vlv_index   Entry created
      west.example.com.getauduent vlv_index   Entry created
      west.example.com.getauthent vlv_index   Entry created
      west.example.com.getexecent vlv_index   Entry created
      west.example.com.getprofent vlv_index   Entry created
      west.example.com.getmailent vlv_index   Entry created
      west.example.com.getbootent vlv_index   Entry created
      west.example.com.getethent vlv_index   Entry created
      west.example.com.getngrpent vlv_index   Entry created
      west.example.com.getipnent vlv_index   Entry created
      west.example.com.getmaskent vlv_index   Entry created
      west.example.com.getprent vlv_index   Entry created
      west.example.com.getip4ent vlv_index   Entry created
      west.example.com.getip6ent vlv_index   Entry created

idsconfig: Setup of DSEE server myserver is complete.


Note: idsconfig has created entries for VLV indexes.

      For DS5.x, use the directoryserver(1m) script on myserver
      to stop the server.  Then, using directoryserver, follow the
      directoryserver examples below to create the actual VLV indexes.

      For DSEE6.x, use dsadm command delivered with DS on myserver
      to stop the server.  Then, using dsadm, follow the
      dsadm examples below to create the actual VLV indexes.

  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getgrent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.gethostent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getnetent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getpwent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getrpcent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getspent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauhoent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getsoluent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauduent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauthent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getexecent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprofent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmailent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getbootent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getethent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getngrpent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getipnent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmaskent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip4ent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip6ent

<install-path>/bin/dsadm reindex -l -t west.example.com.getgrent <directory-instance-path>
 dc=west,dc=example,dc=com
<install-path>/bin/dsadm reindex -l -t west.example.com.gethostent <directory-instance-path>
```

EJEMPLO 11–1 Ejecución del comando idsconfig para la red de Ejemplo, Inc *(Continuación)*

```
 dc=west,dc=example,dc=com
.
.
.
<install-path>/bin/dsadm reindex -l -t west.example.com.getip6ent <directory-instance-path>
 dc=west,dc=example,dc=com
```

Relleno del servidor de directorios mediante el comando ldapaddent

Nota – Antes de rellenar el servidor de directorios con datos, debe configurar el servidor para almacenar las contraseñas en formato Crypt de UNIX si usa los módulos pam_unix_*. Si utiliza pam_ldap, puede almacenar contraseñas en cualquier formato. Para obtener más información acerca de la configuración de la contraseña en formato crypt de UNIX, consulte los documentos de Oracle Directory Server Enterprise Edition.

ldapaddent lee desde la entrada estándar (/etc/filename como passwd) y coloca estos datos en el contenedor asociado con el servicio. La configuración de cliente determina cómo se escribirán los datos de manera predeterminada.

▼ Cómo rellenar Oracle Directory Server Enterprise Edition con datos de contraseña de usuario mediante el comando ldapaddent

- **Utilice el comando ldapaddent para agregar entradas de /etc/passwd al servidor.**

  ```
  # ldapaddent -D "cn=directory manager" -f /etc/passwd passwd
  ```

  Consulte la página del comando man ldapaddent(1M). Consulte también el Capítulo 9, “Introducción a los servicios de nombres LDAP (descripción general)” para obtener información acerca del acceso de escritura y la seguridad LDAP para el servidor de directorios.

Especificación de pertenencias a grupos mediante el atributo de miembro

El borrador de Internet rfc2307bis especifica que la clase de objeto `groupOfMembers` también se puede utilizar como la clase estructural práctica para las entradas LDAP del servicio de grupo. Dichas entradas de grupo pueden tener valores de atributo de miembros que especifican la asociación de grupos en nombres distinguidos (DN). Los clientes LDAP de Oracle Solaris admiten esas entradas de grupo y utilizan los valores de atributo de miembros para la resolución de pertenencia a grupos.

Los clientes LDAP también admiten las entradas de grupo que utilizan la clase de objeto `groupOfUniqueNames` y el atributo `uniqueMember`. Sin embargo, el uso de esta clase de objeto y este atributo no se recomienda.

La forma existente de definir las entradas de grupo con la clase de objeto `posixGroup` y el atributo `memberUid` sigue siendo admitida. Este tipo de entradas de grupo aún son las que el comando `ldapaddent` crea al rellenar los servidores LDAP para los servicios de grupo. No agrega el atributo `member` a las entradas de grupo.

Para agregar entradas de grupo con la clase de objeto `groupOfMembers` y los valores de atributo `member`, utilice la herramienta `ldapadd` y un archivo de entrada similar al siguiente:

```
dn: cn=group1,ou=group,dc=mkg,dc=example,dc=com
objectClass: posixGroup
objectClass: groupOfNames
objectClass: top
cn: group1
gidNumber: 1234
member: uid=user1,ou=people,dc=mkg,dc=example,dc=com
member: uid=user2,ou=people,dc=mkg,dc=example,dc=com
member: cn=group2,ou=group,dc=mkg,dc=example,dc=com
```

Los clientes LDAP manejarán las entradas de grupo con una combinación de ningún atributo, cualquier atributo o todos los atributos `memberUid`, `member` y `uniqueMember`. El resultado de la evaluación de pertenencia será que un grupo tiene como pertenencia la unión de los tres con duplicados eliminados. Es decir, si la entrada de un grupo `G` tiene un valor `memberUid` que hace referencia al usuario `U1` y `U2`, un valor `member` que hace referencia al usuario `U2`, y un valor `uniqueMember` que hace referencia al usuario `U3`, entonces el grupo `G` tiene tres miembros, `U1`, `U2` y `U3`. Los grupos anidados también son compatibles, es decir, un atributo de miembro puede tener los valores que apuntan a otros grupos.

Para evaluar de manera eficaz la pertenencia a grupos y determinar los grupos (incluidos los anidados) a los que pertenece un usuario, el complemento `memberOf` debe estar configurado y activado en los servidores LDAP. Si no es así, sólo los grupos contenedores, y no los anidados, se

resolverán. De manera predeterminada, el complemento `memberOf` es activado por el servidor ODSEE. Si el complemento no está activado, utilice la herramienta `dsconf` de ODSEE para activarlo.

Rellenado del servidor de directorios con más perfiles

Utilice el comando `ldapclient` con la opción `genprofile` para crear una representación LDIF de un perfil de configuración, en función de los atributos especificados. El perfil que se crea se puede cargar en un servidor LDAP para utilizarlo como perfil de cliente. El cliente puede descargar el perfil de cliente con `ldapclient init`.

Consulte `ldapclient(1M)` para obtener información sobre cómo usar `ldapclient genprofile`.

▼ Cómo rellenar el servidor de directorios con perfiles adicionales mediante el comando `ldapclient`

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Use `ldapclient` con el comando `genprofile`.

```
# ldapclient genprofile \
-a profileName=myprofile \
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a "defaultServerList=192.168.0.1 192.168.0.2:386" \> myprofile.ldif
```

3 Cargue el nuevo perfil en el servidor.

```
# ldapadd -h 192.168.0.1 -D "cn=directory manager" -f myprofile.ldif
```

Configuración del servidor de directorios para activar la gestión de cuentas

La gestión de cuentas se puede implementar para los clientes que utilizan `pam_ldap` y para los clientes que utilizan los módulos `pam_unix_*`.

Precaución – No utilice los módulos `pam_ldap` y `pam_unix_*` en el mismo dominio de nombres LDAP. Todos los clientes utilizan `pam_ldap` o todos los clientes utilizan los módulos `pam_unix_*`. Esta limitación podría indicar que usted necesita un servidor LDAP dedicado.

Para clientes que utilizan el módulo pam_ldap

Para que `pam_ldap` funcione correctamente, la contraseña y la directiva de bloqueo de cuentas deben estar correctamente configuradas en el servidor. Puede utilizar la consola del servidor de directorios o `ldapmodify` para configurar la política de gestión de cuentas del directorio LDAP. Para obtener procedimientos y más información, consulte el capítulo "Gestión de cuentas de usuario" en la *Guía de administración* para la versión de Oracle Directory Server Enterprise Edition que está utilizando.

Nota – Antes, si se activaba la gestión de cuentas `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación en cualquier momento que iniciaran sesión en el sistema. Por lo tanto, los inicios de sesión que no se basan en contraseña realizados con herramientas, como `ssh`, fallarán.

Realice la gestión de cuentas y recupere el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios como el usuario que inicia sesión. El nuevo control en el servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8` , que está activado de manera predeterminada.

Para cambiar este control por otro que no sea el predeterminado, agregue las instrucciones de control de acceso (ACI) en el servidor de directorios:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

Las contraseñas de usuarios `proxy` *nunca* deben vencer. Si las contraseñas proxy caducan, los clientes que utilizan el nivel de credenciales `proxy` no podrán recuperar información del servicio de nombres del servidor. Para asegurarse de que los usuarios proxy tienen contraseñas que no caducan, modifique la cuentas proxy con la siguiente secuencia de comandos.

```
# ldapmodify -h ldapserver -D administrator DN \
-w administrator password <<EOF
```

```
dn: proxy user DN
DNchangetype: modify
replace: passwordexpirationtime
passwordexpirationtime: 20380119031407Z
EOF
```

Nota – La gestión de cuentas `pam_ldap` depende de Oracle Directory Server Enterprise Edition para mantener y proporcionar información a los usuarios sobre la fecha de las contraseñas y la caducidad de las cuentas. El servidor de directorios no interpreta los datos correspondientes a entradas shadow para validar cuentas de usuario. Los módulos `pam_unix_*`, sin embargo, examinan los datos shadow para determinar si las cuentas están bloqueadas o si las contraseñas están vencidas. Debido a que ni el servicio de nombres LDAP ni el servidor de directorios mantienen los datos shadow actualizados, los módulos no permitirán el acceso según los datos shadow. La datos shadow se recuperan mediante la identidad `proxy`. Por lo tanto, no permita que los usuarios `proxy` tengan acceso de lectura al atributo `userPassword`. Denegar a los usuarios `proxy` acceso de lectura de `userPassword` impide que el servicio PAM realice una validación de la cuenta no válida.

Para clientes que utilizan los módulos pam_unix_*

Si desea activar clientes LDAP con el fin de que utilicen los módulos `pam_unix_*` para la gestión de cuentas, el servidor debe estar configurado para permitir la actualización de datos shadow. A diferencia de la gestión de cuentas de `pam_ldap`, los módulos `pam_unix_*` no requieren pasos de configuración adicionales. Toda la configuración se puede realizar mediante la ejecución de la utilidad `idsconfig`. Para una ejecución básica de `idsconfig`, consulte elEjemplo 11–1.

A continuación, se muestra el resultado de dos ejecuciones de `idsconfig`.

La primera ejecución de `idsconfig` utiliza un perfil de cliente existente.

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server
```

```
Enter the profile name (h=help): [default] WestUserProfile

Profile 'WestUserProfile' already exists, it is possible to enable
shadow update now. idsconfig will exit after shadow update
is enabled. You can also continue to overwrite the profile
or create a new one and be given the chance to enable
shadow update later.


Just enable shadow update (y/n/h)? [n] y
Add the administrator identity (y/n/h)? [y]
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:
  ADDED: Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com.
         Proxy ACI LDAP_Naming_Services_proxy_password_read does not
         exist for dc=west,dc=example,dc=com.
  ACI SET: Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access
           to shadow data.
  ACI SET: Non-Admin access to shadow data denied.

  Shadow update has been enabled.
```

La segunda ejecución de `idsconfig` crea un nuevo perfil para utilizarlo más tarde. Sólo se muestra parte del resultado.

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile-new
Default server list (h=help): [192.168.0.1]
.
.
.
Do you want to enable shadow update (y/n/h)? [n] y

              Summary of Configuration

  1  Domain to serve              : west.example.com
  2  Base DN to setup             : dc=west,dc=example,dc=com
        Suffix to create          : dc=west,dc=example,dc=com
  3  Profile name to create       : WestUserProfile-new
```

```
.
.
.
 19  Enable shadow update          : TRUE
.
.
.
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:


WARNING: About to start committing changes. (y=continue, n=EXIT) y

  1. Changed timelimit to -1 in cn=config.
  2. Changed sizelimit to -1 in cn=config.
.
.
.
  11. ACI for dc=test1,dc=mpklab,dc=sfbay,dc=sun,dc=com modified to
      disable self modify.
.
.
.
  15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com write permission for shadow.
...
```

◆ ◆ ◆ CAPÍTULO 12

Configuración de clientes LDAP (tareas)

En este capítulo se describe cómo configurar un cliente de servicios de nombres LDAP. En este capítulo, se tratan los siguientes temas:

Requisitos previos para la configuración del cliente LDAP

Para que un cliente de Oracle Solaris utilice LDAP como servicio de nombres, se deben cumplir los siguientes requisitos:

- El nombre de dominio del cliente debe tener servicio del servidor LDAP.
- El cambio de servicio de nombres debe apuntar a LDAP para los servicios necesarios.
- El cliente debe estar configurado con todos los parámetros establecidos que definen su comportamiento.
- `ldap_cachemgr` se debe estar ejecutando en el cliente.
- Al menos un servidor para el que se configura un cliente debe estar activo y en ejecución.

La utilidad `ldapclient` es la clave para configurar un cliente LDAP, ya que realiza todos los pasos anteriores, excepto para iniciar el servidor. En el resto de este capítulo se muestran ejemplos de cómo utilizar la utilidad `ldapclient` para configurar un cliente LDAP y utilizar las diferentes utilidades LDAP para obtener información acerca de un cliente LDAP y comprobar su estado.

LDAP y la utilidad de gestión de servicios

El servicio de cliente LDAP es gestionado mediante la utilidad de gestión de servicios. Para obtener una descripción general de la SMF, consulte el Capítulo 1, "Gestión de servicios (descripción general)" de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M) y `svcs`(1) para obtener más detalles.

En la siguiente lista, se ofrece una breve descripción general de la información importante necesaria para utilizar el servicio SMF con el fin de administrar el servicio de cliente LDAP.

- Las acciones administrativas de este servicio de cliente LDAP, como la activación, la desactivación o el reinicio, pueden realizarse con el comando `svcadm`.

  Consejo – La desactivación temporal de un servicio mediante la opción `-t` proporciona protección para la configuración del servicio. Si el servicio se desactiva con la opción `-t`, los valores originales se restaurarán para el servicio tras un reinicio. Si el servicio se desactiva sin `-t`, permanecerá desactivado después de reiniciar.

- El identificador de recursos de gestión de errores (FMRI) para el servicio de cliente LDAP es `svc:/network/ldap/client`.
- Durante el proceso de configuración, el servicio `network/nis/domain` también estará activado para proporcionar el nombre de dominio utilizado por el servicio `network/ldap/client`.
- Puede consultar el estado del cliente LDAP y el daemon `ldap_cachemgr` mediante el comando `svcs`.
  - A continuación, se muestran ejemplos del comando `svcs` y su salida:

    ```
    # svcs \*ldap\*
    STATE          STIME    FMRI
    online         15:43:46 svc:/network/ldap/client:default
    ```

  - Ejemplo del comando `svcs -l` y el resultado. Para obtener el resultado que se muestra a continuación, debe utilizar el nombre de la instancia en el FMRI.

    ```
    # svcs -l network/ldap/client:default
    fmri         svc:/network/ldap/client:default
    name         LDAP Name Service Client
    enabled      true
    state        online
    next_state   none
    restarter    svc:/system/svc/restarter:default
    manifest     /lib/svc/manifest/network/ldap/client.xml
    manifest     /lib/svc/manifest/network/network-location.xml
    manifest     /lib/svc/manifest/system/name-service/upgrade.xml
    manifest     /lib/svc/manifest/milestone/config.xml
    dependency   require_all/none svc:/system/filesystem/minimal (online)
    dependency   require_all/none svc:/network/initial (online)
    dependency   optional_all/none svc:/network/location:default (online)
    ```

```
dependency    require_all/restart svc:/network/nis/domain (online)
dependency    optional_all/none svc:/system/name-service/upgrade (online)
dependency    optional_all/none svc:/milestone/config (online)
dependency    optional_all/none svc:/system/manifest-import (online)
dependency    require_all/none svc:/milestone/unconfig (online)
```

- Puede comprobar la presencia de un daemon mediante los siguientes comandos:
  - En un servidor, use el comando `ptree`:

    ```
    # ptree 'pgrep slapd'
    6410 zsched
    11565 /export/dsee/dsee6/ds6/lib/64/ns-slapd -D /export/dsee/test1 -i /export
    ```

  - En un cliente, use el siguiente comando:

    ```
    # ldapsearch -h server-name -b "" -s base "objectclass=*" |grep -i context
    namingContexts: dc=example,dc=com
    ```

Inicialización de un cliente LDAP

El comando `ldapclient` se usa para configurar clientes LDAP en un sistema de Oracle Solaris. El comando asume que el servidor ya se ha configurado con los perfiles de cliente apropiados. Debe instalar y configurar el servidor con los perfiles adecuados antes de configurar los clientes.

Nota – Debido a que LDAP y NIS usan el mismo componente de nombre de dominio que está definido en el servicio `network/nis/domain`, el sistema operativo Oracle Solaris no admite una configuración en la que un cliente NIS y un cliente LDAP nativo coexisten en el mismo sistema de cliente.

Hay dos formas principales para configurar un cliente mediante `ldapclient` .

- *Perfil*

  Como mínimo, debe especificar la dirección del servidor que contiene el perfil y el dominio que desea utilizar. Si no se especifica ningún perfil, se toma el perfil "predeterminado". El servidor proporcionará el resto de la información necesaria, excepto la información de proxy y de base de datos de certificados. Si un nivel de credencial de un cliente es `proxy` o `proxy anonymous`, debe proporcionar el DN vinculado de proxy y la contraseña. Consulte "Asignación de niveles de credencial de cliente" en la página 143 para obtener más información.

  Para activar la actualización de datos shadow, debe proporcionar las credenciales de administración (`adminDN` más `adminPassword`).

- *Manual*

  Debe configurar el perfil en el cliente mismo, lo que significa que debe definir todos los parámetros desde la línea de comandos. Por lo tanto, la información de perfil se almacena en archivos de caché y el servidor nunca la actualiza.

Nota – En entornos empresariales, el uso de un perfil de configuración LDAP puede reducir la complejidad si el perfil se comparte entre equipos.

▼ Cómo inicializar un cliente LDAP mediante perfiles

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Ejecute el comando `ldapclient` con la opción `init`.**

```
# ldapclient init -a profileName=new \
-a domainName=west.example.com 192.168.0.1
System successfully configured
```

▼ Cómo inicializar un cliente LDAP utilizando credenciales por usuario

Antes de empezar

Antes de configurar un cliente LDAP con las credenciales por usuario, los siguientes elementos ya deben estar configurados:

- Uno o más servidores de centro de distribución de claves de Kerberos (KDC) deben estar configurados y en ejecución.
- DNS, el acceso de cliente a un servidor DNS y, al menos, un servidor DNS deben estar configurados y en ejecución.
- Kerberos debe estar configurado y activado en el equipo cliente.
- Debe existir un perfil de instalación de cliente Kerberos como el siguiente:

```
# cat /usr/tmp/krb5.profile
REALM EXAMPLE.COM
KDC kdc.example.com
ADMIN super/admin
FILEPATH /usr/tmp/krb5.conf
NFS 1
DNSLOOKUP none
```

- El servidor LDAP debe estar instalado y configurado para admitir `sasl/GSSAPI`.
- Debe haber configuraciones de asignación de identidad adecuadas.
- Los principales del host de Kerberos para el servidor de directorios y el KDC deben estar configurados en el KDC.
- El comando `idsconfig` se debe haber ejecutado en el DIT del servidor de directorios que se va a utilizar.
- Un perfil por usuario `gssapi` adecuado (como `gssapi_example.com`) debe estar creado.

En el siguiente ejemplo parcial, se muestra una ilustración de un perfil por usuario en el comando `idsconfig`:

```
# /usr/lib/ldap/idsconfig
Do you wish to continue with server setup (y/n/h)? [n] y
Enter the Directory Server's hostname to setup: kdc.example.com
Enter the port number for DSEE (h=help): [389] <Enter your port>
Enter the directory manager DN: [cn=Directory Manager] <Enter your DN>
Enter passwd for cn=Directory Manager : <Enter your password>
Enter the domainname to be served (h=help): [example.com] <Enter your domain>
Enter LDAP Base DN (h=help): [dc=example,dc=com] <Enter your DN>
GSSAPI is supported. Do you want to set up gssapi:(y/n) [n] y
Enter Kerberos Realm: [EXAMPLE.COM] EXAMPLE.COM
```

Nota – Además, para un perfil `gssapi`, debe proporcionar un nivel de credencial de `4 self` y un método de autenticación de `6 sasl/GSSAPI`.

- Los principales de usuario necesarios deben existir en el KDC.
- En el equipo cliente, Kerberos se debe inicializar mediante el perfil de cliente con un comando, como el siguiente:

  ```
  # /usr/sbin/kclient -p /usr/tmp/krb5.profile
  ```
- El cambio de servicio de nombres debe estar configurado para usar `dns` para `hosts`. El siguiente comando comprueba los siguientes valores de repositorio:

  ```
  % svcprop -p config/host system/name-service/switch
  files\ dns\ nis
  ```
- DNS debe estar configurado y el servicio DNS debe estar en ejecución. Consulte los capítulos de DNS en este documento para obtener detalles.
- El DIT del servidor de directorios debe estar cargado previamente con (como mínimo) los usuarios de este equipo cliente, el host de cliente y las entradas LDAP `auto_home` necesarias. Consulte otras secciones de este manual para obtener detalles sobre cómo agregar entradas con el comando `ldapaddent`.

Nota – No edite ningún archivo de configuración de cliente directamente. Utilice el comando `ldapclient` para crear o modificar el contenido de estos archivos.

1 Ejecute `ldapclient init` para inicializar el cliente mediante el perfil gssapi.

```
# /usr/sbin/ldapclient init -a profilename=gssapi_EXAMPLE.COM -a \
domainname=example.com 9.9.9.50
```

2 Intente iniciar sesión como usuario:

- **Ejecute `kinit -p` *user***
- **Ejecute `ldaplist -l passwd` *user* en la sesión del usuario y debería ver `userpassword`.**

- **Ejecute `ldaplist -l passwd bar` para poder obtener la entrada sin `userpassword`. De manera predeterminada, `root` puede seguir viendo `userpassword` para todos.**

Más información

Notas sobre el uso por de credenciales por usuario

- Si el archivo `syslog` tiene este mensaje: `libsldap: Status: 7 Mesg: openConnection: GSSAPI bind failed - 82 Local error`, es probable que Kerberos no se haya inicializado o que el ticket haya caducado. Ejecute el comando `klist` para buscar. Por ejemplo, ejecute `kinit -p foo` o `kinit -R -p foo` e intente nuevamente.
- Si lo desea, puede agregar `pam_krb5.so.1` a `/etc/pam.conf` de manera que se ejecute automáticamente el comando `kinit` al iniciar sesión.

  Por ejemplo:

```
login   auth optional pam_krb5.so.1
rlogin  auth optional pam_krb5.so.1
other   auth optional pam_krb5.so.1
```

- Si un usuario ha ejecutado el comando `kinit` y el mensaje `syslog` indica `Invalid credential`, entonces el problema podría ser que la entrada de host `root` o la entrada de usuario no está en el directorio LDAP o que las reglas de asignación no son correctas.
- Cuando se ejecuta el comando `ldapclient init`, comprueba si el perfil LDAP contiene una configuración self/ sasl/GSSAPI. Si se produce un error en la comprobación de conmutador, entonces el motivo es, generalmente, que DNS no era el criterio de búsqueda para la base de datos de host.
  - Si se produce un error en la comprobación porque el ID de cliente de DNS no está activado, ejecute `svcs -l dns/client` para determinar si el servicio está desactivado. Ejecute `svcadm enable dns/client` para activar el servicio.
  - Si se produce un error en la comprobación por una vinculación sasl/GSSAPI, compruebe `syslog` para determinar el problema.

Consulte otras referencias en esta guía y en *Administración de Oracle Solaris 11.1: servicios de seguridad* para obtener más detalles.

▼ Cómo inicializar un cliente LDAP mediante credenciales de proxy

Nota – No edite ninguno de los archivos de configuración de cliente directamente. Utilice el comando `ldapclient` para crear o modificar el contenido de estos archivos.

1. **Conviértase en administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Defina valores de proxy.

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

Las opciones `-a proxyDN` y `-a proxyPassword` son *necesarias* si el perfil que se va a utilizar está configurado para `proxy` . Debido a que las credenciales no se almacenan en el perfil guardado en el servidor, debe proporcionar la información al inicializar el cliente. Este método es más seguro que el método anterior para almacenar las credenciales de proxy en el servidor.

La información de proxy está almacenada en el servicio `svc:/network/ldap/client` en los grupos de propiedad `config` y `cred`.

▼ Cómo inicializar un cliente LDAP para permitir la actualización de datos shadow

1 Conviértase en administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Para establecer el conmutador `enableShadowUpdate` y definir la credencial de administración, ejecute el comando `ldapclient`.

- **Para actualizar un cliente LDAP que ya está en funcionamiento, ejecute este comando:**

  ```
  # ldapclient mod -a enableShadowUpdate=TRUE \
  -a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
  -a adminPassword=admin-password
  System successfully configured
  ```

- **Para inicializar un cliente LDAP, ejecute este comando:**

  ```
  # ldapclient init \
  -a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
  -a adminPassword=admin-password
  -a domainName=west.example.com \
  -a profileName=WestUserProfile \
  -a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
  -a proxyPassword=<proxy_password> \
  192.168.0.1
  System successfully configured
  ```

3 **Para comprobar la configuración, muestre los contenidos de la propiedad `cred` del servicio `network/ldap/client`.**

El resultado es similar al siguiente:

```
# svcprop -p cred svc:/network/ldap/client
cred/read_authorization astring solaris.smf.value.name-service.ldap.client
cred/value_authorization astring solaris.smf.value.name-service.ldap.client
cred/bind_dn astring cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
cred/bind_passwd astring {NS1}4a3788f8eb85de11
cred/enable_shadow_update boolean true
cred/admin_bind_dn astring cn=admin,ou=profile,dc=west,dc=example,dc=com
cred/admin_bind_passwd astring {NS1}4a3788f8c053434f
```

▼ Cómo inicializar un cliente LDAP manualmente

Los usuarios root o los administradores con un rol equivalente, pueden realizar configuraciones de cliente LDAP manuales. Sin embargo, muchas de las comprobaciones se omiten durante el proceso, por lo que es relativamente fácil configurar de forma incorrecta el sistema. Además, debe cambiar los valores *en cada equipo*, en lugar de hacerlo en un solo lugar central, como cuando se utilizan perfiles.

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Inicialice el cliente.**

```
# ldapclient manual \
-a domainName=dc=west.example.com -a credentialLevel=proxy \
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a proxyPassword=testtest 192.168.0.1
```

3 **Verifique la configuración de cliente LDAP.**

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_CREDENTIAL_LEVEL= proxy
```

▼ Cómo modificar una configuración de cliente LDAP manual

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Utilice el comando `ldapclient mod` para cambiar el método de autenticación a `simple`.**

```
# ldapclient mod -a authenticationMethod=simple
```

3 **Verifique que el cambio se haya realizado para la configuración de cliente LDAP.**

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_CREDENTIAL_LEVEL= proxy
```

Errores más frecuentes

No puede cambiar algunos atributos de la configuración de un cliente LDAP con el subcomando `mod`. Por ejemplo, no puede cambiar los atributos `profileName` y `profileTTL`. Para cambiar estos atributos, cree un nuevo perfil mediante el comando `ldapclient init`, como se describe en "Cómo inicializar un cliente LDAP mediante perfiles" en la página 190. O, ejecute el comando `ldapclient manual`, como se describe en "Cómo inicializar un cliente LDAP manualmente" en la página 194.

▼ Cómo cancelar la inicialización de un cliente LDAP

El comando `ldapclient uninit` restaura el servicio de nombres de cliente a lo que estaba antes de la operación `init`, `modify` o `manual` más reciente. En otras palabras, el comando "deshace" la acción al último paso realizado. Por ejemplo, si el cliente se configuró para usar `profile1` y luego se modificó para usar `profile2`, con `ldapclient uninit` volverá a hacer que el cliente use `profile1`.

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Cancele la inicialización del cliente LDAP.**

```
# ldapclient uninit
System successfully recovered
```

Configuración de seguridad TLS

Nota – Los archivos de la base de datos de seguridad deben ser legibles para todos los usuarios. No incluya ninguna clave privada en el archivo `key3.db`.

Si utiliza seguridad de la capa de transporte (TLS), las bases de datos de seguridad necesarias deben estar instaladas. En concreto, se necesitan el certificado y los archivos clave de la base de datos. Por ejemplo, si utiliza un nuevo formato de base de datos desde Mozilla Firefox, tres archivos `cert8.db`, `key3.db` y `secmod.db`, son necesarios. El archivo `cert8.db` contiene certificados de confianza. El archivo `key3.db` contiene las claves del cliente. Incluso si el servicio de nombres LDAP no utiliza las claves del cliente, este archivo debe estar presente. El archivo `secmod.db` contiene los módulos de seguridad, como el módulo `PKCS#11`. Este archivo no es necesario si se utiliza el formato antiguo.

Nota – Antes de ejecutar `ldapclient`, debe configurar e instalar los archivos de base de datos necesarios que se describen en esta sección.

Consulte la sección acerca de la configuración de clientes LDAP para usar SSL en el capítulo "Gestión de SSL" de la Guía del Administrador de la versión de Oracle Directory Server Enterprise Edition que está utilizando, para obtener información sobre cómo crear y gestionar estos archivos. Una vez configurados, estos archivos se deben almacenar en la ubicación prevista por el cliente de servicios de nombres LDAP. El atributo `certificatePath` se utiliza para determinar esta ubicación. Ésta es, de manera predeterminada `/var/ldap`.

Por ejemplo, después de configurar los archivos `cert8.db`, `key3.db` y `secmod.db` necesarios utilizando Mozilla Firefox, copie los archivos a la ubicación predeterminada de la siguiente manera:

```
# cp $HOME/.mozilla/firefox/*.default/cert8.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/key3.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/secmod.db /var/ldap
```

A continuación, otorgue acceso de lectura a todos.

```
# chmod 444 /var/ldap/cert8.db
# chmod 444 /var/ldap/key3.db
# chmod 444 /var/ldap/secmod.db
```

Nota – Mozilla Firefox tiene sus archivos `cert8.db`, `key3.db` y `secmod.db` gestionados en subdirectorios en `$HOME/.mozilla`. Se deben almacenar copias de estas bases de datos de seguridad en un sistema de archivos local, si está utilizándolos para el cliente de servicios de nombres LDAP.

Configuración de PAM

El módulo `pam_ldap` es una opción de módulo de PAM de gestión de cuentas y autenticación para LDAP. Consulte la página del comando man `pam_ldap(5)` para obtener más información sobre las funciones actualmente admitidas con `pam_ldap`.

Si ha seleccionado el modo por usuario y la opción de credenciales self, también debe activar el módulo PAM Kerberos `pam_krb5`. Consulte la página del comando man `pam_krb5(5)` y la documentación *Administración de Oracle Solaris 11.1: servicios de seguridad* para obtener más información.

Configuración de PAM para utilizar policy

Para configurar PAM para utilizar UNIX `policy`, use el archivo `/etc/pam.conf` predeterminado. No es preciso realizar ningún cambio. Para obtener detalles, consulte la página del comando man `pam.conf(4)`.

Sin embargo, si la caducidad de la contraseña y la política de contraseña controladas por los datos `shadow` son necesarias, el cliente debe estar configurado y se debe ejecutar con el conmutador `enableShadowUpdate`. Consulte "Cómo inicializar un cliente LDAP para permitir la actualización de datos shadow" en la página 193 para obtener más información.

Configuración de PAM para utilizar server_policy de LDAP

Para configurar PAM para utilizar LDAP `server_policy`, siga el ejemplo en "Ejemplo de archivo `pam_conf` que utiliza el módulo para gestión de cuentas `pam_ldap`" en la página 210. Agregue las líneas que contienen `pam_ldap.so.1` al archivo `/etc/pam.conf` de cliente. Además, si algún módulo PAM del archivo `pam.conf` de muestra especifica el indicador `binding` y la opción `server_policy`, utilice el mismo indicador y la misma opción para el módulo correspondiente en el archivo `/etc/pam.conf`. Asimismo, agregue la opción `server_policy` a la línea que contiene el módulo de servicio `pam_authtok_store.so.1`.

Nota – Antes, si se activaba la gestión de cuentas `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación en cualquier momento que iniciaran sesión en el sistema. Por lo tanto, los inicios de sesión que no se basan en contraseña realizados con herramientas, como `ssh`, fallarán.

Realice la gestión de cuentas y recupere el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios como el usuario que inicia sesión. El nuevo control en el servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8` , que está activado de manera predeterminada.

Para cambiar este control por otro que no sea el predeterminado, agregue las instrucciones de control de acceso (ACI) en el servidor de directorios:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

- Indicador de control `binding`

  El uso del indicador de control `binding` permite que una contraseña local anule una contraseña remota (LDAP). Por ejemplo, si la cuenta de usuario se encuentra en los archivos locales y el espacio de nombres LDAP, la contraseña asociada con la cuenta local tiene precedencia con respecto a la contraseña remota. Por lo tanto, si la contraseña local caduca, la autenticación falla incluso si la contraseña remota LDAP aún es válida.

- Opción `server_policy`

  La opción `server_policy` da la instrucción a `pam_unix_auth`, `pam_unix_account` y `pam_passwd_auth` de ignorar a un usuario encontrado en el espacio de nombres LDAP y permitir a `pam_ldap` realizar la autenticación o la validación de cuenta. En el caso de `pam_authtok_store`, una contraseña nueva se transfiere al servidor LDAP sin cifrar. La contraseña se almacena en el directorio según el esquema de cifrado de contraseña configurado en el servidor. Para obtener más información, consulte `pam.conf(4)` y `pam_ldap(5)`.

Recuperación de información de servicios de nombres LDAP

Puede recuperar información sobre servicios de nombres LDAP con la utilidad `ldaplist`. Esta utilidad LDAP muestra la información de nombres de los servidores LDAP en formato LDIF. Puede resultar útil para la resolución de problemas. Consulte `ldaplist(1)` para obtener más información.

Listado de todos los contenedores LDAP

`ldaplist` muestra su resultado con una línea en blanco que separa los registros, que es útil para registros grandes con varias líneas.

Nota – El resultado de `ldaplist` depende de la configuración del cliente. Por ejemplo, si el valor de `ns_ldap_search` es `sub` en lugar de `one`, `ldaplist` muestra todas las entradas de la búsqueda actual `baseDN`.

A continuación se muestra un ejemplo del resultado de `ldaplist`.

```
# ldaplist
dn: ou=people,dc=west,dc=example,dc=com

dn: ou=group,dc=west,dc=example,dc=com

dn: ou=rpc,dc=west,dc=example,dc=com

dn: ou=protocols,dc=west,dc=example,dc=com

dn: ou=networks,dc=west,dc=example,dc=com

dn: ou=netgroup,dc=west,dc=example,dc=com

dn: ou=aliases,dc=west,dc=example,dc=com

dn: ou=hosts,dc=west,dc=example,dc=com

dn: ou=services,dc=west,dc=example,dc=com

dn: ou=ethers,dc=west,dc=example,dc=com

dn: ou=profile,dc=west,dc=example,dc=com

dn: automountmap=auto_home,dc=west,dc=example,dc=com

dn: automountmap=auto_direct,dc=west,dc=example,dc=com

dn: automountmap=auto_master,dc=west,dc=example,dc=com

dn: automountmap=auto_shared,dc=west,dc=example,dc=com
```

Listado de todos los atributos de entrada de usuario

Para mostrar información específica en una lista, como una entrada `passwd` de usuario, utilice `getent` como se indica a continuación:

```
# getent passwd user1
user1::30641:10:Joe Q. User:/home/user1:/bin/csh
```

Si desea ver todos los atributos en una lista, use `ldaplist` con la opción `-l`.

```
# ldaplist -l passwd user1
        dn: uid=user1,ou=People,dc=west,dc=example,dc=com
        uid: user1
        cn: user1
        uidNumber: 30641
        gidNumber: 10
        gecos: Joe Q. User
        homeDirectory: /home/user1
        loginShell: /bin/csh
        objectClass: top
        objectClass: shadowAccount
        objectClass: account
        objectClass: posixAccount
        shadowLastChange: 6445
```

Personalización del entorno de cliente LDAP

En las siguientes secciones, se describe cómo puede personalizar el entorno de cliente LDAP.

Puede cambiar cualquiera de los servicios, pero tenga cuidado, porque si los datos no se completan en el servidor para el servicio especificado, dejará de funcionar. Además, en algunos casos, es posible que los archivos no estén configurados de manera predeterminada.

Modificación del cambio de servicio de nombres para LDAP

Puede modificar el cambio de servicio de nombres para personalizar de dónde cada servicio obtiene su información. Consulte "Gestión del conmutador de servicio de nombres" en la página 39.

Activación de DNS con LDAP

Si desea activar DNS, consulte "Cómo activar un cliente DNS" en la página 49. Si se utiliza la autenticación por usuario, los mecanismos de sasl/GSSAPI y Kerberos esperan que el servicio de nombres DNS esté configurado y activado.

◆ ◆ ◆ CAPÍTULO 13

13 Resolución de problemas de LDAP (referencia)

En este capítulo se describen los problemas de configuración LDAP y se sugieren soluciones para resolverlos.

Supervisión del estado de los cliente LDAP

En las siguientes secciones se muestran varios comandos para ayudar a determinar el estado del entorno del cliente LDAP. Consulte también las páginas del comando man para obtener información adicional sobre las opciones que se pueden utilizar.

Para obtener una descripción general de la Utilidad de gestión de servicios (SMF), consulte el Capítulo 1, "Gestión de servicios (descripción general)" de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M) y `svcs`(1) para obtener más información.

Verificación de que el comando `ldap_cachemgr` está en ejecución

El daemon `ldap_cachemgr` debe estar ejecutándose y funcionando correctamente en todo momento. De lo contrario, el sistema no funciona. Al configurar e iniciar el servicio de cliente LDAP, `svc:/network/ldap/client`, el método SMF de cliente inicia automáticamente el daemon `ldap_cachemgr`. Los siguientes métodos determinan si el servicio de cliente LDAP está en línea:

- Utilice el comando `svcs` para ver si el servicio está activado.

```
# svcs \*ldap\*
STATE          STIME    FMRI
disabled       Aug_24   svc:/network/ldap/client:default
```

- Utilice este comando para ver toda la información sobre el servicio.

```
# svcs -l network/ldap/client:default
fmri svc:/network/ldap/client:default
name LDAP Name Service Client
enabled false
state disabled
next_state none
state_time Thu Oct 20 23:04:11 2011
logfile /var/svc/log/network-ldap-client:default.log
restarter svc:/system/svc/restarter:default
contract_id
manifest /lib/svc/manifest/network/ldap/client.xml
manifest /lib/svc/manifest/milestone/config.xml
manifest /lib/svc/manifest/network/network-location.xml
manifest /lib/svc/manifest/system/name-service/upgrade.xml
dependency optional_all/none svc:/milestone/config (online)
dependency optional_all/none svc:/network/location:default (online)
dependency require_all/none svc:/system/filesystem/minimal (online)
dependency require_all/none svc:/network/initial (online)
dependency require_all/restart svc:/network/nis/domain (online)
dependency optional_all/none svc:/system/manifest-import (online)
dependency require_all/none svc:/milestone/unconfig (online)
dependency optional_all/none svc:/system/name-service/upgrade (online)
```

- Pase la opción `-g` a `ldap_cachemgr`.

  Esta opción proporciona más información sobre el estado, que es útil para diagnosticar un problema.

```
# /usr/lib/ldap/ldap_cachemgr -g
cachemgr configuration:
server debug level          0
server log file "/var/ldap/cachemgr.log"
number of calls to ldapcachemgr         19

cachemgr cache data statistics:
Configuration refresh information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:43:28
Server information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:36:08
  server: 192.168.0.0, status: UP
  server: 192.168.0.1, status: ERROR
    error message: Can't connect to the LDAP server
Cache data information:
  Maximum cache entries:          256
  Number of cache entries:          2
```

Para obtener más información sobre el daemon `ldap_cachemgr`, consulte la página del comando man `ldap_cachemgr(1M)`.

Comprobación de la información actual de perfil

Conviértase en superusuario o adopte un rol equivalente, y ejecute `ldapclient` con la opción `lista`.

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1, 192.168.0.10
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_SEARCH_REF= TRUE
NS_LDAP_SEARCH_SCOPE= one
NS_LDAP_SEARCH_TIME= 30
NS_LDAP_SERVER_PREF= 192.168.0.1
NS_LDAP_PROFILE= pit1
NS_LDAP_CREDENTIAL_LEVEL= proxy
NS_LDAP_SERVICE_SEARCH_DESC= passwd:ou=people,?sub
NS_LDAP_SERVICE_SEARCH_DESC= group:ou=group,dc=west,dc=example,dc=com?one
NS_LDAP_BIND_TIME= 5
```

La información de perfil actual se puede ver mediante el comando `svccfg` o `svcprop`, o el comando `ldapclient` con la opción `lista`. Consulte la página del comando man `ldapclient(1M)` para obtener información específica sobre cada valor de propiedad disponible.

Verificación de comunicación básica cliente-servidor

La mejor manera de mostrar que el cliente está hablando con el servidor LDAP es con el comando `ldaplist`. Con `ldaplist` sin argumentos se vuelcan todos los contenedores en el servidor. Esto funciona siempre que existan contenedores, y no se tienen que rellenar. Consulte la página del comando man `ldaplist(1)` para obtener más información.

Si el primer paso funciona, puede intentar `ldaplist passwd` *username* o `ldaplist hosts` *hostname*, pero si contienen demasiados datos, es posible que desee elegir un servicio no tan lleno o guiarlos a `head` o `more`.

Comprobación de datos del servidor desde un equipo no cliente

La mayoría de los comandos de las secciones anteriores suponen que ya ha creado un cliente LDAP. Si no ha creado un cliente y desea revisar los datos del servidor, utilice el comando `ldapsearch`. En el siguiente ejemplo se muestran todos los contenedores.

```
# ldapsearch -h server1 -b "dc=west,dc=example,dc=com" -s one "objectclass=*"
```

La salida predeterminada para el comando `ldapsearch` es el formato LDIF estándar de la industria que está definido en RFC-2849. Todas las versiones de `ldapsearch` pueden proporcionar resultados en formato LDIF utilizando la opción `-L`.

Problemas y soluciones de la configuración de LDAP

En las siguientes secciones se describen los problemas de la configuración de LDAP y sugiere soluciones a los problemas.

Nombre de host no resuelto

El servidor back-end de cliente LDAP devuelve nombres de host completos para consultas de host, como nombres de host por `gethostbyname()` y `getaddrinfo()`. Si el nombre guardado está completo, es decir, contiene al menos un punto, el cliente devuelve el nombre como está. Por ejemplo, si el nombre almacenado es `hostB.eng`, el nombre devuelto es `hostB.eng`.

Si el nombre almacenado en el directorio de LDAP, no está completo (no contiene un punto), el back-end del cliente agrega la parte de dominio al nombre. Por ejemplo, si el nombre almacenado es `hostA`, el nombre devuelto es `hostA.domainname`.

No se puede acceder a los sistemas de forma remota en el dominio LDAP

Si el nombre de dominio DNS es diferente al nombre de dominio LDAP, el servicio de nombres LDAP no se puede usar para servir nombres de host, a menos que los nombres de host estén almacenados completos.

No funciona el inicio de sesión

Los clientes LDAP usan los módulos PAM para autenticación del usuario durante el inicio de sesión. Cuando se utiliza el módulo PAM de UNIX estándar, la contraseña se lee desde el servidor y se verifica en el cliente. Este proceso puede fallar debido a una de las siguientes razones:

1. `ldap` no está asociado a la base de datos `passwd` en el cambio de servicio de nombres.
2. El usuario del atributo `userPassword` de la lista de servidores no puede ser leído por el agente de proxy. Debe permitir que al menos el agente de proxy pueda leer la contraseña, porque el agente de proxy la devuelve al cliente para su comparación. `pam_ldap` no necesita acceso de lectura a la contraseña.
3. El agente de proxy podría no tener la contraseña correcta.
4. La entrada no contiene la clase de objeto `shadowAccount`.
5. No se ha definido una contraseña para el usuario.

Al usar `ldapaddent`, debe utilizar la opción `-p` para asegurarse de que la contraseña se agregue a la entrada de usuario. Si utiliza `ldapaddent` sin la opción `-p`, la contraseña del usuario no se almacena en el directorio a menos que también agregue el archivo `/etc/shadow` mediante `ldapaddent`.

6. No hay servidores LDAP accesibles.

   Compruebe el estado de los servidores.

   ```
   # /usr/lib/ldap/ldap_cachemgr -g
   ```

7. `pam.conf` se ha configurado incorrectamente.
8. El usuario no está definido en el espacio de nombres LDAP.
9. `NS_LDAP_CREDENTIAL_LEVEL` se establece en `anonymous` para los módulos `pam_unix_*`, y `userPassword` no está disponible para usuarios anónimos.
10. La contraseña no está almacenada en formato `crypt`.
11. Si `pam_ldap` está configurado para admitir la gestión de cuentas, la falla en el inicio de sesión podría ser el resultado de una de las siguientes opciones:
    - La contraseña del usuario ha caducado.
    - La cuenta del usuario está bloqueada debido a demasiados intentos fallidos de inicio de sesión.
    - La cuenta del usuario ha sido desactivada por el administrador.
    - El usuario intentó iniciar sesión mediante un programa no basado en contraseña, como `ssh` o `sftp`.
12. Si se utiliza la autenticación por usuario y sasl/GSSAPI, algún componente de Kerberos o la configuración de `pam_krb5` se establecieron incorrectamente. Consulte *Administración de Oracle Solaris 11.1: servicios de seguridad* para obtener detalles sobre la resolución de estos problemas.

Consulta demasiado lenta

La base de datos de LDAP se basa en índices para mejorar rendimiento de la consulta. Cuando los índices no están configurados correctamente, se produce una mayor degradación del rendimiento. La documentación incluye un conjunto común de atributos que se deben indexar. También puede agregar sus propios índices para mejorar el rendimiento en el sitio.

El comando `ldapclient` no se puede enlazar a un servidor

El comando `ldapclient` no pudo inicializar el cliente al utilizar la opción `init` con el atributo `profileName` especificado. Los posibles motivos de la falla incluyen los siguientes:

1. Se especificó el nombre de dominio incorrecto en la línea de comandos.

2. El atributo `nisDomain` no está configurado en el DIT para representar el punto de entrada para el dominio de cliente especificado.
3. La información de control de acceso no está correctamente configurada en el servidor, por lo que no permite la búsqueda anónima en la base de datos de LDAP.
4. Una dirección de servidor incorrecta que se pasa al comando `ldapclient`. Use el comando `ldapsearch` para verificar la dirección del servidor.
5. Un nombre de perfil incorrecto que se pasa al comando `ldapclient`. Use el comando `ldapsearch` para verificar el nombre de perfil en el DIT.
6. Use `snoop` en la interfaz de red del cliente para ver el tipo de tráfico de salida y determinar a qué servidor le está hablando.

Uso del daemon `ldap_cachemgr` para depuración

La ejecución del daemon `ldap_cachemgr` con la opción `-g` puede ser una manera útil de depurar, ya que puede ver las estadísticas y la configuración del cliente actual. Por ejemplo,

```
# ldap_cachemgr -g
```

podría imprimir la configuración actual y estadísticas en una salida estándar, incluido el estado de todos los servidores LDAP, como se ha mencionado anteriormente. Observe que *no* necesita convertirse en superusuario para ejecutar este comando.

El comando `ldapclient` se bloquea durante la configuración

Si el comando `ldapclient` se bloquea, si pulsa Ctrl-C se cerrará después de restaurar el entorno anterior. Si esto ocurre, consulte al administrador del servidor para asegurarse que el servidor se está ejecutando.

Revise también los atributos de la lista del servidor en el perfil o desde la línea de comandos, y asegúrese de que la información del servidor sea correcta.

◆ ◆ ◆ CAPÍTULO 14

Servicio de nombres LDAP (Referencia)

En este capítulo se tratan los siguientes temas.

Listas de comprobación en blanco para configuración de LDAP

TABLA 14–1 Listas de comprobación en blanco para definiciones de variable de servidor

Variable	Definición para _____ red
Número de puerto en el que se instaló una instancia del servidor de directorios (389)	
Nombre del servidor	
Servidores de réplica (número de IP: número de puerto)	
Gestor de directorios [`dn: cn=directory manager`]	
Nombre de dominio al que se prestará servicio	

TABLA 14–1 Listas de comprobación en blanco para definiciones de variable de servidor *(Continuación)*

Variable	Definición para _____ red
Tiempo máximo (en segundos) para procesar las solicitudes de clientes antes de que se agote el tiempo de espera	
Número máximo de entradas devueltas por cada solicitud de búsqueda	

TABLA 14–2 Listas de comprobación en blanco para definiciones de variables de perfil de cliente

Variable	Definición para _____red
Nombre del perfil	
Lista de servidores (de manera predeterminada, la subred local)	
Lista de servidores preferidos (en el orden en que se deben probar los servidores, primero, segundo, etc.)	
Ámbito de búsqueda (número de niveles inferiores en el árbol de directorios; 'One' o 'Sub'	
Credenciales utilizadas para acceder al servidor; el valor predeterminado es anonymous.	
¿Seguir referencias? (un puntero a otro servidor si el servidor principal no está disponible); el valor predeterminado es no	
Límite de tiempo de búsqueda (en segundos) para esperar que el servidor devuelva información. El valor predeterminado es 30 segundos.	
Límite de tiempo de vinculación (en segundos) para ponerse en contacto con el servidor. El valor predeterminado es 30 segundos.	
Valor predeterminado del método de autenticación: none	

Comandos de LDAP

Hay dos conjuntos de comandos relacionados con LDAP en el sistema Oracle Solaris. Un conjunto son las herramientas generales de LDAP, que no necesitan que el cliente esté configurado con servicios de nombres LDAP. El segundo conjunto utiliza la configuración de LDAP común en el cliente y se puede ejecutar en clientes que están configurados con o sin el servicio de nombres LDAP.

Herramientas generales de LDAP

Las herramientas de la línea de comandos de LDAP admiten un conjunto común de opciones, incluidos los parámetros de autenticación y de vínculo. Las siguientes herramientas admiten un formato basado en texto común para representar información del directorio denominada Formato de intercambio de datos LDAP (LDIF). Estos comandos se pueden utilizar para manipular las entradas de directorio directamente.

`ldapsearch`(1)
`ldapmodify`(1)
`ldapadd`(1)
`ldapdelete`(1)

Herramientas de LDAP que requieren servicios de nombres LDAP

TABLA 14–3 Herramientas de LDAP

Herramienta	Función
`ldapaddent`(1M)	Utilizado para crear entradas en contenedores de LDAP de los archivos `/etc` correspondientes. Esta herramienta permite rellenar el directorio desde los archivos. Por ejemplo, lee el archivo de formato `/etc/passwd` y completa las entradas `passwd` en el directorio.
`ldaplist`(1)	Se utiliza para enumerar el contenido de varios servicios desde el directorio.
`idsconfig`(1M)	Se utiliza para configurar Oracle Directory Server Enterprise Edition para servir clientes del servicio de nombres LDAP.

Ejemplo de archivo pam_conf que utiliza el módulo para gestión de cuentas pam_ldap

Nota – Antes, si se activaba la gestión de cuentas `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación en cualquier momento que iniciaran sesión en el sistema. Por lo tanto, los inicios de sesión que no se basan en contraseña realizados con herramientas, como `ssh`, fallarán.

Realice la gestión de cuentas y recupere el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios como el usuario que inicia sesión. El nuevo control en el servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8` , que está activado de manera predeterminada.

Para cambiar este control por otro que no sea el predeterminado, agregue las instrucciones de control de acceso (ACI) en el servidor de directorios:

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

```
#
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login   auth requisite        pam_authtok_get.so.1
login   auth required         pam_dhkeys.so.1
login   auth required         pam_unix_cred.so.1
login   auth required         pam_dial_auth.so.1
login   auth binding          pam_unix_auth.so.1 server_policy
login   auth required         pam_ldap.so.1
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin  auth sufficient       pam_rhosts_auth.so.1
rlogin  auth requisite        pam_authtok_get.so.1
rlogin  auth required         pam_dhkeys.so.1
rlogin  auth required         pam_unix_cred.so.1
rlogin  auth binding          pam_unix_auth.so.1 server_policy
rlogin  auth required         pam_ldap.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh     auth sufficient       pam_rhosts_auth.so.1
```

```
rsh     auth required         pam_unix_cred.so.1
rsh     auth binding          pam_unix_auth.so.1 server_policy
rsh     auth required         pam_ldap.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
ppp     auth requisite        pam_authtok_get.so.1
ppp     auth required         pam_dhkeys.so.1
ppp     auth required         pam_dial_auth.so.1
ppp     auth binding          pam_unix_auth.so.1 server_policy
ppp     auth required         pam_ldap.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other   auth requisite        pam_authtok_get.so.1
other   auth required         pam_dhkeys.so.1
other   auth required         pam_unix_cred.so.1
other   auth binding          pam_unix_auth.so.1 server_policy
other   auth required         pam_ldap.so.1
#
# passwd command (explicit because of a different authentication module)
#
passwd  auth binding          pam_passwd_auth.so.1 server_policy
passwd  auth required         pam_ldap.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
cron    account required      pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite     pam_roles.so.1
other   account binding       pam_unix_account.so.1 server_policy
other   account required      pam_ldap.so.1
#
# Default definition for Session management
# Used when service name is not explicitly mentioned for session management
#
other   session required      pam_unix_session.so.1
#
# Default definition for  Password management
# Used when service name is not explicitly mentioned for password management
#
other   password required     pam_dhkeys.so.1
other   password requisite    pam_authtok_get.so.1
other   password requisite    pam_authtok_check.so.1
other   password required     pam_authtok_store.so.1 server_policy
#
# Support for Kerberos V5 authentication and example configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES" section.
#
```

Esquemas IETF para LDAP

Los esquemas son definiciones que describen los tipos de información que pueden almacenarse como entradas en un directorio del servidor.

Para que un servidor de directorios admita los clientes de nombres LDAP, los esquemas definidos en este capítulo deben estar configurados en el servidor a menos que los esquemas se asignen mediante la función de asignación de esquemas de los clientes.

Varios esquemas LDAP requeridos que define IETF: el esquema del Servicio de información de la red RFC 2307 y RFC 2307bis, y un esquema de perfil de configuración para agentes basados en Protocolo ligero de acceso a directorios (LDAP) (RFC 4876) y el esquema LDAP para servicios de impresora. Para admitir NIS, la definición de estos esquemas se debe agregar al servidor de directorios. Se puede acceder a las distintas RFC desde el sitio web de IETF `http://www.ietf.org`.

Nota – Los borradores de Internet, como RFC 2307bis, son documentos borradores válidos por un máximo de seis meses y se pueden actualizar o se pueden procesar obsoletos mediante otros documentos, en cualquier momento.

Esquema del Servicio de información de la red RFC 2307bis

Los servidores LDAP deben estar configurados para admitir la RFC 2307bis revisada:

El OID `nisSchema` es `1.3.6.1.1`. Los atributos de RFC 2307bis son los siguientes.

```
( nisSchema.1.0 NAME 'uidNumber'
DESC 'An integer uniquely identifying a user in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.1 NAME 'gidNumber'
DESC 'An integer uniquely identifying a group in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.2 NAME 'gecos'
DESC 'The GECOS field; the common name'
EQUALITY caseIgnoreIA5Match
SUBSTRINGS caseIgnoreIA5SubstringsMatch
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.3 NAME 'homeDirectory'
DESC 'The absolute path to the home directory'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )
```

```
( nisSchema.1.4 NAME 'loginShell'
DESC 'The path to the login shell'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.5 NAME 'shadowLastChange'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.6 NAME 'shadowMin'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.7 NAME 'shadowMax'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.8 NAME 'shadowWarning'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.9 NAME 'shadowInactive'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.10 NAME 'shadowExpire'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.11 NAME 'shadowFlag'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.12 NAME 'memberUid'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.13 NAME 'memberNisNetgroup'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )

( nisSchema.1.15 NAME 'ipServicePort'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.16 NAME 'ipServiceProtocol'
SUP name )

( nisSchema.1.17 NAME 'ipProtocolNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.18 NAME 'oncRpcNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.19 NAME 'ipHostNumber'
DESC 'IP address as a dotted decimal, eg. 192.168.1.1
        omitting leading zeros'
SUP name )

( nisSchema.1.20 NAME 'ipNetworkNumber'
DESC 'IP network as a dotted decimal, eg. 192.168,
        omitting leading zeros'
SUP name SINGLE-VALUE )

( nisSchema.1.21 NAME 'ipNetmaskNumber'
DESC 'IP netmask as a dotted decimal, eg. 255.255.255.0,
         omitting leading zeros'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' SINGLE-VALUE )

( nisSchema.1.22 NAME 'macAddress'
DESC 'MAC address in maximal, colon separated hex
      notation, eg. 00:00:92:90:ee:e2'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' )

( nisSchema.1.23 NAME 'bootParameter'
DESC 'rpc.bootparamd parameter'
SYNTAX 'bootParameterSyntax' )

( nisSchema.1.24 NAME 'bootFile'
DESC 'Boot image name'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' )

( nisSchema.1.26 NAME 'nisMapName'
SUP name )

( nisSchema.1.27 NAME 'nisMapEntry'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String{1024}' SINGLE-VALUE )

( nisSchema.1.28 NAME 'nisPublicKey'
DESC 'NIS public key'
SYNTAX 'nisPublicKeySyntax' )

( nisSchema.1.29 NAME 'nisSecretKey'
DESC 'NIS secret key'
SYNTAX 'nisSecretKeySyntax' )

( nisSchema.1.30 NAME 'nisDomain'
DESC 'NIS domain'
SYNTAX 'IA5String' )

( nisSchema.1.31 NAME 'automountMapName'
DESC 'automount Map Name'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.32 NAME 'automountKey'
DESC 'Automount Key value'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.33 NAME 'automountInformation'
DESC 'Automount information'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

El OID de `nisSchema` es `1.3.6.1.1`. Las `objectClasses` de RFC 2307 son las siguientes.

```
( nisSchema.2.0 NAME 'posixAccount' SUP top AUXILIARY
  DESC 'Abstraction of an account with POSIX attributes'
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
  MAY ( userPassword $ loginShell $ gecos $ description ) )

( nisSchema.2.1 NAME 'shadowAccount' SUP top AUXILIARY
  DESC 'Additional attributes for shadow passwords'
  MUST uid
  MAY ( userPassword $ shadowLastChange $ shadowMin
        shadowMax $ shadowWarning $ shadowInactive $
        shadowExpire $ shadowFlag $ description ) )

( nisSchema.2.2 NAME 'posixGroup' SUP top STRUCTURAL
  DESC 'Abstraction of a group of accounts'
  MUST ( cn $ gidNumber )
  MAY ( userPassword $ memberUid $ description ) )

( nisSchema.2.3 NAME 'ipService' SUP top STRUCTURAL
  DESC 'Abstraction an Internet Protocol service.
        Maps an IP port and protocol (such as tcp or udp)
        to one or more names; the distinguished value of
        the cn attribute denotes the service's canonical
        name'
  MUST ( cn $ ipServicePort $ ipServiceProtocol )
  MAY ( description ) )

( nisSchema.2.4 NAME 'ipProtocol' SUP top STRUCTURAL
  DESC 'Abstraction of an IP protocol. Maps a protocol number
        to one or more names. The distinguished value of the cn
        attribute denotes the protocol's canonical name'
  MUST ( cn $ ipProtocolNumber )
  MAY  description )

( nisSchema.2.5 NAME 'oncRpc' SUP top STRUCTURAL
  DESC 'Abstraction of an Open Network Computing (ONC)
        [RFC1057] Remote Procedure Call (RPC) binding.
        This class maps an ONC RPC number to a name.
        The distinguished value of the cn attribute denotes
        the RPC service's canonical name'
  MUST ( cn $ oncRpcNumber $ description )
  MAY  description )
```

```
( nisSchema.2.6 NAME 'ipHost' SUP top AUXILIARY
  DESC 'Abstraction of a host, an IP device. The distinguished
        value of the cn attribute denotes the host's canonical
        name. Device SHOULD be used as a structural class'
  MUST ( cn $ ipHostNumber )
  MAY ( l $ description $ manager $ userPassword ) )

( nisSchema.2.7 NAME 'ipNetwork' SUP top STRUCTURAL
  DESC 'Abstraction of a network. The distinguished value of
        the cn attribute denotes the network's canonical name'
  MUST ipNetworkNumber
  MAY ( cn $ ipNetmaskNumber $ l $ description $ manager ) )

( nisSchema.2.8 NAME 'nisNetgroup' SUP top STRUCTURAL
  DESC 'Abstraction of a netgroup. May refer to other netgroups'
  MUST cn
  MAY ( nisNetgroupTriple $ memberNisNetgroup $ description ) )

( nisSchema.2.9 NAME 'nisMap' SUP top STRUCTURAL
  DESC 'A generic abstraction of a NIS map'
  MUST nisMapName
  MAY description )

( nisSchema.2.10 NAME 'nisObject' SUP top STRUCTURAL
  DESC 'An entry in a NIS map'
  MUST ( cn $ nisMapEntry $ nisMapName )
  MAY description )

( nisSchema.2.11 NAME 'ieee802Device' SUP top AUXILIARY
  DESC 'A device with a MAC address; device SHOULD be
        used as a structural class'
  MAY macAddress )

( nisSchema.2.12 NAME 'bootableDevice' SUP top AUXILIARY
  DESC 'A device with boot parameters; device SHOULD be
  used as a structural class'
  MAY ( bootFile $ bootParameter ) )

( nisSchema.2.14 NAME 'nisKeyObject' SUP top AUXILIARY
  DESC 'An object with a public and secret key'
  MUST ( cn $ nisPublicKey $ nisSecretKey )
  MAY ( uidNumber $ description ) )

( nisSchema.2.15 NAME 'nisDomainObject' SUP top AUXILIARY
  DESC 'Associates a NIS domain with a naming context'
  MUST nisDomain )

( nisSchema.2.16 NAME 'automountMap' SUP top STRUCTURAL
  MUST ( automountMapName )
  MAY description )

( nisSchema.2.17 NAME 'automount' SUP top STRUCTURAL
  DESC 'Automount information'
  MUST ( automountKey $ automountInformation )
  MAY description )

( nisSchema.2.18 NAME 'groupOfMembers' SUP top STRUCTURAL
  DESC 'A group with members (DNs)'
  MUST cn
```

```
  MAY ( businessCategory $ seeAlso $ owner $ ou $ o $
        description $ member ) )
```

Esquema de alias de correo

La información de alias de correo utiliza el esquema definido por este borrador de Internet. Hasta que haya un nuevo esquema disponible, los clientes LDAP seguirán utilizando este esquema para la información de alias de correo.

El esquema de grupos de correo de LDAP original contiene un gran número de atributos y clases de objeto. Los clientes de LDAP utilizan sólo dos atributos y una sola clase de objeto. Estos se muestran a continuación.

Los atributos de alias de correo son los siguientes.

```
( 0.9.2342.19200300.100.1.3
  NAME 'mail'
  DESC 'RFC822 email address for this person'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String(256)'
  SINGLE-VALUE )

( 2.16.840.1.113730.3.1.30
  NAME 'mgrpRFC822MailMember'
  DESC 'RFC822 mail address of email only member of group'
  EQUALITY CaseIgnoreIA5Match
  SYNTAX 'IA5String(256)' )
```

El esquema para la clase de objeto `mailGroup` es la siguiente.

```
( 2.16.840.1.113730.3.2.4
  NAME 'mailGroup'
  SUP top
  STRUCTURAL
  MUST mail
  MAY ( cn $ mailAlternateAddress $ mailHost $ mailRequireAuth $
   mgrpAddHeader $ mgrpAllowedBroadcaster $ mgrpAllowedDomain $
   mgrpApprovePassword $ mgrpBroadcasterModeration $ mgrpDeliverTo $
   mgrpErrorsTo $ mgrpModerator $ mgrpMsgMaxSize $
   mgrpMsgRejectAction $ mgrpMsgRejectText $ mgrpNoMatchAddrs $
   mgrpRemoveHeader $ mgrpRFC822MailMember ))
```

Esquema de perfil de agente de usuario de directorio (DUAProfile)

El `DUAConfSchemaOID` es `1.3.6.1.4.1.11.1.3.1`.

```
DESC 'Default LDAP server host address used by a DUA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
```

```
  SINGLE-VALUE )

( DUAConfSchemaOID.1.0 NAME 'defaultServerList'
  DESC 'Default LDAP server host address used by a DUAList'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.1 NAME 'defaultSearchBase'
  DESC 'Default LDAP base DN used by a DUA'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE )

( DUAConfSchemaOID.1.2 NAME 'preferredServerList'
  DESC 'Preferred LDAP server host addresses to be used by a
  DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.3 NAME 'searchTimeLimit'
  DESC 'Maximum time in seconds a DUA should allow for a
  search to complete'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.4 NAME 'bindTimeLimit'
  DESC 'Maximum time in seconds a DUA should allow for the
  bind operation to complete'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.5 NAME 'followReferrals'
  DESC 'Tells DUA if it should follow referrals
  returned by a DSA search result'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE )

( DUAConfSchemaOID.1.6 NAME 'authenticationMethod'
  DESC 'A keystring which identifies the type of
  authentication method used to contact the DSA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.7 NAME 'profileTTL'
  DESC 'Time to live before a client DUA
  should re-read this configuration profile'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.9 NAME 'attributeMap'
  DESC 'Attribute mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

```
( DUAConfSchemaOID.1.10 NAME 'credentialLevel'
  DESC 'Identifies type of credentials a DUA should
  use when binding to the LDAP server'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE )

( DUAConfSchemaOID.1.11 NAME 'objectclassMap'
  DESC 'Objectclass mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.12 NAME 'defaultSearchScope'
  DESC 'Default search scope used by a DUA'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.13 NAME 'serviceCredentialLevel'
  DESC 'Identifies type of credentials a DUA
  should use when binding to the LDAP server for a
  specific service'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.14 NAME 'serviceSearchDescriptor'
  DESC 'LDAP search descriptor list used by Naming-DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( DUAConfSchemaOID.1.15 NAME 'serviceAuthenticationMethod'
  DESC 'Authentication Method used by a service of the DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

    ( DUAConfSchemaOID.2.4 NAME 'DUAConfigProfile'
        SUP top STRUCTURAL
      DESC 'Abstraction of a base configuration for a DUA'
      MUST ( cn )
      MAY ( defaultServerList $ preferredServerList $
     defaultSearchBase $ defaultSearchScope $
     searchTimeLimit $ bindTimeLimit $
     credentialLevel $ authenticationMethod $
     followReferrals $ serviceSearchDescriptor $
     serviceCredentialLevel $ serviceAuthenticationMethod $
     objectclassMap $ attributeMap $
     profileTTL ) )
```

Esquemas de Oracle Solaris

Los esquemas necesarios para la plataforma de Oracle Solaris son los siguientes.

- Esquema de proyectos
- Esquemas de control de acceso basado en roles y de perfil de ejecución
- Esquemas de impresora

Esquema de proyectos

El archivo `/etc/project` es una fuente local de atributos asociados con los proyectos. Para obtener más información, consulte la página del comando man `user_attr(4)`.

Los atributos del proyecto son los siguientes.

```
( 1.3.6.1.4.1.42.2.27.5.1.1 NAME 'SolarisProjectID'
  DESC 'Unique ID for a Solaris Project entry'
  EQUALITY integerMatch
  SYNTAX INTEGER SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.2 NAME 'SolarisProjectName'
  DESC 'Name of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.3 NAME 'SolarisProjectAttr'
  DESC 'Attributes of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String )

( 1.3.6.1.4.1.42.2.27.5.1.30 NAME 'memberGid'
  DESC 'Posix Group Name'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' )
```

El proyecto `objectClass` es el siguiente.

```
( 1.3.6.1.4.1.42.2.27.5.2.1 NAME 'SolarisProject'
  SUP top STRUCTURAL
  MUST ( SolarisProjectID $ SolarisProjectName )
  MAY ( memberUid $ memberGid $ description $ SolarisProjectAttr ) )
```

Esquema de control de acceso basado en roles y de perfil de ejecución

El archivo `/etc/user_attr` es un origen local de los atributos extendidos asociados a usuarios y roles. Para obtener más información, consulte la página del comando man `user_attr(4)`.

Los atributos de control de acceso basado en roles son los siguientes.

```
( 1.3.6.1.4.1.42.2.27.5.1.4 NAME 'SolarisAttrKeyValue'
  DESC 'Semi-colon separated key=value pairs of attributes'
  EQUALITY caseIgnoreIA5Match
  SUBSTRINGS caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.7 NAME 'SolarisAttrShortDesc'
  DESC 'Short description about an entry, used by GUIs'
  EQUALITY caseIgnoreIA5Match
```

```
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.8 NAME 'SolarisAttrLongDesc'
  DESC 'Detail description about an entry'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.9 NAME 'SolarisKernelSecurityPolicy'
  DESC 'Solaris  kernel security policy'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.10 NAME 'SolarisProfileType'
  DESC 'Type of object defined in profile'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.11 NAME 'SolarisProfileId'
  DESC 'Identifier of object defined in profile'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.12 NAME 'SolarisUserQualifier'
  DESC 'Per-user login attributes'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.13 NAME 'SolarisReserved1'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.14 NAME 'SolarisReserved2'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )
```

El control de acceso basado en roles `objectClassses` es el siguiente:

```
( 1.3.6.1.4.1.42.2.27.5.2.3 NAME 'SolarisUserAttr' SUP top AUXILIARY
  DESC 'User attributes'
  MAY ( SolarisUserQualifier $ SolarisAttrReserved1 $ \
        SolarisAttrReserved2 $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.4 NAME 'SolarisAuthAttr' SUP top STRUCTURAL
  DESC 'Authorizations data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrShortDesc $ SolarisAttrLongDesc $ \
        SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.5 NAME 'SolarisProfAttr' SUP top STRUCTURAL
  DESC 'Profiles data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrLongDesc $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.6 NAME 'SolarisExecAttr' SUP top AUXILIARY
```

```
  DESC 'Profiles execution attributes'
  MAY ( SolarisKernelSecurityPolicy $ SolarisProfileType $ \
        SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisProfileId $ SolarisAttrKeyValue ) )
```

Información de Internet Print Protocol para LDAP

Las siguientes secciones proporcionan información sobre los atributos y `ObjectClasses` para el protocolo de impresión de Internet y la impresora.

Atributos de protocolo de impresión de Internet

```
( 1.3.18.0.2.4.1140
NAME 'printer-uri'
DESC 'A URI supported by this printer.
This URI SHOULD be used as a relative distinguished name (RDN).
If printer-xri-supported is implemented, then this URI value
MUST be listed in a member value of printer-xri-supported.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1107
NAME 'printer-xri-supported'
DESC 'The unordered list of XRI (extended resource identifiers) supported
by this printer.
Each member of the list consists of a URI (uniform resource identifier)
followed by optional authentication and security metaparameters.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( 1.3.18.0.2.4.1135
NAME 'printer-name'
DESC 'The site-specific administrative name of this printer, more end-user
friendly than a URI.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1119
NAME 'printer-natural-language-configured'
DESC 'The configured language in which error and status messages will be
generated (by default) by this printer.
Also, a possible language for printer string attributes set by operator,
system administrator, or manufacturer.
Also, the (declared) language of the "printer-name", "printer-location",
"printer-info", and "printer-make-and-model" attributes of this printer.
For example: "en-us" (US English) or "fr-fr" (French in France) Legal values of
```

```
language tags conform to [RFC3066] "Tags for the Identification of Languages".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1136
NAME 'printer-location'
DESC 'Identifies the location of the printer. This could include
things like: "in Room 123A", "second floor of building XYZ".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1139
NAME 'printer-info'
DESC 'Identifies the descriptive information about this printer.
This could include things like: "This printer can be used for
printing color transparencies for HR presentations", or
"Out of courtesy for others, please print only small (1-5 page)
jobs at this printer", or even "This printer is going away on July 1, 1997,
please find a new printer".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1134
NAME 'printer-more-info'
DESC 'A URI used to obtain more information about this specific printer.
For example, this could be an HTTP type URI referencing an HTML page
accessible to a Web Browser.
The information obtained from this URI is intended for end user consumption.'
EQUALITY caseIgnoreMatch ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1138
NAME 'printer-make-and-model'
DESC 'Identifies the make and model of the device.
The device manufacturer MAY initially populate this attribute.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1133
NAME 'printer-ipp-versions-supported'
DESC 'Identifies the IPP protocol version(s) that this printer supports,
including major and minor versions,
i.e., the version numbers for which this Printer implementation meets
the conformance requirements.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )
```

```
( 1.3.18.0.2.4.1132
NAME 'printer-multiple-document-jobs-supported'
DESC 'Indicates whether or not the printer supports more than one
document per job, i.e., more than one Send-Document or Send-Data
operation with document data.'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

( 1.3.18.0.2.4.1109
NAME 'printer-charset-configured'
DESC 'The configured charset in which error and status messages will be
generated (by default) by this printer.
Also, a possible charset for printer string attributes set by operator,
system administrator, or manufacturer.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the "(preferred MIME name)" SHALL be used as the tag.
For coherence with IPP Model, charset tags in this attribute SHALL be
lowercase normalized.
This attribute SHOULD be static (time of registration) and SHOULD NOT be
dynamically refreshed attributetypes: (subsequently).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} SINGLE-VALUE )

( 1.3.18.0.2.4.1131
NAME 'printer-charset-supported'
DESC 'Identifies the set of charsets supported for attribute type values of
type Directory String for this directory entry.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the preferred MIME name.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1137
NAME 'printer-generated-natural-language-supported'
DESC 'Identifies the natural language(s) supported for this directory entry.
For example: "en-us" (US English) or "fr-fr" (French in France).
Legal values conform to [RFC3066], Tags for the Identification of Languages.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1130
NAME 'printer-document-format-supported'
DESC 'The possible document formats in which data may be interpreted
and printed by this printer.
Legal values are MIME types come from the IANA Registry of Internet Media Types.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1129
NAME 'printer-color-supported'
DESC 'Indicates whether this printer is capable of any type of color printing
at all, including highlight color.'
EQUALITY booleanMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.7  SINGLE-VALUE )
```

```
( 1.3.18.0.2.4.1128
NAME 'printer-compression-supported'
DESC 'Compression algorithms supported by this printer.
For example: "deflate, gzip".  Legal values include; "none", "deflate"
attributetypes: (public domain ZIP), "gzip" (GNU ZIP), "compress" (UNIX).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1127
NAME 'printer-pages-per-minute'
DESC 'The nominal number of pages per minute which may be output by this
printer (e.g., a simplex or black-and-white printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1126 NAME 'printer-pages-per-minute-color'
DESC 'The nominal number of color pages per minute which may be output by this
printer (e.g., a simplex or color printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1125 NAME 'printer-finishings-supported'
DESC 'The possible finishing operations supported by this printer.
Legal values include; "none", "staple", "punch", "cover", "bind", "saddle-stitch",
"edge-stitch", "staple-top-left", "staple-bottom-left", "staple-top-right",
"staple-bottom-right", "edge-stitch-left", "edge-stitch-top", "edge-stitch-right",
"edge-stitch-bottom", "staple-dual-left", "staple-dual-top", "staple-dual-right",
"staple-dual-bottom".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1124 NAME 'printer-number-up-supported'
DESC 'The possible numbers of print-stream pages to impose upon a single side of
an instance of a selected medium. Legal values include; 1, 2, and 4.
Implementations may support other values.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27 )

( 1.3.18.0.2.4.1123 NAME 'printer-sides-supported'
DESC 'The number of impression sides (one or two) and the two-sided impression
rotations supported by this printer.
Legal values include; "one-sided", "two-sided-long-edge", "two-sided-short-edge".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1122 NAME 'printer-media-supported'
DESC 'The standard names/types/sizes (and optional color suffixes) of the media
supported by this printer.
For example: "iso-a4",  "envelope", or "na-letter-white".
```

```
Legal values  conform to ISO 10175, Document Printing Application (DPA), and any
IANA registered extensions.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1117 NAME 'printer-media-local-supported'
DESC 'Site-specific names of media supported by this printer, in the language in
"printer-natural-language-configured".
For example: "purchasing-form" (site-specific name) as opposed to
(in "printer-media-supported"): "na-letter" (standard keyword from ISO 10175).'
EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1121 NAME 'printer-resolution-supported'
DESC 'List of resolutions supported for printing documents by this printer.
Each resolution value is a string with 3 fields:
1) Cross feed direction resolution (positive integer), 2) Feed direction
resolution (positive integer), 3) Resolution unit.
Legal values are "dpi" (dots per inch) and "dpcm" (dots per centimeter).
Each resolution field is delimited by ">".  For example:  "300> 300> dpi>".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1120 NAME 'printer-print-quality-supported'
DESC 'List of print qualities supported for printing documents on this printer.
For example: "draft, normal".  Legal values include; "unknown", "draft", "normal",
"high".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1110 NAME 'printer-job-priority-supported'
DESC 'Indicates the number of job priority levels supported.
An IPP conformant printer which supports job priority must always support a
full range of priorities from "1" to "100"
(to ensure consistent behavior), therefore this attribute describes the
"granularity".
 Legal values of this attribute are from "1" to "100".'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1118
NAME 'printer-copies-supported'
DESC 'The maximum number of copies of a document that may be printed as a single job.
A value of "0" indicates no maximum limit.
A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1111
NAME 'printer-job-k-octets-supported'
DESC 'The maximum size in kilobytes (1,024 octets actually) incoming print job that
this printer will accept.
A value of "0" indicates no maximum limit.  A value of "-1" indicates unknown.'
EQUALITY integerMatch
```

```
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1113
NAME 'printer-service-person'
DESC 'The name of the current human service person responsible for servicing this
printer.
It is suggested that this string include information that would enable other humans
to reach the service person, such as a phone number.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1114
NAME 'printer-delivery-orientation-supported'
DESC 'The possible delivery orientations of pages as they are printed and ejected
from this printer.
Legal values include; "unknown", "face-up", and "face-down".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1115
NAME 'printer-stacking-order-supported'
DESC 'The possible stacking order of pages as they are printed and ejected from
this printer.
Legal values include; "unknown", "first-to-last", "last-to-first".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1116
NAME 'printer-output-features-supported'
DESC 'The possible output features supported by this printer.
Legal values include; "unknown", "bursting", "decollating", "page-collating",
"offset-stacking".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1108
NAME 'printer-aliases'
DESC 'Site-specific administrative names of this printer in addition the printer
name specified for printer-name.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.6.1.4.1.42.2.27.5.1.63
NAME 'sun-printer-bsdaddr'
DESC 'Sets the server, print queue destination name and whether the client generates
protocol extensions.
"Solaris" specifies a Solaris print server extension. The value is represented b the
following value: server "," destination ", Solaris".'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.64
NAME 'sun-printer-kvp'
```

```
DESC 'This attribute contains a set of key value pairs which may have meaning to the
print subsystem or may be user defined.
Each value is represented by the following: key "=" value.'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Protocolo de impresión de Internet ObjectClasses

```
objectclasses: ( 1.3.18.0.2.6.2549
NAME 'slpService'
DESC 'DUMMY definition'
SUP 'top' MUST (objectclass) MAY ())

objectclasses: ( 1.3.18.0.2.6.254
NAME 'slpServicePrinter'
DESC 'Service Location Protocol (SLP) information.'
AUXILIARY SUP 'slpService')

objectclasses: ( 1.3.18.0.2.6.258
NAME 'printerAbstract'
DESC 'Printer related information.'
ABSTRACT SUP 'top' MAY ( printer-name
$ printer-natural-language-configured
$ printer-location
$ printer-info
$ printer-more-info
$ printer-make-and-model
$ printer-multiple-document-jobs-supported
$ printer-charset-configured
$ printer-charset-supported
$ printer-generated-natural-language-supported
$ printer-document-format-supported
$ printer-color-supported
$ printer-compression-supported
$ printer-pages-per-minute
$ printer-pages-per-minute-color
$ printer-finishings-supported
$ printer-number-up-supported
$ printer-sides-supported
$ printer-media-supported
$ printer-media-local-supported
$ printer-resolution-supported
$ printer-print-quality-supported
$ printer-job-priority-supported
$ printer-copies-supported
$ printer-job-k-octets-supported
$ printer-current-operator
$ printer-service-person
$ printer-delivery-orientation-supported
$ printer-stacking-order-supported $ printer! -output-features-supported ))

objectclasses: ( 1.3.18.0.2.6.255
NAME 'printerService'
DESC 'Printer information.'
STRUCTURAL SUP 'printerAbstract' MAY ( printer-uri
$ printer-xri-supported ))
```

```
objectclasses: ( 1.3.18.0.2.6.257
NAME 'printerServiceAuxClass'
DESC 'Printer information.'
AUXILIARY SUP 'printerAbstract' MAY ( printer-uri $ printer-xri-supported ))

objectclasses: ( 1.3.18.0.2.6.256
NAME 'printerIPP'
DESC 'Internet Printing Protocol (IPP) information.'
AUXILIARY SUP 'top' MAY   ( printer-ipp-versions-supported $
printer-multiple-document-jobs-supported ))

objectclasses: ( 1.3.18.0.2.6.253
NAME 'printerLPR'
DESC 'LPR information.'
AUXILIARY SUP 'top' MUST ( printer-name ) MAY ( printer-aliases))

objectclasses: ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME 'sunPrinter'
DESC 'Sun printer information'
SUP 'top' AUXILIARY MUST (objectclass $ printer-name)  MAY
(sun-printer-bsdaddr $ sun-printer-kvp))
```

Atributos de la impresora

```
ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.63
NAME sun-printer-bsdaddr
DESC 'Sets the server, print queue destination name and whether the
     client generates protocol extensions. "Solaris" specifies a
     Solaris print server extension.  The value is represented by
     the following value: server "," destination ", Solaris".'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
)


ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.64
NAME sun-printer-kvp
DESC 'This attribute contains a set of key value pairs which may have
      meaning to the print subsystem or may be user defined.  Each
      value is represented by the following: key "=" value.'
EQUALITY caseIgnoreIA5Match
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15  )
```

Impresora de Sun ObjectClasses

```
OBJECTCLASS ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME sunPrinter
DESC 'Sun printer information'
SUP  top
AUXILIARY
MUST ( printer-name )
MAY  ( sun-printer-bsdaddr $ sun-printer-kvp ))
```

Requisitos genéricos del servidor de directorios para LDAP

Para admitir clientes LDAP, todos los servidores deben admitir el protocolo v3 de LDAP, los nombres compuestos y las clases de objeto auxiliares. Además, se debe admitir al menos uno de los siguientes controles.

- Modo de página simple (RFC 2696)
- Controles de vista de lista virtual

  El servidor debe admitir al menos uno de los siguientes métodos de autenticación.

```
anonymous
simple
sasl/cram-MD5
sasl/digest-MD5
sasl/GSSAPI
```

Si un cliente LDAP utiliza los módulos `pam_unix_*`, el servidor debe admitir el almacenamiento de contraseñas en el formato crypt de UNIX.

Si un cliente LDAP utiliza TLS, el servidor debe admitir SSL o TLS.

Si un cliente LDAP utiliza `sasl/GSSAPI`, el servidor debe admitir autenticación SASL, GSSAPI y Kerberos 5. El soporte para la transmisión del cifrado GSS es opcional.

Filtros predeterminados utilizados por los servicios de nombres LDAP

Si no especifica manualmente un parámetro para un servicio determinado que usa un SSD, se utiliza el filtro predeterminado. Para mostrar los filtros predeterminados para un servicio determinado, utilice `ldaplist` con la opción `-v`.

En el siguiente ejemplo, `filter=(&(objectclass=iphost)(cn=abcde)` define los filtros predeterminados.

```
database=hosts
filter=(&(objectclass=iphost)(cn=abcde)
user data=(&(%s) (cn=abcde))
```

`ldaplist` genera la siguiente lista de filtros predeterminados, donde `%s` significa una cadena y `%d`, un número.

```
hosts
(&(objectclass=iphost)(cn=%s))
--------------
```

```
passwd
(&(objectclass=posixaccount)(uid=%s))
--------------
services
(&(objectclass=ipservice)(cn=%s))
--------------
group
(&(objectclass=posixgroup)(cn=%s))
--------------
netgroup
(&(objectclass=nisnetgroup)(cn=%s))
--------------
networks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
netmasks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
rpc
(&(objectclass=oncrpc)(cn=%s))
--------------
protocols
(&(objectclass=ipprotocol)(cn=%s))
--------------
bootparams
(&(objectclass=bootableDevice)(cn=%s))
--------------
ethers
(&(objectclass=ieee802Device)(cn=%s))
--------------
publickey
(&(objectclass=niskeyobject)(cn=%s))
or
(&(objectclass=niskeyobject)(uidnumber=%d))
--------------
aliases
(&(objectclass=mailGroup)(cn=%s))
--------------
```

TABLA 14–4 Filtros LDAP utilizados en llamadas getXbyY

Filtro	Definición
bootparamByName	(&(objectClass=bootableDevice)(cn=%s))
etherByHost	(&(objectClass=ieee802Device)(cn=%s))
etherByEther	(&(objectClass=ieee802Device)(macAddress=%s))
groupByName	(&(objectClass=posixGroup)(cn=%s))
groupByGID	(&(objectClass=posixGroup)(gidNumber=%ld))
groupByMember	(&(objectClass=posixGroup)(memberUid=%s))
hostsByName	(&(objectClass=ipHost)(cn=%s))
hostsByAddr	(&(objectClass=ipHost)(ipHostNumber=%s))

TABLA 14–4 Filtros LDAP utilizados en llamadas getXbyY *(Continuación)*

Filtro	Definición
keyByUID	(&(objectClass=nisKeyObject)(uidNumber=%s))
keyByHost	(&(objectClass=nisKeyObject)(cn=%s))
netByName	(&(objectClass=ipNetwork)(cn=%s))
netByAddr	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
nisgroupMember	(membernisnetgroup=%s)
maskByNet	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
printerByName	(&(objectClass=sunPrinter)(|(printer-name=%s) (printer-aliases=%s)))
projectByName	(&(objectClass=SolarisProject)(SolarisProjectName=%s))
projectByID	(&(objectClass=SolarisProject)(SolarisProjectID=%ld))
protoByName	(&(objectClass=ipProtocol)(cn=%s))
protoByNumber	(&(objectClass=ipProtocol)(ipProtocolNumber=%d))
passwordByName	(&(objectClass=posixAccount)(uid=%s))
passwordByNumber	(&(objectClass=posixAccount)(uidNumber=%ld))
rpcByName	(&(objectClass=oncRpc)(cn=%s))
rpcByNumber	(&(objectClass=oncRpc)(oncRpcNumber=%d))
serverByName	(&(objectClass=ipService)(cn=%s))
serverByPort	(&(objectClass=ipService)(ipServicePort=%ld))
serverByNameAndProto	(&(objectClass=ipService)(cn=%s)(ipServiceProtocol=%s))
specialByNameserver	(ipServiceProtocol=%s))
ByPortAndProto	(&(objectClass=shadowAccount)(uid=%s))
netgroupByTriple	(&(objectClass=nisNetGroup)(cn=%s))
netgroupByMember	(&(objectClass=nisNetGroup)(cn=%s))
authName	(&(objectClass=SolarisAuthAttr)(cn=%s))
auditUserByName	(&(objectClass=SolarisAuditUser)(uid=%s))
execByName	(&(objectClass=SolarisExecAttr)(cn=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))
execByPolicy	(&(objectClass=SolarisExecAttr)(SolarisProfileId=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))

TABLA 14–4 Filtros LDAP utilizados en llamadas getXbyY *(Continuación)*

Filtro	Definición
profileByName	(&(objectClass=SolarisProfAttr)(cn=%s))
userByName	(&(objectClass=SolarisUserAttr)(uid=%s))

La siguiente tabla muestra los filtros de atributo `getent`.

TABLA 14–5 Filtros de atributo `getent`

Filtro	Definición
aliases	(objectClass=rfc822MailGroup)
auth_attr	(objectClass=SolarisAuthAttr)
audit_user	(objectClass=SolarisAuditUser)
exec_attr	(objectClass=SolarisExecAttr)
group	(objectClass=posixGroup)
hosts	(objectClass=ipHost)
networks	(objectClass=ipNetwork)
prof_attr	(objectClass=SolarisProfAttr)
protocols	(objectClass=ipProtocol)
passwd	(objectClass=posixAccount)
printers	(objectClass=sunPrinter)
rpc	(objectClass=oncRpc)
services	(objectClass=ipService)
shadow	(objectclass=shadowAccount)
project	(objectClass=SolarisProject)
usr_attr	(objectClass=SolarisUserAttr)

◆ ◆ ◆ CAPÍTULO 15

Transición de NIS a LDAP (tareas)

En este capítulo, se describe cómo activar el soporte de clientes NIS que utilizan información de nombres almacenados en el directorio LDAP. Mediante los procedimientos de este capítulo, puede realizar una transición de un servicio de nombres NIS a un servicio de nombres LDAP.

Para determinar los beneficios de la transición a LDAP, consulte "Servicios de nombres LDAP comparados con otros servicios de nombres" en la página 131.

En este capítulo, se incluye la siguiente información:

Descripción general del servicio NIS a LDAP

El servicio de transición NIS a LDAP (*servicio N2L*) reemplaza los daemons NIS existentes en el servidor maestro NIS con los daemons de transición NIS a LDAP. El servicio N2L también crea un archivo de asignación NIS a LDAP en ese servidor. El archivo de asignación especifica la asignación entre las entradas de asignación NIS y las entradas del árbol de información de directorios (DIT) equivalentes en LDAP. Un servidor maestro NIS que ha pasado por esta transición se denomina *servidor N2L*. Los servidores esclavos no tienen un archivo `NISLDAPmapping`, por lo que siguen funcionando de la forma usual. Los servidores esclavos actualizan periódicamente sus los datos del servidor N2L, como si se tratase de un maestro NIS normal.

El comportamiento del servicio N2L es controlado por los archivos de configuración `ypserv` y `NISLDAPmapping`. Una secuencia de comandos, `inityp2l`, ayuda para con la configuración inicial de estos archivos de configuración. Una vez que el servidor N2L se ha establecido, puede mantener N2L mediante la edición directa de los archivos de configuración.

El servicio N2L admite lo siguiente:

- Importación de asignaciones NIS al árbol de información de directorios (DIT) de LDAP
- Acceso de cliente a la información del DIT con la velocidad y extensibilidad de NIS

En cualquier sistema de nombres, sólo una fuente de información puede ser el origen con autoridad. En general, es NIS, los orígenes NIS son la información con autoridad. Cuando se utiliza el servicio N2L, el origen de datos con autoridad es el directorio LDAP. El directorio se gestiona mediante herramientas de gestión de directorios, como se describe en el Capítulo 9, “Introducción a los servicios de nombres LDAP (descripción general)”.

Los orígenes NIS se conservan para la restauración o la copia de seguridad de emergencia únicamente. Después de utilizar el servicio N2L, debe eliminar gradualmente los clientes NIS. Finalmente, todos los clientes NIS deben ser reemplazados por los clientes de servicios de nombres LDAP.

La descripción general adicional se proporciona en las siguientes subsecciones:

- “Suposiciones de los destinatarios de NIS a LDAP” en la página 237
- “Cuándo no utilizar el servicio de NIS a LDAP” en la página 237
- “Efectos del servicio de NIS a LDAP en los usuarios” en la página 237
- “Terminología de la transición de NIS a LDAP” en la página 238
- “Comandos, archivos y asignaciones de NIS a LDAP” en la página 239
- “Asignaciones estándar admitidas” en la página 240

Herramientas de NIS a LDAP y utilidad de gestión de servicios

Los servicios NIS y LDAP se gestionan mediante la utilidad de gestión de servicios. Las acciones administrativas de estos servicios, como la activación, la desactivación o el reinicio, pueden llevarse a cabo con el comando `svcadm`. Puede consultar el estado de los servicios con el comando `svcs`. Para obtener más información sobre el uso de SMF con LDAP y NIS, consulte “LDAP y la utilidad de gestión de servicios” en la página 188 y “NIS y la utilidad de gestión de servicios” en la página 78. Para obtener una descripción general de la SMF, consulte el Capítulo 1, “Gestión de servicios (descripción general)” de *Gestión de servicios y errores en Oracle Solaris 11.1*. También consulte las páginas del comando man `svcadm`(1M) y `svcs`(1) para obtener más información.

Suposiciones de los destinatarios de NIS a LDAP

Debe estar familiarizado con los conceptos, la terminología y los IDs de NIS y LDAP para realizar los procedimientos de este capítulo. Para obtener más información sobre los servicios de nombres LDAP y NIS, consulte las siguientes secciones de este manual.

- Capítulo 5, "Servicio de información de red (descripción general)", para obtener una descripción general de NIS.
- Capítulo 9, "Introducción a los servicios de nombres LDAP (descripción general)", para obtener una descripción general de LDAP.

Cuándo no utilizar el servicio de NIS a LDAP

El objetivo del servicio N2L es servir como una herramienta de transición de NIS a LDAP. No utilice el servicio N2L en las siguientes situaciones:

- En un entorno en el que no hay ningún plan compartir datos entre clientes del servicio de nombres LDAP y NIS.

  En este tipo de entorno, un servidor N2L será un servidor maestro NIS excesivamente complejo.
- En un entorno en el que las asignaciones NIS están gestionadas por herramientas que modifican los archivos de origen NIS (que no sean `yppasswd`).

  Volver a generar orígenes NIS desde asignaciones DIT es una tarea imprecisa que requiere la verificación manual de las asignaciones resultantes. Una vez que se utiliza el servicio N2L, la nueva generación de orígenes NIS sólo se proporciona para la restauración o la reversión a NIS.
- En un entorno en el que no se utilizan clientes NIS.

  En este tipo de entorno, use los clientes de servicios nombres LDAP y sus correspondientes herramientas.

Efectos del servicio de NIS a LDAP en los usuarios

Con sólo instalar los archivos relacionados con el servicio N2L no se cambia el comportamiento predeterminado del servidor NIS. En el momento de la instalación, el administrador verá algunos cambios en las páginas del comando man de NIS y la agregación de secuencias de comandos de ayuda de N2L, `inityp2l` y `ypmap2src`, en los servidores. Pero mientras `inityp2l` no se ejecute o los archivos de configuración de N2L no se creen manualmente en el servidor NIS, los componentes de NIS seguirán iniciándose en el modo NIS tradicional y funcionarán como siempre.

Después de ejecutar `inityp2l`, los usuarios pueden ver algunos cambios en el comportamiento del servidor y del cliente. A continuación, se muestra una lista de tipos de usuario NIS y LDAP y una descripción de lo que cada tipo de usuario debe observar después de la implementación de N2L.

Tipo de usuario	Efecto del servicio N2L
Administradores del servidor maestro NIS	El servidor maestro NIS se convierte en un servidor N2L. Los archivos de configuración `NISLDAPmapping` y `ypserv` están instalados en el servidor N2L. Después de que se establece el servidor N2L, puede utilizar comandos LDAP para administrar la información de nombres.
Administradores del servidor NIS esclavo	Después de la transición N2L, un servidor NIS esclavo continúa ejecutando NIS de la forma habitual. El servidor N2L transfiere mapas de datos NIS actualizados al servidor esclavo cuando `yppush` es llamado por `ypmake`. Consulte la página del comando man `ypmake(1M)`.
Clientes NIS	Las operaciones de lectura NIS no se diferencian de las operaciones NIS tradicionales. Cuando un cliente de servicios de nombres LDAP cambia información en el DIT, la información se copia en los mapas de datos NIS. La operación de copia se completa una vez que caduca el tiempo de espera configurable. Por ejemplo, el comportamiento es similar al comportamiento de un cliente NIS normal cuando el cliente está conectado a un servidor NIS esclavo. Si un servidor N2L servidor no se puede enlazar al servidor LDAP para una lectura, el servidor N2L devuelve el información de su propia copia en la caché. Como alternativa, el servidor N2L puede devolver un error interno del servidor. Puede configurar el servidor N2L para que responda de cualquiera de las dos formas. Consulte la página del comando man `ypserv(1M)` para obtener más información.
Todos los usuarios	Cuando un cliente NIS realiza una solicitud de cambio de contraseña, el cambio es visible inmediatamente en el servidor maestro N2L y en los clientes LDAP nativos. Si intenta cambiar una contraseña en el cliente NIS y el servidor LDAP no está disponible, el cambio se rechaza y el servidor N2L devuelve un error interno del servidor. Este comportamiento impide que se escriba información incorrecta la caché.

Terminología de la transición de NIS a LDAP

Los siguientes términos están relacionados con a la implementación del servicio N2L servicio.

TABLA 15–1 Terminología relacionada con la transición N2L

Término	Descripción
Archivos de configuración de N2L	Los archivos `/var/yp/NISLDAPmapping` y `/var/yp/ypserv` que utiliza el daemon `ypserv` para iniciar el servidor maestro en el modo N2L. Consulte las páginas del comando man `NISLDAPmapping`(4) e `ypserv`(4) para obtener detalles.

TABLA 15–1 Terminología relacionada con la transición N2L *(Continuación)*

Término	Descripción
asignar	En el contexto del servicio N2L, el término asignar se utiliza de dos formas: ■ Para hacer referencia a un archivo de base de datos en el que NIS almacena un tipo de información específica. ■ Para describir el proceso de asignación de información NIS desde o hacia el DIT de LDAP.
asignación	El proceso de conversión de entradas NIS desde o hacia entradas del DIT de LDAP.
archivo de asignación	El archivo `NISLDAPmapping` que establece cómo asignar las entradas entre archivos NIS y LDAP.
asignaciones estándar	Asignaciones NIS utilizadas con frecuencia, que admite el servicio N2L sin necesidad de modificar manualmente el archivo de asignación. Se proporciona una lista de asignaciones estándar admitidas en "Asignaciones estándar admitidas" en la página 240.
asignaciones no estándar	Asignaciones NIS estándar, personalizadas para utilizar las asignaciones entre NIS y el DIT de LDAP diferentes de las asignaciones identificadas en RFC 2307 o en su sucesor.
mapa personalizado	Cualquier asignación que no es una asignación estándar y que, por lo tanto, necesita modificaciones manuales en el archivo de asignación cuando se realiza la transición de NIS a LDAP.
Cliente LDAP	Cualquier cliente LDAP tradicional que realiza lecturas y escrituras en cualquier servidor LDAP. Un cliente LDAP tradicional es un sistema que realiza lecturas y escrituras en cualquier servidor LDAP. Un cliente de servicios de nombres LDAP maneja un subconjunto personalizado de información de nombres.
cliente de servicios de nombres LDAP	Un cliente LDAP que maneja un subconjunto personalizado de información de nombres.
Servidor N2L	Servidor maestro NIS que se ha reconfigurado como un servidor N2L con el servicio N2L. La reconfiguración incluye el reemplazo de los daemons NIS y la agregación de nuevos archivos de configuración.

Comandos, archivos y asignaciones de NIS a LDAP

Hay dos utilidades, dos archivos de configuración y una asignación asociados a la transición N2L.

TABLA 15–2 Descripciones de los comandos, archivos y asignaciones de N2L

Comando/Archivo/Mapa	Descripción
`/usr/lib/netsvc/yp/inityp2l`	Una utilidad que ayuda con la creación de los archivos de configuración `NISLDAPmapping` y `ypserv`. Esta utilidad no es una herramienta general para la gestión de estos archivos. Un usuario avanzado puede mantener los archivos de configuración de N2L o crear asignaciones personalizadas mediante un editor de texto para examinar y personalizar el resultado de `inityp2l`. Consulte la página del comando man `inityp2l(1M)`.

TABLA 15–2 Descripciones de los comandos, archivos y asignaciones de N2L *(Continuación)*

Comando/Archivo/Mapa	Descripción
`/usr/lib/netsvc/yp/ypmap2src`	Una utilidad que convierte mapas de datos NIS estándar en aproximaciones de los archivos de origen NIS equivalentes. El uso principal para `ypmap2src` es convertir desde un servidor de transición N2L a NIS tradicional. Consulte la página del comando man `ypmap2src(1M)`.
`/var/yp/NISLDAPmapping`	Un archivo de configuración que especifica la asignación entre las entradas del mapa de datos NIS y las entradas del árbol de información de directorios (DIT) equivalentes en LDAP. Consulte la página del comando man `NISLDAPmapping(4)`.
`/var/yp/ypserv`	Un archivo que especifica la información de configuración para los daemons de transición de NIS a LDAP. Consulte la página del comando man `ypserv(4)`.
`ageing.byname`	Asignación utilizada por `yppasswdd` para leer y escribir información sobre la fecha de la contraseña en el DIT cuando se implementa la transición de NIS a LDAP.

Asignaciones estándar admitidas

De manera predeterminada, el servicio N2L admite asignaciones entre la siguiente lista de mapas y RFC 2307, RFC 2307bis y las entradas LDAP de sus sucesores. Estas asignaciones estándar no requieren la modificación manual en el archivo de asignación. Las asignaciones de su sistema que no aparecen en la siguiente lista se consideran asignaciones personalizadas y requieren modificación manual.

El servicio N2L también admite la asignación automática de los mapas `auto.*`. Sin embargo, debido a que la mayoría de los nombres de archivos y el contenido de `auto.*` son específicos para cada configuración de red, esos archivos no están especificados en esta lista. Las excepciones son los mapas `auto.home` y `auto.master`, que son admitidos como mapas estándar.

```
audit_user
auth_attr
auto.home
auto.master
bootparams
ethers.byaddr ethers.byname
exec_attr
group.bygid group.byname group.adjunct.byname
hosts.byaddr hosts.byname
ipnodes.byaddr ipnodes.byname
mail.byaddr mail.aliases
netgroup netgroup.byprojid netgroup.byuser netgroup.byhost
netid.byname
netmasks.byaddr
networks.byaddr networks.byname
passwd.byname passwd.byuid passwd.adjunct.byname
prof_attr
project.byname project.byprojectid
protocols.byname protocols.bynumber
publickey.byname
```

```
rpc.bynumber
services.byname services.byservicename
timezone.byname
user_attr
```

Durante la transición de NIS a LDAP, el daemon `yppasswdd` utiliza la asignación específica de N2L, `ageing.byname`, para leer y escribir información sobre la fecha de la contraseña en el DIT. Si no está utilizando la fecha de la contraseña, se ignora la asignación `ageing.byname`.

Transición de NIS a LDAP (mapa de tareas)

En la siguiente tabla, se identifican los procedimientos necesarios para instalar y gestionar el servicio N2L con asignaciones estándar y personalizadas de NIS a LDAP.

Tarea	Descripción	Para obtener instrucciones
Completar todos los requisitos previos.	Asegúrese de haber configurado correctamente el servidor NIS y Oracle Directory Server Enterprise Edition (servidor LDAP).	"Requisitos previos para la transición de NIS a LDAP" en la página 242
Configurar el servicio N2L.	Ejecutar `inityp2l` en el servidor maestro NIS para configurar una de estas asignaciones:	
	Asignaciones estándar	"Cómo configurar el servicio N2L con asignaciones estándar" en la página 243
	Asignaciones personalizadas o no estándar	"Cómo configurar el servicio N2L con asignaciones personalizadas o no estándar" en la página 245
Personalizar una asignación.	Ver ejemplos de cómo crear asignaciones personalizadas para la transición N2L.	"Ejemplos de asignaciones personalizadas" en la página 248
Configurar Oracle Directory Server Enterprise Edition con N2L.	Configurar y ajustar Oracle Directory Server Enterprise Edition como servidor LDAP para la transición N2L.	"Mejores prácticas de NIS a LDAP con Oracle Directory Server Enterprise Edition" en la página 249
Resolver problemas del sistema.	Identificar y resolver problemas comunes de N2L.	"Resolución de problemas de NIS a LDAP" en la página 252
Revertir a NIS.	Revertir a NIS con la asignación adecuada:	
	Asignaciones basadas en archivos de origen NIS antiguos	"Cómo revertir a asignaciones según los archivos de origen antiguos" en la página 258
	Asignaciones basadas en el DIT actual	"Cómo revertir a asignaciones según el contenido actual del DIT" en la página 259

Requisitos previos para la transición de NIS a LDAP

Antes de implementar el servicio N2L, debe comprobar o completar los siguientes elementos.

- Asegúrese de que el sistema está configurado como servidor NIS tradicional en funcionamiento antes de ejecutar la secuencia de comandos `inityp2l` para activar el modo N2L.
- Configure el servidor de directorios LDAP en el sistema.

  Oracle Directory Server Enterprise Edition y las versiones compatibles de los servidores de directorios que ofrece Oracle son compatibles con las herramientas de migración de NIS a LDAP. Si utiliza Oracle Directory Server Enterprise Edition, configure el servidor mediante el comando `idsconfig` *antes* de configurar el servicio N2L. Para obtener más información sobre `idsconfig`, consulte el Capítulo 11, "Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP (tareas)" y la página del comando man `idsconfig(1M)`.

  Los servidores LDAP de otros fabricantes podrían funcionar con el servicio N2L, pero no son admitidos por Oracle. Si está utilizando un servidor LDAP que no es Oracle Directory Server Enterprise Edition o un servidor Oracle compatible, debe configurar manualmente el servidor para que sea compatible con RFC 2307bis, RFC 4876 o los esquemas de los sucesores *antes* de configurar el servicio N2L.
- Utilice `files` antes de `dns` para la propiedad `config/host`.
- Asegúrese de que las direcciones del servidor maestro N2L y el servidor LDAP estén presentes en el archivo `hosts` del servidor maestro N2L.

  Una solución alternativa es enumerar las direcciones del servidor LDAP, y no su nombre de host, en `ypserv`. Esto significa que la dirección del servidor LDAP se muestra en otro lugar, por lo que cambiar la dirección del servidor LDAP o el servidor maestro N2L requiere modificaciones de archivo adicionales.

Configuración del servicio de NIS a LDAP

Puede configurar el servicio N2L con asignaciones estándar o asignaciones personalizadas, como se describe en los siguientes dos procedimientos.

Como parte de la conversión de NIS a LDAP, debe ejecutar el comando `inityp2l`. Este comando ejecuta una secuencia de comandos interactiva para la que debe proporcionar información de configuración. La siguiente lista muestra el tipo de información deberá especificar. Consulte la página del comando man `ypserv(1M)` para obtener explicaciones sobre estos atributos.

- El nombre del archivo de configuración que se creará (predeterminado = `/etc/default/ypserv`)
- El DN que almacena información de configuración en LDAP (predeterminado = `ypserv`)

- Lista de servidores preferidos para la asignación datos desde o hacia LDAP
- Método de autenticación para la asignación datos desde o hacia LDAP
- Método Seguridad de la capa de transporte (TLS) de asignación datos desde o hacia LDAP
- Usuario de proxy con vínculo a DN para leer o escribir datos desde o hacia LDAP
- Contraseña de usuario de proxy para leer o escribir datos desde o hacia LDAP
- Valor de tiempo de espera (en segundos) para la operación de vínculo de LDAP
- Valor de tiempo de espera (en segundos) para la operación de búsqueda de LDAP
- Valor de tiempo de espera (en segundos) para la operación de modificación de LDAP
- Valor de tiempo de espera (en segundos) para la operación de agregación de LDAP
- Valor de tiempo de espera (en segundos) para la operación de supresión de LDAP
- Límite de tiempo (en segundos) para la operación de búsqueda en el servidor LDAP
- Límite de tamaño (en bytes) para la operación de búsqueda en el servidor LDAP
- Si N2L debe seguir referencias de LDAP
- Acción de error de recuperación de LDAP, cantidad de intentos de recuperación y tiempo de espera (en segundos) entre cada intento
- Acción de error de almacenamiento, cantidad de intentos y tiempo de espera (en segundos) entre cada intento
- Asignación de nombre de archivo
- Si se debe generar información de asignación para la asignación `auto_direct`

  La secuencia de comandos coloca información importante relacionada con las asignaciones personalizadas en lugares apropiados del archivo de asignación.
- Contexto de nombres
- Si se deben activar los cambios de contraseña
- Si debe cambiar los valores de TTL predeterminados para cualquier asignación

---

Nota – La autenticación `sasl/cram-md5` *no* es admitida por la mayoría de los servidores LDAP, incluido Oracle Directory Server Enterprise Edition.

▼ Cómo configurar el servicio N2L con asignaciones estándar

Utilice este procedimiento si realiza una transición de las asignaciones enumeradas en "Asignaciones estándar admitidas" en la página 240. Si utiliza asignaciones estándar o no estándar, consulte "Cómo configurar el servicio N2L con asignaciones personalizadas o no estándar" en la página 245.

Cuando el servidor LDAP se ha configurado, ejecute la secuencia de comandos `inityp2l` y proporcione información de configuración cuando se le solicite. `inityp2l` realiza la configuración y los archivos de asignación para asignaciones estándar y `auto.*`.

1 **Complete los pasos de requisitos previos enumerados en "Requisitos previos para la transición de NIS a LDAP" en la página 242.**

2 **Conviértase en administrador en el servidor maestro NIS.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

3 **Convierta el servidor maestro NIS en un servidor N2L.**

```
# inityp2l
```

Ejecute la secuencia de comandos `inityp2l` en el servidor maestro NIS maestro y siga las indicaciones. Consulte "Configuración del servicio de NIS a LDAP" en la página 242 para obtener una lista de la información que necesita para proporcionar.

Consulte la página del comando man `inityp2l(1M)` para obtener más información.

4 **Determine si el árbol de información de directorios (DIT) de LDAP se inició por completo.**

El DIT se inició por completo si ya contiene la información necesaria para rellenar todas las asignaciones que aparecen en el archivo `NISLDAPmapping`.

- Si esto no ocurre, continúe con el Paso 5 y omita el paso 6.
- Si esto ocurre, omita el paso 5 y vaya al Paso 6.

5 **Inicializar el DIT para la transición desde los archivos de origen NIS.**

Realice estos pasos únicamente si el DIT *no* se ha inicializado por completo.

a. **Asegúrese de que las asignaciones NIS antiguas estén actualizadas.**

```
# cd /var/yp
# make
```

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

b. **Detenga el servicio NIS.**

```
# svcadm disable network/nis/server:default
```

c. **Copie las asignaciones antiguas en el DIT, a continuación, inicie el soporte N2L para las asignaciones.**

```
# ypserv -IR
```

Espere a que `ypserv` finalice.

Consejo – Los archivos NIS originales `dbm` no se sobrescriben. Puede recuperar estos archivos, si es necesario.

d. Inicie los servicios DNS y NIS para asegurarse de que usen los nuevos mapas.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

Esto completa la configuración del servicio N2L con asignaciones estándar. No es necesario realizar Paso 6.

6 Inicie las asignaciones NIS.

Realice estos pasos sólo si el DIT se inició por completo y omitió el Paso 5.

a. Detenga el servicio NIS.

```
# svcadm disable network/nis/server:default
```

b. Inicie las asignaciones NIS a partir de la información del DIT.

```
# ypserv -r
```

Espere a que `ypserv` finalice.

Consejo – Los archivos NIS originales `dbm` no se sobrescriben. Puede recuperar estos archivos, si es necesario.

c. Inicie los servicios DNS y NIS para asegurarse de que usen los nuevos mapas.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ Cómo configurar el servicio N2L con asignaciones personalizadas o no estándar

Utilice este procedimiento si se dan las siguientes circunstancias:

- Tiene asignaciones que no aparecen en "Asignaciones estándar admitidas" en la página 240.
- Tiene asignaciones NIS estándar que desea asignar a asignaciones LDAP que no pertenecen a RFC 2307.

1 Complete los pasos de requisitos previos enumerados en "Requisitos previos para la transición de NIS a LDAP" en la página 242.

2 Conviértase en administrador en el servidor maestro NIS.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte el Capítulo 9, "Uso del control de acceso basado en roles (tareas)" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

3 Configure el servidor maestro NIS en el servidor N2L.

```
# inityp2l
```

Ejecute la secuencia de comandos `inityp2l` en el servidor maestro NIS maestro y siga las indicaciones. Consulte "Configuración del servicio de NIS a LDAP" en la página 242 para obtener una lista de la información que necesita para proporcionar.

Consulte la página del comando man `inityp2l`(1M) para obtener más información.

4 Modifique el archivo `/var/yp/NISLDAPmapping`.

Consulte "Ejemplos de asignaciones personalizadas" en la página 248 para ver ejemplos de cómo modificar el archivo de asignación.

5 Determine si el árbol de información de directorios (DIT) de LDAP se inició por completo.

El DIT se inició por completo si ya contiene la información necesaria para rellenar todas las asignaciones que aparecen en el archivo `NISLDAPmapping`.

- De lo contrario, complete los pasos 6, 8 y 9.
- Si se inició por completo, omita el Paso 6 y complete el Paso 7, el Paso 8 y el Paso 9.

6 Inicializar el DIT para la transición desde los archivos de origen NIS.

a. Asegúrese de que las asignaciones NIS antiguas estén actualizadas.

```
# cd /var/yp
# make
```

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

b. Detenga los daemons NIS.

```
# svcadm disable network/nis/server:default
```

c. Copie las asignaciones antiguas en el DIT, a continuación, inicie el soporte N2L para las asignaciones.

```
# ypserv -Ir
```

Espere a que `ypserv` finalice.

Consejo – Los archivos NIS originales `dbm` no se sobrescriben. Puede recuperar estos archivos, si es necesario.

d. Inicie los servicios DNS y NIS para asegurarse de que usen los nuevos mapas.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

e. Omita el Paso 7 y continúe con el Paso 8.

7 Inicie las asignaciones NIS.

Realice este paso sólo si el DIT se inició por completo.

a. Detenga los daemons NIS.

```
# svcadm disable network/nis/server:default
```

b. Inicie las asignaciones NIS a partir de la información del DIT.

```
# ypserv -r
```

Espere a que `ypserv` finalice.

Consejo – Los archivos NIS originales `dbm` no se sobrescriben. Puede recuperar estos archivos, si es necesario.

c. Inicie los servicios DNS y NIS para asegurarse de que usen los nuevos mapas.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

8 Compruebe que las entradas de LDAP sean correctas.

Si las entradas no son correctas, no se podrán encontrar por clientes de servicios de nombres LDAP.

```
# ldapsearch -h server -s sub -b "ou=servdates, dc=..." \ "objectclass=servDates"
```

9 Verifique el contenido de los mapas `LDAP_`.

En la siguiente salida de ejemplo, se muestra cómo utilizar el comando `makedm` para verificar el contenido del mapa `hosts.byaddr`.

```
# makedbm -u LDAP_servdate.bynumber
plato: 1/3/2001
johnson: 2/4/2003,1/3/2001
yeats: 4/4/2002
poe: 3/3/2002,3/4/2000
```

Si el contenido es como se esperaba, la transición de NIS a LDAP se ha realizado correctamente.

Tenga en cuenta que los archivos NIS `dbm` originales no se sobrescriben, por lo que siempre puede recuperarlos. Consulte "Reversión a NIS" en la página 257 para obtener más información.

Ejemplos de asignaciones personalizadas

Los siguientes dos ejemplos muestran cómo puede utilizar las asignaciones personalizadas. Utilice el editor de texto que prefiera para modificar el archivo `/var/yp/NISLDAPmapping` según sea necesario. Para obtener más información sobre los atributos de archivos y su sintaxis, consulte la página del comando man `NISLDAPmapping(4)` y la información de servicios de nombres LDAP en el Capítulo 9, “Introducción a los servicios de nombres LDAP (descripción general)”.

EJEMPLO 15–1 Traspaso de entradas de host

En este ejemplo, se muestra cómo mover entradas de host de la ubicación predeterminada a otra ubicación (no estándar) en el DIT.

Cambie el atributo `nisLDAPobjectDN` en el archivo `NISLDAPmapping` al nuevo nombre distintivo (DN) LDAP base. En este ejemplo, la estructura interna de los objetos LDAP no cambia, por lo que las entradas `objectClass` no cambian.

Cambie:

```
nisLDAPobjectDN hosts: \
                        ou=hosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

Por:

```
nisLDAPobjectDN hosts: \
                        ou=newHosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

Este cambio produce que las entradas se asignen en

```
dn: ou=newHosts, dom=domain1, dc=sun, dc=com
```

en lugar de asignarse en

```
dn: ou=hosts, dom=domain1, dc=sun, dc=com.
```

EJEMPLO 15–2 Implementación de un mapa personalizado

En este ejemplo, se muestra cómo implementar una asignación personalizada.

Una asignación hipotética, *servdate.bynumber*, contiene información sobre las fechas de servicio para los sistemas. Esta asignación está indexada por el número de serie del equipo que, en este ejemplo, es 123. Cada entrada consiste en el nombre del propietario del equipo, dos puntos y una lista separada por comas de fechas de servicio, como John Smith:1/3/2001,4/5/2003.

La estructura antigua asignación se debe asignar a las entradas de LDAP de la siguiente manera:

EJEMPLO 15–2 Implementación de un mapa personalizado *(Continuación)*

```
dn: number=123,ou=servdates,dc=... \
                number: 123 \
                userName: John Smith \
                date: 1/3/2001 \
                date: 4/5/2003 \
                 .
                 .
                 .
                objectClass: servDates
```

Mediante el análisis del archivo `NISLDAPmapping`, puede ver que la asignación más cercana al patrón necesario es `group`. La asignaciones personalizadas se pueden modelar en la asignación `group`. Debido a que hay sólo una asignación, no es necesario el atributo `nisLDAPdatabaseIdMapping`. Los atributos que se van a agregar a `NISLDAPmapping` son los siguientes:

```
nisLDAPentryTtl servdate.bynumber:1800:5400:3600

nisLDAPnameFields servdate.bynumber: \
                        ("%s:%s", uname, dates)

nisLDAPobjectDN servdate.bynumber: \
                        ou=servdates, ?one? \
                        objectClass=servDates:

nisLDAPattributeFromField servdate.bynumber: \
                        dn=("number=%s,", rf_key), \
                        number=rf_key, \
                        userName=uname, \
                        (date)=(dates, ",")

nisLDAPfieldFromAttribute servdate.bynumber: \
                        rf_key=number, \
                        uname=userName, \
                        dates=("%s,", (date), ",")
```

Mejores prácticas de NIS a LDAP con Oracle Directory Server Enterprise Edition

El servicio N2L admite Oracle Directory Server Enterprise Edition. Los servidores LDAP de otros fabricantes podrían funcionar con el servicio N2L, pero no son admitidos por Oracle. Si utiliza un servidor LDAP que no es Oracle Directory Server Enterprise Edition o un servidor Oracle compatible, debe configurar manualmente el servidor para que admita RFC 2307, RFC 2307bis y RFC 4876, o los esquemas de sus sucesores.

Si está utilizando el Oracle Directory Server Enterprise Edition, puede mejorar el servidor de directorios para mejorar el rendimiento. Para realizar estas mejoras, debe tener privilegios de administrador LDAP en Oracle Directory Server Enterprise Edition. Además, es posible que el

servidor de directorios deba ser reiniciado, una tarea que debe coordinarse con los clientes LDAP del servidor. La documentación de Oracle Directory Server Enterprise Edition se encuentra disponible en el sitio web Sun Java System Directory Server Enterprise Edition 6.2.

Creación de índices de vista de lista virtual de Oracle Directory Server Enterprise Edition

Para asignaciones grandes, se deben usar índices de vista de lista virtual (VLV) de LDAP para garantizar las búsquedas de LDAP devuelvan resultados completos. Para obtener información sobre la configuración de los índices de VLV en Oracle Directory Server Enterprise Edition, consulte la documentación Sun Java System Directory Server Enterprise Edition 6.2.

Los resultados de la búsqueda VLV utilizan un tamaño de página fijo de 50000. Si se utilizan VLV con Oracle Directory Server Enterprise Edition, el servidor LDAP y el servidor N2L server deben poder para manejar las transferencias de este tamaño. Si sabe que todas las asignaciones son más pequeñas que este límite, no necesita utilizar los índices VLV. Sin embargo, si sus asignaciones son más grandes que el límite de tamaño, o no está seguro del tamaño de todas las asignaciones, use los índices VLV para evitar devoluciones incompletas.

Si está utilizando los índices VLV, configure los límites de tamaño adecuado que se indica a continuación.

- En Oracle Directory Server Enterprise Edition: el atributo `nsslapd-sizelimit` debe ser mayor o igual que 50.000 o `-1`. Consulte la página del comando man `idsconfig(1M)`.
- En el servidor N2L: el atributo `nisLDAPsearchSizelimit` debe ser mayor o igual que 50000 o cero. Para obtener más información, consulte la página del comando man `NISLDAPmapping(4)`.

Después de crear los índices VLV, actívelos mediante la ejecución de `dsadm` con la opción `vlvindex` en el servidor Oracle Directory Server Enterprise Edition. Consulte la página del comando man `dsadm`(1M) para obtener más información.

VLV para asignaciones estándar

Utilice el comando `idsconfig` de Oracle Directory Server Enterprise Edition para configurar las VLV si se aplican las siguientes condiciones:

- Está utilizando Oracle Directory Server Enterprise Edition.
- Está asignando mapas estándar a entradas LDAP de RFC 2307bis.

Las VLV son específicas del dominio, por lo que cada vez que se ejecuta `idsconfig`, se crean VLV para un dominio NIS. Por lo tanto, durante la transición de NIS a LDAP, debe ejecutar `idsconfig` una vez para *cada* atributo `nisLDAPdomainContext` incluido en el archivo `NISLDAPmapping`.

VLV para asignaciones personalizadas y no estándar

Debe crear manualmente nuevas VLV de Oracle Directory Server Enterprise Edition para asignaciones, o copiar y modificar los índices VLV existentes, si se aplican las siguientes condiciones:

- Está utilizando Oracle Directory Server Enterprise Edition.
- Tiene asignaciones de gran tamaño o tiene asignaciones estándar asignadas a ubicaciones del DIT no estándar.

Para ver los índices VLV existentes, escriba lo siguiente:

```
% ldapsearch -h hostname -s sub -b "cn=ldbm database,cn=plugins,cn=config" "objectclass=vlvSearch"
```

Evitar tiempos de espera del servidor con Oracle Directory Server Enterprise Edition

Cuando el servidor N2L actualiza una asignación, el resultado puede ser un acceso al directorio LDAP de gran tamaño. Si Oracle Directory Server Enterprise Edition no está configurado correctamente, la operación de actualización puede tener un tiempo de espera antes de terminar. Para evitar que se superen los tiempos de espera en el servidor de directorios, modifique los siguientes atributos de Oracle Directory Server Enterprise Edition manualmente o ejecutando el comando `idsconfig`.

Por ejemplo, para aumentar la cantidad de tiempo mínima en segundos que debe dedicar el servidor a realizar la solicitud de búsqueda, modifique estos atributos:

```
dn: cn=config
nsslapd-timelimit: -1
```

Para la realización de pruebas, puede utilizar un valor de atributo `-1`, que indica que no hay ningún límite. Cuando haya determinado el valor de límite óptimo, cambie el valor del atributo. *No* deje ningún valor de atributo en `-1` en un servidor de producción. Sin límites, el servidor puede estar vulnerable a ataques de denegación de servicio.

Para obtener más información sobre la configuración de Oracle Directory Server Enterprise Edition con LDAP, consulte el Capítulo 11, “Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP (tareas)” de esta guía.

Evitar sobrecarga de memoria intermedia con Oracle Directory Server Enterprise Edition

Para evitar la sobrecarga de memoria intermedia, modifique los atributos de Oracle Directory Server Enterprise Edition manualmente o ejecute el comando `idsconfig`.

1. Por ejemplo, para aumentar el número máximo de entradas que se devuelven a una consulta de búsqueda de cliente, modifique los siguientes atributos:

```
dn: cn=config
nsslapd-sizelimit: -1
```

2. Para aumentar el número máximo de entradas que se verifican para una consulta de búsqueda de cliente, modifique los siguientes atributos:

```
dn: cn=config, cn=ldbm database, cn=plugins, cn=config
nsslapd-lookthroughlimit: -1
```

Para la realización de pruebas, puede utilizar un valor de atributo `-1`, que indica que no hay ningún límite. Cuando haya determinado el valor de límite óptimo, cambie el valor del atributo. *No* deje ningún valor de atributo en `-1` en un servidor de producción. Sin límites, el servidor puede estar vulnerable a ataques de denegación de servicio.

Si se están utilizando VLV, los valores del atributo `sizelimit` se deben establecer como se define en "Creación de índices de vista de lista virtual de Oracle Directory Server Enterprise Edition" en la página 250. Si se no se utilizan VLV, el límite de tamaño se debe definir lo suficientemente grande como para ajustarse al contenedor más grande.

Para obtener más información sobre la configuración de Oracle Directory Server Enterprise Edition con LDAP, consulte el Capítulo 11, "Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP (tareas)".

Restricciones de NIS a LDAP

Cuando el servidor N2L se ha configurado, los archivos de origen NIS ya no se utilizan. Por lo tanto, no ejecute `ypmake` en un servidor N2L. Si `ypmake` se ejecuta accidentalmente, por ejemplo, para un trabajo `cron` existente, el servicio N2L no se ve afectado. Sin embargo, se registra una advertencia que indica que `yppush` se debe llamar explícitamente.

Resolución de problemas de NIS a LDAP

En esta sección, se tratan dos áreas de resolución de problemas:

Mensajes de error de LDAP comunes

A veces, el servidor N2L registra errores que se relacionan con problemas internos de LDAP, lo que resulta en mensajes de error relacionados con LDAP. Aunque los errores no son fatales, indican problemas para investigar. Por ejemplo, el servidor N2L podría seguir funcionando, pero proporcionar resultados incompletos y desactualizados.

La siguiente lista incluye algunos de los mensajes de error de LDAP comunes que pueden aparecer al implementar el servicio N2L. Se incluyen descripciones del error y las posibles causas y soluciones.

`Administrative limit exceeded`

`Error Number: 11`

Causa: Se realizó una búsqueda LDAP que era mayor que la permitida por el atributo `nsslapd-sizelimit` del servidor de directorios. Sólo se devolverá información parcial.

Solución: Aumente el valor del atributo `nsslapd-sizelimit` o implemente un índice VLV para la búsqueda que falla.

`Invalid DN Syntax`

`Error Number: 34`

Causa: Se ha intentado escribir una entrada LDAP con un DN que contiene caracteres no válidos. El servidor N2L intenta evitar caracteres no válidos, como el símbolo +, que se generan en los DN.

Solución: Compruebe el registro de errores del servidor LDAP para averiguar qué DN no válidos se escribieron y luego modifique el archivo `NISLDAPmapping` que generó los DN no válidos.

`Object class violation`

`Error Number: 65`

Causa: Se ha intentado escribir una entrada LDAP que no es válida. Por lo general, este error se debe a que faltan atributos `MUST`, lo que puede ocurrir debido a cualquiera de las siguientes circunstancias.

- Errores en el archivo `NISLDAPmapping` que crea entradas con atributos faltantes.
- Intenta añadir un atributo `AUXILIARY` a un objeto que no existe.

  Por ejemplo, si un nombre de usuario no se ha creado todavía desde la asignación `passwd.byxxx`, un intento de agregar información auxiliar a ese usuario fallará.

Solución: Para los errores en el archivo `NISLDAPmapping`, compruebe lo que se escribió en el registro de errores del servidor para determinar la naturaleza del problema.

`No es posible contactar con servidor LDAP`

`Error Number: 81`

Causa: El archivo `ypserv` puede estar configurado incorrectamente y apuntar al servidor de directorios LDAP equivocado. Como alternativa, el servidor de directorios podría no estar ejecutándose.

Solución: Vuelva a configurarlo y confírmelo.

- Vuelva a configurar el archivo `ypserv` para apuntar al servidor de directorios LDAP correcto.
- Para confirmar que el servidor LDAP está en ejecución, escriba:

```
% ping hostname 5 | grep "no answer" || \
      (ldapsearch -h hostname -s base -b ""  \
      "objectclass=*" >/dev/null && echo Directory accessible)
```

  Si el servidor no está disponible, se muestra este mensaje: `no answer from` *hostname*. Si hay problemas con el servidor LDAP, se muestra este mensaje: `ldap_search: Can't connect to the LDAP server - Connection refused`. Por último, si todo funciona, se muestra el siguiente mensaje: `Directory accessible`.

`Timeout`

`Error Number: 85`

Causa: Una operación LDAP superó el tiempo de espera, posiblemente cuando se actualizaba un mapa desde el DIT. Es posible que ahora la asignación tenga información desactualizada.

Solución: Aumente los atributos `nisLDAPxxxTimeout` en el archivo de configuración `ypserv`.

Problemas de NIS a LDAP

Se pueden producir los siguientes problemas al ejecutar el servidor N2L. Se proporcionan posibles causas y soluciones.

Depuración del archivo `NISLDAPmapping`

El archivo de asignación `NISLDAPmapping` es complejo. Muchos de los errores potenciales hacen que la asignación se comporte en forma inesperada. Utilice las siguientes técnicas para resolver dichos problemas.

`Console Message Displays When ypserv -ir (or - Ir) Runs`

Descripción: Un simple mensaje aparece en la consola y el servidor se cierra (una descripción detallada se escribe en `syslog`.

Causa: Es posible que la sintaxis del archivo de asignación sea incorrecta.

Solución: Compruebe y corrija la sintaxis del archivo `NISLDAPmapping`.

`El daemon NIS finaliza en el inicio`

Descripción: Cuando se ejecuta `ypserv` u otros daemons NIS, se registra un mensaje de error relacionado con LDAP y se cierra el daemon.

Causa: Es posible que esto se deba a uno de los siguientes motivos:

- No se puede establecer contacto con el servidor LDAP.

- Una entrada encontrada en una asignación NIS o en el DIT no es compatible con la asignación especificada.
- Un intento de lectura o escritura en el servidor LDAP devuelve un error.

Solución: Examine el registro de errores en el servidor LDAP. Consulte los errores LDAP que aparecen en "Mensajes de error de LDAP comunes" en la página 252.

`Resultados inesperados de operaciones NIS`

Descripción: Las operaciones NIS no devuelven los resultados esperados, pero no se registran errores.

Causa: Es posible que existan entradas incorrectas en los mapas de datos NIS o LDAP, lo que da como resultado asignaciones que no finalizan como deberían.

Solución: Compruebe y corrija entradas en el DIT de LDAP y en las versiones de N2L de los mapas de datos NIS.

1. Compruebe que estén las entradas correctas en el DIT de LDAP y corrija las entradas según sea necesario.

   Si utiliza Oracle Directory Server Enterprise Edition, inicie la consola de gestión mediante la ejecución del comando `dsadm startconsole`.

2. Compruebe que las versiones de N2L de los mapas de datos NIS en el directorio `/var/yp` contengan las entradas esperadas comparando el mapa generado recientemente con el mapa original. Corrija las entradas según sea necesario.

   ```
   # cd /var/yp/domainname
   # makedbm -u test.byname
   # makedbm -u test.byname
   ```

   Tenga en cuenta lo siguiente cuando verifique los resultados para las asignaciones:

   - El orden de las entradas podría no ser el mismo en los dos archivos.

     Utilice el comando `sort` antes de comparar el resultado.

   - El uso de espacios en blanco podría no ser el mismo en los dos archivos.

     Utilice el comando `diff -b` al comparar la salida.

`Procesamiento del orden de las asignaciones NIS`

Descripción: Se producen infracciones de clases de objetos.

Causa: Cuando se ejecuta el comando `ypserv -i`, cada mapa de datos NIS se lee, y su contenido se escribe en el DIT. Varias asignaciones podrían contribuir atributos al mismo objeto del DIT. Por lo general, un mapa crea la mayor parte del objeto, incluidos todos los atributos `MUST` del objeto. Otras asignaciones contribuyen atributos `MAY` adicionales.

Los mapas se procesan en el mismo orden en el que aparecen los atributos `nisLDAPobjectDN` en el archivo `NISLDAPmapping`. Si se procesan asignaciones que contienen

los atributos MAY antes que las asignaciones que contienen los atributos MUST, se producen infracciones en la clase de objeto. Consulte el Error 65 en "Mensajes de error de LDAP comunes" en la página 252 para obtener más información sobre este error.

Solución: Vuelva a ordenar los atributos nisLDAPobjectDN para que los mapas se procesen en el orden correcto.

Como corrección temporal, vuelva a ejecutar el comando ypserv -i varias veces. Cada vez se ejecuta el comando, se construye más la entrada de LDAP.

Nota – La asignación de manera tal que no se puedan crear todos los atributos MUST a partir de al menos una asignación, *no* se admite.

Problema de tiempo de espera del servidor N2L

`The server times out.`

Causa: Cuando el servidor N2L actualiza una asignación, el resultado puede ser un acceso al directorio LDAP de gran tamaño. Si Oracle Directory Server Enterprise Edition no está configurado correctamente, esta operación puede tener un tiempo de espera antes de terminar.

Solución: Para evitar que se superen los tiempos de espera del servidor de directorios, modifique los atributos de Oracle Directory Server Enterprise Edition manualmente o ejecutando el comando idsconfig. Consulte "Mensajes de error de LDAP comunes" en la página 252 y "Mejores prácticas de NIS a LDAP con Oracle Directory Server Enterprise Edition" en la página 249 para obtener información.

Problema de archivo de bloqueo de N2L

`The ypserv command starts but does not respond to NIS requests.`

Causa: Los archivos de bloqueo del servidor N2L no están sincronizando correctamente el acceso a los mapas de datos NIS. Esto no debería ocurrir nunca.

Solución: Escriba los siguientes comandos en el servidor N2L:

```
# svcadm disable network/nis/server:default
# rm /var/run/yp_maplock /var/run/yp_mapupdate
# svcadm enable network/nis/server:default
```

Problema de interbloqueo de N2L

`The N2L server deadlocks.`

Causa: Si las direcciones del servidor maestro N2L y el servidor LDAP no se muestran correctamente en los archivos hosts, ipnodes o ypserv, podría ocurrir un interbloqueo.

Para obtener detalles sobre la correcta configuración de direcciones para N2L, consulte "Requisitos previos para la transición de NIS a LDAP" en la página 242.

Para ver un ejemplo de un escenario de interbloqueo, tenga en cuenta la siguiente secuencia de eventos:

1. Un cliente NIS intenta buscar una dirección IP.
2. El servidor N2L descubre que la entrada `hosts` está desactualizada.
3. El servidor N2L intenta actualizar la entrada `hosts` de LDAP.
4. El servidor N2L obtiene el nombre de su servidor LDAP desde `ypserv` y luego realiza una búsqueda mediante `libldap`.
5. `libldap` intenta convertir el nombre del servidor LDAP a una dirección IP mediante una llamada al cambio de servicio de nombres.
6. El cambio de servicio de nombres puede ser una llamada NIS al servidor N2L, con interbloqueo.

Solución: Enumere las direcciones del servidor maestro N2L y el servidor LDAP en los archivos `hosts` o `ipnodes` del servidor maestro N2L. El hecho de que las direcciones del servidor se deban enumerar en `hosts` o `ipnodes`, o en ambos archivos, depende del modo en que estos archivos están configurados para resolver nombres de host locales. Además, compruebe que la propiedad `config/hosts` del servicio `svc:/network/name-service/switch` enumere `files` antes que `nis` en el orden de búsqueda.

Una solución alternativa a este problema de interbloqueo es enumerar la dirección del servidor LDAP, no su nombre de host, en el archivo `ypserv`. Esto significa que la dirección del servidor LDAP aparecerá en otro lugar. Por lo tanto, cambiar la dirección del servidor LDAP o N2L requeriría más esfuerzo.

Reversión a NIS

Se espera que un sitio que ha pasado de NIS a LDAP mediante el servicio N2L reemplace gradualmente todos los clientes NIS con clientes de servicios de nombres LDAP. El soporte para los clientes NIS se vuelve redundante, eventualmente. Sin embargo, si es necesario, el servicio N2L proporciona dos formas para volver al tradicional NIS, como se explica en los siguientes dos procedimientos.

Consejo – NIS tradicional ignora las versiones de N2L de las asignaciones NIS si esas asignaciones están presentes. Después revertir a NIS, si deja las versiones de N2L de las asignaciones en el servidor, las asignaciones N2L no causan problemas. Por lo tanto, puede resultar útil para mantener las asignaciones N2L, en caso de que más tarde decida volver a activar N2L. Sin embargo, las asignaciones ocupan espacio en el disco.

▼ Cómo revertir a asignaciones según los archivos de origen antiguos

1. **Conviértase en administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Detenga los daemons `NIS`.**

   ```
   # svcadm disable network/nis/server:default
   ```

3. **Desactive N2L.**

   Este comando realiza copias de seguridad y mueve el archivo de asignación N2L.

   ```
   # mv /var/yp/NISLDAPmapping backup_filename
   ```

4. **Defina la variable de entorno `NOPUSH` para que las asignaciones nuevas no sean desplazadas por `ypmake`.**

   ```
   # NOPUSH=1
   ```

5. **Realice un nuevo conjunto de asignaciones NIS que se basan en archivos de origen anteriores.**

   ```
   # cd /var/yp
   # make
   ```

6. **(Opcional) Elimine las versiones de N2L de las asignaciones NIS.**

   ```
   # rm /var/yp/domainname/LDAP_*
   ```

7. **Inicie el servicio DNS y el servicio NIS.**

   ```
   # svcadm enable network/dns/client:default
   # svcadm enable network/nis/server:default
   ```

▼ Cómo revertir a asignaciones según el contenido actual del DIT

Realice una copia de seguridad de los archivos de origen NIS antiguos antes de realizar este procedimiento.

1 **Conviértase en administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Detenga los daemons `NIS`.**

```
# svcadm disable network/nis/server:default
```

3 **Actualice las asignaciones desde el DIT.**

```
# ypserv -r
```

Espere a que `ypserv` finalice.

4 **Desactive N2L.**

Este comando realiza copias de seguridad y mueve el archivo de asignación N2L.

```
# mv /var/yp/NISLDAPmapping backup_filename
```

5 **Vuelva a generar los archivos de origen NIS.**

```
# ypmap2src
```

6 **Compruebe manualmente que los archivos de origen NIS regenerados tienen el contenido y la estructura correctos.**

7 **Mueva los archivos de origen NIS regenerados a los directorios adecuados.**

8 **(Opcional) Elimine las versiones de N2L de los archivos de asignación.**

```
# rm /var/yp/domainname/LDAP_*
```

9 **Inicie el servicio DNS y el servicio NIS.**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

Glosario

árbol de información de directorios El DIT es la estructura de directorio distribuida para una red determinada. De manera predeterminada, los clientes acceden a la información suponiendo que el DIT tiene una estructura determinada. Para cada dominio admitido por el servidor LDAP, existe un supuesto subárbol con una supuesta estructura.

archivos de zona DNS Conjunto de archivos en que el software DNS almacena los nombres y las direcciones IP de todas las estaciones de trabajo de un dominio.

asignación El proceso de conversión de entradas NIS desde o hacia entradas del DIT. Este proceso se controla mediante un archivo de *asignación*.

Asignaciones NIS Archivo que utiliza NIS que contiene información de un tipo concreto, por ejemplo, las entradas de las contraseñas para todos los usuarios de una red o los nombres de todos los equipos host de una red. Los programas que forman parte del servicio NIS consultan estos mapas. Consulte también *NIS*.

atributo Cada entrada LDAP consta de un número de *atributos* con nombre cada uno de los cuales tiene uno o más valores.

Además, los archivos de configuración y asignación de servicios N2L se componen de una serie de *atributos* con nombre. Cada atributo tiene uno o más valores.

autenticación Medio por el que un servidor puede verificar la identidad de un cliente.

baseDN El DN en el que parte del DIT tiene raíz. Cuando este valor es el baseDN para entradas de dominios NIS también se denomina *contexto*.

caché de directorio Archivo local utilizado para almacenar datos asociados con objetos de directorio.

cambio de servicio de nombres Servicio `svc:/system/name-service/switch` que define los orígenes a partir de los cuales un cliente del servicio de nombres puede obtener información de red.

campo Una entrada de asignación NIS podría constar de una serie de componentes y caracteres de separación. Como parte del proceso de asignación de servicio N2L, la entrada primero se descomponen en una serie de *campos* con nombre.

cifrado Los medios a través de los cuales se protege la privacidad de los datos.

clave (cifrado) Clave utilizada para cifrar y descifrar otras claves, como parte de una gestión de claves y el sistema de distribución. Compare con *clave de cifrado de datos*.

clave de cifrado Consulte *clave de cifrado de datos*.

clave de cifrado de datos Clave utilizada para cifrar y descifrar datos destinados a programas que realizan el cifrado. Compare con *clave de encriptación de claves*.

clave privada El componente privado de un par de números generados matemáticamente que, cuando se combina con una clave privada, genera la clave DES. La clave DES se utiliza para codificar y decodificar información. La clave privada del remitente sólo está disponible para el propietario de la clave. Cada usuario o equipo tiene su propio par de claves pública y privada.

clave pública El componente público de un par de números generados matemáticamente que, cuando se combina con una clave privada, genera la clave DES. La clave DES se utiliza para codificar y decodificar información. La clave pública está disponible para todos los usuarios y equipos. Cada usuario o equipo tiene su propio par de claves pública y privada.

cliente (1) El cliente es un principal (usuario o equipo) que solicita un servicio de nombres de un servidor de nombres.

(2) En el modelo cliente-servidor para sistemas de archivos, el cliente es un equipo que accede de forma remota a los recursos de un servidor de cálculo, como potencia de cálculo y gran capacidad de memoria.

(3) En el modelo cliente-servidor, el cliente es una *aplicación* que accede a los servicios desde un "proceso del servidor". En este modelo, el cliente y el servidor pueden ejecutarse en el mismo equipo o en equipos diferentes.

contexto Para el servicio N2L, un contexto es algo bajo el que un domino NIS está generalmente asignado. Consulte también baseDN.

contraseña de red Consulte contraseña de RPC segura.

contraseña de RPC segura Contraseña que necesita el protocolo de RPC segura. Esta contraseña se utiliza para cifrar la clave privada. Esta contraseña debe ser siempre idéntica a la contraseña de inicio de sesión del usuario.

credenciales La información de autenticación que el software de cliente envía a lo largo con cada solicitud a un servidor de nombres. Esta información verifica la identidad de un usuario o equipo.

DBM DBM es la base de datos utilizada originalmente para almacenar mapas NIS.

DES Consulte *estándar de cifrado de datos (DES)*.

dirección de Internet Dirección de 32 bits asignada a hosts mediante *TCP/IP*. Consulte *notación decimal con punto*.

dirección IP Número único que identifica cada host en una red.

directorio (1) Un directorio LDAP es un contenedor de los objetos LDAP. En UNIX, un contenedor de archivos y subdirectorios.

DIT Consulte árbol de información de directorios.

DN Un nombre distintivo de LDAP. Esquema de direcciones estructurado como un árbol del directorio LDAP que ofrece a un nombre único para cada entrada LDAP.

DNS Consulte *Sistema de nombres de dominio*.

dominio (1) En Internet, es una parte de una jerarquía de nombres normalmente perteneciente a una red de área local (LAN) o una red de área extensa (WAN) o una parte de dicha red. Sintácticamente, un nombre de dominio de Internet consta de una secuencia de nombres (etiquetas) separados por puntos. Por ejemplo, `sales.example.com`.

(2) En la interconexión de sistemas abiertos (OSI) de la Organización Internacional de Estandarización, "dominio" se usa generalmente como una partición administrativa de un sistema distribuido complejo, como en el dominio de gestión privado MHS (PRMD) y el dominio de gestión de directorios (DMD).

entrada Una única fila de datos en una tabla de la base de datos, como un elemento LDAP en un DIT.

espacio de nombres (1) Un espacio de nombres almacena información que los usuarios, las estaciones de trabajo y las aplicaciones deben tener para comunicarse a través de la red.

(2) El conjunto de todos los nombres de un sistema de nombres.

esquema Un conjunto de reglas que definen qué tipos de datos se pueden almacenar en cualquier DIT LDAP determinado.

estándar de cifrado de datos (DES) Algoritmo comúnmente utilizado, muy sofisticado desarrollado por la Oficina nacional de normas de los Estados Unidos para cifrar y descifrar datos. Consulte también SUN-DES-1.

GID Consulte *ID de grupo*.

hosts de correo Estación de trabajo que funciona como enrutador de correo electrónico y receptor de un sitio.

ID de base de datos Para el servicio N2L, el ID de base de datos es un alias para un grupo de mapas que contienen entradas NIS del mismo formato (con las mismas asignaciones para LDAP). Los mapas pueden tener claves diferentes.

ID de grupo Número que identifica el *grupo* predeterminado para un usuario.

IP Protocolo de Internet. Protocolo de *capa de red* para el conjunto de protocolos de Internet.

LDAP El Protocolo ligero de acceso a directorios es un protocolo de acceso a directorio estándar y extensible utilizado por clientes del servicio de nombres LDAP y servidores para comunicarse entre sí.

lista de servidores *Consulte* lista de servidores preferidos.

lista de servidores preferidos Una tabla `client_info` o un archivo `client_info`. Las listas de servidores preferidos especifican los servidores preferidos de un cliente o dominio.

llamada de procedimiento remoto (RPC) Paradigma simple y común para implementar el modelo cliente-servidor de informática distribuida. Se envía una solicitud a un sistema remoto para ejecutar un procedimiento designado, con los argumentos suministrados, y el resultado se devuelva al emisor de la llamada.

máscara de red Número utilizado por el software para separar la dirección de subred local del resto de una dirección de protocolo de Internet determinada.

MIS Sistemas de información de gestión (o servicios).

modelo cliente-servidor Forma habitual de describir los servicios de red y el modelo los procesos de usuario (programas) de esos servicios. Los ejemplos incluyen el paradigma nombre-servidor/nombre-solucionador del *Sistema de nombres de dominio (DNS)*. Consulte también *cliente*.

NDBM NDBM es una versión mejorada de DBM.

NIS Servicio de información de la red distribuido que contiene información clave sobre los sistemas y los usuarios de la red. La base de datos NIS se almacena en el *servidor maestro* y todos los *servidores de réplica* o *servidores esclavos*.

nombre de dominio Nombre asignado a un grupo de sistemas en una red local que comparte archivos administrativos de DNS. El nombre de dominio es necesario para que la base de datos del servicio de información de la red funcione adecuadamente. Consulte también *dominio*.

nombre distintivo Un nombre distintivo es una entrada en una base de información de directorios (DIB) X. 500 compuesta por atributos seleccionados de cada entrada del árbol a lo largo de una ruta desde la raíz hasta la entrada mencionada.

nombre indexado Formato de nombres utilizado para identificar una entrada en una tabla.

notación decimal con punto La representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP en Internet, por ejemplo: 192.67.67.20.

origen Archivos de origen NIS

Protocolo de control de transporte (TCP) Protocolo de transporte principal del conjunto de protocolos de Internet que proporciona secuencias dobles completas, confiables, orientadas a la conexión. Utiliza IP para la entrega. Consulte TCP/IP.

RDN Nombre distintivo relativo. Una parte de un DN.

red de área extensa (WAN) Una red que conecta varias redes de área local (LAN) o sistemas en distintos sitios geográficos por teléfono, fibra óptica o enlaces de satélite.

red de área local (LAN) Varios sistemas en un solo sitio geográfico conectados para compartir e intercambiar datos y software.

red de nivel empresarial Una red "de nivel empresarial" puede ser una única red de área local (LAN) que comunica por cable, haz infrarrojo o transmisión de radio; o un grupo de dos o más LANs vinculadas por cable o conexiones telefónicas directas. Dentro de una red de nivel empresarial, cada equipo puede comunicarse con todos los demás equipos sin referencia a un servicio de nombres global, como DNS o X.500/LDAP.

reenvío DNS Servidor NIS que reenvía solicitudes que no puede responder a servidores DNS.

registro Consulte *entrada*.

registros de intercambio de correo Archivos que contienen una lista de nombres de dominio DNS y sus hosts de correo correspondientes.

resolución de nombres Proceso de convertir nombres de estación de trabajo o de usuario a direcciones.

resolución inversa El proceso de conversión de direcciones IP de estación de trabajo a nombres de estación de trabajo que utilizan el software DNS.

RFC 2307 RFC que especifica una asignación de información de mapas NIS estándar a entradas DIT. De manera predeterminada, el servicio N2L implementa la asignación especificada en la versión actualizada RFC 2307bis.

RPC Consulte llamada de procedimiento remoto (RPC).

SASL Autenticación sencilla y capa de seguridad. Estructura para negociar la semántica de la capa de autenticación y seguridad en los protocolos de capa de aplicación.

searchTriple Descripción de dónde buscar un atributo determinado en el DIT. searchTriple se compone de 'base dn', 'ámbito' y 'filtro'. Esto es parte del formato URL de LDAP como se define en RFC 2255.

Seguridad de la capa de transporte (TLS) TLS protege la comunicación entre un cliente LDAP y el servidor de directorios, proporcionando privacidad e integridad de los datos. El protocolo TLS es un superconjunto del protocolo de la capa de sockets seguros (SSL).

servicio de nombres Un servicio de red que maneja nombres y direcciones de equipo, usuario, impresora, dominio, enrutador y otros.

Servicio de nombres de dominios (DNS) Servicio que proporciona las políticas y los mecanismos de nombres para la asignación de dominio y los nombres del equipo para direcciones fuera de la empresa, como las de Internet. DNS es el servicio de información de la red utilizado por Internet.

servicio de nombres del nivel de aplicación Los servicios de nombres de nivel de aplicación se incorporan en aplicaciones que ofrecen servicios, como archivos, correo e impresión. Estos servicios están vinculados debajo de los servicios de nombres de nivel de compañía. Los servicios de nombres de nivel de aplicación proporcionan contextos en los que estos servicios pueden vincularse.

servicio de nombres global Un servicio de nombres global identifica (nombres) las redes de nivel empresarial de todo el mundo que están enlazadas por teléfono, satélite u otros sistemas de comunicación. Esta colección de redes vinculadas de todo el mundo se conoce como "Internet". Además de las redes de nombres, un servicio de nombres global también identifica equipos y usuarios individuales dentro de una red determinada.

servidor (1) En NIS, DNS y LDAP es un equipo host que proporciona los servicios de nombres a una red.

(2) En el *modelo cliente-servidor* para sistemas de archivos, el servidor es un equipo con recursos informáticos (y se denomina, a veces, servidor de cálculo) y gran capacidad de memoria. Los equipos cliente pueden acceder de forma remota a estos recursos y utilizarlos. En el modelo cliente-servidor para sistemas de ventanas, el servidor es un proceso que proporciona servicios de ventanas para una aplicación o “proceso de cliente”. En este modelo, el cliente y el servidor pueden ejecutarse en el mismo equipo o en equipos diferentes.

(3) Un *daemon* que gestiona realmente la prestación de archivos.

servidor de claves Proceso del entorno operativo de Oracle Solaris que almacena claves privadas.

servidor de nombres Servidores que ejecutan uno o más servicios de nombres de red.

servidor esclavo Sistema servidor que mantiene una copia de la base de datos NIS. Tiene un disco y una copia completa del entorno operativo.

servidor maestro El servidor que mantiene la copia maestra de la base de datos del servicio de información de la red para un dominio determinado. Los cambios en el espacio de nombres siempre se realizan en la base de datos del servicio de nombres almacenada por el servidor maestro del dominio. Cada dominio tiene sólo *un* servidor maestro.

servidor N2L Servidor NIS a LDAP. Servidor maestro NIS que se ha reconfigurado como un servidor N2L con el servicio N2L. La reconfiguración incluye el reemplazo de los daemons NIS y la agregación de nuevos archivos de configuración.

SSL SSL es el protocolo de capa de sockets seguros. Se trata de un mecanismo de seguridad de la capa de transporte genérico, diseñado para proteger los protocolos de aplicación, como LDAP.

subred Un esquema de trabajo que divide una red lógica única en redes físicas más pequeñas para simplificar el enrutamiento.

sufijo En LDAP, el nombre distintivo (DN) del DIT.

TCP Consulte *Protocolo de control de transporte (TCP)*.

TCP/IP Acrónimo de Protocolo de control de transporte/Programa de interfaz (en inglés Transport Control Protocol/Interface Program). Conjunto de protocolos desarrollado originalmente para Internet. También se denomina conjunto de protocolos de *Internet*. Las redes de Oracle Solaris se ejecutan en TCP/IP de manera predeterminada.

X.500 Un servicio de directorios de nivel global definido por una interconexión de sistema abierto (OSI) estándar. Precursor de LDAP.

yp Yellow Pages (Páginas amarillas). Nombre anterior de NIS que se sigue utilizando en el código NIS.

zonas DNS Límites administrativos dentro de un dominio de red, a menudo compuesto por uno o más subdominios.

Índice

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Y

Z