Gestión de servicios de protocolo de ubicación de servicios en Oracle® Solaris 11.1

Referencia: E36528–01
Octubre de 2012

ORACLE®

130327@25097

Contenido

Lista de figuras

Lista de tablas

Lista de ejemplos

Prefacio

Gestión de servicios de protocolo de ubicación de servicios en Oracle Solaris 11.1 forma parte de un conjunto de varios volúmenes que tratan de manera exhaustiva la información de administración de sistemas Oracle Solaris. En esta guía, se da por sentado que ya instaló el sistema operativo Oracle Solaris y que configuró el software de red que tiene previsto usar.

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

Quién debe utilizar este manual

Esta guía está dirigida a las personas responsables de administrar uno o varios sistemas que ejecutan Oracle Solaris. Para utilizar esta guía, se debe tener entre uno y dos años de experiencia en la administración de sistemas UNIX. Puede resultar útil participar en cursos de formación para administración de sistemas UNIX.

Acceso a Oracle Support

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

Convenciones tipográficas

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

TABLA P–1 Convenciones tipográficas

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

Indicadores de los shells en los ejemplos de comandos

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

TABLA P–2 Indicadores de shell

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

◆ ◆ ◆ CAPÍTULO 1

1 SLP (descripción general)

El protocolo de ubicación de servicios (SLP) proporciona una estructura portátil independiente de plataforma para la detección y el aprovisionamiento de servicios de red activados para SLP. En este capítulo, se describen la arquitectura del SLP y la implementación de Oracle Solaris del SLP para intranets de IP.

Arquitectura del SLP

En esta sección, se detalla el funcionamiento esencial del SLP y se describen los agentes y procesos que se utilizan en la administración del SLP.

SLP proporciona todos los siguientes servicios automáticamente, con poca o sin configuración.

- La aplicación cliente solicita información necesaria para acceder a un servicio.
- Anuncio de servicios en servidores de software o dispositivos de hardware de red; por ejemplo, impresoras, servidores de archivos, cámaras de vídeo y servidores HTTP.
- Recuperación gestionada tras fallos de servidores principales.

Además, puede hacer lo siguiente para administrar y ajustar el funcionamiento del SLP si es necesario.

- Organizar los servicios y usuarios en *ámbitos* que están compuestos por grupos lógicos o funcionales.
- Permitir el registro del SLP para supervisar y solucionar problemas del funcionamiento del SLP en la red.
- Ajustar los parámetros de sincronización del SLP para mejorar el rendimiento y la escalabilidad.

- Configurar el SLP para que no envíe ni procese mensajes de multidifusión cuando el SLP se implementa en redes que no admiten el enrutamiento de multidifusión.
- Implementar agentes de directorio del SLP para mejorar la escalabilidad y el rendimiento.

Resumen del diseño del SLP

Las bibliotecas del SLP informan a los agentes para redes que anuncian servicios para que dichos servicios se detecten por medio de una red. Los agentes del SLP mantienen información actualizada sobre el tipo y la ubicación de servicios. Esos agentes también pueden utilizar registros de proxy para anunciar servicios que no están directamente activados para SLP. Para obtener más información, consulte el Capítulo 4, “Incorporación de servicios antiguos”.

Las aplicaciones cliente dependen de bibliotecas del SLP que realizan solicitudes directamente a los agentes que anuncian servicios.

Agentes y procesos del SLP

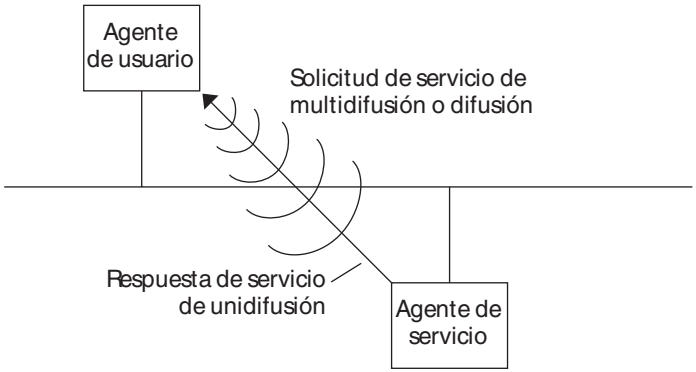
En la siguiente tabla, se describen los agentes del SLP.

TABLA 1–1 Agentes del SLP

Agente del SLP	Descripción
Agente de directorio (DA)	Proceso que almacena en la memoria caché anuncios del SLP que son registrados por agentes de servicio (SA). El DA reenvía anuncios de servicios a agentes de usuario (UA) a petición.
Agente de servicio (SA)	Agente del SLP que actúa en nombre de un servicio para distribuir anuncios de servicios y registrar el servicio con agentes de directorio (DA).
Agente de usuario (UA)	Agente del SLP que actúa en nombre de un usuario o una aplicación para obtener información sobre anuncios de servicios.
Ámbito	Una agrupación administrativa o lógica de servicios.

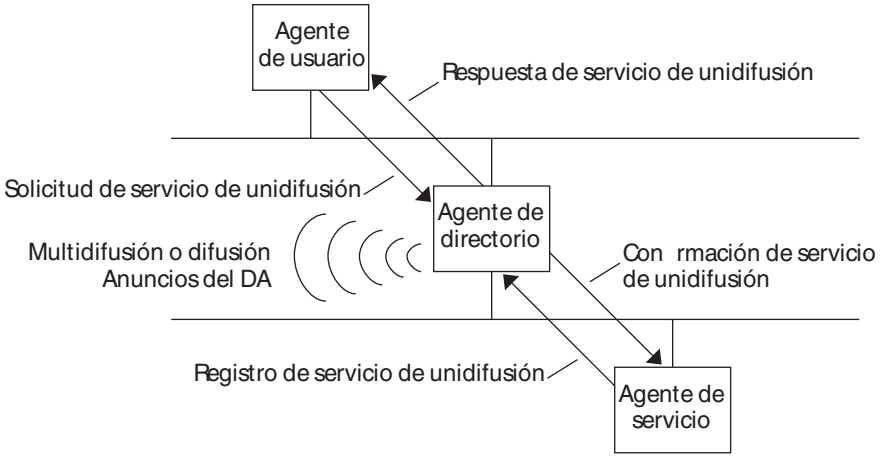
En la siguiente figura, se muestran los agentes y procesos básicos que implementan la arquitectura del SLP. La figura representa una implementación predeterminada del SLP. No se ha realizado ninguna configuración especial. Sólo dos agentes son necesarios: el UA y el SA. La estructura del SLP permite al UA enviar una multidifusión de solicitudes de servicios al SA. El SA envía una unidifusión de una respuesta al UA. Por ejemplo, cuando el UA envía un mensaje de solicitud de servicio, el SA responde con un mensaje de respuesta de servicio. La respuesta de servicio contiene la ubicación de los servicios que coinciden con los requisitos del cliente. Otras solicitudes y respuestas son posibles para atributos y tipos de servicio. Para obtener más información, consulte el Capítulo 5, “SLP (referencia)”.

FIGURA 1–1 Agentes y procesos básicos del SLP



En la siguiente figura, se muestran los agentes y procesos básicos que implementan la arquitectura del SLP cuando un DA se implementa en la estructura.

FIGURA 1–2 Agentes y procesos arquitectónicos del SLP implementados con un DA



Al implementar DA, menos mensajes se envían en la red, y los UA pueden recuperar información mucho más rápido. Los DA son esenciales cuando el tamaño de una red aumenta o en situaciones en las que no se admite el enrutamiento de multidifusión. El DA sirve como una memoria caché para anuncios de servicios registrados. Los SA envían mensajes de registro (`SrvReg`) que muestran todos los servicios que anuncian para los DA. Los SA, a continuación, reciben confirmaciones (`SrvAck`) en respuesta. Los anuncios de servicios se actualizan con el

DA o caducan según la duración que se establece para el anuncio. Después de que un UA detecta un DA, el UA envía una unidifusión de una solicitud al DA en lugar de enviar una multidifusión de solicitudes a los SA.

Para obtener más información sobre los mensajes del SLP de Oracle Solaris, consulte el Capítulo 5, “SLP (referencia)”.

Implementación del SLP

En la implementación del SLP de Oracle Solaris, los SA, los UA, los DA, los servidores de SA, los ámbitos y otros componentes arquitectónicos del SLP en la Tabla 1–1 son parcialmente asignados en `slpd` y en procesos de aplicación. El daemon del SLP, `slpd`, organiza determinadas interacciones del SLP fuera del host para realizar lo siguiente:

- Emplear la detección pasiva y activa de agentes de directorio para detectar todos los DA en la red.
- Mantener una tabla actualizada de DA para utilizar los UA y SA en el host local.
- Actuar como un servidor de SA de proxy para anuncios de servicios antiguos (registro de proxy).

Además, puede establecer la propiedad `net.slpisDA` para configurar `slpd` para que actúe como DA. Consulte el Capítulo 3, “Administración del SLP (tareas)”.

Para obtener más información sobre el daemon del SLP, consulte `slpd(1M)`.

Además de `slpd`, las bibliotecas de cliente de Java y C/C++ (`libslp.so` y `slp.jar`) permiten el acceso a la estructura del SLP para los clientes de UA y SA. Las bibliotecas de cliente proporcionan las siguientes funciones:

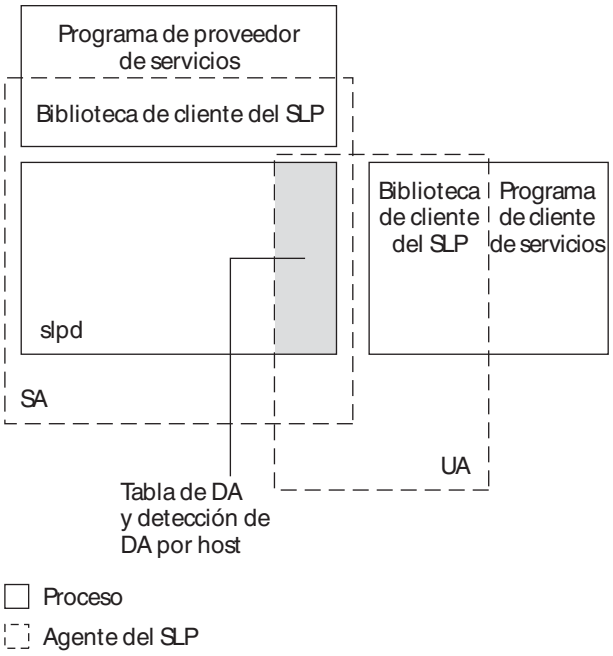
- Software que ofrece servicios de red que pueden registrar y anular registros de anuncios de servicios.
- Software cliente que puede solicitar servicios emitiendo consultas de anuncios de servicios.
- La lista de ámbitos del SLP disponibles para registro y solicitudes.

No se necesita ninguna configuración especial para activar la comunicación entre procesos entre `slpd` y las bibliotecas de cliente que proporcionan los servicios anteriores. Sin embargo, debe ejecutar el proceso `slpd` antes de cargar las bibliotecas de cliente para que las bibliotecas funcionen.

En la siguiente figura, la biblioteca de cliente del SLP en el programa de proveedor de servicios emplea la funcionalidad del SA. El programa de proveedor de servicios utiliza la biblioteca de cliente del SLP para registrar y anular registros de servicios con `slpd`. La biblioteca de cliente del SLP en el programa de cliente de servicios emplea la funcionalidad del UA. El programa de cliente de servicios utiliza la biblioteca de cliente del SLP para realizar solicitudes. La biblioteca

de cliente del SLP envía multidifusiones de solicitudes a los SA o envía unidifusiones de solicitudes a los DA. Esta comunicación es transparente para la aplicación, excepto que el método de unidifusión para emitir solicitudes es más rápido. El comportamiento de la biblioteca de cliente puede verse afectado al establecer distintas propiedades de configuración del SLP. Para obtener más información, consulte el Capítulo 3, “Administración del SLP (tareas)”. El proceso `slpd` gestiona todas las funciones del SA, como la respuesta a solicitudes de multidifusión y el registro con DA.

FIGURA 1–3 Implementación del SLP



Otras fuentes de información del SLP

Consulte los siguientes documentos para obtener más información sobre el SLP:

- Kempf, James y St. Pierre, Pete. *Service Location Protocol for Enterprise Networks (Protocolo de ubicación de servicios para redes empresariales)*. John Wiley & Sons, Inc. Número ISBN: 0–471–31587–7.
- *Authentication Management Infrastructure Administration Guide (Guía de administración de infraestructura de gestión de autenticación)*. Número de referencia: 805–1139–03.

- Guttman, Erik; Perkins, Charles; Veizades, John; y Day, Michael. *Service Location Protocol, Version 2, RFC 2608 (Protocolo de ubicación de servicios, versión 2, RFC 2608)* del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [http://www.ietf.org/rfc/rfc2608.txt]
- Kempf, James y Guttman, Erik. *An API for Service Location, RFC 2614 (Una API para ubicación de servicios, RFC 2614)* del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [http://www.ietf.org/rfc/rfc2614.txt]

◆ ◆ ◆ CAPÍTULO 2

Planificación y habilitación del SLP (tareas)

En este capítulo, se proporciona información sobre la planificación y habilitación del SLP. En las siguientes secciones, se tratan la configuración del SLP y el proceso para habilitar el SLP.

Consideraciones para la configuración del SLP

El daemon del SLP está preconfigurado con propiedades predeterminadas. Si su empresa funciona bien con los valores predeterminados, la implementación del SLP prácticamente no exige ninguna administración.

En algunas situaciones, sin embargo, quizá desee modificar las propiedades del SLP para ajustar las operaciones de red o activar ciertas características. Con unos pocos cambios de configuración, por ejemplo, puede activar el registro del SLP. La información en un registro del SLP y en los rastreos de `snoop` puede ayudar a decidir si es necesario realizar una configuración adicional.

Las propiedades de configuración del SLP residen en el archivo `slp.conf`, que se encuentra en el directorio `/etc/inet`. Si decide cambiar los valores predeterminados de las propiedades, consulte el Capítulo 3, "Administración del SLP (tareas)" para obtener los procedimientos apropiados.

Antes de modificar los valores de configuración del SLP, tenga en cuenta las siguientes preguntas que están relacionadas con aspectos clave de la administración de redes:

- ¿Qué tecnologías de red funcionan en la empresa?
- ¿Cuánto tráfico de red pueden manejar las tecnologías sin inconvenientes?
- ¿Cuántos servicios hay disponibles en la red? ¿De qué tipo son?
- ¿Cuántos usuarios hay en la red? ¿Qué servicios necesitan? ¿Dónde se encuentran los usuarios en relación con los servicios a los que acceden con más frecuencia?

Toma de decisiones con respecto a qué reconfigurar

Puede usar la utilidad `snoop` habilitada para SLP y las utilidades de registro del SLP para decidir si la reconfiguración es necesaria y qué propiedades necesita modificar. Por ejemplo, puede reconfigurar determinadas propiedades para realizar lo siguiente:

- Incluir una combinación de medios de red que tienen distintas latencias y características de ancho de banda.
- Recuperar la empresa de fallos de red o particiones no planificadas.
- Agregar DA para reducir la proliferación de multidifusiones del SLP.
- Implementar nuevos ámbitos para organizar usuarios con los servicios a los que acceden con más frecuencia.

Uso de `snoop` para supervisar la actividad del SLP

La utilidad `snoop` es una herramienta administrativa pasiva que proporciona información sobre el tráfico de la red. La propia utilidad genera un tráfico mínimo y permite ver toda la actividad en su red a medida que se produce.

La utilidad `snoop` proporciona rastreos del tráfico de mensajes del SLP real. Por ejemplo, cuando ejecuta `snoop` con el argumento de línea de comandos `slp`, la utilidad muestra rastreos con información sobre los registros y las anulaciones de registros del SLP. Puede utilizar la información para evaluar la carga de la red mediante la comprobación de los servicios que se registran y de cuánta actividad de reregistro se produce.

La utilidad `snoop` también es útil para observar el flujo del tráfico entre los hosts del SLP de la empresa. Cuando ejecuta `snoop` con el argumento de línea de comandos `slp`, puede supervisar los siguientes tipos de actividad del SLP para determinar si es necesaria la reconfiguración de la red o el agente:

- El número de hosts que está utilizando un DA determinado. Utilice esta información para decidir si se deben implementar más DA para el equilibrio de carga.
- El número de hosts que está utilizando un DA determinado. Utilice esta información para determinar si se deben configurar ciertos hosts con ámbitos nuevos o diferentes.
- Si el UA solicita un tiempo de espera o la confirmación del DA es lenta. Puede determinar si un DA está sobrecargado mediante la supervisión de los tiempos de espera y las retransmisiones del UA. También puede comprobar si el DA requiere más de unos segundos para enviar confirmaciones de registro a un SA. Utilice esta información para volver a equilibrar la carga de la red en el DA, si es necesario, implementando más DA o cambiando las configuraciones del ámbito.

Mediante `snoop` con el argumento de línea de comandos `-V` (detallado), puede obtener duraciones de registro y el valor del indicador fresh en `SrvReg` para determinar si el número de reregistros debe reducirse.

También puede utilizar snoop para rastrear otros tipos de tráfico del SLP, como los siguientes:

- El tráfico entre clientes de UA y DA.
- El tráfico entre clientes de UA de multidifusión y SA de respuesta.

Para obtener más información sobre snoop, consulte snoop(1M).

Consejo – Utilice el comando netstat junto con snoop para ver estadísticas de congestión y tráfico. Para obtener más información sobre netstat, consulte netstat(1M).

▼ Cómo utilizar snoop para ejecutar rastreos del SLP

1 Conviértase en administrador.

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

2 Ejecute snoop con el argumento de línea de comandos slp.

```
Brief Mode:
# snoop slp
```

Al ejecutar snoop en el modo *breve* predeterminado, una salida continua se entrega a la pantalla. Los mensajes del SLP se truncan para que entren en una línea por rastreo de SLP.

```
Verbose Mode:
# snoop -v slp
```

Al ejecutar snoop en modo *detallado*, snoop entrega una salida sin abreviar y continua a su pantalla, que proporciona la siguiente información:

- La dirección completa de la URL del servicio.
- Todos los atributos del servicio.
- La duración del registro.
- Todos los parámetros y los indicadores de seguridad, si hay alguno disponible.

Nota – Puede utilizar el argumento de línea de comandos slp con otras opciones de snoop.

Análisis de un rastreo de snoop slp

En el siguiente ejemplo, slpd se ejecuta en *slphost1* en el modo predeterminado como un servidor de SA. El daemon del SLP se inicializa y registra *slphost2* como un servidor de eco. A continuación, el proceso snoop slp se invoca en *slphost1*.

Nota – Para simplificar la descripción de los resultados del rastreo, las líneas en la siguiente salida `snoop` se marcan con números de línea.

```
(1) slphost1 -> 239.255.255.253 SLP V@ SrvRqst [24487] service:directory-agent []
(2) slphost2 -> slphost1 SLP V2 DAAdvert [24487] service:directory-agent://129
(3) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(4) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(5) slphost1 -> slphost2 SLP V2 SrvReg [24488/tcp]service:echo.sun:tcp://slphost1:
(6) slphost2 -> slphost1 SLP V2 SrvAck [24488/tcp] ok
(7) slphost1 -> slphost2 SLP V2 SrvDereg [24489/tcp] service:echo.sun:tcp://slphost1:
(8) slphost2 -> slphost1 SLP V2 SrvAck [24489/tcp] ok
```

1. Muestra un `slpd` en *slphost1* que realiza una detección activa de agentes de directorio mediante el envío de una multidifusión a la dirección de grupo de multidifusión del SLP en búsqueda de agentes de directorio. El número de mensaje, 24487, para la detección activa se indica entre corchetes en la pantalla de rastreo.
2. Indica que la solicitud de detección activa 24487 del rastreo 1 es respondida por `slpd`, que se está ejecutando como un DA en el host *slphost2*. La URL del servicio de *slphost2* se ha truncado para que entre en una única línea. El DA ha enviado un anuncio de DA en respuesta al mensaje de detección de agentes de directorio de multidifusión, según lo indicado por los números de mensaje coincidentes en los rastreos 1 y 2.
3. Muestra multidifusiones de los UA en *slphost1* para DA adicionales. Debido a que *slphost2* ya ha respondido la solicitud, se abstiene de responder de nuevo, y ningún otro DA responde.
4. Repite la operación de multidifusión que se muestra en la línea anterior.
5. Muestra un `slpd` en *slphost1* que reenvía registros de clientes de SA al DA en *slphost2*. Un registro de servicio de unidifusión (`SrvReg`) para un servidor de eco es realizado por *slphost1* para el DA en *slphost2*.
6. Muestra un *slphost2* que responde a *slphost1* `SrvReg` con una confirmación de servicio (`SrvAck`) que indica que el registro se ha realizado correctamente.

   El tráfico entre el servidor de eco que ejecuta el cliente del SA y el daemon del SLP en *slphost1* no aparece en el rastreo de `snoop`. Esta falta de información se debe a que la operación de `snoop` se realiza por medio de un bucle de retorno de red.
7. Muestra el servidor de eco en *slphost1* que anula el registro del anuncio del servicio de eco. El daemon del SLP en *slphost1* reenvía la anulación del registro al DA en *slphost2*.
8. Muestra un *slphost2* que responde a *slphost1* con una confirmación de servicio (`SrvAck`) que indica que la anulación del registro se ha realizado correctamente.

   El parámetro `/tcp` que se agrega al número de mensaje en las líneas 5, 6, 7 y 8 indica que el intercambio de mensajes ocurrió por TCP.

Dónde proseguir

Después de controlar el tráfico del SLP, puede utilizar la información que se recopiló de los rastreos de snoop para determinar si es necesario realizar la reconfiguración de los valores predeterminados del SLP. Utilice la información relacionada en el Capítulo 3, "Administración del SLP (tareas)" para configurar los valores de las propiedades del SLP. Para obtener más información sobre los registros de servicios y el envío de mensajes del SLP, consulte el Capítulo 5, "SLP (referencia)".

◆ ◆ ◆ CAPÍTULO 3

Administración del SLP (tareas)

En las secciones siguientes, se proporcionan información y tareas para configurar agentes y procesos del SLP.

Configuración de propiedades del SLP

Las propiedades de configuración del SLP controlan las interacciones de red, las características de agente del SLP, el estado y el registro. En la mayoría de las situaciones, la configuración predeterminada de estas propiedades no requiere ninguna modificación. Sin embargo, puede utilizar los procedimientos de este capítulo cuando el medio de red o la topología cambian, y para lograr los siguientes objetivos:

- Compensar las latencias de red
- Reducir la congestión de la red
- Agregar agentes o reasignar direcciones IP
- Activar el registro del SLP

Puede editar el archivo de configuración del SLP, `/etc/inet/slp.conf`, para realizar operaciones, como las que se muestran en la siguiente tabla.

TABLA 3–1 Operaciones de configuración del SLP

Operación	Descripción
Especifique si `slpd` debe actuar como servidor de DA. El servidor de SA es el valor predeterminado.	Establezca la propiedad `net.slpisDA` en `True`.
Establezca el intervalo para mensajes de multidifusión de DA.	Establezca la propiedad `net.slp.DAHeartBeat` para controlar la frecuencia con la que un DA envía una multidifusión de un anuncio no solicitado del DA.
Active el registro de DA para supervisar el tráfico de la red.	Establezca la propiedad `net.slp.traceDATraffic` en `True`.

Archivo de configuración del SLP: elementos básicos

El archivo `/etc/inet/slp.conf` define y activa toda la actividad del SLP cada vez que reinicia el daemon del SLP. El archivo de configuración consta de los siguientes elementos:

- Propiedades de configuración
- Líneas de comentario y notaciones

Propiedades de configuración

Todas las propiedades básicas del SLP, como, por ejemplo, `net.slp.isDA` y `net.slp.DAHeartBeat`, se nombran en el siguiente formato.

```
net.slp.<keyword>
```

El comportamiento del SLP es definido por el valor de una propiedad o una combinación de propiedades en el archivo `slp.conf`. Las propiedades se estructuran como pares de clave y valor en el archivo de configuración del SLP. Como se muestra en el siguiente ejemplo, un par de clave y valor consta de un nombre de propiedad y un valor de configuración asociado.

```
<property name>=<value>
```

La clave para cada propiedad es el nombre de la propiedad. El valor establece los parámetros numéricos (distancia o tiempo), de estado true/false o de valor de cadena para la propiedad. Los valores de propiedades constan de uno de los siguientes tipos de datos:

- Configuración True/False (booleana)
- Números enteros
- Lista de números enteros
- Cadenas
- Lista de cadenas

Si el valor definido no está permitido, se utiliza el valor predeterminado para dicho nombre de propiedad. Además, se registra un mensaje de error mediante syslog.

Líneas de comentario y notaciones

Puede agregar comentarios al archivo `slp.conf`, que describen la naturaleza y la función de la línea. Las líneas de comentario son opcionales en el archivo, pero pueden resultar útiles para la administración.

Nota – Los valores en el archivo de configuración no distinguen mayúsculas de minúsculas. Para obtener más información, consulte: Guttman, Erik, James Kempf, and Charles Perkins, "Service Templates and service: scheme," (Plantillas de servicio y servicio: esquema), RFC 2609 del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [http://www.ietf.org/rfc/rfc2609.txt]

▼ Cómo cambiar la configuración del SLP

Utilice este procedimiento para cambiar los valores de propiedades del archivo de configuración del SLP. El software de servicio o cliente activado para SLP también puede alterar la configuración del SLP mediante la API del SLP. Esta API está documentada en "An API for Service Location" (Una API para ubicación de servicios), RFC 2614 del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [http://www.ietf.org/rfc/rfc2614.txt]

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad de SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Edite los valores de propiedades en el archivo `/etc/inet/slp.conf` según sea necesario.**

   Consulte "Propiedades de configuración" en la página 28 para obtener información general sobre los valores de propiedades del SLP. Consulte las secciones que siguen este procedimiento para ver ejemplos de distintos escenarios en los que puede cambiar las propiedades de `slp.conf`. Consulte `slp.conf(4)`.

5. **Guarde los cambios y cierre el archivo.**

6. **Reinicie `slpd` para activar los cambios.**

   ```
   # svcadm enable network/slp
   ```

Nota – El daemon del SLP obtiene información del archivo de configuración cuando se detiene o se inicia `slpd`.

Ejemplo 3–1 Configuración de `slpd` para funcionar como servidor de DA

Puede cambiar el servidor de SA predeterminado para permitir que `slpd` funcione como un servidor de DA estableciendo la propiedad `net.slp.isDA` en `True` en el archivo `slpd.conf`.

```
net.slp.isDA=True
```

En cada área, varias propiedades controlan diferentes aspectos de la configuración. En las secciones siguientes, se describen distintos escenarios en los que puede cambiar los valores de propiedades predeterminados que se utilizan en la configuración del SLP.

Modificación de frecuencia de detección y anuncios del DA

En situaciones como las siguientes, puede modificar las propiedades que controlan el intervalo de anuncios y solicitudes de detección del DA.

- Cuando desee que el SA o UA obtengan información de la configuración del DA estáticamente de la propiedad `net.slp.DAAddresses` en el archivo `slp.conf`, puede desactivar la detección del DA.
- Cuando la red está sujeta a particiones recurrentes, puede cambiar la frecuencia de anuncios pasivos y detección activa.
- Si los clientes de UA y SA acceden a DA en el otro lado de una conexión de acceso telefónico, puede reducir la frecuencia de latidos del DA y el intervalo de detección activa para disminuir el número de veces que una línea de acceso telefónico se activa.
- Si la congestión de la red es alta, puede limitar la multidifusión.

Los procedimientos de esta sección explican cómo modificar las siguientes propiedades.

TABLA 3–2 Propiedades de solicitud de detección e intervalo de anuncios del DA

Propiedad	Descripción
`net.slp.passiveDADetection`	Valor booleano que especifica si `slpd` escucha anuncios no solicitados del DA
`net.slp.DAActiveDiscoveryInterval`	Valor que especifica con qué frecuencia `slpd` realiza la detección activa del DA para un nuevo DA
`net.slp.DAHeartBeat`	Valor que especifica con qué frecuencia un DA envía una multidifusión de un anuncio no solicitado del DA

Limitación de UA y SA a DA configurados estáticamente

Es posible que, a veces, necesite limitar los UA y SA para obtener direcciones de DA de la información de la configuración estática en el archivo `slp.conf`. En el siguiente procedimiento, puede modificar dos propiedades que hacen que `slpd` obtenga información del DA exclusivamente de la propiedad `net.slp.DAAddresses`.

▼ Cómo limitar UA y SA a DA configurados estáticamente

Utilice el siguiente procedimiento para cambiar las propiedades `net.slp.passiveDADetection` y `net.slp.DAActiveDiscoveryInterval`.

Nota – Utilice este procedimiento sólo en hosts que ejecutan UA y SA que están restringidos a configuraciones estáticas.

---

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad de SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Establezca la propiedad `net.slp.passiveDADetection` en `False` en el archivo `slp.conf` para desactivar la detección pasiva. Este valor hace que `slpd` ignore los anuncios no solicitados del DA.**

   ```
   net.slp.passiveDADetection=False
   ```

5. **Establezca `net.slp.DAActiveDiscoveryInterval` en `-1` para desactivar la detección activa inicial y periódica.**

   ```
   net.slp.DAActiveDiscoveryInterval=-1
   ```

6. **Guarde los cambios y cierre el archivo.**

7. **Reinicie `slpd` para activar los cambios.**

   ```
   # svcadm enable network/slp
   ```

Configuración de detección de DA para redes de acceso telefónico

Si los UA o SA están separados del DA por una red de acceso telefónico, puede configurar la detección de DA para reducir o eliminar el número de solicitudes de detección y anuncios del DA. Las redes de acceso telefónico, normalmente, generan un costo cuando se activan. La minimización de llamadas externas puede reducir el costo de utilizar la red de acceso telefónico.

Nota – Puede desactivar la detección de DA completamente con el método que se describe en "Limitación de UA y SA a DA configurados estáticamente" en la página 31.

▼ Cómo configurar la detección de DA para redes de acceso telefónico

Puede utilizar el siguiente procedimiento para reducir los anuncios no solicitados del DA y la detección activa mediante el aumento del período de latidos del DA y el intervalo de detección activa.

1 Conviértase en administrador.

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

2 Detenga `slpd` y toda la actividad de SLP en el host.

```
# svcadm disable network/slp
```

3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

4 Aumente la propiedad `net.slp.DAHeartbeat` en el archivo `slpd.conf`.

`net.slp.DAHeartbeat=`*value*

value Un número entero de 32 bits que establece el número de segundos para el latido de anuncio de DA pasivo

Valor predeterminado= 10.800 s (3 h)

Rango de valores= de 2000 s a 259.200.000 s

Por ejemplo, puede establecer el latido del DA en 18 h aproximadamente en un host que está ejecutando un DA:

```
net.slp.DAHeartbeat=65535
```

5 **Aumente la propiedad `net.slp.DAActiveDiscoveryInterval` en el archivo `slpd.conf`:**

```
net.slp.DAActiveDiscoveryInterval value
```

value Un número entero de 32 bits que establece el número de segundos para consultas de detección activa del DA

Valor predeterminado= 900 s (15 min)

Rango de valores= de 300 s a 10.800 s

Por ejemplo, puede establecer el intervalo de detección activa del DA en 18 h en un host que está ejecutando un UA y un SA:

```
net.slp.DAActiveDiscoveryInterval=65535
```

6 **Guarde los cambios y cierre el archivo.**

7 **Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

Configuración del latido del DA para particiones frecuentes

Los SA son necesarios para registrarse con todos los DA que admiten sus ámbitos. Un DA puede aparecer después de que `slpd` ha realizado la detección activa. Si el DA admite ámbitos `slpd`, el daemon del SLP registra todos los anuncios en su host con el DA.

Una manera en la que `slpd` detecta DA es por el anuncio no solicitado inicial que un DA envía cuando se inicia. El daemon del SLP utiliza el anuncio no solicitado periódico (el latido) para determinar si un DA aún está activo. Si el latido no aparece, el daemon elimina los DA que el daemon utiliza y los DA que el daemon ofrece a los UA.

Por último, cuando un DA sufre un cierre controlado, transmite un anuncio de DA especial que informa a los servicios de SA de escucha que estará fuera de servicio. El daemon del SLP también utiliza este anuncio para eliminar DA inactivos de la memoria caché.

Si la red está sujeta a particiones frecuentes y los SA son de larga duración, `slpd` puede eliminar DA de la memoria caché durante la partición si no se reciben anuncios de latidos. Al disminuir el tiempo de latidos, puede reducir el retraso antes de que un DA desactivado se restaure en la memoria caché después de que la partición se ha reparado.

▼ Cómo configurar latidos del DA para particiones frecuentes

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.DAHeartBeat` con el fin de reducir el período de latidos del DA.

Nota – Si la detección de DA está completamente desactivada, la propiedad `net.slp.DAAddresses` se debe establecer en `slp.conf` en los hosts que ejecutan UA y SA para que accedan al DA correcto.

---

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad de SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Reduzca el valor `net.slp.DAHeartBeat` a 1 h (3600 s). De manera predeterminada, el período de latidos del DA se establece en 3 h (10.800 s).**

   ```
   net.slp.DAHeartBeat=3600
   ```

5. **Guarde los cambios y cierre el archivo.**

6. **Reinicie `slpd` para activar los cambios.**

   ```
   # svcadm enable network/slp
   ```

Liberación de la congestión de la red

Si la congestión de la red es alta, puede limitar la cantidad de actividad de multidifusión. Si los DA aún no han sido implementados en la red, su implementación puede reducir drásticamente la cantidad de multidifusión relacionada con el SLP.

Sin embargo, incluso después de implementar los DA, la multidifusión es necesaria para la detección de DA. Puede reducir la cantidad de multidifusión necesaria para la detección de DA con el método que se describe en "Cómo configurar la detección de DA para redes de acceso telefónico" en la página 32. Puede eliminar totalmente la multidifusión para la detección de DA con el método que se describe en "Limitación de UA y SA a DA configurados estáticamente" en la página 31.

Adaptación de diferentes medios de red, topologías o configuraciones

En esta sección, se describen escenarios posibles en los que puede cambiar las siguientes propiedades para ajustar el rendimiento del SLP.

TABLA 3–3 Propiedades de rendimiento del SLP

Propiedad	Descripción
`net.slp.DAAttributes`	El intervalo de actualización mínimo que un DA acepta para los anuncios.
`net.slp.multicastTTL`	El valor *time-to-live* especificado para los paquetes de multidifusión.
`net.slp.MTU`	El tamaño en bytes establecido para los paquetes de red. El tamaño incluye encabezados IP y TCP o UDP.
`net.slp.isBroadcastOnly`	El valor booleano que se establece para indicar si la difusión se debe utilizar para la detección de servicios basada en DA y no basada en DA.

Reducción de reregistros de SA

Los SA necesitan actualizar periódicamente los anuncios de servicios antes de caducar. Si un DA maneja una carga extremadamente pesada de muchos UA y SA, las actualizaciones frecuentes pueden provocar que el DA se sobrecargue. Si el DA se sobrecarga, las solicitudes del UA comienzan a agotar el tiempo de espera y, luego, se eliminan. Hay muchas causas posibles por las que las solicitudes de UA pueden agotar su tiempo de espera. Antes de asumir que la sobrecarga del DA es el problema, utilice un rastreo de `snoop` para comprobar la duración de los anuncios de servicios que se han registrado con un registro de servicio. Si las duraciones son cortas y los reregistros se producen con frecuencia, los tiempos de espera agotados, probablemente, sean el resultado de reregistros frecuentes.

Nota – Un registro de servicio es un *reregistro* si el indicador FRESH no está definido. Consulte el Capítulo 5, “SLP (referencia)” para obtener más información sobre los mensajes de registro de servicios.

▼ Cómo reducir reregistros de SA

Utilice el siguiente procedimiento para aumentar el intervalo de actualización mínimo de los SA y reducir los reregistros.

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad de SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Aumente el valor del atributo `min-refresh-interval` de la propiedad `net.slp.DAAttributes`.**

   El período de reregistro mínimo predeterminado es cero. El valor predeterminado de cero permite que los SA se vuelvan a registrar en cualquier punto. En el siguiente ejemplo, el intervalo se aumenta a 3600 s (1 h).

   ```
   net.slp.DAAttributes(min-refresh-interval=3600)
   ```

5. **Guarde los cambios y cierre el archivo.**

6. **Reinicie `slpd` para activar los cambios.**

   ```
   # svcadm enable network/slp
   ```

Configuración de la propiedad Time-to-Live de multidifusión

La propiedad time–to-live de multidifusión (`net.slp.multicastTTL`) determina el rango en el que un paquete de multidifusión se propaga en la intranet. La propiedad TTL de multidifusión se configura estableciendo la propiedad `net.slp.multicastTTL` en un número entero entre 1 y 255. El valor predeterminado de la propiedad TTL de multidifusión es de 255, lo que significa que, en teoría, el enrutamiento de paquetes no está restringido. Sin embargo, una TTL de 255 hace que un paquete de multidifusión penetre la intranet hasta los enrutadores de límite en el borde del dominio administrativo. Se necesita una configuración correcta de multidifusión en los enrutadores de límite para evitar que los paquetes de multidifusión se filtren en la red principal de multidifusión de Internet o en su ISP.

El ámbito de la TTL de multidifusión es similar a la TTL de IP estándar, con la excepción de que se realiza una comparación de TTL. A cada interfaz en un enrutador activado para multidifusión se le asigna un valor TTL. Cuando llega un paquete de multidifusión, el enrutador compara la TTL del paquete con la TTL de la interfaz. Si la TTL del paquete es mayor o igual que la TTL de la interfaz, la TTL del paquete se reduce en uno, al igual que con la TTL de IP estándar. Si la TTL pasa a cero, el paquete se descarta. Al utilizar el ámbito TTL para la multidifusión del SLP, los enrutadores deben estar correctamente configurados para limitar los paquetes a una determinada subsección de la intranet.

▼ Cómo configurar la propiedad Time-to-Live de multidifusión

Utilice el siguiente procedimiento para restablecer la propiedad `net.slp.multicastTTL`.

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad de SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Cambie la propiedad `net.slp.multicastTTL` en el archivo `slpd.conf`:**

   `net.slp.multicastTTL=`*value*

   value Un número entero positivo menor o igual que 255 que define la TTL de multidifusión

   Nota – Puede reducir el rango de propagación de multidifusión reduciendo el valor TTL. Si el valor TTL es 1, el paquete está restringido a la subred. Si el valor es 32, el paquete está restringido al sitio. Lamentablemente, el término *sitio* no es definido por la RFC 1075, donde se tratan las TTL de multidifusión. Los valores superiores a 32 hacen referencia al enrutamiento teórico en Internet y no deben utilizarse. Los valores inferiores a 32 se pueden utilizar para restringir la multidifusión a un conjunto de subredes accesibles si los enrutadores están correctamente configurados con TTL.

5. **Guarde los cambios y cierre el archivo.**

6. **Reinicie `slpd` para activar los cambios.**

   ```
   # svcadm enable network/slp
   ```

Configuración del tamaño de paquete

El tamaño de paquete predeterminado para el SLP es 1400 bytes. El tamaño debe ser suficiente para la mayoría de las redes de área local. Para redes inalámbricas o redes de área extensa, puede reducir el tamaño de paquete para evitar la fragmentación de mensajes y disminuir el tráfico en la red. Para redes de área local que tienen paquetes más grandes, el aumento del tamaño de paquete puede mejorar el rendimiento. Puede determinar si el tamaño de paquete se tiene que

reducir al comprobar el tamaño de paquete mínimo para su red. Si el medio de red tiene un tamaño de paquete más pequeño, puede reducir el valor `net.slp.MTU` en consecuencia.

Puede aumentar el tamaño de paquete si el medio de red tiene paquetes más grandes. Sin embargo, a menos que los anuncios de servicios de SA o las consultas de UA desborden con frecuencia el tamaño de paquete predeterminado, no debe tener que cambiar el valor `net.slp.MTU`. Puede utilizar `snoop` para determinar si las solicitudes de UA desbordan con frecuencia el tamaño de paquete predeterminado y se vuelven a implementar para utilizar TCP en lugar de UDP.

La propiedad `net.slp.MTU` mide el tamaño de paquete de IP completo, incluidos el encabezado de capa de enlace, el encabezado IP, el encabezado UDP o TCP, y el mensaje SLP.

▼ Cómo configurar el tamaño de paquete

Utilice el siguiente procedimiento para cambiar el tamaño de paquete predeterminado ajustando la propiedad `net.slp.MTU`.

1 Conviértase en administrador.

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

2 Detenga `slpd` y toda la actividad de SLP en el host.

```
# svcadm disable network/slp
```

3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

4 Cambie la propiedad `net.slp.MTU` en el archivo `slpd.conf`:

`net.slp.MTU=`*value*

value Un número entero de 16 bits que especifica en bytes el tamaño de paquete de red

Valor predeterminado= 1400

Rango de valores= de 128 a 8192

5 Guarde los cambios y cierre el archivo.

6 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

Configuración de enrutamiento de sólo difusión

SLP está diseñado para utilizar la multidifusión para la detección de servicios en la ausencia de DA y para la detección de DA. Si la red no implementa el enrutamiento de multidifusión, puede configurar el SLP para utilizar la difusión estableciendo la propiedad `net.slp.isBroadcastOnly` en `True`.

A diferencia de la multidifusión, los paquetes de difusión no se propagan por subredes de manera predeterminada. Por este motivo, la detección de servicios sin DA en una red que no es de multidifusión funciona sólo en una única subred. Además, se deben tener en cuenta consideraciones especiales al implementar DA y ámbitos en las redes en las que se utiliza la difusión. Un DA en un host múltiple puede unir la detección de servicios entre varias subredes con la multidifusión desactivada. Consulte "Asignación de nombre de ámbito y colocación de DA" en la página 55 para obtener más información sobre cómo implementar DA en hosts múltiples.

▼ Cómo configurar el enrutamiento de sólo difusión

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.isBroadcastOnly` a `True`.

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad de SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Cambie la propiedad `net.slp.isBroadcastOnly` en el archivo `slpd.conf` a `True`:**

   ```
   net.slp.isBroadcastOnly=True
   ```

5. **Guarde los cambios y cierre el archivo.**

6. **Reinicie `slpd` para activar los cambios.**

   ```
   # svcadm enable network/slp
   ```

Modificación de tiempos de espera en solicitudes de detección de SLP

Es posible que dos situaciones requieran la modificación de los tiempos de espera para solicitudes de detección de SLP:

- Si los agentes del SLP están separados por varias subredes, líneas de acceso telefónico u otras WAN, la latencia de red puede ser lo suficientemente alta como para que los tiempos de espera predeterminados sean insuficientes para que una solicitud o un registro se completen. Por el contrario, si la red tiene una latencia baja, puede mejorar el rendimiento disminuyendo los tiempos de espera.
- Si la red está sujeta a un gran volumen de tráfico o a tasas altas de colisión, el período máximo que los SA y UA tienen que esperar antes de enviar un mensaje podría ser insuficiente para garantizar transacciones sin colisión.

Cambio de tiempos de espera predeterminados

La latencia alta de red puede provocar que los UA y SA agoten el tiempo de espera antes de que se devuelva una respuesta para solicitudes y registros. La latencia puede ser un problema si un UA está separado de un SA o si ambos, un UA y un SA, están separados de un DA por varias subredes, una línea de acceso telefónico o una WAN. Puede determinar si la latencia es un problema al comprobar si las solicitudes del SLP fallan debido a tiempos de espera en solicitudes y registros de UA y SA. También puede utilizar el comando `ping` para medir la latencia real.

En la siguiente tabla, se muestran las propiedades de configuración que controlan los tiempos de espera. Puede utilizar los procedimientos de esta sección para modificar estas propiedades.

TABLA 3–4 Propiedades de tiempo de espera

Propiedad	Descripción

`net.slp.multicastTimeouts`
`net.slp.DADiscoveryTimeouts`
`net.slp.datagramTimeouts`
	Las propiedades que controlan los tiempos de espera para transmisiones de mensajes UDP de unidifusión y multidifusión antes de que la transmisión se abandone.

`net.slp.multicastMaximumWait`	La propiedad que controla la cantidad máxima de tiempo que un mensaje de multidifusión se transmite antes de ser abandonado.

TABLA 3–4 Propiedades de tiempo de espera *(Continuación)*

Propiedad	Descripción
`net.slp.datagramTimeouts`	El límite superior de un tiempo de espera de DA que está especificado por la suma de los valores que se muestran para esta propiedad. Un datagrama UDP se envía repetidamente a un DA hasta que se recibe una respuesta o hasta que se alcanza el límite de tiempo de espera.

Si los tiempos de espera se agotan con frecuencia durante la detección de servicios de multidifusión o la detección de DA, aumente la propiedad `net.slp.multicastMaximumWait` del valor predeterminado de 15.000 ms (15 s). Al aumentar el período máximo de espera se genera más tiempo para que las solicitudes en redes de latencia alta se completen. Después de cambiar `net.slp.multicastMaximumWait`, también debe modificar `net.slp.multicastTimeouts` y `net.slp.multicastTimeouts`. La suma de los valores de tiempo de espera para estas propiedades es igual al valor `net.slp.multicastMaximumWait`.

▼ Cómo cambiar tiempos de espera predeterminados

Utilice el siguiente procedimiento para cambiar las propiedades del SLP que controlan los tiempos de espera.

1 Conviértase en administrador.

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

2 Detenga `slpd` y toda la actividad de SLP en el host.

```
# svcadm disable network/slp
```

3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

4 Cambie la propiedad `net.slp.multicastMaximumWait` en el archivo `slpd.conf`:

`net.slp.multicastMaximumWait=`*value*

value Un número entero de 32 bits que muestra la suma de los valores que se establecen para `net.slp.multicastTimeouts` y `net.slp.DADiscoveryTimeouts`

Valor predeterminado= 15.000 ms (15 s)

Rango de valores= de 1000 ms a 60.000 ms

Por ejemplo, si determina que las solicitudes de multidifusión requieren 20 s (20.000 ms), debe ajustar a 20.000 ms los valores enumerados para las propiedades `net.slp.multicastTimeouts` y `net.slp.DADiscoveryTimeouts`.

```
net.slp.multicastMaximumWait=20000
net.slp.multicastTimeouts=2000,5000,6000,7000
net.slp.DADiscoveryTimeouts=3000,3000,6000,8000
```

5 Si es necesario, cambie la propiedad `net.slp.datagramTimeouts` en el archivo `slpd.conf`:

`net.slp.datagramTimeouts=`*value*

value Una lista de números enteros de 32 bits que especifican tiempos de espera, en milisegundos, para implementar la transmisión de datagramas de unidifusión en DA

Valor predeterminado= 3000, 3000, 3000

Por ejemplo, puede aumentar el tiempo de espera de datagramas a 20.000 ms para evitar que los tiempos de espera se agoten con frecuencia.

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

En redes de alto rendimiento, puede reducir el límite de tiempo de espera para la transmisión de datagramas UDP de unidifusión y multidifusión. Al reducir el límite de tiempo de espera, disminuye la latencia que es necesaria para cumplir las solicitudes del SLP.

6 Guarde los cambios y cierre el archivo.

7 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

Configuración del límite de espera aleatoria

En redes con un gran volumen de tráfico o una tasa alta de colisión, la comunicación con un DA puede resultar afectada. Cuando las tasas de colisión son altas, el agente de envío debe retransmitir el datagrama UDP. Puede determinar si la retransmisión se está produciendo mediante `snoop` para supervisar el tráfico de una red de hosts que están ejecutando `slpd` como un servidor de SA y un host que está ejecutando `slpd` como un DA. Si varios mensajes de registro de servicios para el mismo servicio aparecen en el rastreo de `snoop` del host que está ejecutando `slpd` como servidor de SA, es posible que haya notado colisiones.

Las colisiones pueden ser especialmente preocupantes en el momento del inicio. Cuando un DA se inicia por primera vez, envía anuncios no solicitados, y los SA responden con registros. El SLP requiere que los SA esperen durante una cantidad de tiempo aleatoria tras recibir un anuncio del DA antes de responder. El límite de espera aleatoria se distribuye de manera

uniforme con un valor máximo que está controlado por `net.slp.randomWaitBound`. El límite de espera aleatoria predeterminado es 1000 ms (1 s).

Cómo configurar el límite de espera aleatoria

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.RandomWaitBound` en el archivo `slp.conf`.

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad de SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Cambie la propiedad `net.slp.RandomWaitBound` en el archivo `slpd.conf`:**

   `net.slp.RandomWaitBound=`*value*

   value El límite superior para calcular el tiempo de espera aleatoria antes de intentar ponerse en contacto con un DA

   Valor predeterminado= 1000 ms (1 s)

   Rango de valores= de 1000 ms a 3000 ms

   Por ejemplo, puede alargar el tiempo máximo de espera a 2000 ms (2 s).

   ```
   net.slp.randomWaitBound=2000
   ```

   Cuando alarga el límite de espera aleatoria, ocurre un retraso más prolongado en el registro. Los SA pueden completar los registros con DA recién detectados más lentamente para evitar colisiones y tiempos de espera agotados.

5. **Si es necesario, cambie la propiedad `net.slp.datagramTimeouts` en el archivo `slpd.conf`:**

   `net.slp.datgramTimeouts=`*value*

   value Una lista de números enteros de 32 bits que especifican tiempos de espera, en milisegundos, para implementar la transmisión de datagramas de unidifusión en DA

   Valor predeterminado= 3000, 3000, 3000

Por ejemplo, puede aumentar el tiempo de espera de datagramas a 20.000 ms para evitar que los tiempos de espera se agoten con frecuencia.

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

En redes de alto rendimiento, puede reducir el límite de tiempo de espera para la transmisión de datagramas UDP de unidifusión y multidifusión. Este valor reduce la cantidad de latencia al cumplir solicitudes SLP.

6 **Guarde los cambios y cierre el archivo.**

7 **Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

Implementación de ámbitos

Con ámbitos, puede proporcionar servicios que dependen de agrupaciones lógicas, físicas y administrativas de usuarios. Puede utilizar ámbitos para administrar el acceso a anuncios de servicios.

Utilice la propiedad `net.slp.useScopes` para crear ámbitos. Por ejemplo, en el archivo `/etc/inet/slp.conf` en un host, agregue un nuevo ámbito, denominado `newscope`, tal como se muestra:

```
net.slp.useScopes=newscope
```

Es posible que su organización, por ejemplo, tenga un sector de dispositivos conectados en red, como impresoras y faxes, al final de la sala sur, en el segundo piso del edificio 6. Esos dispositivos podrían ser utilizados por todas las personas del segundo piso, o usted podría restringir el uso para los miembros de un departamento determinado. Los ámbitos ofrecen una manera de otorgar acceso a los anuncios de servicios de esos equipos.

Si los dispositivos están dedicados a un solo departamento, puede crear un ámbito con el nombre del departamento, por ejemplo, `mktg`. Los dispositivos que pertenecen a otros departamentos se pueden configurar con nombres de ámbitos diferentes.

En otra situación, los departamentos podrían estar separados. Por ejemplo, los departamentos de ingeniería mecánica y CAD/CAM podrían estar divididos entre los pisos 1 y 2. Sin embargo, puede proporcionar los equipos del piso 2 para los hosts en ambos pisos asignándolos al mismo ámbito. Puede implementar los ámbitos de cualquier manera que funcione bien con su red y sus usuarios.

Nota – Los UA que tienen un ámbito particular no tienen prohibido utilizar los servicios que están anunciados en otros ámbitos. La configuración de ámbitos controla sólo qué anuncios de servicios detecta un UA. El servicio es responsable de aplicar cualquier restricción de control de acceso.

Cuándo configurar ámbitos

El SLP puede funcionar adecuadamente sin la configuración de ningún ámbito. En el entorno operativo de Oracle Solaris, el ámbito predeterminado para SLP es `default`. Si no se configuran ámbitos, `default` es el ámbito de todos los mensajes del SLP.

Puede configurar ámbitos en cualquiera de las siguientes circunstancias.

- Las organizaciones que respalda desean restringir el acceso a los anuncios de servicios para sus propios miembros.
- La distribución física de la organización sugiere que los servicios en una determinada área pueden ser utilizados por usuarios concretos.
- Los anuncios de servicios que son adecuados para usuarios específicos deben ser particionados.

Un ejemplo de la primera circunstancia fue citado en "Configuración de detección de DA para redes de acceso telefónico" en la página 32. Un ejemplo de la segunda circunstancia es una situación en la que una organización está dividida entre dos edificios, y usted desea que los usuarios de un edificio accedan a los servicios locales de dicho edificio. Puede configurar a los usuarios en el edificio 1 con el ámbito `B1` y configurar a los usuarios en el edificio 2 con el ámbito `B2`.

Consideraciones al configurar ámbitos

Cuando modifica la propiedad `net.slp.useScopes` en el archivo `slpd.conf`, configura ámbitos para todos los agentes en el host. Si el host está ejecutando algún SA o está actuando como un DA, debe configurar esta propiedad si desea configurar el SA o DA en ámbitos que no sean `default`. Si sólo UA se están ejecutando en el equipo, y los UA deben detectar SA y DA que admiten ámbitos que no sean `default`, no es necesario configurar la propiedad, a menos que desee restringir los ámbitos que los UA utilizan. Si la propiedad no está configurada, los UA pueden detectar automáticamente DA y ámbitos disponibles mediante `slpd`. El daemon del SLP utiliza la detección activa y pasiva de DA para encontrar DA, o utiliza la detección de SA si no hay DA en ejecución. Como alternativa, si la propiedad está configurada, los UA usan sólo los ámbitos configurados y no los descartan.

Si decide configurar ámbitos, debe considerar mantener el ámbito `default` en la lista de ámbitos configurados, a menos que esté seguro de que todos los SA de la red tienen ámbitos configurados. Si algunos SA se dejan sin configurar, los UA con ámbitos configurados no los pueden encontrar. Esta situación se produce porque los SA no configurados tienen automáticamente el ámbito `default`, pero los UA tienen los ámbitos configurados.

Si también decide configurar DA estableciendo la propiedad `net.slp.DAAddresses`, asegúrese de que los ámbitos admitidos por los DA configurados sean los mismos que los ámbitos que ha configurado con la propiedad `net.slp.useScopes`. Si los ámbitos son diferentes, `slpd` imprime un mensaje de error cuando se reinicia.

▼ Cómo configurar ámbitos

Utilice el siguiente procedimiento para agregar nombres de ámbitos a la propiedad `net.slp.useScopes` en el archivo `slp.conf`.

1 Conviértase en administrador.

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

2 Detenga `slpd` y toda la actividad de SLP en el host.

```
# svcadm disable network/slp
```

3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

4 Cambie la propiedad `net.slp.useScopes` en el archivo `slpd.conf`:

`net.slp.useScopes=`<*scope names*>

scope names Una lista de cadenas que indican qué ámbitos un DA o SA está autorizado a utilizar al realizar solicitudes o qué ámbitos un DA debe admitir

Valor predeterminado= valor predeterminado para SA y DA/sin asignar para UA

Nota –

Utilice lo siguiente para construir nombres de ámbitos:

- Cualquier carácter alfanumérico, mayúscula o minúscula
- Cualquier carácter de puntuación (excepto: ", \, !, <, =, > y ~)
- Espacios que se consideran parte del nombre

- Caracteres que no son ASCII

  Utilice una barra diagonal inversa para caracteres de escape que no son ASCII. Por ejemplo, la codificación UTF-8 utiliza el código hexadecimal `0xc3a9` para representar la letra *e* con el acento *agudo* francés. Si la plataforma no admite UTF-8, utilice el código hexadecimal UTF-8 como la secuencia de escape `\c3\a9`.

Por ejemplo, para especificar ámbitos para grupos `eng` y `mktg` en `bldg6`, cambie la línea `net.slp.useScopes` a lo siguiente.

```
net.slp.useScopes=eng,mktg,bldg6
```

5 **Guarde los cambios y cierre el archivo.**

6 **Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

Implementación de DA

En esta sección, se describe la implementación estratégica de DA en una red que está ejecutando el SLP.

El SLP funciona adecuadamente sólo con los agentes base (UA y SA) y sin DA implementados ni ámbitos configurados. Todos los agentes que carecen de configuraciones específicas utilizan el ámbito `default`. Los DA funcionan como memorias caché para los anuncios de servicios. La implementación de DA reduce el número de mensajes que se envían en la red y reduce el tiempo que es necesario para recibir respuestas a mensajes. Esta capacidad permite al SLP alojar redes de mayor tamaño.

¿Por qué implementar un DA de SLP?

El motivo principal para implementar DA es reducir la cantidad de tráfico de multidifusión y los retrasos que están asociados con la recopilación de respuestas de unidifusión. En una red grande con muchos UA y SA, la cantidad de tráfico de multidifusión que participa en la detección de servicios puede volverse tan grande que el rendimiento de la red disminuye. Mediante la implementación de uno o más DA, los UA deben enviar una unidifusión a los DA para servicios, y los SA deben registrarse con los DA mediante la unidifusión. La única multidifusión registrada con SLP en una red con DA es para la detección activa y pasiva de DA.

Los SA se registran automáticamente con cualquier DA que detectan dentro de un conjunto de ámbitos comunes, en lugar de aceptar solicitudes de servicio de multidifusión. No obstante, el SA aún responde directamente solicitudes de multidifusión en ámbitos que no son admitidos por el DA.

Las solicitudes de servicio de UA se envían por unidifusión a los DA en lugar de enviarse por multidifusión en la red cuando un DA se implementa dentro de los ámbitos del UA. Por lo tanto, los DA dentro de los ámbitos del UA reducen la multidifusión. Al eliminar la multidifusión para solicitudes de UA comunes, el tiempo que se necesita para obtener respuestas a las preguntas se reduce en gran medida (de segundos a milisegundos).

Los DA actúan como un punto focal para la actividad de SA y UA. La implementación de uno o varios DA para una colección de ámbitos proporciona un punto centralizado para supervisar la actividad del SLP. Es más sencillo supervisar los registros y las solicitudes activando el registro de DA que comprobando los registros de varios SA que están distribuidos por toda la red. Puede implementar cualquier número de DA para un determinado ámbito o para varios ámbitos, según la necesidad de equilibrar la carga.

En redes que no tienen el enrutamiento de multidifusión activado, puede configurar el SLP para utilizar la difusión. Sin embargo, la difusión es muy ineficaz, porque necesita que cada host procese el mensaje. Además, la difusión, por lo general, no se propaga entre enrutadores. Como resultado, en una red sin enrutamiento de multidifusión, los servicios se pueden detectar sólo en la misma subred. Si el enrutamiento de multidifusión se admite parcialmente, se genera una capacidad inconsistente para detectar servicios en una red. Los mensajes de multidifusión se utilizan para detectar DA. La compatibilidad parcial con el enrutamiento de multidifusión, por lo tanto, implica que los UA y SA registran servicios con todos los DA conocidos en el ámbito del SA. Por ejemplo, si un UA consulta a un DA denominado `DA1`, y el SA ha registrado servicios con `DA2`, el UA no podrá detectar un servicio. Consulte "Configuración de enrutamiento de sólo difusión" en la página 39 para obtener más información sobre cómo implementar el SLP en redes que no tienen la multidifusión activada.

En una red con compatibilidad inconsistente de todo el sitio para el enrutamiento de multidifusión, debe configurar los UA y SA del SLP con una lista consistente de ubicaciones de DA mediante la propiedad `net.slp.DAAdresseses`.

Por último, el DA de SLPv2 admite la interoperabilidad con SLPv1. La interoperabilidad con SLPv1 está activada de manera predeterminada en el DA. Si la red contiene dispositivos SLPv1, como las impresoras, o si es necesario interoperar con Novell Netware 5, que utiliza SLPv1 para la detección de servicios, debe implementar un DA. Sin un DA, los UA del SLP de Oracle Solaris no pueden encontrar servicios anunciados de SLPv1.

Cuándo implementar DA

Implemente DA en su empresa si se cumple alguna de las siguientes condiciones:

- El tráfico SLP de multidifusión se excede en un 1 % del ancho de banda de la red, medido por `snoop`.
- Los clientes de UA experimentan retrasos o tiempos de espera largos durante las solicitudes de servicio de multidifusión.
- Desea centralizar la supervisión de anuncios de servicios de SLP para ámbitos particulares en uno o varios hosts.
- La red no tiene la multidifusión activada y se compone de varias subredes que deben compartir servicios.
- La red emplea dispositivos que admiten las versiones anteriores de SLP (SLPv1), o usted desea que la detección de servicios del SLP interopere con Novell Netware 5.

▼ Cómo implementar DA

Utilice el siguiente procedimiento para establecer la propiedad `net.slp.isDA` en `True`, en el archivo `slp.conf`.

Nota – Sólo puede asignar un DA por host.

---

1. **Conviértase en administrador.**

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

2. **Detenga `slpd` y toda la actividad del SLP en el host.**

   ```
   # svcadm disable network/slp
   ```

3. **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

4. **Establezca la propiedad `net.slp.isDA` del archivo `slpd.conf` en `True`:**

   ```
   net.slp.isDA=True
   ```

5. **Guarde los cambios y cierre el archivo.**

6. **Reinicie `slpd` para activar los cambios.**

   ```
   # svcadm enable network/slp
   ```

Dónde colocar DA

En esta sección, se proporcionan sugerencias acerca de dónde colocar DA en diferentes situaciones.

- Cuando el enrutamiento de multidifusión no está activado y los DA son necesarios para unir la detección de servicios entre subredes

  En esta situación, un DA debe colocarse en un host con interfaces y todas las subredes que comparten servicios. La propiedad de configuración `net.slp.interfaces` *no* se debe establecer, a menos que los paquetes IP no se enruten entre las interfaces. Consulte "Configuración de la función de hosts múltiples para SLP" en la página 51 para obtener más información sobre cómo configurar la propiedad `net.slp.interfaces`.
- Cuando se implementan DA para escalabilidad y la consideración principal es la optimización del acceso de agentes

  Los UA, normalmente, realizan muchas solicitudes de servicios a los DA. Un SA se registra con el DA una vez y puede actualizar el anuncio en intervalos periódicos, pero con poca frecuencia. Como resultado, el acceso de UA a DA es mucho más frecuente que el acceso de SA. El número de anuncios de servicios también suele ser menor que el número de solicitudes. Por lo tanto, la mayoría de las implementaciones de DA son más eficaces si la implementación se optimiza para el acceso de UA.
- Colocación de los DA de manera que estén topológicamente cerca de los UA en la red para optimizar el acceso de los UA

  Naturalmente, debe configurar el DA con un ámbito que sea compartido por los clientes de UA y SA.

Colocación de varios DA para el equilibrio de carga

Puede implementar varios DA para el mismo conjunto de ámbitos como una manera de equilibrio de carga. Implemente los DA en cualquiera de las siguientes circunstancias:

- Las solicitudes de UA a un DA están agotando el tiempo de espera o se están devolviendo con el error `DA_BUSY_NOW`.
- El registro de DA muestra que muchas solicitudes del SLP se están perdiendo.
- La red de los usuarios que comparten servicios en los ámbitos abarca un número de edificios o sitios físicos.

Puede ejecutar un rastreo de `snoop` de tráfico del SLP para determinar cuántas solicitudes de UA regresan con el error `DA_BUSY_NOW`. Si el número de solicitudes de UA devuelto es alto, los UA en los edificios que se encuentran física y topológicamente alejados del DA pueden presentar respuestas lentas o tiempos de espera excesivos. En este escenario, se puede implementar un DA en cada edificio para mejorar la respuesta para los clientes de UA dentro del edificio.

Los enlaces que conectan edificios son, por lo general, más lentos que las redes de área local dentro de los edificios. Si la red abarca varios edificios o sitios físicos, establezca la propiedad `net.slp.DAAddresses` en el archivo `/etc/inet/slp.conf` para una lista de direcciones o nombres de host específicos para que los UA sólo accedan a los DA que especifique.

Si un DA determinado está utilizando grandes cantidades de memoria de host para los registros de servicios, reduzca el número de registros de SA disminuyendo el número de ámbitos que el DA admite. Puede dividir en dos un ámbito que tiene muchos registros. Puede admitir uno de los nuevos ámbitos mediante la implementación de otro DA en otro host.

SLP y función de hosts múltiples

Un servidor de hosts múltiples actúa como un host en varias subredes IP. El servidor puede, a veces, tener más de una tarjeta de interfaz de red y puede actuar como enrutador. Los paquetes IP, incluidos los paquetes de multidifusión, se enrutan entre las interfaces. En algunas situaciones, el enrutamiento entre interfaces está desactivado. En las secciones siguientes, se describe cómo configurar el SLP para esas situaciones.

Configuración de la función de hosts múltiples para SLP

Sin configuración, el `slpd` escucha la multidifusión y la unidifusión UDP/TCP en la interfaz de red predeterminada. Si el enrutamiento de unidifusión y multidifusión está activado entre las interfaces de un equipo de hosts múltiples, no se necesita ninguna configuración adicional. Esto se debe a que los paquetes de multidifusión que llegan a otra interfaz se enrutan correctamente a la interfaz predeterminada. Como resultado, las solicitudes de multidifusión para DA u otros anuncios de servicios llegan a `slpd`. Si el enrutamiento no está activado por algún motivo, es necesario realizar la configuración.

Cuándo realizar la configuración para múltiples interfaces de red no enrutadas

Si existe una de las condiciones siguientes, quizá deba configurar equipos de hosts múltiples.

- El enrutamiento de unidifusión está activado entre las interfaces y el enrutamiento de multidifusión está desactivado.
- El enrutamiento de unidifusión y el enrutamiento de multidifusión están desactivados entre las interfaces.

Cuando el enrutamiento de multidifusión está desactivado entre interfaces, normalmente, se debe a que la multidifusión no ha sido implementada en la red. En tal situación, la difusión se usa, por lo general, para la detección de servicios que no se basa en DA y para la detección de DA en las subredes individuales. La difusión se configura estableciendo la propiedad `net.slp.isBroadcastOnly` en `True`.

Configuración de múltiples interfaces de red no enrutadas (mapa de tareas)

TABLA 3–5 Configuración de múltiples interfaces de red no enrutadas

Tarea	Descripción	Para obtener instrucciones
Configurar la propiedad `net.slp.interfaces`	Establezca esta propiedad para que `slpd` escuche solicitudes del SLP de unidifusión y multidifusión/difusión en las interfaces especificadas.	"Configuración de la propiedad `net.slp.interfaces`" en la página 52
Organizar anuncios de servicios de proxy de modo que los UA en subredes obtengan direcciones URL de servicio con direcciones accesibles	Restrinja anuncios de proxy a un equipo que está ejecutando `slpd` conectado a una única subred en lugar de un host múltiple.	"Anuncios de proxy y hosts múltiples" en la página 54
Colocar DA y configurar ámbitos para garantizar la accesibilidad entre UA y SA	Configure la propiedad `net.slp.interfaces` en hosts múltiples con una dirección o un nombre de host de interfaz único. Ejecute un DA en un host múltiple, pero configure ámbitos para que los SA y UA de cada subred utilicen hosts diferentes.	"Asignación de nombre de ámbito y colocación de DA" en la página 55

Configuración de la propiedad net.slp.interfaces

Si la propiedad `net.slp.interfaces` está establecida, `slpd` escucha solicitudes del SLP de unidifusión y multidifusión/difusión en las interfaces que aparecen en la propiedad, en lugar de la interfaz predeterminada.

Por lo general, establece la propiedad `net.slp.interfaces` junto con la activación de la difusión estableciendo la propiedad `net.slp.isBroadcastOnly`, porque la multidifusión no se ha implementado en la red. Sin embargo, si la multidifusión se ha implementado, pero no se enruta en este host múltiple particular, una solicitud de multidifusión puede llegar a `slpd` de más de una interfaz. Esta situación se puede producir cuando el enrutamiento de paquetes es manejado por otro host múltiple o enrutador que conecta las subredes que son servidas por las interfaces.

Cuando tal situación se produce, el servidor de SA o el UA que envía la solicitud recibe dos respuestas de `slpd` en el host múltiple. Las respuestas se filtran por las bibliotecas del cliente, y el cliente no las ve. Sin embargo, las respuestas están visibles en el rastreo de `snoop`.

Nota –

Si el enrutamiento de unidifusión está desactivado, es posible que no se pueda acceder a los servicios anunciados por clientes de SA en hosts múltiples desde todas las subredes. Si no se puede acceder a los servicios, los clientes de SA pueden realizar lo siguiente:

- Anunciar una URL de servicio para cada subred.
- Garantizar que las solicitudes de una subred particular se respondan con una URL accesible.

La biblioteca del cliente de SA no hace nada para garantizar que las direcciones URL accesibles se anuncien. El programa de servicio, que puede o no manejar un host múltiple sin ningún enrutamiento, es responsable de asegurar que las direcciones URL accesibles sean anunciadas.

Antes de desplegar un servicio en un host múltiple con enrutamiento de unidifusión desactivado, use `snoop` para determinar si el servicio maneja las solicitudes de varias subredes correctamente. Además, si tiene previsto implementar un DA en el host múltiple, consulte "Asignación de nombre de ámbito y colocación de DA" en la página 55.

▼ Cómo configurar la propiedad net.slp.interfaces

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.interfaces` en el archivo `slp.conf`.

1 Conviértase en administrador.

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

2 Detenga `slpd` y toda la actividad de SLP en el host.

```
# svcadm disable network/slp
```

3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

4 Cambie la propiedad `net.slp.interfaces` en el archivo `slpd.conf`:

`net.slp.interfaces=`*value*

value Lista de direcciones IPv4 o nombres de host de las tarjetas de interfaz de red en las que el DA o SA deben escuchar mensajes TCP, UDP de unidifusión y multidifusión en el puerto 427

Por ejemplo, un servidor con tres tarjetas de red y enrutamiento de multidifusión desactivado está conectado a tres subredes. Las direcciones IP de las tres interfaces de red son `192.147.142.42`, `192.147.143.42` y `192.147.144.42`. La máscara de subred es `255.255.255.0`. El siguiente valor de propiedad hace que `slpd` escuche en las tres interfaces mensajes de unidifusión y multidifusión/difusión:

```
net.slp.interfaces=192.147.142.42,192.147.143.42,192.147.144.42
```

Nota – Puede especificar direcciones IP o nombres de host que se pueden resolver para la propiedad `net.slp.interfaces`.

5 **Guarde los cambios y cierre el archivo.**

6 **Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

Anuncios de proxy y hosts múltiples

Si un host con varias interfaces anuncia servicios mediante `slpd` y registro de proxy, las direcciones URL de servicio anunciadas por `slpd` deben contener direcciones o nombres de host accesibles. Si el enrutamiento de unidifusión está activado entre las interfaces, los hosts en todas las subredes pueden acceder a los hosts de otras subredes. Los registros de proxy también se pueden realizar para un servicio en cualquier subred. Sin embargo, si el enrutamiento de unidifusión está desactivado, los clientes de servicio en una subred no pueden acceder a servicios en otra subred por medio del host múltiple. Es posible, no obstante, que dichos clientes puedan acceder a los servicios mediante otro enrutador.

Por ejemplo, suponga que el host con el nombre de host predeterminado `bigguy` tiene tres tarjetas de interfaz en tres subredes enrutadas diferentes. Los nombres de host en estas subredes son `bigguy`, con dirección IP `192.147.142.42`, `bigguy1`, con dirección IP `192.147.143.42` y `bigguy2`, con dirección IP `192.147.144.42`. Ahora, suponga que una impresora antigua, `oldprinter`, está conectada a la subred `143` y que la dirección URL `service:printing:lpr://oldprinter/queue1` está configurada con `net.slp.interfaces` para escuchar en todas las interfaces. La URL `oldprinter` tiene anuncios de proxy en todas las interfaces. Los equipos de las subredes `142` y `144` reciben la dirección URL en respuesta a solicitudes de servicio, pero no pueden acceder al servicio `oldprinter`.

La solución a este problema es realizar los anuncios de proxy con `slpd` ejecutándose en un equipo que está conectado sólo a la subred `143`, en lugar de en el host múltiple. Sólo los hosts de la subred `143` pueden obtener el anuncio en respuesta a una solicitud de servicio.

Asignación de nombre de ámbito y colocación de DA

La colocación de DA y la asignación de nombres de ámbito en una red con un host múltiple se deben realizar cuidadosamente para garantizar que los clientes obtengan servicios accesibles. Sea especialmente cauteloso cuando el enrutamiento esté desactivado y la propiedad `net.slp.interfaces` esté configurada. De nuevo, si el enrutamiento de unidifusión está activado entre las interfaces en un equipo de hosts múltiples, no es necesaria ninguna configuración especial de DA ni ámbito. Los anuncios se almacenan en la memoria caché con los servicios de identificación de DA a los que se puede acceder desde cualquiera de las subredes. Sin embargo, si el enrutamiento de unidifusión está desactivado, la colocación incorrecta de DA puede generar problemas.

Para ver los problemas que pueden ocurrir en el ejemplo anterior, considere qué sucedería si `bigguy` ejecuta un DA y los clientes en todas las subredes tienen los mismos ámbitos. Los SA en la subred `143` registran sus anuncios de servicios con el DA. Los UA en la subred `144` pueden obtener esos anuncios de servicios, aunque no se pueda acceder a los hosts de la subred `143`.

Una solución a este problema es ejecutar un DA en cada subred y no en el host múltiple. En esta situación, la propiedad `net.slp.interfaces` en los hosts múltiples debe configurarse con una dirección o un nombre de host de interfaz único, o debe dejarse sin configurar, con lo que se fuerza el uso de la interfaz predeterminada. La desventaja de esta solución es que los hosts múltiples son, a menudo, grandes equipos que podrían manejar mejor la carga computacional de un DA.

Otro solución es ejecutar un DA en el host múltiple, pero configurar ámbitos para que los SA y UA en cada subred tengan un ámbito diferente. Por ejemplo, en la situación anterior, los UA y SA en la subred `142` pueden tener un ámbito que se denomina `scope142`. Los UA y SA en la subred `143` pueden tener otro ámbito que se denomina `scope143`, y los UA y SA en la subred `144` pueden tener un tercer ámbito que se denomina `scope144`. Puede configurar la propiedad `net.slp.interfaces` en `bigguy` con las tres interfaces, de modo que el DA atienda tres ámbitos en las tres subredes.

Consideraciones al configurar múltiples interfaces de red no enrutadas

La configuración de la propiedad `net.slp.interfaces` permite que un DA en el host múltiple una anuncios de servicios entre las subredes. Dicha configuración es útil si el enrutamiento de multidifusión está desactivado en la red, pero el enrutamiento de unidifusión entre interfaces en un host múltiple está activado. Debido a que la unidifusión se enruta entre las interfaces, los hosts en una subred diferente de la subred en la que el servicio se encuentra pueden ponerse en contacto con el servicio cuando reciben la URL del servicio. Sin el DA, los servidores de SA en

una subred en particular reciben sólo difusiones que se realizaron en la misma subred, por lo que no pueden buscar servicios fuera de su subred.

La situación más común que requiere la configuración de la propiedad `net.slp.interfaces` se produce cuando la multidifusión no está implementada en la red y la difusión se utiliza en su lugar. Otras situaciones exigen una cuidadosa consideración y planificación para evitar respuestas duplicadas innecesarias o servicios inaccesibles.

◆ ◆ ◆ CAPÍTULO 4

Incorporación de servicios antiguos

Los servicios antiguos son servicios de red que anteceden el desarrollo y la implementación del SLP. Los servicios como, por ejemplo, el servicio NFS y el servicio de nombres NIS, por ejemplo, no contienen SA internos para el SLP. En este capítulo, se describen cuándo y cómo anunciar servicios antiguos.

Cuándo anunciar servicios antiguos

Con el anuncio de servicios antiguos, puede habilitar los UA del SLP para buscar dispositivos y servicios, como los que se detallan a continuación, en las redes. Puede buscar dispositivos de hardware y servicios de software que no contienen SA del SLP. Cuando las aplicaciones con UA del SLP necesitan encontrar impresoras o bases de datos que no contienen SA del SLP, por ejemplo, los anuncios antiguos podrían ser necesarios.

Anuncio de servicios antiguos

Utilice cualquiera de los siguientes métodos para anunciar servicios antiguos.

- Modificar el servicio para incorporar un SA del SLP.
- Escribir un programa pequeño que anuncie en nombre de un servicio que no esté habilitado para SLP.
- Utilizar los anuncios de proxy para que `slpd` anuncie el servicio.

Modificación del servicio

Si el código de origen del servidor de software está disponible, se puede incorporar un SA del SLP. Las API de Java y C para SLP son relativamente sencillas de utilizar. Consulte las páginas del comando man para obtener información sobre la API C y documentación sobre la API de Java. Si el servicio es un dispositivo de hardware, el fabricante puede tener una PROM actualizada que incorpora SLP. Póngase en contacto con el fabricante del dispositivo para obtener más información.

Anuncio de un servicio que no está habilitado para SLP

Si el código de origen o una PROM actualizada que contienen el SLP no están disponibles, puede escribir una aplicación pequeña que utiliza la biblioteca de cliente del SLP para anunciar el servicio. Esta aplicación puede funcionar como un daemon pequeño que se inicia o se detiene desde la misma secuencia de comandos del shell que se utiliza para iniciar y detener el servicio.

Registro del proxy de SLP

El comando `slpd` de Oracle Solaris admite anuncios de servicios antiguos con un archivo de registro de proxy. El archivo de registro de proxy es una lista de anuncios de servicios en un formato portátil.

▼ Cómo habilitar el registro del proxy de SLP

1 **Cree un archivo de registro de proxy en el sistema de archivos de host o en cualquier directorio de red al que HTTP puede acceder.**

2 **Determine si hay una plantilla de tipo de servicio para el servicio.**

La plantilla es una descripción de la URL del servicio y los atributos de un tipo de servicio. Una plantilla se usa para definir los componentes de un anuncio para un tipo de servicio determinado:

- Si existe una plantilla de tipo de servicio, utilice la plantilla para construir el registro del proxy. Consulte la RFC 2609 para obtener más información sobre las plantillas de tipo de servicio.
- Si una plantilla de tipo de servicio no está disponible para el servicio, seleccione una colección de atributos que describen precisamente el servicio. Utilice una autoridad de asignación de nombres diferente del valor predeterminado para el anuncio. La autoridad de

asignación de nombres predeterminada sólo se permite para tipos de servicio que se han estandarizado. Consulte la RFC 2609 para obtener más información sobre las autoridades de asignación de nombres.

Por ejemplo, suponga que una compañía que se denomina *BizApp* tiene una base de datos local que se utiliza para realizar un seguimiento de defectos de software. Para anunciar la base de datos, la compañía puede utilizar una dirección URL con el tipo de servicio `service:bugdb.bizapp`. La autoridad de asignación de nombres sería `bizapp`.

3 **Siga los siguientes pasos para configurar la propiedad `net.slp.serializedRegURL` en el archivo `/etc/inet/slp.conf` con la ubicación del archivo de registro que se creó en los pasos anteriores.**

4 **Conviértase en administrador.**

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

5 **Detenga `slpd` y toda la actividad de SLP en el host.**

```
# svcadm disable network/slp
```

6 **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

7 **Especifique la ubicación del archivo de registro de proxy en la propiedad `net.slp.serializedRegURL` del archivo `/etc/inet/slp.conf`.**

`net.slp.net.slp.serializedRegURL=`*proxy registration file URL*

Por ejemplo, si el archivo de registro en serie es `/net/inet/slp.reg`, configure la propiedad como se muestra en el siguiente ejemplo:

```
net.slp.serializedRegURL=file:/etc/inet/slp.reg
```

8 **Guarde los cambios y cierre el archivo.**

9 **Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

Uso del registro del proxy de SLP para anunciar

Un anuncio de servicio consta de líneas que identifican la URL del servicio, un ámbito optativo y una serie de definiciones de atributos. El daemon del SLP lee, registra y mantiene anuncios de proxy exactamente como un cliente de SA lo haría. A continuación se muestra un ejemplo de un anuncio de un archivo de registro de proxy.

En el ejemplo, se anuncian una impresora antigua que admite el protocolo LPR y un servidor FTP. Números de línea se han agregado para fines descriptivos y no forman parte del archivo.

```
(1) #Advertise legacy printer.
(2)
(3) service:lpr://bizserver/mainspool,en,65535
(4) scope=eng,corp
(5) make-model=Laserwriter II
(6) location-description=B16-2345
(7) color-supported=monochromatic
(8) fonts-supported=Courier,Times,Helvetica 9 10
(9)
(10) #Advertise FTP server
(11)
(12) ftp://archive/usr/src/public,en,65535,src-server
(13) content=Source code for projects
(14)
```

Nota – El archivo de registro de proxy admite la misma convención para caracteres que no son ASCII de escape que el archivo de configuración. Para obtener más información sobre el formato del archivo de registro de proxy, consulte la RFC 2614.

TABLA 4–1 Descripción del archivo de registro de proxy de SLP

Números de línea	Descripción
1 y 10	Las líneas de comentario comienzan con un símbolo de número (#) y no afectan la operación del archivo. Todos los caracteres hasta el final de una línea de comentario se ignoran.
2, 9 y 14	Líneas en blanco que delimitan los anuncios.

TABLA 4–1 Descripción del archivo de registro de proxy de SLP *(Continuación)*

Números de línea	Descripción
3, 12	Direcciones URL del servicio que cuentan con tres campos necesarios y un campo opcional que están separados por comas: ■ Genérica o `service: URL` anunciada. Consulte la RFC 2609 para obtener la especificación de cómo formar una service: URL. ■ Idioma del anuncio. En el ejemplo anterior, el campo se ha establecido en inglés, *en*. El idioma es una etiqueta de idioma de RFC 1766. ■ Duración del registro, medida en segundos. La duración se limita a un número entero no firmado de 16 bits. Si la duración es menor que el máximo, 65535, `slpd` agota el tiempo de espera del anuncio. Si la duración es 65535, `slpd` actualiza el anuncio periódicamente, y la duración se considera permanente, hasta que `slpd` se cierra. ■ (Opcional) Campo de tipo de servicio: si se usa, este campo define el tipo de servicio. Si la URL del servicio se define, puede cambiar el tipo de servicio bajo el cual se anuncia la dirección URL. En el ejemplo anterior de un archivo de registro de proxy, la línea 12 contiene una URL de FTP genérica. El campo de tipo opcional hace que la dirección URL se anuncie bajo el nombre de tipo de servicio *src-server*. El prefijo `service` no se ha agregado de manera predeterminada en el nombre del tipo.
4	Designación de ámbito. La línea opcional consta del token `scope`, seguido de un signo igual y una lista separada por comas de nombres de ámbitos. Los nombres de ámbitos están definidos por la propiedad de configuración `net.slp.useScopes`. Sólo ámbitos que se han configurado para el host se deben incluir en la lista. Cuando una línea de ámbito no se ha agregado, el registro se realiza en todos los ámbitos donde `slpd` está configurado. La línea de ámbito debe figurar inmediatamente después de la línea de la dirección URL. De lo contrario, los nombres de ámbitos se reconocen como atributos.
5–8	Definiciones de atributos. Después de la línea de ámbito opcional, la mayor parte del anuncio del servicio contiene líneas de pares de listas de valores o atributos. Cada par consta de la etiqueta de atributo, seguida de un signo igual y un valor de atributo o una lista separada por comas de valores. En el ejemplo anterior de un archivo de registro de proxy, la línea 8 ilustra una lista de atributos con varios valores. Todas las otras listas tienen valores únicos. El formato de los valores y los nombres de atributos es el mismo que el de los mensajes de SLP en el cable.

Consideraciones al anunciar servicios antiguos

Por lo general, se prefiere la modificación del código de origen para agregar un SLP antes que la escritura de un servicio habilitado para SLP que utiliza la API de SLP para anunciar en nombre de otros servicios. También se prefiere la modificación del código de origen antes que el registro del proxy. Al modificar el código de origen, puede agregar funciones específicas del servicio y realizar detenidamente un seguimiento de la disponibilidad del servicio. Si el código de origen

no está disponible, la escritura de un servicio auxiliar habilitado para SLP que anuncia en nombre de otros servicios se prefiere antes que el registro del proxy. Idealmente, este servicio auxiliar está integrado en el procedimiento de inicio o detención del servicio que se utiliza para controlar la activación y la desactivación. El anuncio del proxy es, normalmente, la tercera opción, cuando no hay ningún código de origen disponible y la escritura de un SA independiente es poco práctica.

Los anuncios de proxy sólo se mantienen si `slpd` se ejecuta para leer el archivo de registro de proxy. No existe ninguna conexión directa entre el anuncio del proxy y el servicio. Si un anuncio agota el tiempo de espera o `slpd` se detiene, el anuncio del proxy ya no está disponible.

Si el servicio se cierra, `slpd` se debe detener. El archivo de registro en serie se edita para comentar o eliminar el anuncio del proxy, y `slpd` se reinicia. Debe seguir el mismo procedimiento cuando el servicio se reinicia o se vuelve a instalar. La falta de conexión entre el anuncio del proxy y el servicio es una desventaja importante de los anuncios de proxy.

◆ ◆ ◆ CAPÍTULO 5

5 SLP (referencia)

En este capítulo, se describen los códigos de estado y los tipos de mensaje del SLP. Los tipos de mensaje del SLP se muestran con las abreviaturas y los códigos de función. Los códigos de estado del SLP se muestran con descripciones y códigos de función que se utilizan para indicar que se recibe una solicitud (código 0) o que el receptor está ocupado.

Nota – El daemon del SLP (`slpd`) devuelve códigos de estado para mensajes de unidifusión solamente.

Códigos de estado del SLP

TABLA 5–1 Códigos de estado del SLP

Tipo de estado	Código de estado	Descripción
Ningún error	0	La solicitud se procesó sin errores.
LANGUAGE_NOT_SUPPORTED	1	Para un mensaje AttrRqst o SrvRqst, hay datos para el tipo de servicio en el ámbito, pero no en el idioma que se indica.
PARSE_ERROR	2	El mensaje no puede seguir la sintaxis del SLP.
INVALID_REGISTRATION	3	El mensaje SrvReg tiene problemas. Por ejemplo, una duración igual a cero o una etiqueta de idioma omitida.
SCOPE_NOT_SUPPORTED	4	El mensaje del SLP no incluía un ámbito en su lista de ámbitos admitida por el SA o el DA que respondieron la solicitud.
AUTHENTICATION_UNKNOWN	5	El DA o SA recibieron una solicitud para una SPI del SLP no admitida.

TABLA 5–1 Códigos de estado del SLP *(Continuación)*

Tipo de estado	Código de estado	Descripción
AUTHENTICATION_ABSENT	6	El UA o DA esperaban una autenticación de URL y atributo en el mensaje SrvReg, pero no la recibieron.
AUTHENTICATION_FAILED	7	El UA o DA detectaron un error de autenticación en un bloque de autenticación.
VER_NOT_SUPPORTED	9	Número de versión no admitido en el mensaje.
INTERNAL_ERROR	10	Se produjo un error desconocido en el DA o SA. Por ejemplo, el sistema operativo no tenía espacio de archivo restante.
DA_BUSY_NOW	11	El UA o SA deben reintentar mediante la interrupción exponencial. El DA está ocupado con el procesamiento de otros mensajes.
OPTION_NOT_UNDERSTOOD	12	El DA o SA recibieron una opción desconocida del rango obligatorio.
INVALID_UPDATE	13	El DA recibió un mensaje SrvReg sin FRESH establecido para un servicio no registrado o con tipos de servicio inconsistentes.
MSG_NOT_SUPPORTED	14	El SA recibió un mensaje AttrRqst o SrvTypeRqst, pero no lo admite.
REFRESH_REJECTED	15	El SA envió un mensaje SrvReg o SrvDereg parcial a un DA con más frecuencia que el intervalo de actualización mínimo del DA.

Tipos de mensaje del SLP

TABLA 5–2 Tipos de mensaje del SLP

Tipo de mensaje	Abreviatura	Código de función	Descripción
Solicitud de servicio	`SrvRqst`	1	Emitido por un UA para buscar servicios o por un servidor de UA o SA durante la detección activa de DA.
Respuesta de servicio	`SrvRply`	2	La respuesta del DA o SA a una solicitud de servicio.
Registro de servicio	`SrvReg`	3	Permite que los SA registren nuevos anuncios para actualizar los anuncios existentes con atributos nuevos y modificados, y para actualizar las duraciones de las direcciones URL.

TABLA 5–2 Tipos de mensaje del SLP *(Continuación)*

Tipo de mensaje	Abreviatura	Código de función	Descripción
Anulación de registro de servicio	`SrvDereg`	4	Utilizado por el SA para anular el registro de sus anuncios cuando el servicio que representan ya no está disponible.
Confirmación	`SrvAck`	5	La respuesta del DA a una solicitud de servicio o un mensaje de anulación de registro de servicio del SA.
Solicitud de atributo	`AttrRqst`	6	Realizado por la dirección URL o por el tipo de servicio para solicitar una lista de atributos.
Respuesta de atributo	`AttrRply`	7	Utilizado para devolver la lista de atributos.
Anuncio de DA	`DAAdvert`	8	La respuesta del DA para realizar la multidifusión de solicitudes de servicio.
Solicitud de tipo de servicio	`SrvTypeRqst`	9	Utilizado para consultar sobre tipos de servicio registrados que tienen una autoridad de asignación de nombres particular y se encuentran en un conjunto determinado de ámbitos.
Respuesta de tipo de servicio	`SrvTypeRply`	10	El mensaje que se devuelve en respuesta a la solicitud de tipo de servicio.
Anuncio de SA	`SAAdvert`	11	Los UA utilizan el mensaje `SAAdvert` para detectar SA y sus ámbitos en las redes en las que no hay DA implementados.

Índice

R

S

T

U