Trabajo con servicios de nombres y de directorio en Oracle® Solaris 11.2: LDAP

Referencia: E53900
Julio de 2014

ORACLE®

Contenido

Uso de esta documentación

- **Descripción general**: se describe el servicio de nombres LDAP, los métodos para planificar su uso y los pasos para implementar LDAP.
- **Destinatarios**: administradores de sistemas.
- **Conocimientos necesarios**: estar familiarizado con los conceptos y la terminología de LDAP.

Biblioteca de documentación del producto

En la biblioteca de documentación (http://www.oracle.com/pls/topic/lookup?ctx=E36784), se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

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

Comentarios

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

♦ ♦ ♦ CAPÍTULO 1

Introducción al servicio 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.

Nota - Hoy en día, LDAP es un término que se usa para referirse al servicio de nombres, en lugar de al protocolo en sí. En este manual, el término LDAP se utiliza para referirse al servicio, en lugar de al protocolo.

A continuación, encontrará fuentes de lectura complementaria:

- *Guía de implementación de Oracle Directory Server Enterprise Edition*
- *Guía de administración de Oracle Directory Server Enterprise Edition*
- Guía de instalación para la versión de Oracle Directory Server Enterprise Edition que está utilizando

En este capítulo, se ofrece una descripción general del servicio LDAP.

LDAP en esta versión de Oracle Solaris

En Oracle Solaris 11.2, la clase de objeto `SolarisQualifiedUserAttr` se agrega al esquema RBAC de Oracle Solaris existente. Esta clase tiene atributos a los que se pueden especificar varios valores y, por lo tanto, mejora la clase `SolarisUserQualifier` actual. Para ver el esquema RBAC modificado con la nueva clase de objeto, consulte “Esquema de control de acceso basado en roles y de perfil de ejecución” [99].

Si ya dispone de una configuración de LDAP antes de la disponibilidad de la clase `SolarisQualifiedUserAttr`, puede agregar la clase a la configuración con el comando `ldapadd`.

Descripción general de servicio de nombres LDAP

Oracle Solaris es compatible con LDAP junto con Oracle Directory Server Enterprise Edition (anteriormente, Sun Java System Directory Server). Sin embargo, cualquier servidor de directorios genérico puede funcionar como servidor LDAP. En este manual, los términos *servidor de directorios* y *servidor LDAP* son sinónimos y se utilizan de manera indistinta.

El servicio de nombres LDAP es uno de los distintos servicios de nombres que se admiten en Oracle Solaris. Otros servicios de nombres se describen en “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”. Para ver una comparación de los diferentes servicios de nombres en Oracle Solaris, consulte “Comparación: servicio de nombres LDAP y otros servicios de nombres.” [13].

LDAP realiza los siguientes servicios:

- Servicio de nombres: LDAP proporciona datos de nombres en función de una solicitud de cliente. Por ejemplo, al resolver nombres de host, LDAP funciona como DNS, proporcionando los nombres de dominio completos. Suponga que el nombre de un dominio es `west.example.net`. Si el nombre del host es requerido por una aplicación mediante `gethostbyname()` o `getnameinfo()`, LDAP devuelve el valor *server*`.west.example.net`.
- Servicio de autenticación: LDAP gestiona y proporciona información relacionada con la identidad de cliente, la autenticación y las cuentas. Por lo tanto, LDAP implementa medidas de seguridad para proporcionar información sólo a los solicitantes autorizados.

El servicio de nombres LDAP ofrece las ventajas siguientes:

- Con la sustitución de las bases de datos específicas de la aplicación, la información se consolida y la cantidad de bases de datos distintas que se deben gestionar se reduce.
- Se pueden compartir los datos mediante distintos servicios de nombres.
- Se usa un repositorio central para los datos.
- Se puede llevar a cabo una sincronización de datos más frecuente entre los maestros y las réplicas.
- LDAP es compatible con varias plataformas y varios proveedores.

Las siguientes restricciones se aplican al servicio de nombres LDAP:

- Un servidor LDAP no puede ser su propio cliente.
- Un cliente no puede ser un cliente de NIS y LDAP al mismo tiempo.

Nota - En caso de falta de restricción, configurar y gestionar un servicio de nombres LDAP resulta complejo y requiere una planificación cuidadosa.

Modo en que LDAP almacena información

La información LDAP proporcionada se almacena en un árbol de información de directorios (DIT). Los datos se encuentran en formato de intercambio de datos LDAP (LDIF). El DIT consta de contenedores estructurados jerárquicamente con información que sigue un esquema LDAP definido.

Normalmente, el esquema predeterminado que utilizan la mayoría de los DIT es suficiente para la mayoría de las redes que utilizan LDAP. Sin embargo, el DIT es flexible. Puede sustituir la estructura predeterminada de un DIT especificando los descriptores de búsqueda en el perfil de cliente. Para ver una explicación más detallada de los descriptores de búsqueda, consulte “Descriptores de búsqueda de servicios y asignación de esquemas” [41].

En la siguiente tabla, se muestran los contenedores de un DIT y el tipo de información que cada contenedor almacena.

TABLA 1-1 Tipos de información en contenedores predeterminados 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_*` (mapas de montaje automático)

Comparación: servicio de nombres LDAP y otros servicios de nombres.

Además del servicio de nombres LDAP, comúnmente se utilizan otros tipos de servicios de nombres.

En la siguiente tabla, se muestra una comparación de funciones de cada servicio de nombres. Todos estos servicios se admiten en Oracle Solaris.

TABLA 1-2 Comparación de funciones de los servicios de nombres

	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
Servidores	Maestro/esclavo	Maestro/esclavo	Maestro/réplica Réplicas de varios maestros	Ninguno
Seguridad	DNSSEC, variado	Ninguna (raíz o nada)	Kerberos, TLS, SSL, variado	Ninguno
Transporte	TCP/IP	RPC	TCP/IP	E/S de archivo
Escala	Global	LAN	Global	Sólo host local
Datos	Host	Todas	Todas	Todas

Comandos de LDAP

El SO Oracle Solaris proporciona dos conjuntos de comandos relacionados con LDAP. El primer conjunto está conformado por comandos LDAP generales que requieren la configuración de un servicio 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.

En las siguientes secciones, se enumeran los comandos y se proporciona una referencia a sus correspondientes páginas del comando man.

Comandos LDAP generales

Los comandos LDAP generales se pueden ejecutar en cualquier sistema y no requieren que el sistema se configure con un servicio de nombres 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 herramientas admiten un formato basado en texto común para representar información del directorio denominada Formato de intercambio de datos LDAP (LDIF). Puede utilizar los siguientes comandos para manipular directamente las entradas de directorio:

Comando	Descripción	Página del comando man
`ldapsearch`	Busca en el esquema LDAP las entradas especificadas.	`ldapsearch`(1)
`ldapmodify`	Modifica las entradas de LDAP en el esquema.	`ldapmodify`(1)
`ldapadd`	Agrega las entradas de LDAP en el esquema.	`ldapadd`(1)
`ldapdelete`	Elimina entradas de LDAP desde el esquema.	`ldapdelete`(1)

Comandos LDAP específicos de las operaciones LDAP

En la siguiente tabla, se muestran comandos LDAP que configuran el sistema cliente o que requieren que el sistema cliente sea configurado.

Comando	Descripción	Página del comando man
`ldapaddent`	Crear entradas LDAP en el esquema desde los archivos `/etc` correspondientes.	`ldapaddent`(1M)
`ldaplist`	Mostrar la información recuperada desde el servidor LDAP.	`ldaplist`(1)
`idsconfig`	Rellenar el DIT con datos para servir a los clientes.	`idsconfig`(1M)
`ldapclient`	Inicializar una máquina cliente LDAP.	`ldapclient`(1M)

♦ ♦ ♦ CAPÍTULO 2

LDAP y servicio de autenticación

Los servicios de nombres LDAP pueden utilizar el repositorio LDAP de dos maneras diferentes.

- Una fuente del servicio de nombres y el servicio de autenticación
- Un origen exclusivo de datos de nombres

En este capítulo, se tratan específicamente los servicios de autenticación de LDAP y se incluyen los siguientes temas:

Modelo de seguridad de servicios de nombres LDAP

LDAP admite distintas funciones de seguridad, como la autenticación y acceso controlado, que permiten garantizar la integridad y la privacidad de la información que los clientes obtienen.

Para acceder a la información en el repositorio LDAP, un cliente primero debe establecer su identidad con el servidor de directorios. La identidad puede ser anónima o como un host o usuario que sea 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 permite 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.

Hay dos tipos de autenticación:

- En la autenticación de proxy, la identidad se basa en el host en el que se origina la solicitud. Cuando el host se autentica, todos los usuarios de ese host pueden acceder al servidor de directorios.

- En la autenticación por usuario, la identidad se basa en cada usuario. Cada usuario debe estar autenticado para tener acceso al servidor de directorios y emitir varias solicitudes de LDAP.

El servicio del módulo de autenticación conectable (PAM) determina si el inicio de sesión de un usuario se realizó correctamente o no. La base para la autenticación varía en función de qué módulo PAM se utiliza, como se muestra en la siguiente lista:

- Módulo `pam_krb5`: el servidor Kerberos es la base para la autenticación. Para obtener más información sobre este módulo, consulte la página del comando man `pam_krb5`(5). Consulte también "Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ", donde Kerberos se trata de manera más detallada que en esta guía.
- Módulo `pam_ldap`: el servidor LDAP y el host local sirven como base para la autenticación. Para obtener más información sobre este módulo, consulte la página del comando man `pam_ldap`(5). Para saber cómo utilizar el módulo `pam_ldap`, consulte "Gestión de cuentas de LDAP" [30].
- Módulos `pam_unix_*` equivalentes: el host proporciona la información y la autenticación se determina de manera local.

Nota - El módulo `pam_unix` se ha eliminado y ya no se admite en Oracle Solaris. El módulo ha sido reemplazado por otro conjunto diferente de módulos de servicio que proporciona una funcionalidad equivalente o superior. En esta guía, `pam_unix` hace referencia a los módulos que proporcionan una funcionalidad equivalente, no al módulo `pam_unix` en sí.

Si se usa `pam_ldap`, el servicio de nombres y el servicio de autenticación acceden al directorio de manera diferente.

- El servicio de nombres lee las distintas entradas y sus atributos del directorio según una identidad predefinida.
- El servicio de autenticación autentica el nombre y la contraseña del usuario con el servidor LDAP para determinar si se ha especificado la contraseña correcta.

Puede utilizar Kerberos y LDAP al mismo tiempo para proporcionar autenticación y servicios de nombres a la red. Con Kerberos, es posible acompañar un entorno de inicio de sesión único (SSO) en la empresa. El mismo sistema de identidad de Kerberos también se puede utilizar para consultar datos de nombres LDAP por usuario o por host.

Si se utiliza Kerberos para realizar la autenticación, los servicios de nombres LDAP también deben estar activados como requisito del 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

Puede usar la Seguridad de la capa de transporte (TLS) para proteger la comunicación entre un cliente LDAP y el servidor de directorios, y así garantizar la privacidad y la integridad de los datos. El protocolo TLS es un superconjunto del protocolo Capa de sockets seguros (SSL). El servicio de nombres LDAP admite conexiones TLS. Tenga en cuenta que el uso de SSL agrega carga al servidor de directorios y al cliente.

A continuación, se muestra una lista de los requisitos para utilizar TLS:

- Configuración del servidor de directorios y los clientes LDAP para SSL.

  Para configurar Oracle Directory Server Enterprise Edition para SSL, consulte la Guía de administración para la versión de Oracle Directory Server Enterprise Edition que está utilizando.
- Instalación de las bases de datos de seguridad necesarias, específicamente el certificado y archivos de base de datos clave.
  - Si utiliza un formato de base de datos más antiguo desde Netscape Communicator, instale `cert7.db` y `key3.db`.
  - Si utiliza un nuevo formato de base de datos desde Mozilla, instale `cert8.db`, `key3.db` y `secmod.db`.

  Los archivos `cert*` contienen certificados de confianza. El archivo `key3.db` contiene las claves del cliente. Debe instalar el archivo `key3.db` incluso si el cliente del servicio de nombres de LDAP no utiliza claves de cliente. El archivo `secmod.db` contiene el los módulos de seguridad, como el módulo `PKCS#11`.

Para configurar la seguridad TLS, consulte “Configuración de seguridad TLS” [77].

Niveles de credencial de cliente

El servidor LDAP autentica los clientes LDAP según el nivel de credencial de cliente. Los clientes LDAP pueden estar asignados a uno de los siguientes niveles de credencial:

`anonymous`
: Con un nivel de credencial `anonymous`, puede acceder únicamente a los datos que están disponibles para todos. No se produce ninguna operación de enlace de LDAP.

  El nivel de credencial anonymous constituye un elevado riesgo de seguridad. Cualquier cliente puede cambiar la información en el DIT al que el cliente tiene acceso de escritura, incluso contraseñas de usuarios o su propia identidad. Además, el nivel `anonymous` permite que todos los clientes puedan tener acceso de lectura a todos los atributos y las entradas de nombres LDAP.

Nota - Oracle Directory Server Enterprise Edition permite restringir el acceso en función de direcciones IP, un nombre DNS, un método de autenticación y la hora del día. Por lo tanto, puede implementar medidas de seguridad. 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.

`proxy`

Con un nivel de credencial `proxy`, el cliente se enlaza a un único conjunto compartido de credenciales de enlace LDAP. Al conjunto compartido también se lo denomina *cuenta proxy*. Esta cuenta proxy puede ser cualquier entrada que pueda enlazarse 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. Esto significa que todos los usuarios (incluido el usuario root) que estén conectados a un sistema mediante acceso de proxy ven la misma información. Debe configurar los atributos `proxyDN` y `proxyPassword` en cada sistema cliente que utiliza el nivel de credencial `proxy`. Además, `proxyDN` debe tener igual `proxyPassword` en todos los servidores.

La contraseña cifrada `proxyPassword` se almacena localmente en el cliente. Si se cambia la contraseña para un usuario de proxy, debe actualizarla en cada sistema cliente que utilice ese usuario proxy. Además, si utiliza la función de fecha de la contraseña en cuentas LDAP, asegúrese de que los usuarios de proxy queden exentos.

Puede configurar distintos proxies para los diferentes grupos de clientes. Por ejemplo, puede configurar un proxy que limite todos los clientes de ventas para que sólo tengan acceso a los directorios a los que puede acceder toda la compañía y a los de ventas. Está prohibido el acceso a directorios de recursos humanos que contengan 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.

Si tiene previsto configurar varios proxies para distintos clientes, analice las opciones en detalle. Muy pocos agentes proxy pueden limitar la capacidad para controlar el acceso del usuario a los recursos. Sin embargo, tener demasiados proxies complica 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” [22] para obtener información acerca de cómo determinar el método de autenticación más adecuado para su configuración.

El nivel de credencial de proxy se aplica a todos los usuarios y los procesos de cualquier sistema específico. Los usuarios que necesiten

utilizar diferentes políticas de nombres deben iniciar sesión en sistemas distintos o usar el modelo de autenticación por usuario.

`proxy anonymous`

El `proxy anonymous` es un nivel de credencial de entrada de varios valores, donde hay más de un nivel de credenciales definido. Con este nivel, a un cliente se le asignan los primeros intentos de autenticación mediante su identidad proxy. Si la autenticación falla, por ejemplo, porque se bloquea el usuario o se vence la contraseña, el cliente utiliza el acceso anónimo. Según el modo en que está configurado el directorio, diferentes niveles de credenciales se pueden asociar a diferentes niveles de servicio.

`self`

El nivel de credencial `self` también se conoce como modo por usuario. Este modo usa la identidad de Kerberos, denominada "el principal", para realizar una consulta para cada sistema o usuario para la autenticación. 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.

Para utilizar el modelo de autenticación por usuario, se requiere lo siguiente:

- Implementación del servicio de inicio de sesión único de Kerberos
- Admisión de los mecanismos de autenticación SASL y SASL/GSSAPI en uno o más servidores de directorio
- Configuración de DNS, que Kerberos utiliza junto con archivos para realizar las consultas de nombre de host
- Activación del daemon `nscd`

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` del servidor de directorios. Las credenciales de administrador están definidas por los valores de los atributos `adminDN` y `adminPassword`, como se describe en “Definición de los atributos de cliente local” [71].

Las credenciales de administrador tienen propiedades similares a las credenciales `proxy`. Sin embargo, para las credenciales de administrador, el usuario debe tener todos los privilegios para la zona o tener un UID efectivo de `root` para leer o actualizar los datos shadow.

Atención - Las credenciales de administrador se pueden asignar a cualquier entrada que pueda enlazarse al directorio. Sin embargo, **no** use la misma identidad de gestor de directorio (`cn=Directory Manager`) del servidor LDAP.

Esta entrada con credenciales de administrador debe tener acceso suficiente para leer y escribir los datos shadow en el directorio. La entrada es un recurso compartido por sistema. Por lo tanto, debe configurar los atributos `adminDN` y `adminPassword` 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. Todos los usuarios y los procesos de un sistema específico utilizan las credenciales de administrador para leer y actualizar los datos shadow.

Almacenamiento de credenciales de clientes LDAP

En la implementación actual de LDAP, las credenciales de proxy que se establecen durante la inicialización se almacenan en el repositorio SMF en vez de en un perfil del cliente. Esta implementación mejora la seguridad en torno al nombre distintivo (DN) de un proxy y la información de contraseña.

El repositorio SMF es `svc:/network/ldap/client`. Almacena la información de proxy de los clientes que utilizan identidad proxy. Del mismo modo, las actualizaciones de los datos shadow de clientes cuyo nivel de credencial no es `self` también se guardan en este repositorio.

Para los clientes que utilicen autenticación por usuario, la identidad Kerberos y la información de ticket Kerberos para cada principal (cada usuario o host) se utilizan durante la autenticación. El servidor de directorios asigna el principal de Kerberos para un DN y las credenciales de Kerberos se utilizan para autenticar 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 este entorno, la información de ticket Kerberos se utiliza para la autenticación en el servidor de directorios. Este sistema no almacena contraseñas ni DN de autenticación. Por tanto, no es necesario definir los atributos `adminDN` y `adminPassword` al inicializar el cliente con el comando `ldapclient`.

Métodos de autenticación para el servicio de nombres LDAP

Al asignar los niveles de credencial `proxy` o `proxy-anonymous` a un cliente, también debe seleccionar un método mediante el cual se autentique el proxy. De manera predeterminada, el método de autenticación es `none`, que implica el acceso anónimo. El método de autenticación también podría tener 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 establecer un enlace con el método `simple` protegido por TLS. Si no funciona, el cliente deberá intentar vincular con el método `sasl/digest-MD5`. En este caso, habría que configurar el atributo `authenticationMethod` de la siguiente manera: `tls:simple;sasl/digest-MD5`.

El servicio de nombres LDAP admite 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. Busque la RFC 4422 en el sitio web de IETF (http://datatracker.ietf.org/) para obtener información sobre SASL.

Los siguientes mecanismos de autenticación son compatibles.

`none`	El cliente no se autentica en el directorio. Este método es equivalente al nivel de credencial `anonymous`.
`simple`	El sistema cliente se enlaza al 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 del cliente está protegida durante la autenticación, pero la sesión no está cifrada. La principal ventaja de `digest-MD5` es que la contraseña no se envía en texto no cifrado durante la autenticación y es más seguro que el método de autenticación `simple`. Busque la RFC 2831 en el sitio web de IETF (http://datatracker.ietf.org/) para obtener información sobre `digest-MD5`. `digest-MD5` es una versión mejorada de `cram-MD5`. Con `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` La sesión LDAP no está cifrada, pero la contraseña del cliente está protegida durante la autenticación. No utilice este método de autenticación, está obsoleto.

`sasl/GSSAPI` Este método de autenticación se utiliza junto con el modo por usuario para activar las consultas por usuario. Una sesión `nscd` por usuario con las credenciales del cliente se enlaza 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 enlaza usando 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`.

Atención - Para utilizar `digest-MD5`, Oracle Directory Server Enterprise Edition requiere que se almacenen las contraseñas sin cifrar. Las contraseñas para el usuario de proxy que utiliza el método de autenticación `sasl/digest-MD5` o `tls:sasl/digest-MD5` deben almacenarse sin cifrar. En este caso, configure el atributo `userPassword` con la ACI adecuada a fin de evitar que se pueda leer.

La siguiente tabla resume los diferentes métodos de autenticación y sus respectivas características.

TABLA 2-1 Métodos de autenticación

Método	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 atributo `serviceAuthenticationMethod` determina el método de autenticación de un servicio específico. Si no se define este atributo para el servicio, se usa el valor del atributo `authenticationMethod`.

Si el conmutador `enableShadowUpdate` se establece en `true`, el daemon `ldap_cachemgr` también sigue la misma frecuencia para enlazar el servidor LDAP: use el valor para el atributo `authenticationMethod` si el atributo `serviceAuthenticationMethod` no está configurado. El daemon no usa el método de autenticación `none`.

Puede seleccionar métodos de autenticación para los siguientes servicios:

- `passwd-cmd`: utilizado por el comando `passwd` para cambiar la contraseña de inicio de sesión y los atributos de contraseña. Consulte la página del comando man `passwd`(1) para obtener más información.
- `keyserv`: que usa las utilidades `chkey` y `newkey` para crear y cambiar el par de claves Diffie-Hellman de un usuario. Para obtener más información, consulte las páginas del comando man `chkey`(1) y `newkey`(1M).
- `pam_ldap`: utilizado para autenticar usuarios que utilizan el servicio pam_ldap. El servicio `pam_ldap` admite la gestión de cuentas.

Nota - En el modo por usuario, el módulo de servicio Kerberos se utiliza como el servicio de autenticación, y `ServiceAuthenticationMethod` no es necesario.

El siguiente ejemplo muestra una sección de un perfil de cliente en el que los usuarios usan `sasl/digest-MD5` para autenticarse en el servidor de directorios, pero usan una sesión SSL para modificar la contraseña.

```
serviceAuthenticationMethod=pam_ldap:sasl/digest-MD5
serviceAuthenticationMethod=passwd-cmd:tls:simple
```

Métodos de autenticación conectables

Con la estructura PAM, puede elegir entre varios servicios de autenticación, incluidos los módulos `pam_unix_*`, `pam_krb5` y `pam_ldap_*`.

Para emplear la autenticación por usuario, debe activar `pam_krb5`. Sin embargo, podrá seguir usando la autenticación `pam_krb5` incluso si no asigna el nivel de credencial por usuario. Si se utilizan los niveles de credencial de proxy o anonymous para acceder a los datos del servidor de directorios, no es posible restringir el acceso a los datos de directorio por usuario.

Si selecciona la autenticación anonymous o proxy, utilice el módulo `pam_ldap` en lugar de los módulos equivalentes `pam_unix_*`. El módulo `pam_ldap` es más flexible, admite métodos de autenticación más sólidos y puede realizar la gestión de cuentas.

Módulo de servicio LDAP

Como se indicó anteriormente, el atributo `serviceAuthenticationMethod`, si se ha definido, determina el modo en que el usuario se enlaza con el servidor LDAP. De lo contrario, se aplica el atributo `authenticationMethod`. Una vez que el módulo `pam_ldap` se enlaza correctamente al servidor con la identidad del usuario y la contraseña proporcionada, el módulo autentica al usuario.

Nota - Antes, con la gestión de cuentas de `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación cuando iniciaban sesión en el sistema. Por lo tanto, los inicios de sesión que no se basaban en contraseñas y usaban herramientas como `ssh` fallaban.

Ahora puede llevar a cabo la gestión de cuentas y recuperar el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios cuando el usuario inicia sesión.

El nuevo control del servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8`. Este control se encuentra activado de manera predeterminada. Para modificar la configuración de control predeterminada, agregue las instrucciones de control de acceso (ACI) al servidor de directorios. Por ejemplo:

```
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
```

El módulo `pam_ldap` no lee el atributo `userPassword`. Si no hay ningún cliente que use la autenticación UNIX, el otorgamiento de acceso de lectura al atributo `userPassword` es innecesario. Asimismo, el módulo no admite `none` como método de autenticación.

Atención - Si se utiliza el método de autenticación `simple`, el atributo `userPassword` sin cifrar puede ser leído por terceros.

En la tabla siguiente, se resumen las diferencias principales entre los mecanismos de autenticación.

TABLA 2-2 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
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. La contraseña no se ha guardado sin cifrar. El usuario no puede autenticarse.	Sí. Siempre que el esquema de almacenamiento predeterminado se establezca en `clear`, el usuario puede autenticarse.	No. Se utiliza `sasl/GSSAPI`. No hay transferencia de contraseña 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` se debe establecer en `true`.	Sí, si se ha configurado esta opción.	Consulte la página del comando man `pam_krb5(5)` y el módulo de gestión de cuentas de Kerberos V5.

Módulos de servicio `pam_unix_*`

Si el archivo `/etc/pam.conf` no está configurado, la autenticación UNIX está activada de manera predeterminada.

Nota - El módulo `pam_unix` se ha eliminado y ya no se admite en Oracle Solaris. El módulo ha sido reemplazado por otro conjunto diferente de módulos de servicio que proporciona una funcionalidad equivalente o superior. En esta guía, `pam_unix` hace referencia a los módulos que proporcionan una funcionalidad equivalente, no al módulo `pam_unix` en sí.

Los siguientes módulos ofrecen la funcionalidad equivalente como el módulo `pam_unix` original. Los módulos se muestran con sus correspondientes páginas del comando man.

`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:

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.

Los módulos `pam_unix_*` tienen las siguientes restricciones:

- La contraseña debe almacenarse en formato `crypt` de UNIX.
- 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 es incompatible con el método de autenticación `sasl/digest-MD5`. En Oracle Directory Server Enterprise Edition, para utilizar `digest-MD5`, las contraseñas se deben almacenar sin cifrar. La autenticación UNIX requiere que la contraseña se almacene en formato `crypt`.

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 como se aplican los controles a una cuenta de usuario local que se ha definido en los archivos `passwd` y `shadow`. Para la cuenta LDAP, en el modo `enableShadowUpdate`, el sistema actualiza y utiliza los datos shadow del servidor LDAP para la función de fecha de la contraseña y el bloqueo de cuenta. 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 aplican al usuario en todos los sistemas cliente.

La comprobación del historial de la contraseña sólo se admite para el cliente local, no para una cuenta de usuario LDAP.

Módulo de servicio Kerberos

Kerberos se trata de manera más detallada en las siguientes fuentes:

- Página del comando man `pam_krb5`(5)
- "Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 "

PAM y cambio de contraseñas

Use el comando `passwd` para cambiar una contraseña. Si el conmutador `enableShadowUpdate` no está activado, el atributo `userPassword` debe permitir la escritura al usuario y a las credenciales de administrador. Recuerde que el `serviceAuthenticationMethod` para `passwd-cmd` sustituye el `authenticationMethod` de esta operación. Según el método de autenticación, la contraseña actual puede ser descifrada.

En la autenticación UNIX, el nuevo atributo `userPassword` está cifrado con el formato `crypt` de UNIX. El atributo se etiqueta antes de ser escrito en LDAP. Por lo tanto, la nueva contraseña se cifra, independientemente del método de autenticación utilizado para enlazar con el servidor. Consulte la página del comando man `pam_authtok_store`(5) para obtener más información.

Si el conmutador `enableShadowUpdate` está activado, 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.

La admisión de actualización de contraseña del módulo `pam_ldap` se ha sustituido por el módulo `pam_authtok_store` con la opción `server_policy`. Al utilizar `pam_authtok_store`, la nueva contraseña se envía al servidor LDAP sin cifrar. Para garantizar la privacidad, utilice TLS. De lo contrario, la nueva `userPassword` puede ser espiada.

Si ha definido una contraseña sin etiquetas 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.

En el caso de que NIS, o cualquier otro cliente que use la autenticación UNIX, use LDAP como repositorio, debe configurar el atributo `passwordStorageScheme` con `crypt`. Además, si utiliza la autenticación LDAP `sasl/digest-MD5` con Oracle Directory Server Enterprise Edition, debe establecer `passwordStorageScheme` en texto no cifrado.

Gestión de cuentas de LDAP

Si `pam_krb5` realiza la gestión de cuentas y contraseñas, el entorno de Kerberos gestiona todos los detalles de cuentas, contraseñas y bloqueos de cuentas, y otros aspectos de la gestión de cuentas.

Si no utiliza `pam_krb5`, los servicios de nombres LDAP se pueden configurar para aprovechar la admisión de la política de bloqueo de cuentas y contraseñas en Oracle Directory Server Enterprise Edition. Puede configurar `pam_ldap` para que admita la gestión de cuentas de usuario. Con la configuración PAM adecuada, el comando `passwd` refuerza las reglas de sintaxis de contraseña definidas por la política de contraseñas de Oracle Directory Server Enterprise Edition. Sin embargo, no active la gestión de cuentas para las cuentas `proxy`.

Las siguientes funciones de gestión de cuentas son admitidas por `pam_ldap`. Estas funciones dependen de la configuración de la directiva de bloqueo de contraseña y cuenta de Oracle Directory Server Enterprise Edition. Puede activar cualquier cantidad de estas funciones.

- Función de fecha de la contraseña y notificación de caducidad: los usuarios deben cambiar sus contraseñas de acuerdo con una programación. De lo contrario, la contraseña caduca y la autenticación del usuario falla.

  Los usuarios reciben una advertencia cuando inician sesión durante el período de advertencia de caducidad. La advertencia incluye el tiempo restante antes de la caducidad de la contraseña.
- Comprobación de sintaxis de la contraseña: las nuevas contraseñas deben cumplir los requisitos de longitud mínima de la contraseña. 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. 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 falla de autenticación continuará hasta que pase el tiempo de bloqueo de la cuenta o que el administrador vuelva a activarla.

Nota - Estas funciones de gestión de cuentas sólo funcionan con Oracle Directory Server Enterprise Edition. Para obtener información sobre la configuración de la contraseña y la política 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`” [31].

Antes de configurar la contraseña y la política de bloqueo de cuenta en Oracle Directory Server Enterprise Edition, asegúrese de que todos los hosts utilicen la versión más reciente del cliente LDAP con la gestión de cuentas de `pam_ldap`. Además, asegúrese de que los clientes tengan el

archivo pam.conf configurado correctamente. De lo contrario, el servicio de nombres LDAP falla cuando las contraseñas de usuario o el proxy caducan.

Gestión de cuentas LDAP con los módulos pam_unix_*

Si el conmutador enableShadowUpdate está activado, la función de gestión de cuentas se hace disponible en las cuentas locales y en las cuentas LDAP. La funcionalidad incluye la función de fecha de la contraseña, la caducidad de la cuenta y la notificación, el bloqueo de cuenta a causa de fallo en inicio de sesión, etcétera. Además, las opciones -dluNfnwx del comando passwd ahora 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 conmutadorenableShadowUpdate permite implementar la gestión de cuentas de manera coherente para usuarios que están definidos en los archivos y en el ámbito LDAP.

Los módulos pam_ldap y pam_unix_* son incompatibles. El módulo pam_ldap requiere que las contraseñas se puedan modificar mediante usuarios. Los módulos pam_unix_* requieren exactamente lo opuesto. Por lo tanto, no podrá utilizar los dos juntos en el mismo dominio de nombres de LDAP. Todos los clientes utilizan el módulo pam_ldap o todos los clientes utilizan los módulos pam_unix_*. A consecuencia de esta limitación, puede que necesite utilizar un servidor LDAP dedicado en los casos en que una aplicación web o de correo electrónico, por ejemplo, requiera que los usuarios cambien sus propias contraseñas en el servidor LDAP.

La implementación de enableShadowUpdate también requiere que la credencial del administrador (adminDN más adminPassword) se almacene localmente en cada cliente, en el servicio svc:/network/ldap/client.

El uso de los módulos pam_unix_* para la gestión de cuentas no requiere el cambio del archivo /etc/pam.conf. El archivo /etc/pam.conf predeterminado es suficiente.

Ejemplo de archivo pam_conf que utiliza el módulo para gestión de cuentas pam_ldap

En esta sección se da un ejemplo de un archivo pam_conf.

```
#
# 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.
#
```

♦ ♦ ♦ CAPÍTULO 3

Requisitos de planificación para servicios de nombres LDAP

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

La planificación de LDAP consiste principalmente en determinar qué información se debe incluir en el perfil del cliente LDAP. Un cliente utiliza la colección de información de configuración en el perfil para acceder a información de servicio de nombres del servidor LDAP. Debe especificar la información de configuración cuando genera el perfil en el servidor LDAP. Durante la configuración del servidor, se le pedirá que introduzca la información. Un parte de la información que se solicita es obligatoria y otra parte es opcional. En la mayoría de los casos, se recomienda aceptar los valores predeterminados que ya vienen incluidos. Los tipos individuales de información que se solicitan para el perfil se denominan **atributos de cliente**.

A medida que acumula la información de configuración para el perfil, puede utilizar las listas de comprobación de plantilla de "Listas de comprobación en blanco para configuración de LDAP " [45]. Puede utilizar estas listas de comprobación como referencia cuando configure el servidor LDAP.

En la siguiente tabla, se muestran los atributos de perfil de cliente LDAP.

TABLA 3-1 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 como una lista de direcciones del servidor separadas por espacios. (No utiliza nombres de host). Los servidores de esta lista se prueban en orden, *antes* de los de `default ServerList` hasta que se realiza una conexión correctamente. Este atributo no tiene valor predeterminado. Se debe especificar al menos un servidor en `preferredServerList` o `defaultServerList`. **Nota -** Si utiliza nombres de host para definir `defaultServerList` y `preferredServerList`, no debe utilizar LDAP para búsquedas de consultas de servidor de host. No configure la propiedad `config/host` del servicio `svc:/network/name-service/switch` con el valor `ldap`.
`defaultServerList`	Las direcciones de host de los servidores predeterminados como una lista de direcciones del servidor separadas por espacios. (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 de los servidores predeterminados restantes, hasta que se establece una conexión. Se debe especificar al menos un servidor en `preferredServerList` o `default ServerList`. 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. Este atributo no tiene valor predeterminado. Sin embargo, este valor se puede sustituir por un servicio determinado mediante 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 una búsqueda de un solo nivel.
`authenticationMethod`	Identifica el método de autenticación utilizado por el cliente. El valor predeterminado es `none` (`anonymous`). Consulte "Métodos de autenticación para el servicio de nombres LDAP" [23] 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`.
`attributeMap`	Asignaciones de atributo utilizadas por el cliente. De manera predeterminada no hay `attributeMap` definido.
`objectclassMap`	Asignaciones de clase de objeto utilizadas por el cliente. De manera predeterminada, no hay `objectclassMap` definido.
`searchTimeLimit`	Tiempo máximo [en segundos] que el cliente debe permitir para realizar la búsqueda antes de un intervalo. Este valor no afecta al tiempo que el servidor LDAP otorga para que se complete la búsqueda. El valor predeterminado es de `30` segundos.

Atributo	Descripción
`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 refrescamientos del perfil de cliente del servidor LDAP por `ldap_cachemgr`(1M). El valor predeterminado es `43.200` segundos o 12 horas. Si tiene un valor de 0, el perfil nunca se actualizará.

Estos atributos se configuran automáticamente cuando se ejecuta el comando `idsconfig` en el servidor.

Otros atributos de cliente se pueden configurar localmente en los sistemas cliente mediante el comando `ldapclient`. Para obtener más información sobre estos atributos, consulte “Definición de los atributos de cliente local” [71].

Planificación de la configuración del perfil del cliente LDAP

Para configurar correctamente el servicio de nombres LDAP, primero debe planear la configuración del perfil del cliente LDAP. Los valores predeterminados de los atributos de perfil son suficientes para la mayoría de las redes. Sin embargo, según la topología de red que posea, puede especificar valores distintos de los valores predeterminados para algunos atributos de perfil. En esta sección, se describen los diferentes atributos que quizá desee configurar.

Modelo de red LDAP

La planificación del modelo de red LDAP se relaciona con determinar los servidores físicos que se implementarán para el servicio de nombres LDAP. Para garantizar su disponibilidad y rendimiento, cada subred de la red debe tener un servidor LDAP para dar servicio a los clientes de esa subred. Cuando planifique este modelo, debe tener en cuenta lo siguiente:

- Número de sistemas que se implementarán como servidores LDAP

  ¿Qué servidores están designados como servidores maestros? ¿Cuáles son los servidores que son de réplica y funcionan como copias de seguridad?
- Modo de acceso a servidores

  ¿Todos los servidores LDAP deben tener la misma prioridad de acceso por solicitudes de cliente? O bien, ¿los servidores tendrán prioridades distintas, y se accede primero a los de prioridad más alta? Si el acceso a los servidores no es igual, establezca el orden en que se accede a los servidores.

La información especificada se gestiona mediante los atributos `defaultServerList` y `preferredServerList`.

- Factores de tiempo de espera

  Determine los valores de tiempo de espera de la siguiente manera:

  - El atributo `bindTimeLimit` determina durante cuánto tiempo continúa una solicitud de conexión TCP continúa antes de ser eliminada.
  - El atributo `searchTimeLimit` determina durante cuánto tiempo una operación de búsqueda LDAP continúa antes de ser cancelada.
  - El atributo `profileTTL` determina la frecuencia con que un cliente descarga los perfiles de los servidores.

  Por ejemplo, en una red lenta, puede aumentar la cantidad de tiempo necesario para realizar búsquedas y permitir las solicitudes de conexión TCP. En un entorno de desarrollo, puede limitar la frecuencia de descarga de un perfil por un cliente.

Árbol de información de directorios

El servicio de nombres LDAP utiliza un árbol de información de directorios (DIT) predeterminado para almacenar información. El DIT se basa en un esquema LDAP.

El DIT consta de contenedores de información que están jerárquicamente estructurados. La estructura sigue un esquema LDAP estándar que se describe en RFC 2307 (http://tools.ietf.org/html/rfc2307) y RFC 4876 (http://tools.ietf.org/html/rfc4876).

La estructura predeterminada del DIT es suficiente para la mayoría de configuraciones de red para implementar LDAP. Con la estructura predeterminada, sólo es necesario determinar lo siguiente:

- Nombre distintivo (DN) del nodo base del árbol que el servicio de nombres se busca para obtener información sobre un dominio específico. La información del nodo base es gestionada por el atributo `defaultSearchBase`.
- El ámbito de búsqueda que la función de consulta de un servicio de nombres debe abarcar. El ámbito puede incluir un solo nivel por debajo del DN, o bien en todo el subárbol por debajo del DN. Esta información se gestiona mediante el atributo `defaultSearchScope`

Un DIT también puede tener una estructura más compleja para el almacenamiento de los datos. Por ejemplo, datos sobre las cuentas de usuario pueden almacenarse en diferentes partes del DIT. Debe determinar cómo personalizar el comportamiento de la operación de búsqueda, como el DN base, el ámbito y los filtros que desee utilizar, para sustituir la secuencia de búsqueda predeterminada. La información de la secuencia de búsqueda personalizada se gestiona mediante los atributos `serviceSearchDescriptor`, `attributeMap` y `objectclassMap`. Para obtener una explicación detallada acerca de la personalización de la operación de la secuencia de búsqueda, consulte “Descriptores de búsqueda de servicios y asignación de esquemas” [41].

Varios servidores pueden servir a un solo DIT. En esta configuración, los subárboles de un DIT se pueden distribuir entre varios servidores. Por consiguiente, debe realizar más tareas de configuración de servidores LDAP para redirigir correctamente las solicitudes de clientes a los servidores LDAP correspondientes que puedan proporcionar la información solicitada. La información acerca de cómo redirigir las solicitudes de clientes al servidor correcto se gestiona mediante el atributo `followReferrals`.

Tener un único servidor LDAP que proporcione todos los datos de nombres para un dominio específico es la configuración normal y recomendada. Incluso en esta situación, sin embargo, puede configurar el atributo `followReferrals` con fines útiles. Con referencias, puede dirigir a los clientes a servidores de réplica de sólo lectura para la mayoría de las solicitudes de información. El acceso a un servidor maestro para realizar operaciones de lectura y escritura sólo se proporciona de casos excepcionales. Con la configuración de referencia, se impide que el servidor maestro se sobrecargue.

Consideraciones de seguridad

Para mantener la seguridad de las operaciones LDAP que procesan solicitudes de información de directorios, debe tener en cuenta lo siguiente:

- La manera en que los clientes se identifican a sí mismos para obtener acceso a la información. La manera en que se realiza la identificación viene determinada por el nivel de credencial que se especifique para los clientes. El nivel de credencial es gestionado por el atributo `credentialLevel`, al que puede asignar uno de los siguientes valores:
  - `anonymous`
  - `proxy`
  - `proxy anonymous`
  - `self`

  Para obtener descripciones detalladas de cada uno de estos valores, consulte “Niveles de credencial de cliente” [19].
- El método de la autenticación del cliente. El método que se especifica se gestiona mediante el atributo `authenticationMethod`. Puede especificar el método de autenticación mediante la asignación de una de las siguientes opciones:
  - `none`
  - `simple`
  - `sasl/digest-MD5`
  - `sasl/cram-MD5`
  - `sasl/GSSAPI`
  - `tls:simple`
  - `tls:sasl/cram-MD5`

- `tls:sasl/digest-MD5`

  Para obtener descripciones detalladas de cada uno de estos valores, consulte "Métodos de autenticación para el servicio de nombres LDAP" [23].

Además del nivel de credencial que se asignará a los clientes y el método de autenticación que desea usar, también debe tener en cuenta lo siguiente:

- Si se va a utilizar Kerberos y la autenticación por usuario
- El valor que se debe especificar para el atributo `passwordStorageScheme` de los servidores
- La configuración de 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.
- Si los clientes utilizan el módulo `pam_unix_*` o `pam_ldap` para realizar la gestión de cuentas de LDAP

  Esta consideración depende de que el servicio de nombres LDAP sea compatible con NIS.

Planificación de la implementación de los servidores LDAP maestro y de réplica

Los servidores maestro y de réplica se pueden implementar de los siguientes modos:

- Replicación de maestro único
- Replicación de maestro flotante
- Replicación de varios maestros

En la siguiente tabla, se comparan las tres estrategias para implementar los servidores LDAP maestro y de réplica.

TABLA 3-2 Servidores LDAP maestro y de réplica

Estrategia	Descripción	Riesgos
Replicación de maestro único	Existe un servidor maestro para una red o subred específica. El servidor maestro almacena copias de los directorios que se pueden escribir. Los servidores de réplica almacenan copias de sólo lectura. Sólo el servidor maestro puede realizar las operaciones de escritura.	Único punto de fallo. Si el servidor maestro deja de estar disponible, no hay ningún otro servidor que pueda realizar las operaciones de escritura.
Replicación de maestro flotante	Similar a la replicación de maestro único. Sin embargo, si el servidor maestro deja de estar disponible, otro servidor de réplica puede realizar las operaciones de escritura. El servidor de réplica que se encarga	La estrategia no es flexible para los cambios de configuración de red. Por ejemplo, una red está subdividida en subredes. Los servidores de réplica en ambas subredes se convierten en servidores maestros.

Estrategia	Descripción	Riesgos
	de las operaciones de escritura se selecciona en función de un algoritmo.	Si, posteriormente, con el paso del tiempo, las subredes se vuelven a unir, el proceso de reconfiguración para volver a implementar los servidores mediante la estrategia de replicación de maestro flotante se hace complejo.
Replicación de varios maestros	Varios servidores maestros almacenan copias de lectura y escritura de los mismos directorios.	Pueden ocurrir conflictos de actualización de los mismos directorios en los distintos servidores maestros. Se debe establecer una política de resolución de conflictos de actualización (por ejemplo, "la última escritura es la que vale") si se adopta esta estrategia.

Para obtener información acerca de cómo configurar servidores de réplica, consulte la Guía de administración para la versión de Oracle Directory Server Enterprise Edition que está utilizando. Para las implementaciones empresariales a gran escala, la replicación de varios maestros es la opción recomendada.

Planificación para completar los datos de LDAP

Una vez que el servidor LDAP se ha configurado con el esquema y el DIT adecuados, se debe rellenar el DIT con datos. El origen de los datos son los archivos `/etc` de varios sistemas. Es necesario considerar qué método va a utilizar para rellenar el DIT:

- Fusione los archivos `/etc` de un tipo de datos específico en un solo archivo para el tipo de datos, como todos los archivos `/etc/passwd` de distintos sistemas en un solo archivo `/etc/passwd`. A continuación, rellene el servidor desde ese único host que almacena todos los archivos `/etc` fusionados.
- Rellene el servidor emitiendo el comando adecuado en cada sistema cliente que tiene acceso al servidor de directorios.

Para conocer los pasos que se deben seguir para rellenar el servidor de directorios, consulte “Rellenado del servidor LDAP con datos” [59].

Descriptores de búsqueda de servicios y asignación de esquemas

Como se dijo anteriormente, el servicio de nombres LDAP espera que el DIT esté estructurado de algún modo. 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 filtros predeterminados, utilice el siguiente comando:

```
ldaplist -v
```

Nota - Los filtros predeterminados también se muestran en "Filtros predeterminados utilizados por los servicios de nombres LDAP" [109].

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).

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. `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 filtros de ámbito y base definidos para un servicio determinado, cuando ese servicio busque una entrada en particular, buscará en cada base con el ámbito y el filtro especificados.

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 solo nivel en `ou=west,dc=example,dc=com` seguida de una búsqueda de un solo 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`. Para buscar los datos`passwd` para el `username` de usuario, se realizaría la búsqueda en el subárbol `ou=west,dc=example,dc=com` con el filtro LDAP `(&(fulltimeEmployee=TRUE)(uid=username))` .

```
serviceSearchDescriptor: passwd:ou=west,dc=example,
dc=com?sub?fulltimeEmployee=TRUE
```

También puede asociar varios contenedores con un determinado tipo de servicio. 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 `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. 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.

Tal vez le resulte conveniente utilizar asignaciones de esquemas en situaciones en las que desea asignar atributos de mapas 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
```

Tenga en cuenta que puede asignar el atributo `gecos` del servicio `passwd` a varios atributos, como se muestra en el siguiente ejemplo:

```
attributeMap: gecos=cn sn title
```

En este ejemplo, se asignan 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
```

Resumen: atributos de perfil de cliente predeterminados para preparar la implementación de LDAP

En la siguiente lista, se identifican los atributos relevantes que normalmente podrían configurarse para implementar el servicio de nombres LDAP. Tenga en cuenta que no todos estos atributos requieren configuración. De los atributos que figuran en la lista, sólo `cn`, `defaultServerList` y `defaultSearchBase` requieren que proporcione valores. Para el resto, puede aceptar los valores predeterminados o dejar el resto de los atributos sin ninguna configuración.

- `cn`
- `defaultServerList`
- `preferredServerList`
- `bindTimeLimit`
- `searchTimeLimit`
- `profileTTL`
- `defaultSearchBase`
- `defaultSearchScope`
- `serviceSearchDescriptor`
- `attributeMap`
- `objectclassMap`
- `followReferrals`
- `credentialLevel`
- `authenticationMethod`
- `serviceCredentialLevel`
- `serviceAuthenticationMethod`

Listas de comprobación en blanco para configuración de LDAP

TABLA 3-3 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 (*IP number*:*port number*)	
Gestor de directorios [`dn: cn=directory manager`]	
Nombre de dominio al que se prestará servicio	
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 3-4 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; los valores posibles son '`One`' o '`Sub`')	
Credenciales utilizadas para acceder al servidor; El valor predeterminado es `anonymous`.	
¿Seguir las referencias? (Las referencias son 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.	
Métodos de autenticación. El valor predeterminado es `none`.	

♦ ♦ ♦ CAPÍTULO 4

Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP

En este capítulo, se describe cómo configurar Oracle Directory Server Enterprise Edition para admitir clientes LDAP. La información es específica de Oracle Directory Server Enterprise Edition.

Nota - Oracle Directory Server Enterprise Edition ya debe estar instalado y configurado para que pueda configurarlo para que funcione con los clientes LDAP. En este capítulo, no se describen todas las funciones de Oracle Directory Server Enterprise Edition. Consulte la documentación de la versión específica del servidor de directorios que tiene para obtener información más detallada.

En este capítulo, se tratan los siguientes temas:

Preparación de información para configurar el servidor de directorios

Para configurar el servidor de directorios para el servicio de nombres LDAP, debe tener dos conjuntos de información disponibles: la información del servidor y la información de perfil de cliente.

Información del servidor para LDAP

Cuando configure el servidor de directorios, se le pedirá la siguiente información sobre el servidor:

- Número de puerto de la instancia del servidor de directorios. De manera predeterminada, el número de puerto es 389.
- Nombre del servidor.
- Direcciones IP y números de puerto de servidores de réplica.
- Gestor de directorios, representado por la variable `cn`. De manera predeterminada, `cn` se establece en `directory manager`.
- Nombre de dominio al que se prestará servicio.
- Duración máxima de tiempo en segundos para procesar las solicitudes del cliente antes de que se exceda el tiempo de espera de las solicitudes.
- Número máximo de información de registro que se facilita con cada solicitud de búsqueda.

Parte de la información sobre el servidor son los atributos de perfil del cliente LDAP que se analizaron en “Planificación de la configuración del perfil del cliente LDAP” [37].

Para facilitar la preparación de información del servidor, puede utilizar el ejemplo de lista de comprobación de “Listas de comprobación en blanco para configuración de LDAP ” [45], donde se enumeran estas variables y los valores correspondientes que desea asignar.

Información de perfil de cliente para LDAP

Debe tener la información de los atributos de perfil del cliente LDAP. Estos atributos regulan el acceso de cliente al servidor cuando se solicita información. Para obtener descripciones de estos atributos, consulte “Planificación de la configuración del perfil del cliente LDAP” [37].

- Nombre de perfil de cliente.
- Lista de servidores LDAP.
- Orden preferido por el cual se accede a los servidores.

  Normalmente, la lista de servidores y su orden de acceso consta de direcciones IP de los servidores. Como alternativa, puede especificar los nombres de host de los servidores. Sin embargo, si utiliza nombres de host, no debe utilizar LDAP para operaciones de consultas de host. Por lo tanto, no debe configurar `ldap` en la propiedad `config/host` del servicio `svc:/network/name-service/switch`. Para obtener más información acerca de LDAP y la utilidad de gestión de servicios (SMF), consulte “LDAP y la utilidad de gestión de servicios” [69].
- Ámbito de la búsqueda en el árbol de directorios. El valor predeterminado es `one`, pero puede especificar `sub`.
- Credencial para acceder al servidor
- Las referencias a otros servidores LDAP si la información en el directorio se distribuye entre varios servidores. Los valores son `No`, el valor predeterminado o `Yes`.
- Tiempo de espera para recibir respuesta del servidor a una solicitud antes de que se exceda el tiempo de espera.
- Tiempo máximo para ponerse en contacto con el servidor antes de que se exceda el tiempo de espera.

- Método de autenticación.

Nota - Los perfiles de cliente se definen por dominio. Al menos un perfil debe estar definido para un dominio determinado.

Para facilitar la preparación de información del perfil del cliente, puede utilizar el ejemplo de lista de comprobación de “Listas de comprobación en blanco para configuración de LDAP ” [45], donde se enumeran estas variables y los valores correspondientes que desea asignar.

Uso de índices de exploración

La función de índice de exploración de Oracle Directory Server Enterprise Edition se denomina vista de lista virtual (VLV). Con VLV, un cliente puede ver un subconjunto seleccionado de entradas de una lista extensa, lo cual reduce el tiempo de búsqueda de cada cliente.

La creación del árbol de información de directorios incluye al final del proceso la creación de VLV para el árbol. Las instrucciones para ejecutar comandos para crear VLV se proporcionan en la pantalla. Debe ejecutar estos comandos en el servidor de directorios.

Creación de las definiciones del árbol de directorios

Después de recopilar la información necesaria de perfil de servidor y de cliente, debe configurar Oracle Directory Server Enterprise Edition para LDAP. Debe utilizar `idsconfig` para crear el árbol de información de directorios con las definiciones de las listas de comprobación.

Al crear el DIT mediante el comando `idsconfig`, crea de hecho el perfil de cliente y sus atributos, como se muestra en la Tabla 3-1, “Atributos de perfil de cliente LDAP”. Almacene los perfiles de clientes en una ubicación conocida en el servidor LDAP. Un único perfil en el servidor proporciona la ventaja de definir la configuración de todos los clientes que utilizan dicho servidor. Cualquier cambio posterior en los atributos de perfil se propaga automáticamente a los clientes. 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.

Puede crear definiciones del directorio desde cualquier sistema Oracle Solaris de la red. Sin embargo, en este caso, la salida del comando `idsconfig` incluye la contraseña del gestor de directorios en texto sin cifrar. Como alternativa para evitar que se publique la contraseña, emita el comando en el servidor de directorios.

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

Nota - Puede crear descriptores de búsqueda de servicios (SSD) junto con la creación del árbol de directorios. Ambas operaciones se inician usando el mismo comando: `idsconfig`. Sin embargo, si lo prefiere, puede crear SSD realizando una operación independiente. Para obtener una descripción de los SSD y de su finalidad, consulte “Descriptores de búsqueda de servicios y asignación de esquemas” [41].

▼ Cómo configurar Oracle Directory Server Enterprise Edition para el servicio de nombres LDAP

1. **Asegúrese de que el Oracle Directory Server Enterprise Edition de destino esté en ejecución.**
2. **Cree el árbol de información de directorios.**

   ```
   # /usr/lib/ldap/idsconfig
   ```

3. **Proporcione la información que se le solicita.**
4. **Siga las instrucciones de la pantalla para crear los índices de VLV.**

   Los índices de VLV se crean mediante una operación independiente al final de la creación del DIT. La pantalla proporciona la sintaxis de comando correspondiente. Asegúrese de seguir estas instrucciones en el servidor. Las instrucciones aparecerán como se indica a continuación al finalizar los procesos `idsconfig`:

   ```
   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.
   ```

   Vea la pantalla ejemplo de “Creación del árbol de información de directorios” [51] para obtener la salida completa al ejecutar el comando `idsconfig`.

Ejemplos de la configuración de servidores para LDAP

En esta sección, se proporcionan ejemplos de distintos aspectos en la configuración de Oracle Directory Server Enterprise Edition para el uso del servicio de nombres LDAP. En los ejemplos,

se menciona la compañía `Example, Inc.`, que tiene sucursales en todo el país. Específicamente, los ejemplos se centran en la configuración de LDAP de la división de la costa oeste de la compañía, cuyo nombre de dominio es `west.example.com`.

Creación del árbol de información de directorios

En la siguiente tabla, se muestra la información del servidor para `west.example.com`.

TABLA 4-1 Variables del servidor definidas para el dominio `west.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`

En la siguiente tabla, se muestra la información de perfil de cliente.

TABLA 4-2 Variables del perfil de cliente definidas para el dominio `west.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`, el predeterminado o `sub`)	`one` (predeterminado)
Credenciales utilizadas para acceder al servidor; El valor predeterminado es `anonymous`.	`proxy`
Seguir 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`

Variable	Definición para la red de ejemplo
Límite de tiempo de vínculo (el valor predeterminado es 10 segundos) para ponerse en contacto con el servidor.	`default`
Métodos de autenticación. El valor predeterminado es `none`.	`simple`

Con esta información, puede crear el árbol de directorios.

```
# 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 ...
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         :
 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
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.
```

En las siguientes pantallas, se incluyen instrucciones adicionales que puede seguir para completar la configuración de `idsconfig`.

```
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 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
```

Puede utilizar la utilidad `idsconfig` para activar la actualización de shadow cuando se genera el DIT de un nuevo perfil. Para activar la actualización shadow, debe escribir **`y`** cuando se le solicite mediante `Do you want to enable shadow update (y/n/h)? [n]`. Debe escribir la contraseña del administrador cuando se le solicita mediante `Enter passwd for the administrator:`.

En el siguiente ejemplo, se muestra cómo activar la actualización shadow mediante la utilidad `idsconfig`.

```
# 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 ...
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] y
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        :
 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          : TRUE
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:proxy-password
Re-enter passwd:proxy-password
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:admin-password
Re-enter passwd:admin-password
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. Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com added.
15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access to\
    shadow data.
16. Non-Admin access to shadow data denied.
17. Generated client profile and loaded on server.
18. 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.
19. Processing eq,pres,sub indexes:
ipHostNumber (eq,pres,sub)   Finished indexing.
membernisnetgroup (eq,pres,sub)   Finished indexing.
nisnetgrouptriple (eq,pres,sub)   Finished indexing.
20. 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
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.
```

Para obtener información sobre cómo inicializar un cliente LDAP para permitir la actualización LDAP, consulte “Inicialización de un cliente LDAP” [72]. Al inicializar un cliente LDAP, debe utilizar el mismo DN y la misma contraseña del administrador que ha proporcionado al crear el DIT.

Definición de descriptores de búsqueda de servicios

En Example, Inc., la configuración de LDAP anterior almacenaba información de usuario en el contenedor `ou=Users` del árbol de directorios. En la versión de Oracle Solaris que se describe en este manual, se asume que las entradas de usuario están almacenadas en el contenedor `ou=People`. Por lo tanto, si se busca el servicio `passwd`, y el cliente busca el contenedor `ou=People`, no se puede obtener la información.

Para evitar las complicaciones de volver a crear el árbol de información de directorios existente de la compañía y el impacto en otras operaciones, en su lugar puede crear los descriptores de búsqueda de servicios (SSD). Estos SSD le indican al cliente LDAP que busque la información de usuario desde el contenedor `ou=Users` en lugar de hacerlo desde el contenedor predeterminado.

Para obtener información acerca de los descriptores de búsqueda, consulte “Descriptores de búsqueda de servicios y asignación de esquemas” [41].

Para crear SSD, también se usa el comando `idsconfig`. La línea de indicación que hace referencia a los SSD aparece del siguiente modo:

```
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
```

Rellenado del servidor LDAP con datos

Después de que se crea el DIT, debe rellenar el árbol de información con datos. Los datos derivan de todos los sistemas que contengan archivos `/etc`. Por lo tanto, debe realizar esta tarea en esos sistemas en lugar de en el servidor. La manera en que se realiza el rellenado del árbol de información depende de la planificación que se describe en “Planificación para completar los datos de LDAP” [41].

A continuación, se presentan algunos ejemplos de archivos cuyos datos se usarían para rellenar el árbol de información:

- `aliases`
- `auto_*`
- `bootparams`
- `ethers`
- `group`
- `hosts`

Del mismo modo, la información de los archivos relacionados con derechos en `/etc` también se agregan al árbol de información, como `user_attr`, `~/security/auth_attr`, `~/security/prof_attr` y `~/security/exec_attr`.

Para rellenar el árbol de información, se utiliza el comando `ldapaddent`. También debe especificar la base de datos o el archivo `/etc` cuyos datos está cargando en el árbol. Algunos archivos se deben cargar en secuencia para obtener un mejor rendimiento. Los archivos y su secuencia de carga son los siguientes:

1. `passwd`
2. `shadow`
3. `networks`
4. `netmasks`
5. `bootparams`
6. `ethers`

Tenga en cuenta que, si está cargando información del montador automático, el nombre de la base de datos o el archivo utiliza el formato de nombres `auto_*`, como `auto_home`.

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 definición de contraseñas en formato `crypt` de UNIX, consulte los documentos de Oracle Directory Server Enterprise Edition. Para obtener más información sobre el comando `ldapaddent`, consulte la página del comando man `ldapaddent`(1M).

▼ Cómo rellenar el servidor con datos

En este procedimiento, se explican los pasos para rellenar el árbol de información en el servidor con los datos de los archivos `/etc` de un sistema cliente. Para esta tarea, se asume que los archivos `/etc` de diferentes sistemas cliente no se fusionan en un solo archivo. Debe realizar

esta tarea en todos los sistemas que tengan archivos `/etc` de origen con los cuales se rellenará el servidor.

Esta tarea utiliza el dominio `west.example.com` que se utilizó para preparar el perfil de cliente en “Ejemplos de la configuración de servidores para LDAP” [50].

Antes de empezar Asegúrese de que Oracle Directory Server Enterprise Edition ya esté configurado. En particular, asegúrese de que el árbol de información de directorios se haya configurado con el comando `idsconfig`, como se describe en Cómo configurar Oracle Directory Server Enterprise Edition para el servicio de nombres LDAP [50].

1. **Conviértase en administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Rellene el servidor con los datos de cada archivo o base de datos en `/etc`.**

   ```
   # ldapaddent -D "cn=directory manager" -f /etc/filename  container
   ```

   Donde *container* tiene el mismo nombre que *filename*, como `passwd`.

Tareas adicionales de configuración del servidor de directorios

Después de que se crea el DIT en el servidor y las SSD se definen según sea necesario, pueden efectuar las siguientes tareas adicionales.

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. Las entradas de grupo pueden tener valores de atributo de pertenencia que especifican la asociación de grupos en nombres distintivos (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.

Se sigue admitiendo la manera existente de definir las entradas de grupo con la clase de objeto `posixGroup` y el atributo `memberUid`. 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`, 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 (formato de intercambio de datos LDAP) 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 el uso de `ldapclient genprofile`.

▼ Cómo rellenar el servidor de directorios con perfiles adicionales mediante el comando `ldapclient`

1. **Conviértase en administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Use `ldapclient` con el comando `genprofile`.**

   ```
   # ldapclient genprofile \
   -a profileName=myprofile \
   -a defaultSearchBase=dc=west,dc=example,dc=com \
   -a "defaultServerList=xxx.xxx.x.x yyy.yyy.y.y:portnum" \> myprofile.ldif
   ```

3. **Cargue el nuevo perfil en el servidor.**

   ```
   # ldapadd -h xxx.xxx.x.x -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_*`.

Atención - No utilice los módulos `pam_ldap` y `pam_unix_*` a la vez en el mismo dominio de nombres LDAP. O 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.

Gestión de cuentas 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 para el directorio LDAP. Para conocer los procedimientos y obtener 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, con la gestión de cuentas de `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación cuando iniciaban sesión en el sistema. Por lo tanto, los inicios de sesión que no se basaban en contraseñas y usaban herramientas como `ssh` fallaban.

Ahora puede llevar a cabo la gestión de cuentas y recuperar el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios cuando el usuario inicia sesión.

El nuevo control del servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8`. Este control se encuentra activado de manera predeterminada. Para modificar la configuración de control predeterminada, agregue las instrucciones de control de acceso (ACI) al servidor de directorios. Por ejemplo:

```
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 para los usuarios `proxy` *nunca* deben caducar. 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 de pam_ldap depende de Oracle Directory Server Enterprise Edition para mantener y proporcionar información a los usuarios sobre la función de fecha de la contraseña 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 han caducado. 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.

Gestión de cuentas 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. Se puede ajustar toda la configuración mediante la ejecución de la utilidad idsconfig.

En el siguiente ejemplo, se muestra la salida 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 5

Configuración de clientes LDAP

En este capítulo, se describe cómo configurar un cliente de servicios de nombres LDAP. En este capítulo, se tratan los siguientes temas:

Preparación para la configuración del cliente LDAP

A continuación, se indican los requisitos para que un cliente de Oracle Solaris pueda usar LDAP como servicio de nombres:

- 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 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 en ejecución.

La utilidad `ldapclient` realiza todos los pasos enumerados de configuración, salvo para iniciar el servidor. En este capítulo, se muestran ejemplos de cómo usar la utilidad `ldapclient` para configurar un cliente LDAP y usar las diferentes utilidades LDAP para obtener información acerca de un cliente LDAP.

LDAP y la utilidad de gestión de servicios

La utilidad de gestión de servicios (SMF) de Oracle Solaris gestiona el servicio de cliente LDAP. Para obtener más información sobre SMF, consulte "Gestión de los servicios del sistema

en Oracle Solaris 11.2 ". Para obtener más información, consulte las páginas del comando man svcadm(1M) y svcs(1).

En la lista siguiente, se destacan las funciones de la SMF relativas a la administración del servicio de cliente LDAP.

- El comando `svcadm` se utiliza para activar, desactivar o reiniciar el servicio de cliente LDAP.

Sugerencia - 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 restauran en el servicio después de reiniciar. Si el servicio se desactiva sin la opción `-t`, el servicio permanece desactivado después de reiniciar.

- El identificador de recurso 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`.
- El comando `svcs` se utiliza para consultar el estado del cliente LDAP y el daemon `ldap_cachemgr`.
  - En el siguiente ejemplo, se muestra el comando `svcs` y su salida:

```
# svcs \*ldap\*
STATE          STIME    FMRI
online         15:43:46 svc:/network/ldap/client:default
```

  - En el siguiente ejemplo, se muestra el comando `svcs -l` y la salida cuando se usa el nombre de 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, utilice el comando `ldapsearch`:

    ```
    # ldapsearch -h server-name -b "" -s base "objectclass=*" |grep -i context
    namingContexts: dc=example,dc=com
    ```

La información de configuración especificada en los perfiles de cliente LDAP se importa automáticamente en el repositorio SMF cuando se inicia el servicio `svc:/network/ldap/client`.

Definición de los atributos de cliente local

En el Capítulo 3, Requisitos de planificación para servicios de nombres LDAP, se describen los atributos de perfil de cliente LDAP que se definen para configurar el servidor LDAP. El perfil y los atributos se configuran en el servidor mediante el comando `idsconfig`.

Otros atributos de cliente se pueden configurar localmente mediante el comando `ldapclient`. En la siguiente tabla, se enumeran los atributos.

TABLA 5-1 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 distinto de `self`, `adminDN` debe especificarse.
`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 distinto de `self`, `adminPassword` debe especificarse.
`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.
`proxyDN`	Nombre distintivo de proxy. Si el sistema cliente se configura con `credential Level` establecido en `proxy`, `proxyDN` debe especificarse.
`proxyPassword`	Contraseña del proxy. Si el sistema cliente está configurado con `credentialLevel` establecido en proxy, `proxyPassword` debe especificarse.

Atributo	Descripción
`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 de `defaultSearchBase` se agregan a `BaseDN` antes de que se realice una búsqueda.

Administración de los clientes LDAP

En esta sección, se describe el uso del comando `ldapclient` para inicializar y revisar la configuración del cliente LDAP.

Nota - Debido a que LDAP y NIS usan el mismo componente de nombre de dominio que está definido en el servicio `network/nis/domain`, la versión actual de Oracle Solaris no admite una configuración en la que un cliente NIS y un cliente LDAP nativo coexisten en el mismo sistema de cliente.

Inicialización de un cliente LDAP

Puede inicializar el cliente LDAP con `ldapclient` de una de estas dos maneras:

- Usando un perfil

  Al emitir el comando `ldapclient`, debe especificar como mínimo la dirección del servidor del perfil y el dominio. Si no especifica un perfil, se asume que el perfil es el predeterminado. El servidor proporciona el resto de la información requerida del perfil, excepto la información de la base de datos del certificado y el proxy.

  Si un nivel de credencial de un cliente es `proxy` o `proxy anonymous`, debe proporcionar el DN vinculado de proxy y la contraseña. Consulte “Niveles de credencial de cliente” [19] para obtener más información. Para activar la actualización de datos shadow, debe proporcionar las credenciales de administrador (`adminDN` y `adminPassword`).

  El uso de un perfil reduce la complejidad de la configuración de LDAP, especialmente en entornos empresariales.
- Definiendo todos los parámetros en una única línea de comandos

  No existe ningún perfil. De este modo, se crea el perfil en el mismo cliente. Con este método, la información de perfil se almacena en archivos de caché, y el servidor nunca la actualiza.

Puede emplear una sintaxis de comando diferente que utilice el comando `ldapclient` para inicializar el cliente.

- Inicializar un cliente usando un perfil que se ha configurado con los valores predeterminados. Por ejemplo:

```
# ldapclient init -a profilename=new -a domainname=west.example.com 192.168.0.1
System successfully configured
```

- Inicializar un cliente cuyo perfil se haya configurado con credenciales por usuario y utilice el método de autenticación `sasl/GSSAPI`.

  En este ejemplo se supone que, al crear las DIT con el comando `idsconfig`, especificó el método de autenticación y el nivel de credencial adecuados, como `self` para el nivel de credencial y `sasl/GSSAPI` para el método de autenticación. Consulte la siguiente salida parcial del comando `idsconfig` donde se va a crear el perfil por usuario en el servidor.

```
# /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
```

  El nombre del perfil es `gssapi_EXAMPLE.COM`. Después de haber creado el perfil de la manera que se muestra en el ejemplo, puede emitir el comando `ldapclient` para inicializar el cliente con el perfil por usuario.

```
# ldapclient init -a profilename=gssapi_EXAMPLE.COM -a \
domainname=example.com 9.9.9.50
```

Nota - Varios requisitos deben cumplirse al inicializar un cliente configurado con credenciales por usuario, como la configuración de Kerberos y la configuración de servidor DNS para trabajar con LDAP. Para obtener información acerca de Kerberos, consulte "Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ". Para obtener información sobre la configuración de DNS, consulte Capítulo 3, "Gestión de sistema de nombres de dominio" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ". Consulte el Capítulo 2, LDAP y servicio de autenticación para obtener información sobre autenticación y Capítulo 3, Requisitos de planificación para servicios de nombres LDAP para obtener información sobre la creación del DIT.

- Inicializar un cliente que utilice credenciales de proxy. Por ejemplo:

```
# 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
```

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`.

- Inicializar un cliente para activar los datos shadow que se deben actualizar. Por ejemplo:

```
# 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 \
-a enableShadowUpdate=TRUE \
192.168.0.1
System successfully configured
```

Modificación de una configuración de cliente LDAP

Puede utilizar el comando `ldapclient` sin un perfil para modificar una configuración de cliente. Con frecuencia, la modificación afecta sólo a un número limitado de atributos de cliente, por lo que una única línea de comandos modifica todos los sufijos de atributos seleccionados.

- Modificar un cliente LDAP para usar el método de autenticación simple. Por ejemplo:

```
# ldapclient mod -a authenticationMethod=simple
```

- Modificar un cliente LDAP configurado para permitir la actualización de datos shadow. Por ejemplo:

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

Anulación de la inicialización de un cliente LDAP

Anular la inicialización de un cliente LDAP significa restaurar el servicio de nombres de un cliente al estado en que estaba antes de la última ejecución del comando `ldapclient` con las opciones `init`, `modify` o `manual`. En otras palabras, la opción `-uninit` del comando cancela los últimos cambios efectuados por la otras opciones del comando `ldapclient`. 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`.

Para anular la inicialización de un cliente LDAP, use la siguiente sintaxis:

```
# ldapclient uninit
System successfully recovered.
```

Uso de LDAP para la autenticación de cliente

En esta sección, se describen varias tareas de configuración que utilizan servicios de autenticación LDAP.

Configuración de PAM

El módulo `pam_ldap` es una opción del módulo PAM para LDAP para autenticar clientes y gestionar cuentas. Si ha configurado el modo de autenticación del perfil de cliente como `simple` y el nivel de credencial como `self`, deberá activar también el módulo `pam_krb`.

Consulte los siguientes recursos:

- Página del comando man `pam_ldap`(5)
- Página del comando man `pam_krb5`(5)
- “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ”

Configuración de PAM para utilizar `policy` de UNIX

El archivo `/etc/pam.conf` constituye el archivo de configuración predeterminado para que PAM utilice `policy` de UNIX. Normalmente, no es necesario introducir cambios en este archivo.

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 “Inicialización de un cliente LDAP” [72] para obtener un ejemplo de cómo inicializar un cliente LDAP para permitir la actualización de datos shadow.

Para obtener más información sobre el archivo de configuración, consulte la página del comando man `pam.conf`(4).

Configuración de PAM para utilizar `server_policy` de LDAP

Para saber cómo configurar PAM para utilizar `server_policy` de LDAP, consulte “Ejemplo de archivo `pam_conf` que utiliza el módulo para gestión de cuentas `pam_ldap`” [31]. Usando ese archivo de muestra, realice los siguientes pasos adicionales:

- Agregue las líneas que contienen `pam_ldap.so.1` al archivo `/etc/pam.conf` de cliente.
- Además, si algún módulo PAM del archivo 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` del cliente.

  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.

  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).
- Además, agregue la opción `server_policy` a la línea que contiene el módulo de servicio `pam_authtok_store.so.1`.

Nota - Antes, con la gestión de cuentas de `pam_ldap`, todos los usuarios debían proporcionar una contraseña de inicio de sesión para la autenticación cuando iniciaban sesión en el sistema. Por lo tanto, los inicios de sesión que no se basaban en contraseñas y usaban herramientas como `ssh` fallaban.

Ahora puede llevar a cabo la gestión de cuentas y recuperar el estado de la cuenta de los usuarios sin autenticarse en el servidor de directorios cuando el usuario inicia sesión.

El nuevo control del servidor de directorios es `1.3.6.1.4.1.42.2.27.9.5.8`. Este control se encuentra activado de manera predeterminada. Para modificar la configuración de control predeterminada, agregue las instrucciones de control de acceso (ACI) al servidor de directorios. Por ejemplo:

```
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
```

Configuración de seguridad TLS

Nota - Los archivos del certificado PEM deben ser legibles para todos. No cifrar ni limitar los permisos de lectura de estos archivos. De lo contrario, herramientas como `ldaplist` no funcionarán.

Si utiliza seguridad de la capa de transporte (TLS), debe instalar los archivos necesarios del certificado PEM. En particular, se requieren todos los archivos de certificados de CA y certificados de servidor autofirmados que se utilizan para validar el servidor LDAP y, posiblemente, el acceso de cliente al servidor. Por ejemplo, si tiene el certificado de CA PEM `certdb.pem`, debe asegurarse de que este archivo se agregue y se pueda leer en la ruta del certificado.

Nota - Si utiliza TLS, instale primero los archivos necesarios del certificado PEM como se describe en esta sección antes de ejecutar `ldapclient`.

Para obtener información sobre cómo crear y gestionar los certificados de formato PEM, vea la sección sobre configuración de clientes LDAP para utilizar SSL en el capítulo “Gestión de SSL” de la Guía del administrador para la versión de Oracle Directory Server Enterprise Edition que esté utilizando. Después de la configuración, estos archivos se deben almacenar en la

ubicación prevista por el cliente de servicios de nombres LDAP. El atributo `certificatePath` determina esta ubicación. De manera predeterminada, esta ubicación se encuentra en `/var/ldap`.

Por ejemplo, después de crear el archivo necesario de certificado PEM, como `certdb.pem`, cópielo en la ubicación predeterminada de la siguiente manera:

```
# cp certdb.pem /var/ldap
```

A continuación, otorgue acceso de lectura a todos.

```
# chmod 444 /var/ldap/certdb.pem
```

Nota - Más de un archivo de certificado podría residir en la ruta de certificado. Además, cualquier archivo de certificado PEM puede contener varios certificados de formato PEM que estén concatenados juntos. Consulte la documentación de su servidor para obtener más información. Los archivos de certificado deben estar almacenados en un sistema de archivos local si los está utilizando para un cliente del servicio de nombres LDAP.

♦ ♦ ♦ CAPÍTULO 6

Resolución de problemas de LDAP

En este capítulo se describen los problemas de configuración LDAP y se sugieren soluciones para resolverlos. En este capítulo, se tratan los temas siguientes:

Supervisión del estado de los cliente LDAP

En esta sección, se describen varios comandos para ayudar a determinar el estado del entorno del cliente LDAP. Consulte también las páginas del comando man relacionadas para obtener información adicional sobre las opciones que se pueden utilizar.

Para obtener información sobre Service Management Facility (SMF), consulte "Gestión de los servicios del sistema en Oracle Solaris 11.2 ". Para obtener más información, consulte también las páginas del comando man `svcadm`(1M) y `svcs`(1).

Verificación de que el daemon `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`. Puede determinar si el servicio de cliente LDAP está en línea de varias maneras:

- 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 la opción `-l` 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)
```

- Transfiera 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
```

Si el daemon `ldap_cachemgr` está desactivado, actívelo con el siguiente comando:

```
# svcadm enable network/ldap/client
```

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

Comprobación de la información actual de perfil

Para ver la información actual de perfil, conviértase en superusuario o asuma un rol equivalente, y ejecute `ldapclient` con la opción `list`.

```
# 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
```

Además del comando `ldapclient list`, también puede utilizar el comando `svccfg` o `svcprop` para obtener información de perfil actual.

Verificación de comunicación básica cliente-servidor

Para verificar que las comunicaciones existen entre el cliente LDAP y el servidor LDAP, utilice el comando `ldaplist`.

- Si se usa el comando `ldaplist` sin opciones, se muestran todos los contenedores del DIT en el servidor.
- Si se usa el comando `ldaplist` *database*, se muestran los contenidos de la base de datos específica, como `ldaplist passwd` *username* o `ldaplist host` *hostname*.

Comprobación de datos del servidor desde un equipo no cliente

Para comprobar información de un sistema sin cliente LDAP existente, utilice el comando `ldapsearch`. La información que se muestra depende del filtro que utilice para la búsqueda. En el siguiente ejemplo se muestran todos los contenedores en el DIT:

```
# ldapsearch -h server1 -b "dc=west,dc=example,dc=com" -s one "objectclass=*"
```

Para obtener una lista de opciones y filtros que se pueden usar con el comando `ldapsearch`, consulte la página del comando man `ldapsearch`(1).

Problemas y soluciones de la configuración de LDAP

En esta sección, se describen los posibles problemas de configuración LDAP y se sugieren soluciones.

Nombre de host no resuelto

El software de cliente LDAP devuelve nombres de host completos para consultas de host, como nombres de host devueltos 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 software de 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 del 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 utilizan los módulos PAM para la 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:

- `ldap` no está asociado a la base de datos `passwd` en el conmutador de servicio de nombres.
- 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.
- El agente de proxy podría no tener la contraseña correcta.
- La entrada no contiene la clase de objeto `shadowAccount`.
- 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`.
- No hay servidores LDAP accesibles.

  Compruebe el estado de los servidores.

  ```
  # /usr/lib/ldap/ldap_cachemgr -g
  ```
- `pam.conf` se ha configurado incorrectamente.
- El usuario no está definido en el espacio de nombres LDAP.
- `NS_LDAP_CREDENTIAL_LEVEL` se establece en `anonymous` para los módulos `pam_unix_*`, y `userPassword` no está disponible para usuarios anónimos.
- La contraseña no está almacenada en formato `crypt`.
- Si `pam_ldap` está configurado para admitir la gestión de cuentas, el fallo 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`.
- Si se utiliza la autenticación por usuario y `sasl/GSSAPI`, algún componente de Kerberos o la configuración de `pam_krb5` se establecieron incorrectamente. Consulte “Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.2 ” para obtener detalles sobre la resolución 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. En la documentación de LDAP, tanto de Oracle como de otros proveedores, se 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 usando la opción `init` con el atributo `profileName` especificado. Los posibles motivos de la falla incluyen los siguientes:

- Se especificó el nombre de dominio incorrecto en la línea de comandos.
- El atributo `nisDomain` no está configurado en el DIT para representar el punto de entrada para el dominio de cliente especificado.
- 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.
- Se transfirió una dirección de servidor incorrecta al comando `ldapclient`. Use el comando `ldapsearch` para verificar la dirección del servidor.
- Se transfirió un nombre de perfil incorrecto al dominio `ldapclient`. Use el comando `ldapsearch` para verificar el nombre de perfil en el DIT.

Como ayuda de resolución de problemas, use `snoop` en la interfaz de red del cliente para ver el tipo de tráfico de salida y determinar con qué servidor se está comunicando.

Uso del daemon `ldap_cachemgr` para depuración

La ejecución del daemon `ldap_cachemgr` con la opción `-g` para ver las estadísticas y la configuración del cliente actual puede ser útil para la depuración.

Este comando muestra la configuración actual y las estadísticas en una salida estándar, donde se incluye 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. En tal caso, póngase en contacto con el administrador del servidor para asegurarse de que el servidor esté en ejecución.

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.

Resolución de problemas derivados del uso de credenciales por usuario

El uso de credenciales por usuario requiere más configuración como la configuración de Kerberos u otra similar. Consulte las notas siguientes cuando configure perfiles por usuario.

El archivo `syslog` indica `82 Local Error`

Es posible que el archivo `syslog` tenga el siguiente mensaje de error:

```
libsldap: Status: 7 Mesg: openConnection: GSSSAPI bind failed -82 Local error
```

Es posible que Kerberos no se haya inicializado o que sus tickets hayan caducado. `klist` emita el comando para examinar. El problema hace que el comando `kinit -p` o el comando `kinit -R` reinicialicen Kerberos.

Kerberos no se inicializa automáticamente

Para hacer que el comando `kinit` se ejecute automáticamente siempre que se conecte, agregue `pam_krb5.so.1` al archivo `/etc/pam.conf`. Por ejemplo:

```
login      auth optional pam_krb5.so.1
rlogin     auth optional pam_krb5.so.1
other      auth optional pam_krb5.so.1
```

El archivo `syslog` indica credenciales no válidas

Es posible que el archivo `syslog` contenga `Invalid credential` después de emitir el comando `kinit`. El problema puede ser uno de los siguientes:

- La entrada de host `root` o la entrada de usuario no están en el directorio LDAP.
- Las reglas de asignación son incorrectas.

El comando `ldapclient init` falla en la comprobación de conmutador

Cuando se emite el comando `ldapclient init`, se comprueba la presencia de la configuración `self/sasl/GSSAPI` en el perfil LDAP. Si la comprobación de conmutador falla, normalmente el error radica en que el DNS no se está utilizando como criterio de búsqueda de la base de datos del host.

- Ejecute los siguientes dos comandos para comprobar el estado del servicio DNS y para activarlo.

```
# svcs -l dns/client
# svcadm enable dns/client
```

- Si el fallo se produce en la operación de enlace de `sasl/GSSAPI`, compruebe el archivo `syslog` para determinar el problema.

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, que puede resultar útil para la resolución de problemas. Consulte `ldaplist`(1) para obtener más información.

Listado de todos los contenedores LDAP

El comando `ldaplist` muestra su salida con una línea en blanco que separa los registros, lo cual es útil para registros grandes con varias líneas.

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`.

En el siguiente ejemplo, se muestra un ejemplo de la salida 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 el comando `getent`. Por ejemplo:

```
# getent passwd user1
user1::30641:10:Joe Q. User:/home/user1:/bin/csh
```

También se utiliza el comando `getent` para realizar consultas en bases de datos que se muestran en la tabla de montaje automático: por ejemplo, `getent automount/`*`map`* `[`*`key`*`]`. Por ejemplo:

```
# getent automount/auto_home user1
user1 server-name:/home/user1
```

En el ejemplo anterior, `auto_home` es el nombre del mapa de montaje automático y `user1` es la clave de búsqueda. Si no se especifica ninguna clave de búsqueda, todo el contenido del mapa de montaje automático especificado se muestra en una lista.

Para 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
```

♦ ♦ ♦ CAPÍTULO 7

Servicio de nombres LDAP (Referencia)

En este capítulo se tratan los temas siguientes.

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 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 )

( 2.16.840.1.113894.1009.2.100.1.1 NAME 'SolarisUserAttrEntry'
  DESC 'user_attr file format without username'
  EQUALITY caseExactIA5Match
  SYNTAX  'IA5String'  )


( 2.16.840.1.113894.1009.2.100.1.2 NAME 'SolarisUserType'
  DESC 'specifies whether a normal user or a role'
  EQUALITY caseExactIA5Match
  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 ) )

( 2.16.840.1.113894.1009.2.100.2.1 NAME 'SolarisQualifiedUserAttr'
  SUP top AUXILIARY
  DESC 'Host or netgroup qualified user attributes'
  MAY ( SolarisUserAttrEntry $ SolarisUserType ) )
```

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  )
```

`ObjectClasses` de impresora Sun

```
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 7-1 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))`

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))
profileByName	(&(objectClass=SolarisProfAttr)(cn=%s))
userByName	(&(objectClass=SolarisUserAttr)(uid=%s))

La siguiente tabla muestra los filtros de atributo `getent`.

TABLA 7-2 Filtros de atributo `getent`

Filtro	Definición
aliases	(objectClass=rfc822MailGroup)
auth_attr	(objectClass=SolarisAuthAttr)

Filtro	Definición
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 8

Transición de NIS a LDAP

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 las ventajas de la transición a LDAP, consulte “Descripción general de servicio de nombres LDAP” [12].

En este capítulo, se tratan los siguientes temas:

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 1, Introducción al servicio de nombres LDAP.

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 secciones:

- "Suposiciones de los destinatarios de NIS a LDAP" [115]
- "Cuándo no utilizar el servicio de NIS a LDAP" [115]
- "Efectos del servicio de NIS a LDAP en los usuarios" [115]
- "Terminología de la transición de NIS a LDAP" [116]
- "Comandos, archivos y asignaciones de NIS a LDAP" [117]
- "Asignaciones estándar admitidas" [118]

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. Puede llevar a cabo acciones administrativas en estos servicios, como la activación, la desactivación o el reinicio, 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" [69] y "NIS y la utilidad de gestión de servicios" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ". Para obtener información sobre SMF, consulte "Gestión de los servicios del sistema en Oracle Solaris 11.2 ". Para obtener más información, consulte también las páginas del comando man `svcadm`(1M) y `svcs`(1).

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:

- Capítulo 5, “Acerca del servicio de información de red” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”, para obtener una descripción general de NIS
- El Capítulo 1, Introducción al servicio de nombres LDAP, 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 se planea compartir datos entre clientes de servicio de nombres NIS y LDAP.

  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 servicio de 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. Sin embargo, 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 las asignaciones NIS actualizadas al servidor esclavo cuando `yppush` es invocado 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 servicio 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. Este 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 8-1 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.
mapa/mapear	En el contexto del servicio N2L, se utilizan los términos "mapa" y "mapear":

Término	Descripción
	■ 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.
mapas 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" [118].
mapas 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 servicio de nombres LDAP maneja un subconjunto personalizado de información de nombres.
cliente de servicio 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 8-2 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).
`/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).

Comando/archivo/mapa	Descripción
`/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 lista de mapas proporcionada a continuación 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. Los mapas del sistema que no aparezcan en la lista se consideran mapas personalizados y requieren modificación manual.

El servicio N2L también admite asignación automática de las asignaciones `auto.*`. Sin embargo, debido a que la mayoría de los contenidos y los nombres de archivos `auto.*` son específicos para cada configuración de red, esos archivos no están especificados en esta lista. Existen algunas excepciones a estos mapas `auto.home` y `auto.master`, que se admiten como mapas estándar.

Los mapas estándar son:

```
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 el mapa específico de N2L, `ageing.byname` para leer y escribir información sobre la función de 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.	Asegurarse de haber configurado correctamente el servidor NIS y Oracle Directory Server Enterprise Edition (servidor LDAP).	"Requisitos previos para la transición de NIS a LDAP" [119]
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 [121]
	Asignaciones personalizadas o no estándar	Cómo configurar el servicio N2L con asignaciones personalizadas o no estándar [123]
Personalizar un mapa.	Ver ejemplos de cómo crear asignaciones personalizadas para la transición N2L.	"Ejemplos de asignaciones personalizadas" [126]
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" [128]
Resolver problemas del sistema.	Identificar y resolver problemas comunes de N2L.	"Resolución de problemas de NIS a LDAP" [131]
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 [137]
	Asignaciones basadas en el DIT actual	Cómo revertir a asignaciones según el contenido actual del DIT [137]

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.

  Las herramientas de migración de NIS a LDAP admiten Oracle Directory Server Enterprise Edition y las versiones compatibles de servidores de directorios de Oracle. 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 4, Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP 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`. Dado que la dirección del servidor LDAP se muestra en otro lugar, el cambio de 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 procedimientos de esta sección.

Como parte de la conversión de NIS a LDAP, deberá ejecutar el comando `inityp2l`. Este comando ejecuta una secuencia de comandos interactiva para la que debe proporcionar información de configuración. Consulte la página del comando man `ypserv`(1M) para obtener explicaciones de los tipos de información que debe proporcionar.

- 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 el mapa `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* se admite en 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” [118]. Si utiliza asignaciones estándar o no estándar, consulte Cómo configurar el servicio N2L con asignaciones personalizadas o no estándar [123].

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” [119].**

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

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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" [120] 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) LDAP se inicializo 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 el DIT está inicializado por completo, omita el paso 5 y vaya al Paso 6.

5. **Inicialice 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 los mapas NIS antiguos estén actualizados.**

      ```
      # 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.

   Sugerencia - 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
```

El servicio N2L ya está configurado con los mapas 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.

Sugerencia - 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” [118].
- 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” [119].**

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

Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte Capítulo 3, “Asignación de derechos en Oracle Solaris” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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” [120] 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” [126] para ver ejemplos de cómo modificar el archivo de asignación.

5. **Determine si el árbol de información de directorios (DIT) LDAP se inicializo 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 el DIT está inicializado por completo, omita el paso 6.

6. **Inicialice 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.

Sugerencia - 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.

Sugerencia - 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 servicio 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” [136] para obtener más información.

Ejemplos de asignaciones personalizadas

En los ejemplos de esta sección, se muestra cómo se pueden personalizar los mapas. Utilice su editor de texto preferido 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 1, Introducción al servicio de nombres LDAP.

EJEMPLO 8-1 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` para el nuevo nombre distintivo (DN) de la base de LDAP. 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
```

a:

```
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 8-2 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. Este mapa está indexado por el número de serie de la máquina 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:

```
dn: number=123,ou=servdates,dc=... \
number: 123 \
userName: John Smith \
date: 1/3/2001 \
date: 4/5/2003 \
.
.
.
objectClass: servDates
```

Al examinar el archivo `NISLDAPmapping`, puede ver que la asignación más cercana al patrón requerido es `group`. La asignaciones personalizadas se pueden modelar en la asignación `group`. Debido a que hay sólo un mapa, 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 un servidor 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 Oracle Directory Server Enterprise Edition, puede mejorar el servidor de directorios para optimizar el rendimiento. Para realizar estas mejoras, debe tener privilegios de administrador de 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. (Utilice su motor de búsqueda favorito para buscar "oracle.com: sun java system directory server enterprise edition").

Creación de índices de vista de lista virtual con 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 deben poder 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 los mapas son más grandes que el límite de tamaño o si no está seguro del tamaño de todos los mapas, use los índices de VLV para evitar devoluciones incompletas.

Si está utilizando los índices de VLV, configure los límites de tamaño adecuado según lo 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).

Una vez creados los índices de VLV, actívelos ejecutando `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 dan las condiciones siguientes:

- 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 los mapas o copiar y modificar los índices de 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 de VLV existentes, escriba el siguiente comando:

```
% ldapsearch -h hostname -s sub -b "cn=ldbm database,cn=plugins,cn=config"
 "objectclass=vlvSearch"
```

Cómo evitar los 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 se ha configurado correctamente, puede que se exceda el tiempo de espera de la operación de refrescamiento antes de que esta se complete. Para evitar que se excedan los tiempos de espera del servidor de directorios, debe modificar los atributos de Oracle Directory Server Enterprise Edition manualmente o mediante la ejecución del 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 4, Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP de este manual.

Cómo evitar saturaciones del búfer con Oracle Directory Server Enterprise Edition

Para evitar saturaciones del búfer, modifique los atributos Oracle Directory Server Enterprise Edition manualmente o mediante la ejecución del comando `idsconfig`.

- 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
  ```

- 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 con Oracle Directory Server Enterprise Edition” [128]. 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 4, Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP.

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 proporcionando resultados incompletos y desactualizados.

En esta sección, se describen 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 de 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` que puede deberse 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.

`El mensaje de la consola se muestra cuando se ejecuta ypserv -ir (o - Ir)`

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 las descripciones de error LDAP en “Mensajes de error de LDAP comunes” [131].

`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 existan 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, una asignación crea la mayor parte del objeto, incluidos todos los atributos `MUST` del objeto. Otras asignaciones contribuyen atributos `MAY` adicionales.

Las asignaciones se procesan en el mismo orden en 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” [131] 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 que el comando se ejecuta, la entrada LDAP alcanza el estado de completado.

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 un mapa, el resultado puede ser un único acceso del directorio LDAP de gran tamaño. Si Oracle Directory Server Enterprise Edition no se ha configurado correctamente, puede que se exceda el tiempo de espera de la operación antes de que esta se complete.

Solución: Para evitar que se excedan los tiempos de espera del servidor de directorios, debe modificar los atributos de Oracle Directory Server Enterprise Edition manualmente o mediante la ejecución del comando `idsconfig`. Consulte “Mensajes de error de LDAP comunes” [131] y “Mejores prácticas de NIS a LDAP con Oracle Directory Server Enterprise Edition” [128] 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 para describir acciones:

```
# 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” [119].

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, a continuación, 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. Si las direcciones del servidor deben estar enumeradas en `hosts`, `ipnodes`, o en ambos archivos depende de cómo estén configurados estos archivos para resolver nombres de host local. 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`. Dado que la dirección del servidor LDAP aparecería en otro lugar, el cambio de la dirección del servidor LDAP o el servidor N2L requeriría un esfuerzo levemente mayor.

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 maneras de volver al NIS tradicional, como se explica en los procedimientos de esta sección.

Sugerencia - 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 que mantener los mapas N2L resulte útil en caso de que más tarde se decida volver a activar el N2L. Sin embargo, tenga en cuenta que los mapas ocupan espacio en el disco.

▼ Cómo revertir a asignaciones según los archivos de origen antiguos

1. **Conviértase en administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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/domain-name/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 “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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/domain-name/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 (DIT) 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*.

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.

campo Una entrada de mapa 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 máquina) que solicita un servicio de nombres de un servidor de nombres.

(2) En el modelo cliente-servidor para sistemas de archivos, el cliente es una máquina 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 al servicio desde un "proceso de servidor". En este modelo, el cliente y el servidor pueden ejecutarse en la misma máquina o en máquinas diferentes.

conmutador 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.

contexto Para el servicio N2L, un contexto es algo a donde en general se asigna un domino NIS. 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 junto 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 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 de acceso a directorios ligero 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.

mapas NIS Archivo utilizado por NIS que contiene información de un tipo concreto, por ejemplo, las entradas de contraseñas de todos los usuarios de una red o los nombres de todas las máquinas host de una red. Los programas que forman parte del servicio NIS consultan estos mapas. Consulte también *NIS*.

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 (DN) 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 en una ruta que vaya 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: 192.168.67.20.

origen Archivos de origen NIS

Protocolo de control de transporte (TCP) Protocolo de transporte principal del conjunto de protocolos de Internet que proporciona secuencias de dúplex completo, confiables y 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 radiodifusión; o un grupo de dos o más LAN enlazadas 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, y así proporciona 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 direcciones y nombres de red de máquinas, usuarios, dominios, enrutadores, etcétera.

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 enlazadas 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 una máquina host que proporciona los servicios de nombres a una red.

(2) En el *modelo cliente-servidor* para sistemas de archivos, el servidor es una máquina con recursos informáticos (que a veces se denomina *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 la misma máquina o en máquinas 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.

Sistema de nombres de dominios (DNS) Servicio que proporciona las políticas y los mecanismos de nombres para la asignación de dominio y los nombres de máquinas para direcciones fuera de la empresa, como las de Internet. DNS es el servicio de información de la red utilizado por Internet.

SSL SSL es el protocolo de capa de conexión segura. 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™. 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

W

X

Y

Z