

Configuración de un servidor de arranque PXE en SUSE Linux Enterprise Server 16.0

DESCRIPCIÓN

Configure un servidor de arranque PXE compatible con arranque seguro UEFI y el instalador Agama.

INTENCIÓN

Automatizar y agilizar la instalación de varios sistemas SUSE Linux Enterprise Server 16.0 a través de la red.

ESFUERZO

Los administradores de sistemas o redes suelen tardar de 30 a 45 minutos en leer y comprender este artículo.

OBJETIVO

Conseguir un servidor PXE operativo que pueda arrancar varias arquitecturas en el instalador Agama.

REQUISITOS

- Un sistema SUSE Linux Enterprise Server 16.0 con privilegios de administrador
- Conexión a Internet para obtener las imágenes ISO
- Una configuración de IP estática para el servidor PXE

Fecha de publicación: 11 Dic 2025

Contenido

- 1 Descripción general del arranque PXE con SUSE Linux Enterprise Server 16.0 4
- 2 Preparación de la red para los servicios de arranque PXE 7
- 3 Instalación de los componentes necesarios del servidor PXE 13
- 4 Creación de directorios NetBoot de GRUB 2 para el servidor PXE 18
- 5 Preparación del contenido de la imagen del instalador 21
- 6 Configuración de GRUB 2 para el arranque PXE 27
- 7 Configuración de TFTP para el arranque PXE 39
- 8 Configuración de nginx para la entrega HTTP 43
- 9 Configuración de un servidor DNS con dnsmasq 47
- 10 Configuración de un servidor NTP con chrony 52
- 11 Configuración de anuncios de router IPv6 56
- 12 Configuración de un servidor DHCP con dnsmasq 61
- 13 Configuración de un servidor DHCP con Kea 68

- 14 Configuración de un servidor DHCP con ISC DHCP 78
- 15 Validación de la configuración del servidor PXE 88
- 16 Información legal 97
- A GNU Free Documentation License 97

1 Descripción general del arranque PXE con SUSE Linux Enterprise Server 16.0

El arranque PXE permite que los equipos arranquen a través de la red en un entorno de instalación o ejecución sin almacenamiento local. En esta sección se explica cómo funciona PXE en SUSE Linux Enterprise Server 16.0 con imágenes de Agama y del instalador en directo, centrándose en GRUB 2.

1.1 ¿Qué es el arranque PXE?

PXE (entorno de ejecución de prearranque) es un método que permite a los sistemas recuperar cargadores de arranque e instaladores de SO desde un servidor de red utilizando DHCP y TFTP o HTTP. Es ampliamente utilizado para el aprovisionamiento de equipos sin medios físicos ni sistemas operativos preinstalados.

1.2 Ventajas del arranque PXE

El arranque PXE simplifica el aprovisionamiento al eliminar la necesidad de medios de instalación locales o configuración manual. Permite lo siguiente:

- Instalar sin asistencia muchos sistemas a través de la red
- Gestionar de forma centralizada versiones del instalador y configuraciones de arranque
- Ofrecer compatibilidad para diversas arquitecturas y tipos de firmware, incluido el arranque seguro UEFI
- Seleccionar de forma dinámica instaladores o parámetros de instalación mediante los menús de GRUB 2

1.3 Cómo funciona el arranque PXE con SUSE Linux Enterprise Server 16.0

El arranque PXE en SUSE Linux Enterprise Server 16.0 utiliza GRUB 2 como cargador de arranque y el instalador Agama como interfaz de instalación. Los cargadores de arranque y los archivos de instalador se proporcionan a través de la red mediante HTTP o TFTP. GRUB 2 se

encarga de recuperar el kernel, initrd y la imagen en directo. Los clientes PXE pueden utilizar distinto firmware (incluyendo los más comunes como BIOS o UEFI), ejecutables de cargador de arranque o formatos de imagen, según lo requieran sus arquitecturas, por ejemplo AMD64/Intel 64, AArch64, ppc64le y s390x. Además, deben funcionar tanto en redes IPv4 como IPv6. El cargador de arranque pasa parámetros del kernel como `root=live:` para cargar el sistema de archivos raíz basado en squashfs desde una imagen ISO en directo, iniciando la interfaz Agama ya sea localmente o como un servicio Web para una interfaz de usuario Web remota.

1.3.1 Retrocompatibilidad con SLES 15.x

La información de este artículo se aplica principalmente a SUSE Linux Enterprise Server 16.0 y versiones posteriores. Se centra en los flujos de trabajo de arranque PXE que se integran con el instalador Agama y se basan en imágenes de instalación en directo. En el contexto y alcance de este artículo, SLES 16.0 y versiones posteriores difieren de SLES 15.x en los siguientes aspectos:

Instalador

Usa `dracut` y Agama en lugar de `linuxrc` y YaST.

Servidor DHCP

Ya no se usa ISC DHCP (final de vida en 2022). Para un servidor DHCP, use Kea o dnsmasq en su lugar.

Parámetros de arranque

Usa el parámetro `root=live:` para cargar la imagen del instalador Agama y el parámetro `inst.install_url=` opcional para el repositorio de instalación no predeterminado, en lugar del parámetro `install=`.

La elección del cargador de arranque (GRUB 2, pxelinux, etc.) sigue siendo flexible y no depende de la versión.

1.3.2 Diferentes configuraciones y pasos posibles

Este artículo consta de pasos de configuración obligatorios y configuraciones opcionales o alternativas. Siga solo las secciones relevantes para su despliegue y omita cualquier alternativa que no sea aplicable.

Obligatorio

Tareas como instalar componentes, preparar la imagen del instalador, configurar GRUB 2 y validar el servidor deben completarse en todas las configuraciones.

Método de entrega de archivos

Un servidor HTTP (recomendado con Agama) como [nginx](#), o un servidor TFTP como [tftp](#) o [dnsmasq](#).

Servidor DHCP

Elija Kea o dnsmasq.



Nota: limitaciones y características del método elegido

- Use **Kea**, el nuevo servidor DHCP de ISC, para sustituir a ISC DHCP con una opción más moderna. Para obtener más información acerca de Kea, consulte <https://www.isc.org/kea/>. Para el aviso de final de vida de ISC DHCP, consulte <https://www.isc.org/dhcp/>. Kea es un servidor DHCP y requiere software de servidor TFTP separado. El servidor DHCP Kea admite opciones para el arranque TFTP/PXE a través de IPv4 e IPv6, así como para el arranque HTTP a través de IPv4. El arranque HTTP a través de IPv6 requiere que el servidor DHCPv6 pueda enviar la Vendor Class Option (consulte [RFC3315, Section 22.16](#)), que, supuestamente, “un cliente usará para identificar al proveedor” de vuelta al cliente, pero actualmente no se admite.
- **dnsmasq** es una combinación de un servidor DNS, un servidor DHCP y un servidor TFTP. Puede usarlo para proporcionar el cargador de arranque, el kernel, initrd (y otros archivos) a través de TFTP. Para obtener más información sobre dnsmasq, consulte <https://thekelleys.org.uk/dnsmasq/doc.html>. El servidor DHCP dnsmasq admite opciones para el arranque TFTP/PXE a través de IPv4 e IPv6, así como para el arranque HTTP a través de IPv4. El arranque HTTP a través de IPv6 requiere que el servidor DHCPv6 pueda enviar la Vendor Class Option (consulte [RFC3315, Section 22.16](#)), que, supuestamente, “un cliente usará para identificar al proveedor” de vuelta al cliente, pero actualmente no se admite.

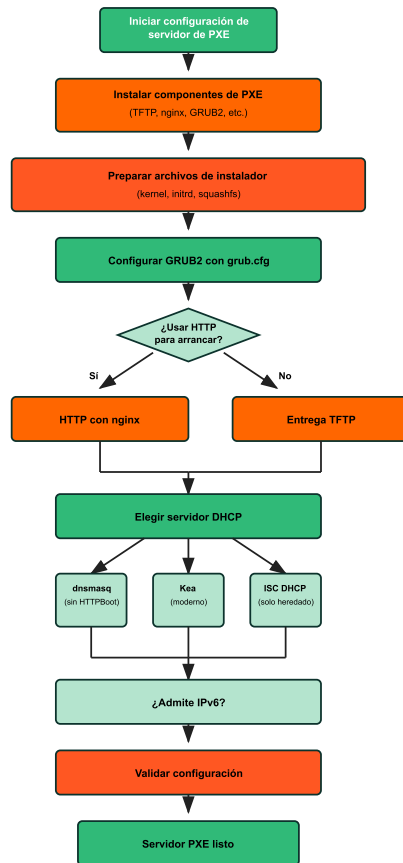


FIGURA 1: FLUJO DE TRABAJO DE CONFIGURACIÓN DEL SERVIDOR PXE DE EJEMPLO

2 Preparación de la red para los servicios de arranque PXE

En esta sección se describen los requisitos de la infraestructura de red para desplegar servicios de arranque PXE en SUSE Linux Enterprise Server 16.0.

2.1 Introducción

Un servidor PXE consta de tres servidores: un servidor DHCP que proporciona la dirección y la ubicación del archivo de arranque (cargador de arranque) y un servidor TFTP y un servidor HTTP para recuperar los archivos. Además, puede haber un servidor DNS, un servidor NTP y un router que admita IPv6; por lo general, están separados del servidor PXE en una red de producción. Un servidor PXE que ejecute SUSE Linux Enterprise Server 16.0 también puede necesitar una configuración de interfaz de red específica, ciertas reglas persistentes añadidas al firewall y algunos permisos en SELinux. Esta sección muestra una red de ejemplo con intervalos de IP adecuados y las reglas necesarias para el firewall y SELinux.

2.2 Suposiciones y configuración de red de muestra

En este artículo, se presupone lo siguiente:

- El servidor PXE se ejecuta en la interfaz de red `eno1` con la siguiente configuración de red:

TABLA 1: CONFIGURACIÓN DE RED PXE DE EJEMPLO

	IPv4	IPv6	Nombre DNS
Red PXE	192.168.1.0/24	2001:db8:0:1::/64	example.net
Servidor PXE	192.168.1.200	2001:db8:0:1::200	pxe.example.net
Gateway PXE	192.168.1.1	2001:db8:0:1::1	
Servidor DNS	192.168.1.200	2001:db8:0:1::200	
Servidor NTP	192.168.1.1	2001:db8:0:1::1	

- De forma predeterminada, los servidores de router, NTP y DNS son externos y se ejecutan en otro equipo. Este artículo proporciona algunas sugerencias, pero no cubre su configuración completa.

2.3 Configuración de la interfaz de red, el firewall y SELinux para servicios PXE

Configure la interfaz de red y el firewall para permitir los servicios de red requeridos por el servidor PXE. Ajuste la configuración de SELinux para habilitar las pruebas de instalación y definir políticas locales persistentes.

1. Compruebe y asigne la interfaz de red PXE a la zona protegida por firewall apropiada.

- a. Compruebe las zonas activas actualmente y sus interfaces asignadas:

```
> sudo firewall-cmd --get-active-zones
```

- b. Si no se asigna `eno1` a la zona `public`, asígnela:

```
> sudo firewall-cmd --zone=public --change-interface=eno1
```

- c. Haga que la asignación de interfaz sea persistente entre arranques:

```
> sudo firewall-cmd --permanent --zone=public --add-interface=eno1
```

2. Configure el firewall para el acceso al servicio DNS.

- a. Permita el servicio DNS para la sesión actual:

```
> sudo firewall-cmd --zone=public --add-service=dns
```

- b. Haga que los cambios sean persistentes:

```
> sudo firewall-cmd --permanent --zone=public --add-service=dns
```

3. Configure el firewall para el acceso al servicio NTP.

- a. Permita el servicio NTP para la sesión actual:

```
> sudo firewall-cmd --zone=public --add-service=ntp
```

- b. Haga que los cambios sean persistentes:

```
> sudo firewall-cmd --permanent --zone=public --add-service=ntp
```

4. Configure el firewall para el acceso al servicio DHCP (IPv4).

- a. Permita el servicio DHCP para la sesión actual:

```
> sudo firewall-cmd --zone=public --add-service=dhcp
```

- b. Haga que los cambios sean persistentes:

```
> sudo firewall-cmd --permanent --zone=public --add-service=dhcp
```

5. Configure el firewall para el acceso al servicio DHCPv6.

- a. Permita el servicio DHCPv6 para la sesión actual:

```
> sudo firewall-cmd --zone=public --add-service=dhcpv6
```

- b. Haga que los cambios sean persistentes:

```
> sudo firewall-cmd --permanent --zone=public --add-service=dhcpv6
```

6. Configure el firewall para el acceso al servicio TFTP.

- a. Permita el servicio TFTP para la sesión actual:

```
> sudo firewall-cmd --zone=public --add-service=tftp
```

- b. Haga que los cambios sean persistentes:

```
> sudo firewall-cmd --permanent --zone=public --add-service=tftp
```

7. Configure el firewall para el acceso al servicio HTTP.

- a. Permita el servicio HTTP para la sesión actual:

```
> sudo firewall-cmd --zone=public --add-service=http
```

- b. Haga que los cambios sean persistentes:

```
> sudo firewall-cmd --permanent --zone=public --add-service=http
```

8. Configure el firewall para el acceso al servicio HTTPS.

- a. Permita el servicio HTTPS para la sesión actual:

```
> sudo firewall-cmd --zone=public --add-service=https
```

- b. Haga que los cambios sean persistentes:

```
> sudo firewall-cmd --permanent --zone=public --add-service=https
```

9. Inhabilite temporalmente SELinux para probar la configuración.

- a. Establezca SELinux en modo permisivo:

```
> sudo setenforce 0
```

- b. Compruebe el estado de SELinux:

```
> sudo sestatus
```

10. Genere e instale módulos de directivas de SELinux locales para los servicios relacionados con PXE.

- a. Cree e instale un módulo para nginx:

```
> sudo if test `ausearch -c 'nginx' --raw | wc -l` -gt 0 ; then
```

```
> sudo ausearch -c 'nginx' --raw | audit2allow -a -M local-nginx
```

```
> sudo semodule -i local-nginx.pp
```

```
> sudo fi
```

- b. Cree e instale un módulo para dnsmasq:

```
> sudo if test `ausearch -c 'dnsmasq' --raw | wc -l` -gt 0 ; then
```

```
> sudo ausearch -c 'dnsmasq' --raw | audit2allow -a -M local-dnsmasq
```

```
> sudo semodule -i local-dnsmasq.pp
```

```
> sudo fi
```

- c. Cree e instale un módulo para in.tftpd:

```
> sudo if test `ausearch -c 'in.tftpd' --raw | wc -l` -gt 0 ; then
```

```
> sudo ausearch -c 'in.tftpd' --raw | audit2allow -a -M local-tftpd
```

```
> sudo semodule -i local-tftpd.pp
```

```
> sudo fi
```

11. Vuelva a habilitar el modo de aplicación de SELinux.

a. Establezca SELinux en el modo de aplicación:

```
> sudo setenforce 1
```

b. Verifique el estado de SELinux:

```
> sudo sestatus
```

2.4 Resumen

Este procedimiento garantiza que la interfaz de red, el firewall y la directiva de SELinux del servidor PXE estén correctamente configurados para un funcionamiento seguro y funcional.

- Se verifica y se asigna la interfaz que proporciona PXE (eno1 en este ejemplo) a la zona public protegida por el firewall.
- Se abren los servicios de firewall necesarios para el funcionamiento de PXE, incluidos dns, ntp, dhcp, dhcpv6, tftp, http y https.
- Se establece temporalmente SELinux en modo permissive para facilitar las pruebas de servicio y registrar denegaciones de acceso AVC.
- Se usan **ausearch** y **audit2allow** para generar e instalar módulos de directivas de SELinux personalizados para servicios como nginx, dnsmasq y in.tftpd.
- Se restablece el modo SELinux a enforcing para proteger el sistema para su uso en producción.

Una vez completados estos pasos, el servidor PXE está configurado de forma segura y listo para proveer equipos cliente a través de la red utilizando IPv4 o IPv6.

3 Instalación de los componentes necesarios del servidor PXE

En esta sección se explica cómo instalar los paquetes necesarios para permitir el arranque PXE en SUSE Linux Enterprise Server 16.0, incluidos los componentes GRUB 2, DHCP, TFTP o HTTP.

3.1 Introducción

Para configurar un servidor de arranque PXE en SUSE Linux Enterprise Server 16.0, debe instalar varios servicios y herramientas. Dependiendo de su configuración, es posible que necesite lo siguiente:

- El paquete `dnsmasq` proporciona una combinación de un servidor DNS, un servidor TFTP y un servidor DHCP (DHCPv4 y DHCPv6) con compatibilidad limitada para anuncios de router IPv6. Incluye lo siguiente:
 - Servidor DHCP `dnsmasq`: admite la entrega condicional de opciones DHCP dependiendo de la solicitud y la arquitectura del cliente para:
 - Solicitudes de arranque PXE con DHCPv4 y DHCPv6
 - Solicitudes de arranque HTTP con DHCPv4



Nota: limitaciones de `dnsmasq` para el arranque HTTP a través de DHCPv6

Actualmente, `dnsmasq` no admite el envío de la opción DHCPv6 `vendor-class` requerida.

- Servidor TFTP `dnsmasq`: entrega archivos de cargador de arranque, de kernel e `initrd` a través de TFTP durante el arranque PXE.

- Servidor DNS `dnsmasq`: proporciona resolución recursiva de nombres de dominio y direcciones IP para firmware y `/etc/resolv.conf` de cliente en el instalador/sistema operativo.
- Anuncios de router IPv6 `dnsmasq`: admite el envío de anuncios de router IPv6 cuando el servidor PXE también actúa como router (configurabilidad limitada a un “patrón común de anuncios de router”).
- El paquete `kea` es un servidor DHCP y un sucesor del servidor ISC DHCP. Admite la entrega condicional de opciones DHCP dependiendo de la solicitud y la arquitectura del cliente para:
 - Solicitudes de arranque PXE con DHCPv4 y DHCPv6
 - Solicitudes de arranque HTTP con DHCPv4



Nota: limitaciones de Kea para el arranque HTTP a través de DHCPv6

Actualmente, Kea no admite el envío de la opción DHCPv6 `vendor-class` requerida. Para obtener más información, consulte <https://kea.readthedocs.io/en/latest/arm/dhcp6-srv.html#id4>.

- Un servidor TFTP entrega los archivos del cargador de arranque, el kernel e `initrd` a través de TFTP, mientras que el arranque PXE con Kea es proporcionado por el paquete `tftp` y no es necesario para el arranque HTTP. Si está usando `dnsmasq`, no necesita el paquete `tftp`.
- Un servidor Web como el paquete `nginx` para proporcionar imágenes del instalador a través de HTTP.



Nota: necesidad de servidores HTTP

Casi siempre se requiere un servidor HTTP/HTTPS como nginx. Su uso va más allá del arranque HTTP. En particular, puede necesitarlo en las siguientes situaciones:

- Es un requisito básico para el arranque HTTP.
 - Se recomienda para proporcionar `squashfs.img`. Puede usar `root=live:ftp://.../squashfs.img` en la línea de comandos de arranque.
 - También se recomienda para proporcionar los RPM a Agama en el parámetro de línea de comandos de arranque `inst.install_url=http://.../install/` en una imagen `SLES-16.0-Full*.inline.iso`, junto con perfiles de instalación y otros archivos para la instalación sin supervisión.
- Los paquetes del cargador de arranque GRUB 2 proporcionan arranque en red para las arquitecturas y los métodos compatibles. Por ejemplo, la arquitectura AMD64/Intel 64 ofrece dos métodos para el arranque en red: BIOS y UEFI. Además, UEFI generalmente admite PXE (TFTP) y arranque HTTP. Otros cargadores de arranque, como pxelinux, no admiten UEFI ni el arranque HTTP.
 - Opcionalmente, un daemon de anuncios de router para IPv6, como el paquete `radvd`. Se requiere en SLES si también actúa como router para una red de instaladores a fin de realizar lo siguiente:
 - Configurar el enrutamiento en una red para clientes de arranque PXE o HTTP.
 - Habilitar el uso de DHCPv6 en una red para clientes de arranque PXE o HTTP.

3.2 Requisitos

- Un sistema que ejecute SUSE Linux Enterprise Server 16.0 con privilegios administrativos, registrado en el Centro de servicios al cliente de SUSE y configurado con acceso a los repositorios en línea apropiados mediante SUSEConnect.
- Módulos de SLE habilitados: módulo de aplicaciones de servidor, módulo heredado y módulo del sistema base.

- Acceso a los repositorios del módulo de SLE para servicios de red y cargadores de arranque.
- Conexión a Internet funcional para obtener las imágenes ISO.

3.3 Instalación de los paquetes

Siga estos pasos para instalar los paquetes principales necesarios para el servidor de arranque PXE.

PROCEDIMIENTO 1: INSTALACIÓN DE LOS PAQUETES NECESARIOS PARA UN SERVIDOR DE ARRANQUE PXE

1. Instale el cargador de arranque GRUB 2 y el servidor HTTP nginx como requisitos comunes.

```
> sudo zypper install grub2 nginx
```

2. Ejecute cualquiera de los siguientes comandos para instalar los paquetes esenciales según su enfoque:

- `kea` para el servidor DHCP o `tftp` para el servidor TFTP

```
> sudo zypper install kea tftp
```

- `dnsmasq` como proveedor común de servidores DHCP, DNS y TFTP

```
> sudo zypper install dnsmasq
```



Nota: limitaciones de los servidores DHCP proporcionados por Kea y dnsmasq

El arranque HTTP a través de IPv6 no es compatible *actualmente* con servidores DHCP proporcionados por los paquetes `kea` y `dnsmasq`. No admite el envío de una opción `vendor-class` al cliente HTTP, como requiere la especificación UEFI.

3. Opcionalmente, puede instalar destinos de GRUB 2 específicos para arquitectura adicionales si planea admitir otras plataformas.

- Para la arquitectura AMD64/Intel 64:

```
> sudo zypper install grub2-x86_64-efi grub2-i386-pc
```

- Para la arquitectura AArch64:

```
> sudo zypper install grub2-aarch64-efi
```

- Para la arquitectura ppc64le:

```
> sudo zypper install grub2-ppc64le-ieee1275
```



Nota: cómo entrega el servidor PXE paquetes de GRUB 2 a clientes que tienen una arquitectura distinta a la del equipo del servidor

Los paquetes `noarch.rpm` específicos de cada arquitectura de GRUB 2 se incluyen en el subdirectorio `noarch` del medio o repositorio de instalación, independientemente de la arquitectura del equipo en el que se configure el servidor PXE. Es decir, puede instalar paquetes `grub2-arm64-efi` y `grub2-powerpc-ieee1275` en un servidor PXE que se ejecute en un equipo AMD64/Intel 64 para admitir clientes con otras arquitecturas.

4. Opcionalmente, puede instalar el paquete `shim` si necesita arranque seguro UEFI para AMD64/Intel 64 o AArch64, pero no desea utilizar los archivos de la ISO del medio de instalación.

```
> sudo zypper install shim
```

5. Opcionalmente, puede instalar el daemon de anuncios de router `radvd` si desea usar el servidor PXE como router (no se recomienda para redes de producción).

```
> sudo zypper install radvd
```

6. Instale la utilidad `rsync` para copiar o sincronizar cómodamente la imagen ISO y el árbol de directorios.

```
> sudo zypper install rsync
```

7. Asegúrese de que los servicios están instalados pero aún no se han iniciado. La configuración se tratará en secciones posteriores.

4 Creación de directorios NetBoot de GRUB 2 para el servidor PXE

Esta sección explica cómo crear directorios NetBoot de GRUB 2 para servidores PXE mediante `grub2-mknetdir`, lo que genera directorios específicos de cada arquitectura para sistemas AMD64/Intel 64 (UEFI y BIOS), AArch64 y ppc64le. Para la compatibilidad con el arranque seguro UEFI, los administradores deben copiar los archivos EFI firmados de los medios de instalación o utilizar el paquete `shim` para sustituir los archivos por defecto del cargador de arranque sin firmar.

4.1 Introducción

En esta sección se describe cómo configurar directorios NetBoot de GRUB 2 para desplegar servidores PXE en varias arquitecturas. El comando `grub2-mknetdir` crea directorios específicos de arquitectura en `/srv/tftpboot/boot/grub2/` para diferentes plataformas. Por ejemplo, los sistemas AMD64/Intel 64 generan directorios UEFI (`x86_64-efi`) y BIOS heredados (`i386-pc`), mientras que los sistemas AArch64 y ppc64le crean sus respectivos directorios UEFI (`arm64-efi` y `powerpc-ieee1275`).

Para la compatibilidad con el arranque seguro UEFI, que los archivos `core.efi` no firmados predeterminados no proporcionan, los administradores pueden copiar archivos EFI firmados desde los medios de instalación o instalar el paquete `shim` y copiar manualmente los archivos del cargador de arranque necesarios (`shim.efi`, `grub.efi` y `MokManager.efi`) en los directorios de la arquitectura apropiada, lo que asegura una resolución de enlace simbólico adecuada para mantener todos los archivos dentro del sistema de archivos raíz TFTP.

4.2 Requisitos

- Asegúrese de haber instalado los siguientes paquetes: `grub2`, `tftp` y cualquier otro paquete de GRUB 2 específico de la arquitectura, como `grub2-x86_64-efi` y `grub2-i386-pc`.
- Asegúrese de tener disponible el medio de instalación (ISO) para el montaje o el paquete `shim` instalado en el sistema. Puede descargar los medios de instalación (ISO) para su arquitectura de destino desde el Centro de servicios al cliente de SUSE.

4.3 Preparación de directorios NetBoot y el arranque seguro UEFI

Este procedimiento crea la estructura de directorios de GRUB 2 necesaria para el arranque de red PXE y, opcionalmente, configura la compatibilidad con el arranque seguro UEFI en varias arquitecturas.

1. Cree una estructura de directorios NetBoot de GRUB 2.

```
> sudo grub2-mknetdir --net-directory=/srv/tftpboot
--subdir=/boot/grub2
```

Esto crea directorios específicos para cada arquitectura:

- AMD64/Intel 64: /srv/tftpboot/boot/grub2/x86_64-efi y /srv/tftpboot/boot/grub2/i386-pc
- AArch64: /srv/tftpboot/boot/grub2/arm64-efi
- ppc64le: /srv/tftpboot/boot/grub2/powerpc-ieee1275



Aviso

No sobrescriba manualmente el archivo `grub.cfg` creado por `grub2-mknetdir`.

2. Copie al servidor TFTP otros directorios independientes de la arquitectura, como `fonts/` y `locale/`, que están disponibles en el directorio `/srv/tftpboot/boot/grub2/`.
3. También puede usar el archivo `/srv/tftpboot/boot/grub2/ARCH-efi/core.efi` instalado por el comando `grub2-mknetdir` para arquitecturas AMD64/Intel 64 o AArch64 para PXE UEFI. Sin embargo, *no están firmados* y no admiten el arranque seguro UEFI. Para habilitar opcionalmente el arranque seguro UEFI para las arquitecturas compatibles AMD64/Intel 64 y AArch64, realice cualquiera de los siguientes pasos:
 - Copie los archivos necesarios del medio de instalación ISO:

- a. Monte la imagen ISO:

```
> sudo mount -o loop /PATH/TO/SLES.ISO /mnt
```

- b. Copie los archivos EFI.

```
> sudo cp -v /mnt/EFI/BOOT/*.efi
/srv/tftpboot/boot/grub2/ARCH-efi/ ①
```

- ① Sustituya `ARCH-efi` por `x86_64-efi` o `arm64-efi`: las arquitecturas compatibles con el arranque seguro UEFI.

c. Desmonte el medio de instalación ISO.

```
> sudo umount /mnt
```

- Use el paquete `shim` si no desea utilizar los archivos del medio de instalación ISO:

a. Si aún no está instalado, instale el paquete `shim`.

```
> sudo zypper install shim
```

b. Copie los archivos del cargador de arranque firmados para la arquitectura necesaria:

i. Copie el archivo `shim.efi`.

- Para la arquitectura AMD64/Intel 64:

```
> sudo cp -v -p -L /usr/share/efi/x86_64/shim.efi /srv/tftpboot/  
boot/grub2/x86_64-efi/bootx64.efi
```

- Para la arquitectura AArch64:

```
> sudo cp -v -p -L /usr/share/efi/aarch64/shim.efi /srv/  
tftpboot/boot/grub2/arm64-efi/bootaa64.efi
```

ii. Copie el archivo `grub.efi`.

- Para la arquitectura AMD64/Intel 64:

```
> sudo cp -v -p -L /usr/share/efi/x86_64/grub.efi /srv/tftpboot/  
boot/grub2/x86_64-efi/
```

- Para la arquitectura AArch64:

```
> sudo cp -v -p -L /usr/share/efi/aarch64/grub.efi /srv/  
tftpboot/boot/grub2/arm64-efi/
```

iii. Copie el archivo `MokManager.efi`.

- Para la arquitectura AMD64/Intel 64:

```
> sudo cp -v -p -L /usr/share/efi/x86_64/MokManager.efi /srv/tftpboot/boot/grub2/x86_64-efi/
```

- Para la arquitectura AArch64:

```
> sudo cp -v -p -L /usr/share/efi/aarch64/MokManager.efi /srv/tftpboot/boot/grub2/arm64-efi/
```



Nota

El indicador `-L` resuelve los enlaces simbólicos para garantizar que los archivos permanezcan dentro de la raíz TFTP.

5 Preparación del contenido de la imagen del instalador

En esta sección se describe cómo extraer y organizar los archivos de instalador de los medios de instalación de SUSE Linux Enterprise Server 16.0 para entornos de arranque PXE. Cubre tanto imágenes `.install.iso` como paquetes RPM, con instrucciones específicas para diferentes arquitecturas y tipos de instalación.

5.1 Introducción

SUSE Linux Enterprise Server 16.0 proporciona archivos de instalador en múltiples formatos para admitir diferentes escenarios de arranque PXE. El instalador Agama requiere tres archivos esenciales: la imagen del kernel (`linux`), el disco RAM inicial (`initrd`) y el sistema de archivos raíz comprimido (`squashfs.img`). Estos archivos deben extraerse del medio de instalación y organizarse en una estructura de directorios a la que se pueda acceder a través de TFTP y HTTP. Esta sección cubre los métodos de preparación tanto para imágenes `.install.iso` como para paquetes RPM, lo que asegura la compatibilidad con varias arquitecturas y tipos de instalación compatibles con SUSE Linux Enterprise Server 16.0.

5.2 Requisitos

- Medio de instalación de SUSE Linux Enterprise Server 16.0, disponible en el Centro de servicios al cliente de SUSE. Elija entre lo siguiente:
 - ISO en línea: solo incluye el instalador para instalaciones de red ([SLES-16.0-Online-ARCH-BUILD.install.iso](#))
 - ISO completa: el instalador con el repositorio de instalación ([SLES-16.0-Full-ARCH-BUILD.install.iso](#))
 - Paquetes RPM: [tftpboot-agama-installer-SUSE_SLE_16_PXE-ARCH](#)
- Un punto de montaje temporal, como [/mnt](#).
- Espacio en disco suficiente en [/srv/tftpboot](#) y [/srv/install](#) para el método de instalación elegido.
- Privilegios administrativos para crear directorios y copiar archivos.

5.3 Preparación de archivos de instalador a partir de imágenes ISO

Las imágenes ISO proporcionan un método sencillo para extraer archivos de instalador. Los siguientes procedimientos cubren los métodos de ISO en línea y de ISO completa para diferentes arquitecturas.

5.3.1 Uso de imágenes ISO en línea

Las imágenes ISO en línea contienen solo los componentes del instalador, por lo que se requiere acceso de red a los repositorios de instalación durante la instalación del sistema. Esto se corresponde con la entrada del menú de arranque [SLES-16.0 Online Installation](#) en GRUB.

PROCEDIMIENTO 2: EXTRACCIÓN DE ARCHIVOS DE ISO EN LÍNEA (X86_64 Y AARCH64)

1. Cree la estructura de directorio para los archivos de instalador:

```
> sudo mkdir -p /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

2. Monte la imagen ISO en línea:

```
> sudo mount -oro,loop /srv/install/iso/SLES-16.0-Online-ARCH-BUILD.install.iso /mnt
```

3. Copie los archivos del kernel y de initrd:

```
> sudo cp /mnt/boot/ARCH/loader/linux /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

```
> sudo cp /mnt/boot/ARCH/loader/initrd /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

4. Copie el sistema de archivos raíz comprimido:

```
> sudo cp /mnt/LiveOS/squashfs.img /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

5. Desmonte la imagen ISO:

```
> sudo umount /mnt
```

PROCEDIMIENTO 3: EXTRAIGA LOS ARCHIVOS DE LA ISO EN LÍNEA (PPC64LE)

1. Cree la estructura de directorio:

```
> sudo mkdir -p /srv/tftpboot/boot/images/SLES-16.0/ppc64le/
```

2. Monte la imagen ISO:

```
> sudo mount -oro,loop /srv/install/iso/SLES-16.0-Online-ppc64le-BUILD.install.iso /mnt
```

3. Copie los archivos del kernel e initrd (observe que la estructura de la vía es distinta para ppc64le):

```
> sudo cp /mnt/boot/ppc64le/linux /srv/tftpboot/boot/images/SLES-16.0/ppc64le/
```

```
> sudo cp /mnt/boot/ppc64le/initrd /srv/tftpboot/boot/images/SLES-16.0/ppc64le/
```

4. Copie el sistema de archivos raíz comprimido:

```
> sudo cp /mnt/LiveOS/squashfs.img /srv/tftpboot/boot/images/SLES-16.0/ppc64le/
```

5. Desmonte la imagen ISO:

```
> sudo umount /mnt
```

5.3.2 Uso de imágenes ISO completas

Las imágenes ISO completas incluyen tanto el instalador como los repositorios de instalación, lo que permite instalaciones locales sin dependencias de red externas. Se corresponde con la entrada del menú de arranque `SLES-16.0 Local Installation` en GRUB con el parámetro `inst.install_url=http://pxe.example.net/install/SLES-16.0/${arch}` adicional.

PROCEDIMIENTO 4: EXTRACCIÓN DE ARCHIVOS DE LA ISO COMPLETA

1. Cree directorios tanto para los archivos de instalador como para el repositorio de instalación:

```
> sudo mkdir -p /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

```
> sudo mkdir -p /srv/install/SLES-16.0
```

2. Monte la imagen ISO completa:

```
> sudo mount -oro,loop /srv/install/iso/SLES-16.0-Full-ARCH-BUILD.install.iso /mnt
```

3. Copie los archivos de kernel y de initrd (ajuste las vías para ppc64le como se muestra en procedimientos anteriores):

```
> sudo cp /mnt/boot/ARCH/loader/linux /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

```
> sudo cp /mnt/boot/ARCH/loader/initrd /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

4. Copie el sistema de archivos raíz comprimido:

```
> sudo cp /mnt/LiveOS/squashfs.img /srv/tftpboot/boot/images/SLES-16.0/ARCH/
```

5. Copie el repositorio de instalación para el acceso local al servidor HTTP:

```
> sudo rsync -avP /mnt/install/ /srv/install/SLES-16.0/ARCH/
```

6. Desmonte la imagen ISO:

```
> sudo umount /mnt
```

5.4 Preparación de los archivos de instalador a partir de paquetes RPM

Los paquetes RPM proporcionan un método alternativo para obtener archivos de instalador en línea.

PROCEDIMIENTO 5: INSTALACIÓN Y USO DE PAQUETES RPM DE TFTPBOOT

1. Instale los paquetes necesarios:

```
> sudo zypper in tftpboot-agama-installer-SUSE_SLE_16-ARCH
```

2. Copie linux, initrd y squashfs.img en tftpboot:

```
> sudo mkdir -p  
/srv/tftpboot/boot/images/SLES-16.0/ARCH
```

```
> sudo cd  
/srv/tftpboot/boot/images/SLES-16.0/ARCH
```

```
> sudo cp -v /usr/share/tftpboot-installation/agama-installer-SUSE_SLE_16/ARCH/  
loader/linux .
```

```
> sudo cp -v /usr/share/tftpboot-installation/agama-installer-SUSE_SLE_16/ARCH/  
loader/initrd .
```

```
> sudo cp -v /usr/share/tftpboot-installation/agama-installer-SUSE_SLE_16/ARCH/  
loader/squashfs.img .
```

5.5 Estructura de directorios recomendada

Organice los archivos extraídos de acuerdo con el siguiente diseño de directorio para garantizar la consistencia y facilidad de mantenimiento. Esta estructura admite múltiples arquitecturas y tipos de instalación.

EJEMPLO 1: DISEÑO COMPLETO DEL DIRECTORIO DEL SERVIDOR PXE

```
/srv/tftpboot/  
├─ boot/  
│ └─ grub2/  
│   │ └─ x86_64-efi/  
│   │   └─ bootx64.efi  
│   └─ grub.cfg
```

```

├── i386-pc/
│   └── core.0
├── arm64-efi/
│   └── bootaa64.efi
├── powerpc-ieee1275/
│   └── core.elf
└── images/
    ├── SLES-16.0/
    │   ├── x86_64/
    │   │   ├── linux ❶
    │   │   ├── initrd ❷
    │   │   └── squashfs.img ❸
    │   ├── aarch64/
    │   └── ppc64le/
├── /srv/install/
└── SLES-16.0/
    ├── x86_64/ ❹
    ├── aarch64/
    └── ppc64le/

```

- ❶ Imagen del kernel extraída del medio de instalación
- ❷ Imagen de disco RAM inicial
- ❸ Sistema de archivos raíz comprimido para el instalador Agama
- ❹ Repositorio de instalación desde el directorio `install` de la imagen ISO completa (opcional)

5.6 Verificación de la instalación

Después de extraer y organizar los archivos de instalador, compruebe que todos los componentes necesarios están presentes y se puede acceder a ellos.

PROCEDIMIENTO 6: PASOS DE VERIFICACIÓN

1. Compruebe que los archivos esenciales están presentes:

```
> ls -la /srv/tftpboot/boot/images/SLES-16.0/ARCH/*
```

2. Asegúrese de que los permisos del archivo sean correctos:

```
> sudo find /srv/tftpboot/boot/images/ -type d -exec chmod 0755 {} \;
```

```
> sudo find /srv/tftpboot/boot/images/ -type f -exec chmod 0644 {} \;
```



Importante: accesibilidad de los archivos

Asegúrese de que los servicios TFTP y HTTP puedan leer todos los archivos extraídos. Los clientes PXE accederán a los archivos durante el proceso de arranque, por lo que para que el despliegue se realice correctamente, es esencial que se disponga de los permisos y la configuración del servicio adecuados.

5.7 Pasos siguientes

Con los archivos de instalador correctamente preparados y organizados, puede proceder a:

- Configurar GRUB 2 para el arranque PXE con entradas de menú que hagan referencia a estos archivos
- Configurar los servicios HTTP y TFTP para proporcionar el contenido extraído
- Configurar DHCP para dirigir a los clientes PXE a los cargadores de arranque apropiados

En la configuración de GRUB 2 se hará referencia a los archivos extraídos usando vías como `root=live:http://pxe.example.net/boot/images/SLES-16.0/ARCH/squashfs.img`.

6 Configuración de GRUB 2 para el arranque PXE

En esta sección se describe cómo configurar el cargador de arranque de GRUB 2 para el arranque basado en PXE en SUSE Linux Enterprise Server 16.0. Cubre la creación de la estructura de directorios de arranque de red, la configuración de cargadores de arranque específicos de arquitectura y la implementación de un sistema de configuración flexible que admite múltiples arquitecturas y escenarios de instalación.

6.1 Introducción

GRUB 2 sirve como cargador de arranque de red para clientes PXE. Carga los archivos de kernel e initrd para iniciar el instalador Agama. Esta sección muestra cómo crear una configuración avanzada de GRUB 2 que detecta automáticamente la arquitectura del cliente, gestiona la selección de la interfaz de red y proporciona un menú de arranque unificado que admite múltiples tipos de instalación y arquitecturas de destino.

El enfoque de configuración utiliza un diseño modular con archivos separados para la detección de arquitectura, definiciones de variables y entradas del menú de arranque. Esto permite la compatibilidad con configuraciones específicas del equipo y perfiles de instalación automatizados, manteniendo la coherencia entre las diferentes plataformas de hardware.

6.2 Requisitos

- Asegúrese de que la estructura del directorio de arranque de red de GRUB 2 está instalada, como se describe en las secciones anteriores.
- Asegúrese de que los archivos de instalador están organizados correctamente como se describe en las secciones anteriores.
- Se deben instalar paquetes GRUB 2 para todas las arquitecturas de destino: `grub2-x86_64-efi`, `grub2-i386-pc`, `grub2-aarch64-efi` y `grub2-ppc64le-ieee1275`.
- El paquete `shim` para la compatibilidad con el arranque seguro UEFI (opcional).
- Acceso administrativo a `/srv/tftpboot` o raíz PXE equivalente.

6.3 Creación de la configuración de GRUB 2

El archivo de configuración de GRUB 2 se encarga de tres tareas principales: detectar la arquitectura del cliente, gestionar las interfaces de red y cargar otros archivos de configuración. Este enfoque modular ofrece flexibilidad para diferentes escenarios de despliegue.

PROCEDIMIENTO 7: CONFIGURACIÓN DEL ARCHIVO `grub.cfg` PRINCIPAL

- Cree el archivo de configuración principal de GRUB 2 en `/srv/tftpboot/boot/grub2/grub.cfg`:

```
> sudo cat > /srv/tftpboot/boot/grub2/grub.cfg << 'EOF'  
# Architecture detection and mapping
```

```

if [ "$grub_cpu" == "i386" ]; then
    set arch='x86_64'
elif [ "$grub_cpu" == "x86_64" ]; then
    set arch='x86_64'
elif [ "$grub_cpu" == "arm64" ]; then
    set arch='aarch64'
elif [ "$grub_cpu" == "powerpc" ]; then
    set arch='ppc64le'
fi

if [ "X$arch" == "X" ]; then
    echo "ERROR: No architecture found for ${grub_cpu}"
    exit
else
    echo "Running on $arch CPU architecture"
fi
export arch

# Network interface configuration for PXE-selected NIC
# - dracut based images on SLE-16:
set ipcfg="ifname=pxe0:${net_default_mac} ip=pxe0:dhcp"
export ipcfg
# - linuxrc installer on SLE-15:
set ifcfg="ifcfg=${net_default_mac}=dhcp"
export ifcfg

# Define typical serial console kernel parameter
#set sconsole="console=tty0 console=ttyS0,115200n8"
#export sconsole

# Load machine-specific configuration if available
if [ -s "${config}/${net_default_mac}/grub.cfg" ]; then
    ## Source a host specific configuration of grub menu:
    source "${config}/${net_default_mac}/grub.cfg"
else
    ## Source default grub boot menu:
    source "${prefix}/menu.cfg"
fi
EOF

```

ELEMENTOS CLAVE DE LA CONFIGURACIÓN

Detección de arquitectura

Asigna tipos de CPU de GRUB 2 a arquitecturas de distribución, lo que permite entradas de menú unificadas que funcionan en diferentes plataformas de hardware.

Gestión de la interfaz de red

Define una variable `#{ipcfg}` que usa la variable `#{net_default_mac}` de grub2 para activar dhcp solo en la interfaz de arranque PXE llamada `pxe0`, evitando problemas de sondeo de red en sistemas de varias interfaces.

Definiciones de utilidad

Define una variable `#{sconsole}` típica con parámetros de consola serie.

Configuración específica del equipo

Carga archivos de configuración opcionales por equipo basados en la dirección MAC, lo que permite personalizar los parámetros de arranque por equipo y los perfiles de instalación automatizados.

6.4 Creación del menú de arranque unificado

El menú de arranque utiliza variables de la configuración principal para proporcionar entradas de menú adaptadas a la arquitectura que se adaptan automáticamente a diferentes plataformas de hardware y tipos de instalación.

PROCEDIMIENTO 8: CONFIGURACIÓN DEL ARCHIVO MENU.CFG

- Cree el menú de arranque unificado en `/srv/tftpboot/boot/grub2/menu.cfg`:

```
> sudo cat > /srv/tftpboot/boot/grub2/menu.cfg << 'EOF'
menuentry 'SLES-16.0 Online Installation' {
  linux /boot/images/SLES-16.0/${arch}/linux showopts root=live:http://
pxe.example.net/boot/images/SLES-16.0/${arch}/squashfs.img ${ipcfg} ${sconsole}
  ${autoinstall}
  initrd /boot/images/SLES-16.0/${arch}/initrd
}

menuentry 'SLES-16.0 Local Installation' {
  linux /boot/images/SLES-16.0/${arch}/linux showopts root=live:http://
pxe.example.net/boot/images/SLES-16.0/${arch}/squashfs.img inst.install_url=http://
pxe.example.net/install/SLES-16.0/${arch} ${ipcfg} ${sconsole} ${autoinstall}
  initrd /boot/images/SLES-16.0/${arch}/initrd
}
EOF
```



Nota: flexibilidad de entrada de menú

Las entradas de menú utilizan variables que se rellenan automáticamente en función de la arquitectura y configuración del cliente. La variable `_${arch}` garantiza que se carguen los archivos correctos.

La variable `_${ipcfg}` opcional hace que solo se configure la interfaz de red seleccionada por PXE.

La variable `_${sconsole}` opcional habilita una consola serie en el sistema instalador.

6.5 Configuraciones específicas del equipo

Para despliegues avanzados, puede crear archivos de configuración específicos del equipo que anulen los ajustes predeterminados o proporcionen parámetros de instalación automatizados.

PROCEDIMIENTO 9: CREACIÓN DE UNA CONFIGURACIÓN ESPECÍFICA DEL EQUIPO

1. Cree un directorio para configuraciones específicas del equipo:

```
> sudo mkdir -p /srv/tftpboot/boot/config
```

2. Para un equipo con una dirección MAC `aa:bb:cc:dd:ee:ff`, cree una configuración específica:

```
> sudo mkdir -p /srv/tftpboot/boot/config/aa:bb:cc:dd:ee:ff
```

3. Cree el archivo `grub.cfg` específico del equipo:

```
> sudo cat > /srv/tftpboot/boot/config/aa:bb:cc:dd:ee:ff/grub.cfg << 'EOF'
# Machine-specific configuration for aa:bb:cc:dd:ee:ff
set default='SLES-16.0 Full Installation'

# Activate the menu-entry after 5sec timeout
set timeout=5

# Use know predictable network interface name
set ipcfg="ip=enol:dhcp"

# Set the autoinstall variable for this machine
set autoinstall="inst.auto=http://pxe.example.net/install/profiles/
aa:bb:cc:dd:ee:ff/sles16.json"
export autoinstall
```

```
# Load the default menu
source "/boot/grub2/menu.cfg"
EOF
```

Como alternativa, puede proporcionar su propia entrada de menú en el archivo `grub.cfg` específico del host (por ejemplo, generada para un intento de arranque específico):

```
> sudo cat > /srv/tftpboot/boot/config/aa:bb:cc:dd:ee:ff/grub.cfg << 'EOF'
set default='SLES-16.0 Auto-Installation'
set timeout=5

menuentry 'SLES-16.0 Auto-Installation' {
  linux /boot/images/SLES-16.0/${arch}/linux showopts root=live:http://
pxe.example.net/boot/images/SLES-16.0/${arch}/squashfs.img inst.install_url=http://
pxe.example.net/install/SLES-16.0/${arch} inst.auto=http://pxe.example.net/install/
profiles/${net_default_mac}/sles16.json ip=enol:dhcp
  initrd /boot/images/SLES-16.0/${arch}/initrd
}
EOF
```

EJEMPLO 2: PARÁMETROS COMUNES ESPECÍFICOS DEL EQUIPO

default

Especifica qué entrada de menú se debe arrancar automáticamente.

timeout

Establece el tiempo límite del arranque en segundos.

ipcfg

Anula la configuración de la interfaz de red para hardware específico.

autoinstall

Proporciona URL de perfil de instalación automatizadas específicas del equipo.

6.6 Verificación de la configuración de GRUB 2

Después de crear los archivos de configuración, compruebe que la configuración sea correcta y que todos los archivos necesarios estén en su lugar.

PROCEDIMIENTO 10: PASOS DE VERIFICACIÓN

1. Compruebe la estructura de directorios de GRUB 2:

```
> find /srv/tftpboot/boot/grub2 -type f -name "*.cfg" -o -name "*.efi" -o -name
"core.*"
```

2. Verifique la sintaxis del archivo de configuración probando las herramientas de GRUB 2:

```
> grub2-script-check /srv/tftpboot/boot/grub2/grub.cfg
```

```
> grub2-script-check /srv/tftpboot/boot/grub2/menu.cfg
```

3. Asegúrese de que los permisos del archivo sean correctos:

```
> sudo chmod -R 644 /srv/tftpboot/boot/grub2/*.cfg
```

```
> sudo find /srv/tftpboot/boot/grub2 -type d -exec chmod 0755 {} \;
```



Importante: prueba de configuración

Pruebe la configuración de GRUB 2 con clientes PXE reales para garantizar que se detecta la arquitectura y que los menús funcionan de forma adecuada. La variable `net_default_mac` solo está disponible en situaciones de arranque de red reales.

6.7 Solución de problemas de configuración de GRUB 2

Aquí se explican los problemas comunes y sus soluciones cuando se trabaja con configuraciones PXE de GRUB 2. Cada problema incluye pasos de diagnóstico y comandos específicos para resolverlo.

6.7.1 La detección de la arquitectura falla

Si GRUB 2 no detecta la arquitectura correcta, los clientes pueden arrancar con binarios incorrectos o pueden incluso no cargarse.

PROCEDIMIENTO 11: DEPURACIÓN DE LA DETECCIÓN DE ARQUITECTURA

1. Añada la salida de depuración a la configuración de GRUB 2 para ver los valores detectados:

```
> sudo cat >> /srv/tftpboot/boot/grub2/grub.cfg << 'EOF'
# Debug architecture detection
echo "Detected grub_cpu: ${grub_cpu}"
echo "Mapped arch: ${arch}"
sleep 3
EOF
```

2. Pruebe la sintaxis de configuración:

```
> grub2-script-check /srv/tftpboot/boot/grub2/grub.cfg
```

3. Si la asignación de arquitectura está incompleta, extienda la lógica de detección:

```
> sudo sed -i '/elif \[ "$grub_cpu" == "powerpc" \]/a\nelif [ "$grub_cpu" ==  
"riscv64" ]; then\n set arch=\'\'riscv64\'\'\'\' /srv/tftpboot/boot/grub2/grub.cfg
```

4. Verifique que existen directorios específicos de la arquitectura:

```
> ls -la /srv/tftpboot/boot/grub2/
```

6.7.2 No se encuentra la interfaz de red

Es posible que algunas implementaciones de firmware no definan correctamente la variable `net_default_mac`, lo que provoca fallos de configuración de red.

PROCEDIMIENTO 12: DIAGNÓSTICO DE PROBLEMAS DE INTERFAZ DE RED

1. Añada la salida de depuración para comprobar las variables de red:

```
> sudo sed -i '/set ipcfg=/i\necho "Default MAC: ${net_default_mac}"\necho "Network  
variables set"\nsleep 2' /srv/tftpboot/boot/grub2/grub.cfg
```

2. Cree una configuración de red alternativa:

```
> sudo cat >> /srv/tftpboot/boot/grub2/grub.cfg << 'EOF'  
  
# Fallback network configuration if net_default_mac is empty  
if [ "X${net_default_mac}" == "X" ]; then  
 set ipcfg="ip=dhcp"  
 set ifcfg="ifcfg=*dhcp"  
 echo "WARNING: Using fallback network configuration"  
 sleep 2  
fi  
EOF
```

3. Pruebe la configuración de red con una interfaz específica:

```
> sudo echo 'set ipcfg="ip=en0:dhcp"' > /srv/tftpboot/boot/config/test-network.cfg
```

4. Verifique los nombres de interfaz de red en el sistema de destino:

```
> ip link show
```

6.7.3 No se encuentran las vías de los archivos

Si las vías son incorrectas, GRUB 2 no puede cargar los archivos de kernel e initrd, lo que provoca fallos de arranque.

PROCEDIMIENTO 13: VERIFICACIÓN DE LA ACCESIBILIDAD DE LA RUTA DE ARCHIVO

1. Compruebe si los archivos de instalador se encuentran en las ubicaciones esperadas:

```
> find /srv/tftpboot/boot/images -name "linux" -o -name "initrd" -o -name "squashfs.img"
```

2. Verifique el acceso TFTP a los archivos de arranque:

```
> tftp localhost -c get /boot/grub2/grub.cfg /tmp/test-grub.cfg
```

3. Pruebe el acceso HTTP a los archivos de instalador:

```
> curl -I http://localhost/boot/images/SLES-16.0/x86_64/linux
```

4. Compruebe los permisos y la propiedad del archivo:

```
> ls -la /srv/tftpboot/boot/images/SLES-16.0/*/
```

5. Corrija los permisos si fuera necesario:

```
> sudo chmod -R 644 /srv/tftpboot/boot/images/
```

```
> sudo find /srv/tftpboot/boot/images/ -type d -exec chmod 755 {} \;
```

6. Verifique que los enlaces simbólicos no estén rotos:

```
> find /srv/tftpboot/boot/images/ -type l -exec ls -la {} \;
```

6.7.4 Fallo de arranque EFI

Los problemas de EFI y del arranque seguro pueden impedir que el cargador de arranque se inicialice correctamente, o causar fallos de autenticación.

PROCEDIMIENTO 14: DIAGNÓSTICO DE PROBLEMAS DE ARRANQUE EFI

1. Verifique que los archivos de arranque seguro estén presentes:

```
> ls -la /srv/tftpboot/boot/grub2/x86_64-efi/*.efi
```

2. Compruebe que los archivos shim (bootx64.efi o shim.efi), grub.efi y MokManager.efi se copien correctamente:

```
> file /srv/tftpboot/boot/grub2/x86_64-efi/bootx64.efi
```

3. Verifique la integridad del archivo EFI:

```
> sha256sum /srv/tftpboot/boot/grub2/x86_64-efi/*.efi
```

4. Pruebe si se puede acceder a los archivos a través de TFTP:

```
> tftp localhost -c get /boot/grub2/x86_64-efi/bootx64.efi /tmp/test-shim.efi
```

5. Para los sistemas aarch64, verifique los archivos EFI ARM64:

```
> ls -la /srv/tftpboot/boot/grub2/arm64-efi/*.efi
```

6. Compruebe que la configuración de DHCP proporcione las vías correctas del cargador de arranque:

```
> grep -n "bootx64.efi\|shim.efi\|bootaa64.efi"  
/etc/dnsmasq.d/dhcp.conf /etc/kea/kea-dhcp?.conf /etc/dhcpd?.conf
```

7. Si faltan archivos, vuelva a copiarlos de la ISO montada en /mnt o de los archivos del paquete shim:

```
> sudo cp -v /mnt/EFI/B00T/*.efi /srv/tftpboot/boot/grub2/x86_64-efi/
```

```
> sudo cp -pL /usr/share/efi/x86_64/*.efi /srv/tftpboot/boot/grub2/x86_64-efi/
```

6.7.5 Las entradas de menú no se cargan

Si GRUB 2 se carga, pero las entradas del menú fallan o muestran errores, el problema a menudo está relacionado con la expansión variable o las referencias de archivos.

PROCEDIMIENTO 15: SOLUCIÓN DE PROBLEMAS DE ENTRADA DE MENÚ

1. Pruebe la sintaxis de configuración del menú:

```
> grub2-script-check /srv/tftpboot/boot/grub2/menu.cfg
```

2. Añada la salida de depuración a las entradas del menú:

```
> sudo sed -i '/linux_kernel.*{images}/i\\necho "Loading: ${images}/SLES-16.0/
${arch}/linux"\\necho "Architecture: ${arch}"' /srv/tftpboot/boot/grub2/menu.cfg
```

3. Verifique que la expansión variable funcione correctamente:

```
> sudo cat > /srv/tftpboot/boot/grub2/debug-menu.cfg << 'EOF'
menuentry 'Debug Variables' {
  echo "arch = ${arch}"
  echo "images = ${images}"
  echo "ipcfg = ${ipcfg}"
  sleep 5
}
EOF
```

4. Pruebe con una entrada de menú simplificada:

```
> sudo cat > /srv/tftpboot/boot/grub2/simple-menu.cfg << 'EOF'
menuentry 'Simple Test' {
  linux /boot/images/SLES-16.0/x86_64/linux
  initrd /boot/images/SLES-16.0/x86_64/initrd
}
EOF
```

5. Cargue el menú de prueba temporalmente:

```
> sudo sed -i 's|source "${prefix}/menu.cfg"|source "${prefix}/simple-menu.cfg"|' /
srv/tftpboot/boot/grub2/grub.cfg
```

6. Restaure el menú original después de la prueba:

```
> sudo sed -i 's|source "${prefix}/simple-menu.cfg"|source "${prefix}/menu.cfg"|' /
srv/tftpboot/boot/grub2/grub.cfg
```

6.7.6 Habilitación del registro detallado

Para problemas persistentes, habilite el registro exhaustivo para capturar información detallada sobre el proceso de arranque.

PROCEDIMIENTO 16: CONFIGURACIÓN DEL REGISTRO DE DEPURACIÓN DE GRUB 2

1. Cree una versión de depuración de la configuración principal:

```
> sudo cp /srv/tftpboot/boot/grub2/grub.cfg /srv/tftpboot/boot/grub2/grub.cfg.backup
```

2. Añada la salida de depuración completa:

```
> sudo cat > /srv/tftpboot/boot/grub2/debug.cfg << 'EOF'
# Debug configuration for GRUB troubleshooting
set debug=all
set pager=1

echo "=== GRUB Debug Information ==="
echo "grub_cpu: ${grub_cpu}"
echo "grub_platform: ${grub_platform}"
echo "net_default_mac: ${net_default_mac}"
echo "net_default_server: ${net_default_server}"
echo "======"
sleep 5
EOF
```

3. Incluya la configuración de depuración en el archivo principal:

```
> sudo sed -i 'li\source "${prefix}/debug.cfg"' /srv/tftpboot/boot/grub2/grub.cfg
```

4. Supervise los registros de TFTP durante los intentos de arranque:

```
> sudo journalctl -f -u tftp.socket
```

5. Supervise los registros de DHCP para solicitudes de PXE:

```
> sudo journalctl -f -u dhcpd
```

6. Desactive el modo de depuración después de solucionar el problema:

```
> sudo sed -i '/source "${prefix}\debug.cfg"/d' /srv/tftpboot/boot/grub2/grub.cfg
```

6.8 Pasos siguientes

Cuando GRUB 2 se haya configurado correctamente, puede proceder a:

- Configurar los servicios HTTP y TFTP para proporcionar los archivos de arranque y el contenido del instalador
- Configurar los servicios DHCP para dirigir a los clientes PXE a los cargadores de arranque apropiados
- Probar el proceso de arranque PXE completo en el hardware de destino

El sistema de configuración de GRUB 2 es muy flexible y sirve de base para crear escenarios de despliegue de PXE avanzados, que admitan múltiples arquitecturas y tipos de instalación mediante una interfaz unificada.

7 Configuración de TFTP para el arranque PXE

En esta sección se explica cómo configurar los servicios TFTP para que proporcionen contenido de los cargadores de arranque de GRUB 2 y de arranque PXE a las instalaciones de SUSE Linux Enterprise Server 16.0. Trata sobre el servidor `in.tftpd` tradicional y la funcionalidad de TFTP integrada suministrada por `dnsmasq`.

7.1 Introducción

TFTP proporciona archivos de arranque a clientes PXE durante el proceso de arranque de red. SUSE Linux Enterprise Server 16.0 admite dos implementaciones de servidor TFTP: el servidor `in.tftpd` tradicional del paquete `tftp` y la funcionalidad TFTP integrada dentro de `dnsmasq`.

7.2 Requisitos

- El paquete `tftp` o el paquete `dnsmasq` deben estar instalados
- Los archivos de arranque PXE deben estar organizados en `/srv/tftpboot`
- Privilegios administrativos para configurar servicios

7.3 Configuración del servidor `in.tftpd`

El servidor `in.tftpd` utiliza el archivo de configuración `/etc/sysconfig/tftp` para definir el sistema de archivos raíz TFTP y las opciones del servidor.

PROCEDIMIENTO 17: CONFIGURACIÓN DEL SERVIDOR TFTP IN.TFTPD

1. Opcionalmente, puede habilitar el registro detallado configurando las opciones de TFTP:

```
> sudo sed -i 's/^TFTP_OPTIONS=.*TFTP_OPTIONS="-v"/' /etc/sysconfig/tftp
```

La opción `-v` permite el registro detallado para ver los nombres de archivo obtenidos a través de TFTP.

2. Habilite e inicie el servicio TFTP:

```
> sudo systemctl enable --now tftp.service
```

7.4 Configuración del servidor TFTP dnsmasq

`dnsmasq` proporciona un servidor TFTP integrado que se puede habilitar y configurar para usar el directorio `/srv/tftpboot`.

PROCEDIMIENTO 18: CONFIGURACIÓN DE LA FUNCIONALIDAD TFTP DE DNSMASQ

1. Cree el archivo de configuración de TFTP:

```
> sudo cat > /etc/dnsmasq.d/tftp.conf << 'EOF'  
enable-tftp  
tftp-root=/srv/tftpboot  
EOF
```

2. Habilite e inicie el servicio `dnsmasq`:

```
> sudo systemctl enable --now dnsmasq
```

7.5 Verificación de la configuración de TFTP

Pruebe la funcionalidad del servidor TFTP para asegurarse de que puede proporcionar archivos a clientes PXE.

PROCEDIMIENTO 19: PRUEBA DE LA FUNCIONALIDAD DEL SERVIDOR TFTP

1. Cree un archivo de prueba:

```
> echo "test file" | sudo tee /srv/tftpboot/test.txt
```

2. Recupere el archivo de prueba a través de TFTP:

```
> tftp localhost -c get test.txt /tmp/tftp-test.txt
```

3. Verifique que el archivo se ha recuperado correctamente:

```
> cat /tmp/tftp-test.txt
```

4. Borre los archivos de prueba:

```
> sudo rm /srv/tftpboot/test.txt /tmp/tftp-test.txt
```

7.6 Solución de problemas de la configuración de TFTP

Estos son los problemas comunes al configurar servicios TFTP para entornos de arranque PXE.

7.6.1 Conflictos de servicio en el puerto 69

Tanto `in.tftpd` como `dnsmasq` utilizan el puerto UDP 69 para los servicios TFTP y no pueden ejecutarse simultáneamente.

PROCEDIMIENTO 20: RESOLUCIÓN DE CONFLICTOS DE SERVICIOS TFTP

1. Comprueba qué servicios se están ejecutando:

```
> systemctl status tftp.service dnsmasq
```

2. Compruebe cuál está usando el puerto 69:

```
> ss -ulnp | grep :69
```

3. Detenga el servicio conflictivo (ejemplo para dnsmasq):

```
> sudo systemctl stop dnsmasq
```

4. Inicie su servicio TFTP preferido:

```
> sudo systemctl start tftp.service
```

7.6.2 Problemas con el directorio TFTP

Los problemas de acceso al sistema de archivos raíz TFTP pueden impedir que los archivos se entreguen.

PROCEDIMIENTO 21: VERIFICACIÓN DE LA CONFIGURACIÓN DEL DIRECTORIO TFTP

1. Verifique la configuración del directorio TFTP para in.tftpd:

```
> grep TFTP_DIRECTORY /etc/sysconfig/tftp
```

2. Verifique la configuración del directorio TFTP para dnsmasq:

```
> grep tftp-root /etc/dnsmasq.d/tftp.conf
```

3. Compruebe si el directorio existe:

```
> ls -la /srv/tftpboot/
```

4. Cree la estructura de directorio, si no existe:

```
> sudo mkdir -p /srv/tftpboot
```

7.6.3 Habilitación del registro de TFTP

El registro detallado ayuda a identificar problemas de acceso a archivos con transferencias TFTP.

PROCEDIMIENTO 22: HABILITACIÓN DE UN REGISTRO DETALLADO DE TFTP

1. Compruebe las opciones de TFTP actuales:

```
> grep TFTP_OPTIONS /etc/sysconfig/tftp
```

2. Habilite el registro detallado:

```
> sudo sed -i 's/^TFTP_OPTIONS=.*TFTP_OPTIONS="-v"/' /etc/sysconfig/tftp
```

3. Reinicie el servicio TFTP:

```
> sudo systemctl restart tftp.service
```

4. Compruebe los registros de TFTP:

```
> journalctl -u tftp.service -f
```

7.7 Pasos siguientes

Con TFTP configurado, puede proceder a configurar los servicios HTTP para proporcionar archivos de instalador y servicios DHCP a fin de dirigir a los clientes PXE a los cargadores de arranque apropiados.

8 Configuración de nginx para la entrega HTTP

En esta sección se explica cómo configurar nginx para proporcionar contenido de arranque PXE a través de HTTP, lo que permite a los clientes cargar archivos de instalador como imágenes de kernel, initrd y squashfs desde una ubicación central. La entrega HTTP proporciona un mejor rendimiento que TFTP para archivos grandes y es necesaria para las instalaciones de SUSE Linux Enterprise Server 16.0 Agama.

8.1 Introducción

nginx sirve como servidor HTTP para entornos de arranque PXE, proporcionando acceso a archivos de instalador a través de la entrega basada en Web. El servidor HTTP expone el directorio de arranque TFTP y los repositorios de instalación, lo que permite a los clientes PXE descargar imágenes de kernel, archivos initrd y los componentes del instalador Agama a través de HTTP, en lugar de con el protocolo TFTP, que es más lento.

8.2 Requisitos

- El paquete `nginx` debe estar instalado
- Archivos de arranque PXE organizados en `/srv/tftpboot/boot`
- Repositorios de instalación disponibles en `/srv/install`
- Privilegios administrativos para modificar la configuración de nginx

8.3 Configuración de nginx para el arranque PXE

La configuración de nginx define los alias de ubicación que exponen el directorio de arranque TFTP y los repositorios de instalación a través de varias URL HTTP.

PROCEDIMIENTO 23: CONFIGURACIÓN DEL SERVIDOR HTTP NGINX

1. Edite el archivo de configuración de nginx:

```
> sudo vim /etc/nginx/nginx.conf
```

2. Configure el bloque del servidor HTTP en la sección `http`:

```
> sudo cat > /etc/nginx/nginx.conf << 'EOF'
http {

    include            mime.types;
    default_type      application/octet-stream;

    charset            utf-8;
    sendfile           on;
    keepalive_timeout 65;

    server {
        listen         80 default_server;
        listen         [::]:80 default_server;

        location / {
            root        /srv/www/htdocs/;
            index       index.html index.htm;
        }

        error_page     500 502 503 504 /50x.html;
        location = /50x.html {
            root        /srv/www/htdocs/;
        }

        # Expose TFTP boot directory for HTTP boot
        location /boot {
            alias        /srv/tftpboot/boot;
            autoindex   on;
        }

        # Expose installation repositories and profiles
        location /install {
            alias        /srv/install;
            autoindex   on;
        }
    }
}
```

```
    }  
  }  
}  
  
events {  
    worker_connections 1024;  
}  
EOF
```

3. Pruebe la sintaxis de configuración de nginx:

```
> sudo nginx -t
```

4. Habilite e inicie el servicio nginx:

```
> sudo systemctl enable --now nginx.service
```

8.4 Verificación de la configuración de nginx

Pruebe la funcionalidad del servidor HTTP para asegurarse de que puede proporcionar archivos de arranque PXE y contenido de instalación a los clientes.

PROCEDIMIENTO 24: PRUEBA DEL SERVIDOR HTTP NGINX

1. Pruebe el acceso HTTP a los archivos de arranque:

```
> curl -I http://localhost/boot/
```

2. Pruebe el acceso al directorio de instalación:

```
> curl -I http://localhost/install/
```

3. Compruebe que se pueda acceder a un archivo de instalación específico:

```
> curl -I http://localhost/boot/images/SLES-16.0/x86_64/liveiso/LiveOS/squashfs.img
```

8.5 Solución de problemas de configuración de nginx

Estos son los problemas comunes al configurar nginx para la entrega HTTP de arranque PXE.

8.5.1 Errores de sintaxis de configuración

Una sintaxis incorrecta de la configuración de nginx puede impedir que el servicio se inicie o se recargue correctamente.

PROCEDIMIENTO 25: SOLUCIÓN DE PROBLEMAS DE CONFIGURACIÓN DE NGINX

1. Pruebe la sintaxis de configuración:

```
> sudo nginx -t
```

2. Compruebe el estado del servicio nginx si falla el inicio:

```
> systemctl status nginx.service
```

3. Consulte los registros de error detallados:

```
> journalctl -u nginx.service -f
```

4. Compruebe el archivo de registro de errores de nginx:

```
> tail -f /var/log/nginx/error.log
```

8.5.2 Problemas de acceso a archivos y permisos

Puede que nginx no proporcione archivos porque haya permisos incorrectos o falten directorios.

PROCEDIMIENTO 26: SOLUCIÓN DE PROBLEMAS DE ACCESO A ARCHIVOS

1. Compruebe si el directorio de arranque existe y se puede acceder a él:

```
> ls -la /srv/tftpboot/boot/
```

2. Compruebe si existe el directorio install:

```
> ls -la /srv/install/
```

3. Verifique que nginx pueda leer los directorios:

```
> sudo -u nginx ls /srv/tftpboot/boot/
```

4. Cree los directorios que falten si es necesario:

```
> sudo mkdir -p /srv/install
```

5. Establezca los permisos apropiados:

```
> sudo chmod -R 755 /srv/tftpboot/boot /srv/install
```

8.5.3 Conflictos de vinculación de puertos

Puede que nginx no se inicie si otro servicio está utilizando el puerto 80.

PROCEDIMIENTO 27: RESOLUCIÓN DE CONFLICTOS DE PUERTO

1. Compruebe qué servicio está usando el puerto 80:

```
> ss -tlnp | grep :80
```

2. Detenga los servicios en conflicto si fuera necesario:

```
> sudo systemctl stop apache2
```

3. Inicie el servicio nginx:

```
> sudo systemctl start nginx.service
```

4. Verifique que nginx esté escuchando en el puerto 80:

```
> ss -tlnp | grep :80
```

8.6 Pasos siguientes

Cuando nginx esté configurado para la entrega HTTP, puede proceder a configurar los servicios DHCP para dirigir a los clientes PXE a los cargadores de arranque y recursos HTTP apropiados.

9 Configuración de un servidor DNS con dnsmasq

En esta sección se explica cómo configurar los servicios DNS mediante dnsmasq para proporcionar resolución de nombres de host a los clientes PXE que acceden a los recursos de instalación de SUSE Linux Enterprise Server 16.0. La configuración de DNS permite a los clientes usar nombres de host en lugar de direcciones IP en las URL de arranque y configuraciones DHCP.

9.1 Introducción

Los servicios DNS permiten a los clientes PXE resolver nombres de host en las URL de arranque y en orígenes de instalación. Aunque la configuración completa del servidor DNS está fuera del alcance de este documento, esta sección proporciona una configuración DNS básica mediante `dnsmasq` que permite a los clientes resolver el nombre de host (`PXE.EXAMPLE.NET`) del servidor PXE a sus direcciones IP.

Sin la configuración DNS, las URL de arranque deben usar direcciones IP directamente, como `http://192.168.1.200/` o `http://[2001:db8:0:1::200]/`. Algunas implementaciones de firmware BIOS/UEFI no admiten nombres de host en las URL TFTP DHCP y requieren direcciones IP como `tftp://[2001:db8:0:1::200]/`.

9.2 Requisitos

- El paquete `dnsmasq` debe estar instalado
- Direcciones IP estáticas configuradas para el servidor PXE
- Privilegios administrativos para configurar servicios DNS

9.3 Configuración de los servicios DNS de `dnsmasq`

La configuración de DNS de `dnsmasq` proporciona resolución de nombres de host local y utiliza servidores de nombres ascendentes para consultas externas.

PROCEDIMIENTO 28: CONFIGURACIÓN DEL SERVIDOR DNS DNSMASQ

1. Cree el archivo de configuración de DNS para `dnsmasq`:

```
> sudo cat > /etc/dnsmasq.d/dns.conf << 'EOF'
# DNS configuration file for dnsmasq

# Log DNS queries
log-queries

# DNS cache behavior
cache-size=10000
local-ttl=60
neg-ttl=10

# Never forward A or AAAA queries for plain names to upstream name servers
```

```
domain-needed

# Add local domain to simple names in /etc/hosts and DHCP
expand-hosts

# Specifies DNS domain and networks including local forward and reverse declarations
domain=EXAMPLE.NET,192.168.1.0/24,local
domain=EXAMPLE.NET,2001:db8:0:1::/64,local
EOF
```

2. Añada entradas de nombre de host al archivo de hosts del sistema:

```
> sudo cat >> /etc/hosts << 'EOF'
192.168.1.200 PXE.EXAMPLE.NET
2001:db8:0:1::200 PXE.EXAMPLE.NET
EOF
```

3. Pruebe la configuración de dnsmasq:

```
> sudo dnsmasq --test
```

4. Habilite e inicie el servicio dnsmasq:

```
> sudo systemctl enable --now dnsmasq
```



Nota: comportamiento de reenvío DNS

De forma predeterminada, dnsmasq utiliza los servidores de nombres en `/etc/resolv.conf` como reenviadores y proporciona registros de `/etc/hosts`. Esto permite al servidor PXE resolver nombres de host externos mientras proporciona resolución local para servicios relacionados con PXE.

9.4 Verificación de la configuración de DNS

Pruebe la funcionalidad del servidor DNS para garantizar que la resolución de nombres de host funcione para clientes PXE.

PROCEDIMIENTO 29: PRUEBA DE LA FUNCIONALIDAD DEL SERVIDOR DNS

1. Pruebe la resolución de nombres de host IPv4:

```
> nslookup PXE.EXAMPLE.NET localhost
```

2. Pruebe la resolución de nombres de host IPv6:

```
> nslookup PXE.EXAMPLE.NET localhost | grep 2001:db8
```

3. Pruebe la búsqueda DNS inversa para IPv4:

```
> nslookup 192.168.1.200 localhost
```

4. Compruebe que el reenvío DNS externo siga funcionando:

```
> nslookup google.com localhost
```

9.5 Solución de problemas de configuración de DNS

Estos son los problemas comunes al configurar dnsmasq para servicios DNS en entornos PXE.

9.5.1 Problemas de configuración y servicio

Puede que dnsmasq no se inicie debido a errores de configuración o conflictos de puertos.

PROCEDIMIENTO 30: SOLUCIÓN DE PROBLEMAS DE CONFIGURACIÓN DE DNS

1. Pruebe la sintaxis de configuración de dnsmasq:

```
> sudo dnsmasq --test
```

2. Compruebe el estado del servicio dnsmasq:

```
> systemctl status dnsmasq
```

3. Compruebe qué servicio está usando el puerto DNS 53:

```
> ss -ulnp | grep :53
```

4. Consulte si hay errores en los registros de dnsmasq:

```
> journalctl -u dnsmasq -f
```

5. Detenga los servicios DNS en conflicto si fuera necesario:

```
> sudo systemctl stop systemd-resolved
```

9.5.2 Fallos en la resolución de nombres de host

Las consultas DNS pueden fallar porque la configuración sea incorrecta o porque falten entradas de nombre de host.

PROCEDIMIENTO 31: DIAGNÓSTICO DE PROBLEMAS DE RESOLUCIÓN DE DNS

1. Compruebe si existen entradas de nombre de host en el archivo de hosts:

```
> grep PXE.EXAMPLE.NET /etc/hosts
```

2. Verifique la configuración del dominio en dnsmasq:

```
> grep domain= /etc/dnsmasq.d/dns.conf
```

3. Pruebe la consulta DNS con salida detallada:

```
> dig @localhost PXE.EXAMPLE.NET
```

4. Consulte los registros de consultas de dnsmasq:

```
> journalctl -u dnsmasq | grep "query"
```

5. Reinicie dnsmasq para volver a cargar la configuración:

```
> sudo systemctl restart dnsmasq
```

9.5.3 Problemas de reenvío DNS

Las consultas DNS externas pueden fallar si la configuración del servidor de nombres ascendente es incorrecta.

PROCEDIMIENTO 32: SOLUCIÓN DE PROBLEMAS DE REENVÍO DNS

1. Compruebe la configuración del servidor de nombres ascendente:

```
> cat /etc/resolv.conf
```

2. Pruebe la consulta directa al servidor de nombres ascendente:

```
> nslookup google.com 8.8.8.8
```

3. Compruebe la configuración de reenvío de dnsmasq:

```
> grep -E "server=|no-resolv" /etc/dnsmasq.d/dns.conf
```

4. Añada un servidor de nombres ascendente específico si fuera necesario:

```
> sudo echo "server=8.8.8.8" >> /etc/dnsmasq.d/dns.conf
```

5. Reinicie el servicio dnsmasq:

```
> sudo systemctl restart dnsmasq
```

9.6 Pasos siguientes

Con los servicios DNS configurados, los clientes PXE ahora pueden resolver nombres de host en las URL de arranque y en orígenes de instalación. Puede proceder a configurar los servicios DHCP que hacen referencia al servidor DNS para la configuración del cliente.

10 Configuración de un servidor NTP con chrony

En esta sección se explica cómo configurar los servicios NTP mediante chrony para proporcionar una sincronización horaria precisa a los clientes PXE durante las instalaciones de SUSE Linux Enterprise Server 16.0. Sincronizar adecuadamente la hora es esencial para la validación de certificados y el registro del sistema durante las instalaciones basadas en red.

10.1 Introducción

Los servicios NTP garantizan una sincronización de hora precisa en toda la infraestructura de red. Para entornos de arranque PXE, que la hora esté sincronizada es crucial para la validación de certificados durante las conexiones HTTPS, para tener marcas de tiempo de registro adecuadas y en las operaciones coordinadas del sistema. Esta sección proporciona la configuración básica del servidor NTP mediante chrony.

10.2 Requisitos

- El paquete chrony debe estar instalado

```
> sudo zypper install chrony
```

- Conectividad de red a servidores NTP ascendentes
- Privilegios administrativos para configurar servicios NTP

10.3 Configuración del servicio NTP con chrony.

El servicio `chrony` proporciona funcionalidad NTP con sincronización horaria automática a servidores ascendentes y capacidades de provisión de hora local para clientes de red.

PROCEDIMIENTO 33: CONFIGURACIÓN DEL SERVIDOR TFTP CON `chrony`

- Habilite e inicie el servicio `chrony`:

```
> sudo systemctl enable --now chronyd.service
```

10.4 Verificación de la configuración de NTP

Pruebe la funcionalidad del servicio NTP para garantizar que la sincronización horaria funcione correctamente.

PROCEDIMIENTO 34: PRUEBA DE LA FUNCIONALIDAD DEL SERVIDOR NTP

1. Compruebe el estado del servicio `chrony`:

```
> systemctl status chronyd.service
```

2. Consulte el estado de sincronización de hora actual:

```
> chronyc tracking
```

3. Muestre las fuentes NTP configuradas:

```
> chronyc sources
```

4. Consulte las estadísticas del servidor NTP:

```
> chronyc sourcestats
```

10.5 Solución de problemas de configuración de NTP

Estos son los problemas comunes al configurar `chrony` para servicios NTP en entornos PXE.

10.5.1 Problemas de inicio del servicio

El servicio `chrony` puede no iniciarse debido a errores de configuración o problemas de conectividad de red.

PROCEDIMIENTO 35: SOLUCIÓN DE PROBLEMAS DEL SERVICIO NTP

1. Compruebe el estado del servicio `chrony` y los registros:

```
> systemctl status chronyd.service
```

2. Consulte los registros de servicio detallados:

```
> journalctl -u chronyd.service -f
```

3. Pruebe la configuración de `chrony`:

```
> sudo chronyd -Q
```

4. Si es necesario, reinicie el servicio:

```
> sudo systemctl restart chronyd.service
```

10.5.2 Fallos de sincronización horaria

La sincronización horaria puede fallar debido a problemas de red o a una configuración incorrecta del servidor.

PROCEDIMIENTO 36: DIAGNÓSTICO DE PROBLEMAS DE SINCRONIZACIÓN HORARIA

1. Consulte el estado actual de la sincronización:

```
> chronyc tracking
```

2. Consulte la conectividad del origen NTP:

```
> chronyc sources -v
```

3. Fuerce una sincronización inmediata:

```
> sudo chronyc makestep
```

4. Compare la hora del sistema con la del reloj de hardware:

```
> timedatectl status
```

5. Verifique la conectividad de red a los servidores NTP:

```
> chronyc activity
```

10.5.3 Problemas del firewall y la red

El tráfico NTP puede estar bloqueado por reglas del firewall que impidan la sincronización horaria.

PROCEDIMIENTO 37: RESOLUCIÓN DE PROBLEMAS DE CONECTIVIDAD DE RED

1. Compruebe si el puerto NTP está abierto en el firewall:

```
> firewall-cmd --list-services | grep ntp
```

2. Añada el servicio NTP al firewall si fuera necesario:

```
> sudo firewall-cmd --permanent --add-service=ntp
```

3. Vuelva a cargar la configuración del firewall:

```
> sudo firewall-cmd --reload
```

4. Pruebe manualmente la conectividad NTP:

```
> ntpdate -q pool.ntp.org
```

5. Compruebe el uso del puerto `chrony`:

```
> ss -ulnp | grep :123
```

10.6 Pasos siguientes

Con los servicios NTP configurados, el servidor PXE y los clientes mantendrán una sincronización horaria precisa. Esto garantiza una validación de certificados adecuada y operaciones coordinadas del sistema durante las instalaciones basadas en la red.

11 Configuración de anuncios de router IPv6

En esta sección se describe cómo configurar la funcionalidad de anuncios de router IPv6 para proporcionar anuncios de router adecuados para los clientes PXE. Los anuncios de router IPv6 permiten la configuración de enrutamiento IPv6 y la configuración automática de direcciones DHCPv6 con estado para las instalaciones de SUSE Linux Enterprise Server 16.0.

11.1 Introducción

Los anuncios de router IPv6 proporcionan información esencial de configuración de red a los clientes PXE, incluidos el enrutamiento IPv6 y los ajustes de configuración automática de direcciones DHCPv6. En esta sección se presupone que hay un router IPv6 configurado para proporcionar anuncios de router adecuados a fin de configurar el enrutamiento IPv6 a la red y la vía predeterminada, así como para habilitar la configuración automática de direcciones DHCPv6 con estado mediante `AdvManagedFlag on`.

11.2 Requisitos

- El paquete `radvd` debe estar instalado
- Configuración de red IPv6 en la interfaz de servidor
- Privilegios administrativos para configurar los servicios de anuncios de router

11.3 Configuración de `radvd` para los anuncios de router IPv6

El servicio `radvd` proporciona la funcionalidad de anuncios de router IPv6 mediante la configuración definida en `/etc/radvd.conf`.

1. Configure el servicio `radvd`:

```
> sudo cat > /etc/radvd.conf << 'EOF'
interface en01
{
    # radvd options
    IgnoreIfMissing on;           # Do not fail and exit when interface is
missed
    AdvSendAdvert on;           # Sending RAs on the interface is not
disabled

    # Configuration settings

    AdvManagedFlag on;         # Request IPv6 address and dns options via
DHCPv6
    AdvOtherConfigFlag off;     # Request only dns info via DHCPv6, IP via
SLAAC

    AdvDefaultLifetime 1800;    # Add default route via this router for
1800sec

    prefix 2001:db8:0:1::/64    # Add direct route for this local network/
prefix
    {
        AdvAutonomous          off; # Assign IPv6 address via SLAAC
        AdvValidLifetime        7200;
        AdvPreferredLifetime    3600;
    };
};
EOF
```

2. Habilite e inicie el servicio `radvd`:

```
> sudo systemctl enable --now radvd
```

11.4 Verificación de los anuncios de router IPv6

Pruebe la funcionalidad de anuncios de router IPv6 para garantizar una configuración y un funcionamiento adecuados.

1. Compruebe el estado del servicio `radvd`:

```
> systemctl status radvd
```

2. Revise y verifique la configuración de los anuncios de router IPv6 mediante `radvdump`:

```
> radvdump
```

La utilidad `radvdump` muestra la configuración de anuncios de router de IPv6 enviada por el router IPv6 cada pocos minutos.

11.5 Configuración de reenvío de IP para la funcionalidad del router

Si el servidor PXE también actúa como router, el reenvío de IP debe estar habilitado para permitir que el sistema funcione con dicho rol.

1. Cree el archivo de configuración de red:

```
> sudo cat > /etc/sysctl.d/90-network.conf << 'EOF'
# This machine is a router
net.ipv4.conf.all.forwarding = 1
net.ipv6.conf.all.forwarding = 1

# Accept host autoconf on router uplink
net.ipv6.conf.uplink.accept_ra = 2
EOF
```

2. Aplique la configuración de la red:

```
> sudo sysctl -p /etc/sysctl.d/90-network.conf
```



Nota: asunto a tener en cuenta sobre la configuración del router

Un router no procesa por defecto los anuncios de router IPv6 para la configuración automática del host. Para aceptar los anuncios de router IPv6 en una interfaz de enlace ascendente de router, es preciso el ajuste `accept_ra = 2` de `sysctl`. Consulte la

sección sobre la configuración de la red en la Guía de administración para obtener más detalles sobre la configuración del router, incluidos los ajustes del firewall y otros pasos necesarios.

11.6 Solución de problemas de anuncios de router IPv6

Estos son los problemas comunes al configurar los anuncios de router IPv6 en entornos PXE.

11.6.1 Problemas del servicio radvd

El servicio `radvd` puede no iniciarse debido a errores de configuración o problemas de la interfaz.

PROCEDIMIENTO 41: SOLUCIÓN DE PROBLEMAS DEL SERVICIO `radvd`

1. Compruebe el estado del servicio `radvd` y los registros:

```
> systemctl status radvd
```

2. Consulte los registros de servicio detallados:

```
> journalctl -u radvd -f
```

3. Pruebe la sintaxis de configuración de `radvd`:

```
> sudo radvd -C /etc/radvd.conf
```

4. Compruebe si existe la interfaz especificada:

```
> ip link show eno1
```

5. Reinicie el servicio después de arreglar la configuración:

```
> sudo systemctl restart radvd
```

11.6.2 Problemas de configuración de reenvío de IP

Si la configuración de reenvío de IP es incorrecta, el router podría no funcionar de forma adecuada.

PROCEDIMIENTO 42: DIAGNÓSTICO DE PROBLEMAS DE REENVÍO DE IP

1. Compruebe el estado actual del reenvío de IP:

```
> sysctl net.ipv4.conf.all.forwarding
```

2. Compruebe el estado de reenvío de IPv6:

```
> sysctl net.ipv6.conf.all.forwarding
```

3. Verifique el archivo de configuración de sysctl:

```
> cat /etc/sysctl.d/90-network.conf
```

4. Si los valores no son correctos, aplique la configuración:

```
> sudo sysctl -p /etc/sysctl.d/90-network.conf
```

5. Compruebe el ajuste `accept_ra` en la interfaz del enlace ascendente:

```
> sysctl net.ipv6.conf.uplink.accept_ra
```

11.6.3 Problemas de recepción de anuncios de router

Es posible que los clientes no reciban o procesen correctamente los anuncios de router IPv6.

PROCEDIMIENTO 43: SOLUCIÓN DE PROBLEMAS DE RECEPCIÓN DE ANUNCIOS DE ROUTER

1. Supervise los anuncios de router con `radvdump`:

```
> radvdump -d
```

2. Compruebe la configuración de la interfaz IPv6 en los clientes:

```
> ip -6 addr show
```

3. Verifique la tabla de enrutamiento IPv6 en los clientes:

```
> ip -6 route show
```

4. Pruebe la conectividad IPv6 al router:

```
> ping6 2001:db8:0:1::1
```

5. Compruebe las reglas del firewall para ICMPv6:

```
> firewall-cmd --list-protocols | grep ipv6-icmp
```

11.7 Pasos siguientes

Con los anuncios de router IPv6 configurados, los clientes PXE pueden recibir una configuración de red IPv6 adecuada. Esto permite la funcionalidad de DHCPv6 y la conectividad IPv6 para instalaciones basadas en red.

12 Configuración de un servidor DHCP con dnsmasq

En esta sección se explica cómo configurar los servicios DHCP mediante dnsmasq para proporcionar configuración de red e información de arranque PXE para las instalaciones de SUSE Linux Enterprise Server 16.0. El servidor DHCP dnsmasq utiliza una configuración basada en etiquetas para admitir clientes PXE IPv4 e IPv6 con capacidades de arranque UEFI y BIOS.

12.1 Introducción

El servidor DHCP dnsmasq proporciona configuración de red e información de archivos de arranque a clientes PXE mediante un sistema basado en etiquetas que se corresponden con los tipos de clientes y proporcionan los cargadores de arranque adecuados. Esta configuración admite correspondencias de PXEClient y HTTPClient que funcionan para DHCPv4 y DHCPv6, lo que permite el arranque a través de sistemas UEFI y BIOS en múltiples arquitecturas.



Importante: limitaciones de HTTPClient en dnsmasq

En dnsmasq 2.90 y versiones anteriores, no se admite el envío de la clase de proveedor option6:16 de vuelta a los clientes DHCPv6 para configuraciones de HTTPClient. Para obtener compatibilidad completa con HTTPClient, plantéese usar los servidores Kea o ISC DHCP.

12.2 Requisitos

- El paquete `dnsmasq` debe estar instalado
- Archivos de arranque PXE correctamente organizados en `/srv/tftpboot`
- Interfaz de red configurada para el servicio DHCP
- Privilegios administrativos para configurar servicios DHCP

12.3 Configuración de los servicios DHCP con dnsmasq

La configuración de DHCP con dnsmasq incluye la correspondencia del tipo de cliente, los intervalos de red y las asignaciones de archivos de arranque para redes IPv4 e IPv6.

PROCEDIMIENTO 44: CONFIGURACIÓN DEL SERVIDOR DHCP CON DNSMASQ

1. Cree el archivo de configuración de DHCP para dnsmasq:

```
> sudo cat > /etc/dnsmasq.d/dhcp.conf << 'EOF'
# DHCP configuration file for dnsmasq

# Log DHCP processing
log-dhcp

# This is the only DHCP server, don't ignore unknown clients/send NAK
dhcp-authoritative

# Disable re-use of the DHCPv4 servername and filename fields as extra
# option space, which may confuse old or broken clients
dhcp-no-override

# IPv4 PXE/HTTP boot client matches (no enterprise number)
# Match client type in PXEClient:Arch and map to a tag
dhcp-vendorclass=set:tftp_bios_x86_pc,PXEClient:Arch:00000
dhcp-vendorclass=set:tftp_uefi_x86_64,PXEClient:Arch:00007
dhcp-vendorclass=set:tftp_ieee_ppc_64,PXEClient:Arch:0000e
dhcp-vendorclass=set:tftp_uefi_arm_64,PXEClient:Arch:00011
# Match client type in HTTPClient:Arch and map to a tag
dhcp-vendorclass=set:http_uefi_x86_64,HTTPClient:Arch:00016
dhcp-vendorclass=set:http_uefi_arm_64,HTTPClient:Arch:00019

# IPv6 PXE/HTTP boot client matches (enterprise:343 intel)
# Match client type in PXEClient:Arch and map to a tag
```

```
dhcp-vendorclass=set:tftp_bios_x86_pc,enterprise:343,PXEClient:Arch:00000
dhcp-vendorclass=set:tftp_uefi_x86_64,enterprise:343,PXEClient:Arch:00007
dhcp-vendorclass=set:tftp_ieee_ppc_64,enterprise:343,PXEClient:Arch:0000e
dhcp-vendorclass=set:tftp_uefi_arm_64,enterprise:343,PXEClient:Arch:00011
# Match client type in HTTPClient:Arch and map to a tag
dhcp-vendorclass=set:http_uefi_x86_64,enterprise:343,HTTPClient:Arch:00016
dhcp-vendorclass=set:http_uefi_arm_64,enterprise:343,HTTPClient:Arch:00019
EOF
```

2. Configure el intervalo y las opciones de DHCP de IPv4:

```
> sudo cat >> /etc/dnsmasq.d/dhcp.conf << 'EOF'

# IPv4 range and options
dhcp-range=set:net0v4,192.168.1.100,192.168.1.199,255.255.255.0,1h
dhcp-option=tag:net0v4,option:domain-search,example.net
dhcp-option=tag:net0v4,option:dns-server,192.168.1.200
dhcp-option=tag:net0v4,option:ntp-server,192.168.1.1
dhcp-option=tag:net0v4,option:router,192.168.1.1
EOF
```

3. Configure las opciones de arranque PXE de IPv4:

```
> sudo cat >> /etc/dnsmasq.d/dhcp.conf << 'EOF'

# IPv4 PXEClient boot
dhcp-boot=tag:net0v4,tag:tftp_bios_x86_pc,/boot/grub2/i386-pc/core.0,192.168.1.200
dhcp-boot=tag:net0v4,tag:tftp_uefi_x86_64,/boot/grub2/x86_64-efi/
bootx64.efi,192.168.1.200
dhcp-boot=tag:net0v4,tag:tftp_ieee_ppc_64,/boot/grub2/powerpc-ieee1275/
core.elf,192.168.1.200
dhcp-boot=tag:net0v4,tag:tftp_uefi_arm_64,/boot/grub2/arm64-efi/
bootaa64.efi,192.168.1.200

# IPv4 HTTPClient boot
dhcp-option-force=tag:net0v4,tag:http_uefi_x86_64,option:vendor-class,HTTPClient
dhcp-boot=tag:net0v4,tag:http_uefi_x86_64,http://192.168.1.200/boot/grub2/x86_64-
efi/bootx64.efi
dhcp-option-force=tag:net0v4,tag:http_uefi_arm_64,option:vendor-class,HTTPClient
dhcp-boot=tag:net0v4,tag:http_uefi_arm_64,http://192.168.1.200/boot/grub2/arm64-efi/
bootaa64.efi
EOF
```

4. Configure el intervalo y las opciones de DHCP de IPv6:

```
> sudo cat >> /etc/dnsmasq.d/dhcp.conf << 'EOF'
```

```
# IPv6 range and options
dhcp-range=set:net0v6,2001:db8:0:1:d::,2001:db8:0:1:d::ffff,64,1h
dhcp-option=tag:net0v6,option6:domain-search,example.net
dhcp-option=tag:net0v6,option6:dns-server,[2001:db8:0:1::200]
dhcp-option=tag:net0v6,option6:sntp-server,[2001:db8:0:1::1]
EOF
```

5. Configure las opciones de arranque PXE de IPv6:

```
> sudo cat >> /etc/dnsmasq.d/dhcp.conf << 'EOF'

# IPv6 PXEClient boot
dhcp-option=tag:net0v6,tag:tftp_bios_x86_pc,option6:bootfile-url,tftp://
[2001:db8:0:1::200]/boot/grub2/i386-pc/core.0
dhcp-option=tag:net0v6,tag:tftp_uefi_x86_64,option6:bootfile-url,tftp://
[2001:db8:0:1::200]/boot/grub2/x86_64-efi/bootx64.efi
dhcp-option=tag:net0v6,tag:tftp_ieee_ppc_64,option6:bootfile-url,tftp://
[2001:db8:0:1::200]/boot/grub2/powerpc-ieee1275/core.elf
dhcp-option=tag:net0v6,tag:tftp_uefi_arm_64,option6:bootfile-url,tftp://
[2001:db8:0:1::200]/boot/grub2/arm64-efi/bootaa64.efi

# IPv6 HTTPClient boot
# Note: dnsmasq <= 2.90 does not support sending vendor-class option6:16 back to
client
EOF
```

6. Pruebe la configuración de dnsmasq:

```
> sudo dnsmasq --test
```

7. Habilite e inicie el servicio dnsmasq:

```
> sudo systemctl enable --now dnsmasq
```

12.4 Verificación de la configuración de DHCP

Pruebe la funcionalidad del servidor DHCP para garantizar una configuración de red adecuada y la entrega de archivos de arranque a clientes PXE.

PROCEDIMIENTO 45: PRUEBA DEL SERVIDOR DHCP DNSMASQ

1. Compruebe el estado del servicio dnsmasq:

```
> systemctl status dnsmasq
```

2. Verifique la vinculación de puertos DHCP:

```
> ss -u lnp | grep :67
```

3. Supervise las asignaciones de concesión de DHCP:

```
> journalctl -u dnsmasq -f
```

4. Compruebe las concesiones de DHCP activas:

```
> cat /var/lib/dhcp/dhcpd.leases
```

12.5 Solución de problemas de configuración de DHCP de dnsmasq

Estos son los problemas comunes al configurar dnsmasq para servicios DHCP en entornos PXE.

12.5.1 Problemas de inicio y configuración del servicio

Puede que dnsmasq no se inicie debido a errores de configuración o conflictos de puertos con otros servicios DHCP.

PROCEDIMIENTO 46: SOLUCIÓN DE PROBLEMAS DE SERVICIO DHCP DE DNSMASQ

1. Pruebe la sintaxis de configuración de dnsmasq:

```
> sudo dnsmasq --test
```

2. Compruebe si hay conflictos de puertos DHCP:

```
> ss -u lnp | grep :67
```

3. Detenga los servicios DHCP en conflicto:

```
> sudo systemctl stop dhcpd
```

4. Consulte los registros de servicio detallados:

```
> journalctl -u dnsmasq -f
```

5. Reinicie dnsmasq después de resolver los conflictos:

```
> sudo systemctl restart dnsmasq
```

12.5.2 Problemas de asignación de concesión de DHCP

Puede que los clientes no reciban direcciones IP debido a problemas de configuración del intervalo o la conectividad de la red.

PROCEDIMIENTO 47: DIAGNÓSTICO DE PROBLEMAS DE CONCESIÓN DE DHCP

1. Compruebe la configuración del intervalo de DHCP:

```
> grep dhcp-range /etc/dnsmasq.d/dhcp.conf
```

2. Supervise las solicitudes DHCP en tiempo real:

```
> journalctl -u dnsmasq -f | grep DHCP
```

3. Compruebe el estado de la interfaz de red:

```
> ip addr show
```

4. Verifique la configuración autorizada de DHCP:

```
> grep dhcp-authoritative /etc/dnsmasq.d/dhcp.conf
```

5. Pruebe la respuesta DHCP con dhcping:

```
> dhcping -s 192.168.1.200
```

12.5.3 Problemas de entrega de archivos de arranque PXE

Los clientes PXE pueden recibir direcciones IP, pero no pueden arrancar debido a una configuración incorrecta del archivo de arranque o problemas de correspondencia de tipos de cliente.

PROCEDIMIENTO 48: SOLUCIÓN DE PROBLEMAS DE CONFIGURACIÓN DE ARRANQUE PXE

1. Compruebe que la clase de proveedor cliente coincida:

```
> grep dhcp-vendorclass /etc/dnsmasq.d/dhcp.conf
```

2. Verifique las vías del archivo de arranque:

```
> grep dhcp-boot /etc/dnsmasq.d/dhcp.conf
```

3. Pruebe el acceso TFTP a los archivos de arranque:

```
> tftp 192.168.1.200 -c get /boot/grub2/x86_64-efi/bootx64.efi
```

4. Consulte los registros de DHCP específicos de PXE:

```
> journalctl -u dnsmasq | grep -E "PXE|HTTP"
```

5. Compruebe la asignación de etiquetas en los registros:

```
> journalctl -u dnsmasq | grep "tags:"
```

12.5.4 Problemas de configuración de DHCP de IPv6

Los clientes DHCP IPv6 requieren una configuración adecuada de los anuncios de router y pueden tener requisitos de direccionamiento diferentes a IPv4.

PROCEDIMIENTO 49: RESOLUCIÓN DE PROBLEMAS DE DHCP IPv6

1. Verifique la configuración del intervalo de DHCP de IPv6:

```
> grep "2001:db8" /etc/dnsmasq.d/dhcp.conf
```

2. Compruebe el estado de los anuncios de router IPv6:

```
> systemctl status radvd
```

3. Supervise las solicitudes DHCPv6:

```
> journalctl -u dnsmasq | grep "DHCPv6"
```

4. Pruebe la conectividad IPv6:

```
> ping6 2001:db8:0:1::200
```

5. Compruebe la configuración de la opción IPv6:

```
> grep option6 /etc/dnsmasq.d/dhcp.conf
```

12.6 Pasos siguientes

Con los servicios DHCP de dnsmasq configurados, los clientes PXE pueden recibir la configuración de red y la información del archivo de arranque para entornos IPv4 e IPv6. El sistema basado en etiquetas proporciona una asignación flexible de archivos de arranque basada en la arquitectura del cliente y los requisitos del método de arranque.

13 Configuración de un servidor DHCP con Kea

En esta sección se explica cómo configurar los servicios DHCP mediante Kea para proporcionar información de configuración de red y arranque PXE para las instalaciones de SUSE Linux Enterprise Server 16.0. Kea es un servidor DHCP moderno que admite tanto IPv4 como IPv6 con correspondencia de clases de clientes para escenarios de arranque PXE y HTTP.

13.1 Introducción

Kea es el servidor DHCP moderno desarrollado por ISC como sucesor del servidor ISC DHCP heredado. Proporciona una compatibilidad robusta tanto para DHCPv4 como para DHCPv6 con capacidades de clasificación de clientes que permiten la entrega adecuada de archivos de arranque basados en la arquitectura y el método de arranque del cliente. Kea utiliza archivos de configuración basados en JSON y admite funciones avanzadas como la identificación de la clase del proveedor para el arranque HTTP.

13.2 Requisitos

- Paquetes DHCP de Kea instalados: `kea-dhcp4` y `kea-dhcp6`
- Archivos de arranque PXE correctamente organizados en `/srv/tftpboot`
- Interfaz de red configurada para el servicio DHCP
- Privilegios administrativos para configurar servicios DHCP

13.3 Configuración del servidor DHCPv4 de Kea

La configuración de DHCPv4 de Kea utiliza clases de cliente que se corresponden con los tipos de cliente PXE y HTTP para proporcionar archivos de arranque apropiados para diferentes arquitecturas.

PROCEDIMIENTO 50: CONFIGURACIÓN DEL SERVIDOR DHCPV4 DE KEA

1. Configure el servidor DHCPv4 de Kea:

```
> sudo cat > /etc/kea/kea-dhcp4.conf << 'EOF'
```

```

{
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [
        "enol"
      ]
    },
    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/tmp/kea4-ctrl-socket"
    },
    "lease-database": {
      "type": "memfile",
      "persist": true,
      "name": "/var/lib/kea/dhcp4.leases",
      "lfc-interval": 3600
    },
    "expired-leases-processing": {
      "reclaim-timer-wait-time": 10,
      "flush-reclaimed-timer-wait-time": 25,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 250,
      "unwarned-reclaim-cycles": 5
    },
    "renew-timer": 1800,
    "rebind-timer": 3150,
    "valid-lifetime": 3600,
    "option-data": [],
    "client-classes": [
      {
        "name": "pxeclients#00000",
        "test": "substring(option[60].hex,0,20) == 'PXEClient:Arch:00000'",
        "next-server": "192.168.1.200",
        "boot-file-name": "/boot/grub2/i386-pc/core.0"
      },
      {
        "name": "pxeclients#00007",
        "test": "substring(option[60].hex,0,20) == 'PXEClient:Arch:00007'",
        "next-server": "192.168.1.200",
        "boot-file-name": "/boot/grub2/x86_64-efi/bootx64.efi"
      },
      {
        "name": "pxeclients#0000e",
        "test": "substring(option[60].hex,0,20) == 'PXEClient:Arch:0000e'",
        "next-server": "192.168.1.200",
        "boot-file-name": "/boot/grub2/powerpc-ieee1275/core.elf"
      }
    ]
  }
}

```

```

    },
    {
      "name": "pxeclients#00011",
      "test": "substring(option[60].hex,0,20) == 'PXEClient:Arch:00011'",
      "next-server": "192.168.1.200",
      "boot-file-name": "/boot/grub2/arm64-efi/bootaa64.efi"
    },
    {
      "name": "httpclients#00016",
      "test": "substring(option[60].hex,0,21) == 'HTTPClient:Arch:00016'",
      "boot-file-name": "http://192.168.1.200/boot/grub2/x86_64-efi/bootx64.efi",
      "option-data": [
        {
          "name": "vendor-class-identifier",
          "data": "HTTPClient"
        }
      ]
    },
    {
      "name": "httpclients#00019",
      "test": "substring(option[60].hex,0,21) == 'HTTPClient:Arch:00019'",
      "boot-file-name": "http://192.168.1.200/boot/grub2/arm64-efi/bootaa64.efi",
      "option-data": [
        {
          "name": "vendor-class-identifier",
          "data": "HTTPClient"
        }
      ]
    }
  ],
  "subnet4": [
    {
      "id": 1,
      "subnet": "192.168.1.0/24",
      "pools": [
        {
          "pool": "192.168.1.100 - 192.168.1.199"
        }
      ],
      "option-data": [
        {
          "name": "routers",
          "data": "192.168.1.1"
        },
        {
          "name": "ntp-servers",
          "data": "192.168.1.1"
        }
      ]
    }
  ]
}

```

```

    },
    {
      "name": "domain-name-servers",
      "data": "192.168.1.200"
    },
    {
      "name": "domain-search",
      "data": "example.net"
    }
  ],
  "reservations": []
}
],
"loggers": [
  {
    "name": "kea-dhcp4",
    "output-options": [
      {
        "output": "/var/log/kea/dhcp4.log"
      }
    ],
    "severity": "INFO",
    "debuglevel": 0
  }
]
}
}
EOF

```

2. Cree el directorio de registro de Kea:

```
> sudo mkdir -p /var/log/kea
```

3. Pruebe la configuración de DHCPv4 de Kea:

```
> sudo kea-dhcp4 -t /etc/kea/kea-dhcp4.conf
```

4. Habilite e inicie el servicio DHCPv4 de Kea:

```
> sudo systemctl enable --now kea-dhcp4
```

13.4 Configuración del servidor DHCPv6 de Kea

La configuración de DHCPv6 de Kea proporciona asignación de direcciones IPv6 e información de archivos de arranque mediante la correspondencia con clases de proveedor para diferentes arquitecturas de cliente.

PROCEDIMIENTO 51: CONFIGURACIÓN DEL SERVIDOR DHCPV6 DE KEA

1. Configure el servidor DHCPv6 de Kea:

```
> sudo cat > /etc/kea/kea-dhcp6.conf << 'EOF'
{
  "Dhcp6": {
    "interfaces-config": {
      "interfaces": [
        "en01"
      ]
    },
    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/tmp/kea6-ctrl-socket"
    },
    "lease-database": {
      "type": "memfile",
      "persist": true,
      "name": "/var/lib/kea/dhcp6.leases",
      "lfc-interval": 3600
    },
    "expired-leases-processing": {
      "reclaim-timer-wait-time": 10,
      "flush-reclaimed-timer-wait-time": 25,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 250,
      "unwarned-reclaim-cycles": 5
    },
    "renew-timer": 1800,
    "rebind-timer": 2880,
    "preferred-lifetime": 3600,
    "valid-lifetime": 7200,
    "option-data": [],
    "option-def": [],
    "client-classes": [
      {
        "name": "pxeclients#00000",
        "test": "substring(option[16].hex,6,20) == 'PXEClient:Arch:00000'",
        "option-data": [
```

```

        {
            "name": "bootfile-url",
            "data": "tftp://[2001:db8:0:1::200]/boot/grub2/i386-pc/core.0"
        }
    ]
},
{
    "name": "pxeclients#00007",
    "test": "substring(option[16].hex,6,20) == 'PXEClient:Arch:00007'",
    "option-data": [
        {
            "name": "bootfile-url",
            "data": "tftp://[2001:db8:0:1::200]/boot/grub2/x86_64-efi/bootx64.efi"
        }
    ]
},
{
    "name": "pxeclients#0000e",
    "test": "substring(option[16].hex,6,20) == 'PXEClient:Arch:0000e'",
    "option-data": [
        {
            "name": "bootfile-url",
            "data": "tftp://[2001:db8:0:1::200]/boot/grub2/powerpc-ieee1275/
core.elf"
        }
    ]
},
{
    "name": "pxeclients#00011",
    "test": "substring(option[16].hex,6,20) == 'PXEClient:Arch:00011'",
    "option-data": [
        {
            "name": "bootfile-url",
            "data": "tftp://[2001:db8:0:1::200]/boot/grub2/arm64-efi/bootaa64.efi"
        }
    ]
}
],
"subnet6": [
    {
        "id": 1,
        "subnet": "2001:db8:0:1::/64",
        "interface": "eno1",
        "pools": [
            {
                "pool": "2001:db8:0:1:d::/112"
            }
        ]
    }
]

```

```

    ],
    "option-data": [
      {
        "name": "snmp-servers",
        "data": "2001:db8:0:1::1"
      },
      {
        "name": "dns-servers",
        "data": "2001:db8:0:1::200"
      },
      {
        "name": "domain-search",
        "data": "example.net"
      }
    ],
    "reservations": []
  }
],
"loggers": [
  {
    "name": "kea-dhcp6",
    "output-options": [
      {
        "output": "/var/log/kea/dhcp6.log"
      }
    ],
    "severity": "INFO",
    "debuglevel": 0
  }
]
}
EOF

```

2. Pruebe la configuración de DHCPv6 de Kea:

```
> sudo kea-dhcp6 -t /etc/kea/kea-dhcp6.conf
```

3. Habilite e inicie el servicio DHCPv6 de Kea:

```
> sudo systemctl enable --now kea-dhcp6
```

13.5 Verificación de la configuración de DHCP de Kea

Pruebe la funcionalidad del servidor DHCP de Kea para garantizar una configuración de red adecuada y la entrega de archivos de arranque a clientes PXE.

PROCEDIMIENTO 52: PRUEBA DE LOS SERVIDORES DHCP DE KEA

1. Compruebe el estado del servicio DHCPv4 de Kea:

```
> systemctl status kea-dhcp4
```

2. Compruebe el estado del servicio DHCPv6 de Kea:

```
> systemctl status kea-dhcp6
```

3. Verifique la vinculación de puertos DHCP:

```
> ss -u lnp | grep -E ":67|:547"
```

4. Supervise los registros de DHCPv4:

```
> tail -f /var/log/kea/dhcp4.log
```

5. Supervise los registros de DHCPv6:

```
> tail -f /var/log/kea/dhcp6.log
```

6. Compruebe las concesiones de DHCP activas:

```
> cat /var/lib/kea/dhcp4.leases
```

13.6 Solución de problemas de la configuración de DHCP de Kea

Estos son los problemas comunes al configurar servidores DHCP de Kea para entornos de arranque PXE.

13.6.1 Problemas de configuración y servicio

Los servicios de Kea pueden no iniciarse debido a errores de configuración de JSON o a problemas de la interfaz de red.

PROCEDIMIENTO 53: SOLUCIÓN DE PROBLEMAS DE CONFIGURACIÓN DE KEA

1. Pruebe la sintaxis de configuración de DHCPv4:

```
> sudo kea-dhcp4 -t /etc/kea/kea-dhcp4.conf
```

2. Pruebe la sintaxis de configuración de DHCPv6:

```
> sudo kea-dhcp6 -t /etc/kea/kea-dhcp6.conf
```

3. Compruebe si hay errores de sintaxis de JSON:

```
> python3 -m json.tool /etc/kea/kea-dhcp4.conf
```

4. Verifique la configuración de la interfaz de red:

```
> ip addr show eno1
```

5. Consulte los registros del servicio de Kea:

```
> journalctl -u kea-dhcp4 -f
```

13.6.2 Problemas de asignación de concesión de DHCP

Puede que los clientes no reciban direcciones IP debido a problemas de la configuración de subred o por agotamiento del grupo.

PROCEDIMIENTO 54: DIAGNÓSTICO DE PROBLEMAS DE CONCESIÓN DE KEA

1. Compruebe la configuración de la subred y del grupo:

```
> grep -A 10 "subnet4\|pools" /etc/kea/kea-dhcp4.conf
```

2. Supervise las asignaciones de concesión en tiempo real:

```
> tail -f /var/log/kea/dhcp4.log | grep -E "ALLOC|DISCOVER"
```

3. Compruebe en la base de datos de concesión si hay conflictos:

```
> cat /var/lib/kea/dhcp4.leases | tail -20
```

4. Verifique la vinculación de interfaz:

```
> grep interfaces /etc/kea/kea-dhcp4.conf
```

5. Borre la base de datos de concesiones si fuera necesario:

```
> sudo systemctl stop kea-dhcp4
```

```
> sudo mv /var/lib/kea/dhcp4.leases /var/lib/kea/dhcp4.leases.backup
```

```
> sudo systemctl start kea-dhcp4
```

13.6.3 Problemas de correspondencia de clase de cliente PXE

Los clientes PXE pueden recibir direcciones IP, pero no pueden obtener los archivos de arranque correctos debido a problemas de configuración de la clase de cliente.

PROCEDIMIENTO 55: SOLUCIÓN DE PROBLEMAS DE LA CLASIFICACIÓN DE CLIENTES DE KEA

1. Compruebe las definiciones de clase de cliente:

```
> grep -A 5 "client-classes" /etc/kea/kea-dhcp4.conf
```

2. Consulte la correspondencia de clases de cliente en los registros:

```
> tail -f /var/log/kea/dhcp4.log | grep -i class
```

3. Verifique los patrones del identificador de clase de proveedor:

```
> grep "PXEClient\|HTTPClient" /etc/kea/kea-dhcp4.conf
```

4. Pruebe la accesibilidad del archivo de arranque:

```
> curl -I http://192.168.1.200/boot/grub2/x86_64-efi/bootx64.efi
```

5. Habilite el registro de depuración para realizar un análisis detallado del cliente:

```
> sudo sed -i 's/"debuglevel": 0/"debuglevel": 99/' /etc/kea/kea-dhcp4.conf
```

```
> sudo systemctl restart kea-dhcp4
```

13.6.4 Problemas específicos de DHCPv6

Los clientes DHCP IPv6 requieren una configuración adecuada de los anuncios de router y gestionan la opción de clase de proveedor de forma diferente a como se hace para IPv4.

1. Compruebe la configuración de la subred DHCPv6:

```
> grep -A 10 "subnet6" /etc/kea/kea-dhcp6.conf
```

2. Compruebe el estado de los anuncios de router IPv6:

```
> systemctl status radvd
```

3. Supervise la correspondencia de clases de proveedores DHCPv6:

```
> tail -f /var/log/kea/dhcp6.log | grep "option\[16\]"
```

4. Compruebe el formato de la opción bootfile-url de IPv6:

```
> grep "bootfile-url" /etc/kea/kea-dhcp6.conf
```

5. Pruebe la conectividad IPv6 al servidor de arranque:

```
> ping6 2001:db8:0:1::200
```

13.7 Pasos siguientes

Con los servicios DHCP de Kea configurados, los clientes PXE pueden recibir información completa de configuración de red y archivos de arranque para entornos IPv4 e IPv6. El sistema de clasificación de clientes proporciona una asignación precisa de archivos de arranque basada en la arquitectura del cliente y admite los métodos de arranque PXE tradicionales y HTTP modernos.

14 Configuración de un servidor DHCP con ISC DHCP

En esta sección se explica cómo configurar el servidor ISC DHCP para proporcionar la configuración de red e información de arranque PXE para instalaciones de SUSE Linux Enterprise Server 15. El paquete `dhcp-server` de ISC ya no está disponible en SUSE Linux Enterprise Server 16.0. ISC DHCP utiliza la correspondencia de clases y subclases para admitir escenarios de arranque PXE y HTTP en diferentes arquitecturas de cliente.

14.1 Introducción

ISC DHCP es el servidor DHCP tradicional que proporciona configuración de red e información de archivos de arranque a clientes PXE mediante un sistema de clases y subclasses. Si bien ISC ha declarado que este servidor llegó al final de su vida útil en 2022, sigue siendo ampliamente utilizado en despliegues existentes y proporciona una compatibilidad sólida para escenarios de arranque PXE y HTTP con identificación de clase de proveedor.



Importante: estado de final de vida útil de ISC DHCP

Según ISC, ISC DHCP llegó al final de su vida útil en 2022. Para nuevos despliegues, plantéese usar Kea o dnsmasq en su lugar. Esta configuración se proporciona para la compatibilidad con las instalaciones ISC DHCP existentes.

14.2 Requisitos

- Paquetes de ISC DHCP instalados: `dhcp-server`
- Archivos de arranque PXE correctamente organizados en `/srv/tftpboot`
- Interfaz de red configurada para el servicio DHCP
- Privilegios administrativos para configurar servicios DHCP

14.3 Configuración del servidor ISC DHCPv4

La configuración de ISC DHCPv4 usa declaraciones de clase y subclase que se corresponden con los tipos de clientes PXE y HTTP para proporcionar archivos de arranque apropiados para diferentes arquitecturas.

PROCEDIMIENTO 57: CONFIGURACIÓN DEL SERVIDOR ISC DHCPV4

1. Configure el servidor ISC DHCPv4:

```
> sudo cat > /etc/dhcpd.conf << 'EOF'  
# /etc/dhcpd.conf  
#  
# Sample configuration file for ISC dhcpd  
#  
# *** PLEASE CONFIGURE IT FIRST ***  
#
```

```

# Don't forget to set the DHCPD_INTERFACE in the
# /etc/sysconfig/dhcpd file.
#

# if you want to use dynamical DNS updates, you should first read
# read /usr/share/doc/packages/dhcp-server/DDNS-howto.txt
#
ddns-updates off;

# Use this to enable / disable dynamic dns updates globally.
ddns-update-style none;

# default lease time
default-lease-time          3600;
max-lease-time              7200;

##
## PXE / HTTP boot option declarations
##
class "pxeclients" {
    # PXEClient:Arch:00000:UNDI:002001
    match substring (option vendor-class-identifier, 0, 20);
}
class "httpclients" {
    # HTTPClient:Arch:00016:UNDI:003001
    match substring (option vendor-class-identifier, 0, 21);
}

##
## PXE / HTTP boot subclass request matches
##
subclass "pxeclients" "PXEClient:Arch:00000" {
    next-server      192.168.1.200;
    filename         "/boot/grub2/i386-pc/core.0";
}
subclass "pxeclients" "PXEClient:Arch:00007" {
    next-server      192.168.1.200;
    filename         "/boot/grub2/x86_64-efi/bootx64.efi";
}
subclass "pxeclients" "PXEClient:Arch:0000e" {
    next-server      192.168.1.200;
    filename         "/boot/grub2/powerpc-ieee1275/core.elf";
}
subclass "pxeclients" "PXEClient:Arch:00011" {
    next-server      192.168.1.200;
    filename         "/boot/grub2/arm64-efi/bootaa64.efi";
}
}

```

```

subclass "httpclients" "HTTPClient:Arch:00016" {
    option vendor-class-identifier "HTTPClient";
    filename "http://192.168.1.200/boot/grub2/x86_64-efi/bootx64.efi";
}
subclass "httpclients" "HTTPClient:Arch:00019" {
    option vendor-class-identifier "HTTPClient";
    filename "http://192.168.1.200/boot/grub2/arm64-efi/bootaa64.efi";
}

##
## Subnet declaration for the pxe network
##
subnet 192.168.1.0 netmask 255.255.255.0 {
    authoritative;

    range dynamic-bootp 192.168.1.100 192.168.1.199;

    option subnet-mask 255.255.255.0;

    option routers 192.168.1.1;
    option ntp-servers 192.168.1.1;
    option domain-name-servers 192.168.1.200;
    option domain-name "example.net";
    option domain-search "example.net";
}
EOF

```

2. Configure la interfaz de DHCP en sysconfig:

```
> sudo echo 'DHCPD_INTERFACE="eno1"' > /etc/sysconfig/dhcpd
```

3. Pruebe la configuración de DHCPv4:

```
> sudo dhcpd -t -cf /etc/dhcpd.conf
```

4. Habilite e inicie el servicio ISC DHCPv4:

```
> sudo systemctl enable --now dhcpd
```

14.4 Configuración del servidor ISC DHCPv6

La configuración de ISC DHCPv6 proporciona asignación de direcciones IPv6 e información de archivos de arranque mediante la correspondencia de clases de proveedores con la gestión adecuada de la opción de DHCPv6.

PROCEDIMIENTO 58: CONFIGURACIÓN DEL SERVIDOR ISC DHCPV6

1. Configure el servidor ISC DHCPv6:

```
> sudo cat > /etc/dhcpd6.conf << 'EOF'
# /etc/dhcpd6.conf
#
# Sample DHCPv6 configuration file for ISC dhcpd
#
# *** PLEASE CONFIGURE IT FIRST ***
#
# Don't forget to set the DHCPD6_INTERFACE in the
# /etc/sysconfig/dhcpd file.
#
# if you want to use dynamical DNS updates, you should first
# read /usr/share/doc/packages/dhcp-server/DDNS-howto.txt
ddns-updates off;
# Use this to enable / disable dynamic dns updates globally.
ddns-update-style none;
# IPv6 address valid lifetime
# (at the end the address is no longer usable by the client)
# (set to 30 days, the usual IPv6 default)
default-lease-time 7200;
# IPv6 address preferred lifetime
# (at the end the address is deprecated, i.e., the client should use
# other addresses for new connections)
# (set to 7 days, the usual IPv6 default)
preferred-lifetime 3600;
##
## PXE / HTTP boot option declarations
##
# The dhcp6 option 16 is in fact an:
# { uint32 enterprise-number, array of { uint16 len, string tag} vendor-class-
data }
# this declaration is using the whole option data as string for substring match:
```

```

option dhcp6.vendor-class-as-string code 16 = string;

# this declaration is using the enterprise-number with 1st tag length and string:
option dhcp6.vendor-class-en-len-tag code 16 = {integer 32, integer 16, string};

class "pxeclients" {
    # PXEClient:Arch:00000:UNDI:002001
    # note: +6 to skip the enterprise-number+len until the PXEClient string
    match substring (option dhcp6.vendor-class-as-string, 6, 20);
}
class "httpclients" {
    # HTTPClient:Arch:00016:UNDI:003001
    # note: +6 to skip the enterprise-number+len until the HTTPClient string
    match substring (option dhcp6.vendor-class-as-string, 6, 21);
}

##
## PXE / HTTP boot subclass request matches
##
subclass "pxeclients" "PXEClient:Arch:00000" {
    option dhcp6.bootfile-url "tftp://[2001:db8:0:1::200]/boot/grub2/i386-pc/
core.0";
}
subclass "pxeclients" "PXEClient:Arch:00007" {
    option dhcp6.bootfile-url "tftp://[2001:db8:0:1::200]/boot/grub2/x86_64-efi/
bootx64.efi";
}
subclass "pxeclients" "PXEClient:Arch:0000e" {
    option dhcp6.bootfile-url "tftp://[2001:db8:0:1::200]/boot/grub2/powerpc-
ieee1275/core.elf";
}
subclass "pxeclients" "PXEClient:Arch:00011" {
    option dhcp6.bootfile-url "tftp://[2001:db8:0:1::200]/boot/grub2/arm64-efi/
bootaa64.efi";
}

subclass "httpclients" "HTTPClient:Arch:00016" {
    option dhcp6.vendor-class-en-len-tag 343 10 "HTTPClient";
    option dhcp6.bootfile-url "http://[2001:db8:0:1::200]/boot/grub2/x86_64-efi/
bootx64.efi";
}
subclass "httpclients" "HTTPClient:Arch:00019" {
    option dhcp6.vendor-class-en-len-tag 343 10 "HTTPClient";
    option dhcp6.bootfile-url "http://[2001:db8:0:1::200]/boot/grub2/arm64-efi/
bootaa64.efi";
}

```

```

##
## Subnet declaration for the pxe network
##
subnet6 2001:db8:0:1::/64 {
    authoritative;

    range6 2001:db8:0:1:d:: 2001:db8:0:1:d::ffff;

    option dhcp6.sntp-servers      2001:db8:0:1::1;
    option dhcp6.name-servers      2001:db8:0:1::200;
    option dhcp6.domain-search     "example.net";
}
EOF

```

2. Configure la interfaz de DHCPv6 en sysconfig:

```
> sudo echo 'DHCPD6_INTERFACE="eno1"' >> /etc/sysconfig/dhcpd
```

3. Pruebe la configuración de DHCPv6:

```
> sudo dhcpd -6 -t -cf /etc/dhcpd6.conf
```

4. Habilite e inicie el servicio ISC DHCPv6:

```
> sudo systemctl enable --now dhcpd6
```

14.5 Verificación de la configuración de ISC DHCP

Pruebe la funcionalidad del servidor ISC DHCP para garantizar una configuración de red adecuada y la entrega de archivos de arranque a clientes PXE.

PROCEDIMIENTO 59: PRUEBA DE LOS SERVIDORES ISC DHCP

1. Compruebe el estado del servicio ISC DHCPv4:

```
> systemctl status dhcpd
```

2. Compruebe el estado del servicio ISC DHCPv6:

```
> systemctl status dhcpd6
```

3. Verifique la vinculación de puertos DHCP:

```
> ss -ulnp | grep -E ":67|:547"
```

4. Consulte los registros de DHCP:

```
> journalctl -u dhcpd -f
```

5. Compruebe las concesiones de DHCP activas:

```
> cat /var/lib/dhcp/dhcpd.leases
```

6. Supervise la actividad de DHCPv6:

```
> journalctl -u dhcpd6 -f
```

14.6 Solución de problemas de configuración de ISC DHCP

Estos son los problemas comunes al configurar servidores ISC DHCP para entornos de arranque PXE.

14.6.1 Problemas de configuración y servicio

Los servicios ISC DHCP pueden no iniciarse debido a errores de sintaxis de configuración o problemas de vinculación de interfaz.

PROCEDIMIENTO 60: SOLUCIÓN DE PROBLEMAS DE CONFIGURACIÓN DE ISC DHCP

1. Pruebe la sintaxis de configuración de DHCPv4:

```
> sudo dhcpd -t -cf /etc/dhcpd.conf
```

2. Pruebe la sintaxis de configuración de DHCPv6:

```
> sudo dhcpd -6 -t -cf /etc/dhcpd6.conf
```

3. Compruebe la configuración de la interfaz:

```
> cat /etc/sysconfig/dhcpd
```

4. Verifique el estado de la interfaz de red:

```
> ip addr show eno1
```

5. Compruebe si hay conflictos de puerto:

```
> ss -u lnp | grep :67
```

6. Consulte los registros de servicio detallados:

```
> journalctl -u dhcpd -xe
```

14.6.2 Problemas de asignación de concesión de DHCP

Puede que los clientes no reciban direcciones IP debido a problemas de la configuración de subred o problemas de autorización.

PROCEDIMIENTO 61: DIAGNÓSTICO DE PROBLEMAS DE CONCESIONES DE ISC DHCP

1. Compruebe la configuración de la subred y el intervalo:

```
> grep -A 10 "subnet\|range" /etc/dhcpd.conf
```

2. Verifique la configuración autorizada:

```
> grep authoritative /etc/dhcpd.conf
```

3. Supervise las asignaciones de concesión en tiempo real:

```
> tail -f /var/log/messages | grep dhcpd
```

4. Compruebe en la base de datos de concesiones si hay errores:

```
> tail -20 /var/lib/dhcp/dhcpd.leases
```

5. Pruebe manualmente la respuesta DHCP:

```
> dhcping -s 192.168.1.200 -h aa:bb:cc:dd:ee:ff
```

14.6.3 Problemas de correspondencia de clases y subclases

Los clientes PXE pueden recibir direcciones IP, pero no pueden obtener archivos de arranque correctos debido a problemas de configuración de la correspondencia de clases.

PROCEDIMIENTO 62: SOLUCIÓN DE PROBLEMAS DE LA CORRESPONDENCIA DE CLASES DE ISC DHCP

1. Compruebe las definiciones de clase:

```
> grep -A 3 "class.*clients" /etc/dhcpd.conf
```

2. Verifique las entradas de subclase:

```
> grep -A 5 "subclass" /etc/dhcpd.conf
```

3. Supervise la identificación de la clase de proveedor:

```
> tail -f /var/log/messages | grep -E "PXEClient|HTTPClient"
```

4. Pruebe la accesibilidad del archivo de arranque:

```
> tftp 192.168.1.200 -c get /boot/grub2/x86_64-efi/bootx64.efi
```

5. Habilite el registro detallado:

```
> sudo sed -i 'li\log-facility local7;' /etc/dhcpd.conf
```

```
> sudo systemctl restart dhcpd
```

14.6.4 Problemas con la opción de clase de proveedor DHCPv6

Los clientes DHCP IPv6 gestionan la opción de clase de proveedor de una forma compleja que puede requerir una configuración específica para proporcionar la compatibilidad adecuada para el arranque PXE.

PROCEDIMIENTO 63: RESOLUCIÓN DE PROBLEMAS DE ISC DHCPV6

1. Compruebe las definiciones de la opción DHCPv6:

```
> grep -A 3 "option dhcp6" /etc/dhcpd6.conf
```

2. Verifique el análisis de la cadena de clase de proveedor:

```
> grep "substring.*6.*20\|21" /etc/dhcpd6.conf
```

3. Supervise la correspondencia de clases de proveedores DHCPv6:

```
> journalctl -u dhcpd6 | grep -i vendor
```

4. Compruebe el formato bootfile-url de IPv6:

```
> grep "bootfile-url" /etc/dhcpd6.conf
```

5. Verifique la dependencia de los anuncios de router:

```
> systemctl status radvd
```

6. Pruebe la conectividad IPv6:

```
> ping6 2001:db8:0:1::200
```

14.7 Pasos siguientes

Con los servicios ISC DHCP configurados, los clientes PXE pueden recibir la configuración de la red e información de los archivos de arranque utilizando el sistema tradicional de clases y subclases. Si bien ISC DHCP se encuentra al final de su vida útil, esta configuración proporciona compatibilidad para despliegues existentes que requieren funcionalidad de arranque PXE y HTTP en múltiples arquitecturas de cliente.

15 Validación de la configuración del servidor PXE

En esta sección se describe cómo validar y probar la configuración completa del servidor PXE para garantizar que todos los componentes funcionen correctamente para las instalaciones de red de SUSE Linux Enterprise Server 16.0. Cubre la verificación del servicio, las pruebas de conectividad de red y la validación del arranque PXE de extremo a extremo.

15.1 Introducción

Después de configurar todos los componentes del servidor PXE, incluidos los servicios de arranque TFTP, HTTP, DNS, DHCP y GRUB 2, es esencial validar que el sistema completo funcione correctamente. Esta validación garantiza que los clientes PXE puedan arrancar correctamente en el instalador Agama y realizar instalaciones basadas en red de SUSE Linux Enterprise Server 16.0.

15.2 Requisitos

- Todos los componentes del servidor PXE configurados y en ejecución
- Sistemas cliente de prueba capaces de arrancar PXE
- Conectividad de red entre el servidor PXE y los clientes
- Acceso administrativo para supervisar los servicios del servidor

15.3 Validación de los servicios de servidor PXE

Compruebe que todos los servicios esenciales del servidor PXE se están ejecutando y se han configurado correctamente antes de hacer pruebas con los clientes PXE.

PROCEDIMIENTO 64: COMPROBACIÓN DEL ESTADO DEL SERVICIO DEL SERVIDOR PXE

1. Verifique el estado del servicio TFTP:

```
> systemctl status tftp.socket
```

Resultado esperado: el servicio debe estar activo y a la escucha en el puerto 69.

2. Compruebe el servicio HTTP de nginx:

```
> systemctl status nginx
```

Resultado esperado: el servicio debe estar activo y a la escucha en el puerto 80.

3. Verifique el servicio DNS (si usa dnsmasq):

```
> systemctl status dnsmasq
```

Resultado esperado: el servicio debe estar activo y a la escucha en el puerto 53.

4. Compruebe el estado del servicio DHCP (elija el servicio apropiado):

```
> systemctl status dhcpd
```

Para DHCP dnsmasq:

```
> systemctl status dnsmasq
```

Para DHCP Kea:

```
> systemctl status kea-dhcp4 kea-dhcp6
```

Resultado esperado: el servicio DHCP debe estar activo y a la escucha en los puertos apropiados.

5. Verifique los anuncios de router IPv6 (si están configurados):

```
> systemctl status radvd
```

Resultado esperado: el servicio debe estar activo para entornos IPv6.

6. Compruebe el servicio NTP:

```
> systemctl status chronyd
```

Resultado esperado: el servicio debe estar activo y sincronizado.

15.4 Prueba de conectividad de red y acceso a archivos

Valide que los clientes PXE puedan acceder a los archivos de arranque y al contenido de instalación a través de la red utilizando los protocolos TFTP y HTTP.

PROCEDIMIENTO 65: PRUEBA DE ACCESO A ARCHIVOS DE RED

1. Pruebe el acceso TFTP a los archivos del cargador de arranque:

```
> tftp localhost -c get /boot/grub2/x86_64-efi/bootx64.efi /tmp/test-bootx64.efi
```

Verifique que el archivo se recupera:

```
> file /tmp/test-bootx64.efi
```

Borre el archivo de prueba:

```
> rm /tmp/test-bootx64.efi
```

2. Pruebe el acceso HTTP a la configuración de GRUB 2:

```
> curl -I http://localhost/boot/grub2/grub.cfg
```

Resultado esperado: respuesta correcta de HTTP 200.

3. Verifique el acceso HTTP a los archivos de instalador:

```
> curl -I http://localhost/boot/images/SLES-16.0/x86_64/liveiso/LiveOS/squashfs.img
```

Resultado esperado: respuesta correcta de HTTP 200 con la longitud de contenido adecuada.

4. Pruebe la resolución DNS (si se ha configurado el DNS local):

```
> nslookup pxe.example.net localhost
```

Resultado esperado: resolución de registro A y AAAA adecuada.

5. Verifique la navegación de directorios para ubicaciones de autoíndice:

```
> curl http://localhost/boot/
```

Resultado esperado: listado de directorios que muestra los archivos de arranque.

15.5 Validación de la funcionalidad de DHCP

Pruebe las respuestas del servidor DHCP y compruebe que se proporciona la información de arranque adecuada a los diferentes tipos de clientes.

PROCEDIMIENTO 66: PRUEBA DE LAS RESPUESTAS DEL SERVIDOR DHCP

1. Compruebe la vinculación de puertos DHCP:

```
> ss -u lnp | grep -E ":67|:547"
```

Resultado esperado: los servicios DHCP escuchan en los puertos 67 (IPv4) y 547 (IPv6).

2. Supervise las solicitudes DHCP en tiempo real:

```
> journalctl -u dhcpd -f
```

O para dnsmasq:

```
> journalctl -u dnsmasq -f
```

Deje esto funcionando para observar la actividad de DHCP durante las pruebas.

3. Pruebe la respuesta DHCP usando dhcping (si está disponible):

```
> dhcping -s 192.168.1.200
```

Resultado esperado: respuesta DHCP correcta del servidor.

4. Compruebe las concesiones de DHCP activas:

```
> cat /var/lib/dhcp/dhcpd.leases
```

O para Kea:

```
> cat /var/lib/kea/dhcp4.leases
```

Resultado esperado: entradas de concesión para clientes de prueba.

15.6 Pruebas de arranque PXE de extremo a extremo

Realice pruebas de arranque PXE completas con sistemas cliente reales para validar todo el proceso de arranque desde DHCP hasta el inicio del instalador Agama.

PROCEDIMIENTO 67: PRUEBA DEL PROCESO DE ARRANQUE PXE COMPLETO

1. Prepare un sistema cliente de prueba:

- Configure BIOS/UEFI para habilitar el arranque de red.
- Establezca el arranque de red como primera prioridad de arranque.
- Conecte el cliente a la misma red que el servidor PXE.

2. Consulte los registros del servidor PXE durante el arranque del cliente:

```
> journalctl -f | grep -E "dhcp|tftp|nginx"
```

3. Arranque el cliente de prueba y observe la siguiente secuencia:

1. El cliente debe recibir la dirección IP a través de DHCP.
2. El cliente debe descargar el cargador de arranque a través de TFTP.
3. El menú de GRUB 2 debe aparecer con las opciones de instalación.
4. El kernel e initrd deben cargarse a través de HTTP.
5. El instalador Agama debería iniciarse correctamente.

4. Compruebe que la arquitectura del cliente se detecta probando diferentes tipos de cliente:
 - Sistemas BIOS x86_64 heredados (deberían obtener core.0)
 - Sistemas UEFI x86_64 (debería obtener bootx64.efi)
 - Sistemas UEFI aarch64 (debería obtener bootaa64.efi)
5. Pruebe el arranque PXE IPv6 (si IPv6 está configurado):
 - Habilite la configuración de la red solo IPv6 en el cliente de prueba.
 - Verifique la asignación de direcciones DHCPv6.
 - Confirme la entrega de bootfile-url IPv6.

15.7 Validación de la funcionalidad del instalador Agama

Compruebe que el instalador Agama se inicia correctamente y puede acceder a los orígenes de instalación para completar las instalaciones de SUSE Linux Enterprise Server 16.0.

PROCEDIMIENTO 68: PRUEBAS DE INICIO DEL INSTALADOR AGAMA

1. Verifique la accesibilidad de la interfaz web de Agama:
Durante el arranque del cliente, anote la dirección IP asignada y acceda a:

```
http://CLIENT_IP_ADDRESS
```

Resultado esperado: la interfaz Web de Agama debería cargarse correctamente.

2. Compruebe los registros del instalador Agama en el cliente:
Cambie a la consola (Alt + F2) y ejecute:

```
# journalctl -u agama-web-server -f
```

Resultado esperado: no hay errores críticos en el inicio de Agama.

3. Verifique la accesibilidad del origen de instalación:
Para instalaciones ISO completas, compruebe el acceso al repositorio:

```
# curl -I http://192.168.1.200/install/SLES-16.0/x86_64/
```

Resultado esperado: respuesta correcta de HTTP 200 con listado de directorios.

4. Pruebe la capacidad de instalación del paquete:

En la interfaz de Agama, compruebe que:

- El sistema puede detectar los discos disponibles.
- No se requiere ninguna configuración de red.
- Se puede acceder al repositorio de paquetes.
- La instalación puede continuar hasta su finalización.

15.8 Solución de problemas de fallos de validación

Estos son los problemas comunes durante la validación del servidor PXE y los pasos para solucionarlos.

15.8.1 Fallos en la asignación de DHCP

Los clientes no reciben direcciones IP durante el arranque PXE.

PROCEDIMIENTO 69: SOLUCIÓN DE PROBLEMAS DE VALIDACIÓN DE DHCP

1. Compruebe si hay conflictos del servicio DHCP:

```
> ss -u!np | grep :67
```

2. Verifique que la interfaz de red esté activa:

```
> ip addr show eno1
```

3. Compruebe la disponibilidad del intervalo de DHCP:

```
> nmap -sn 192.168.1.100-199
```

4. Consulte en los registros de DHCP si hay errores:

```
> journalctl -u dhcpd | tail -50
```

15.8.2 Errores de entrega del archivo de arranque

Los clientes reciben direcciones IP, pero no pueden descargar los archivos de arranque.

PROCEDIMIENTO 70: SOLUCIÓN DE PROBLEMAS DEL ARCHIVO DE ARRANQUE

1. Verifique que se puede acceder al servicio TFTP:

```
> tftp 192.168.1.200 -c get /boot/grub2/x86_64-efi/bootx64.efi
```

2. Compruebe los permisos del archivo:

```
> ls -la /srv/tftpboot/boot/grub2/x86_64-efi/
```

3. Consulte los registros de acceso de TFTP:

```
> journalctl -u tftp.socket -f
```

4. Verifique que se detecta la arquitectura del cliente:

```
> grep -E "PXEClient|HTTPClient" /var/log/messages
```

15.8.3 Fallos de inicio del instalador Agama

Los archivos de arranque se cargan correctamente, pero el instalador Agama no se inicia.

PROCEDIMIENTO 71: SOLUCIÓN DE PROBLEMAS DE ARRANQUE DE AGAMA

1. Compruebe el acceso HTTP a los archivos de instalador:

```
> curl -I http://192.168.1.200/boot/images/SLES-16.0/x86_64/liveiso/LiveOS/  
squashfs.img
```

2. Compruebe la sintaxis del parámetro del kernel en la configuración de GRUB 2:

```
> grep "root=live:" /srv/tftpboot/boot/grub2/menu.cfg
```

3. Supervise el proceso de arranque del cliente:

```
> journalctl -f | grep -E "kernel|initrd|agama"
```

4. Compruebe la persistencia de la configuración de red:

```
# ip addr show
```

15.9 Lista de verificación para validar el servidor PXE

Utilice esta lista para verificar sistemáticamente todos los aspectos de la configuración de su servidor PXE.

TABLA 2: LISTA DE VERIFICACIÓN PARA VALIDAR EL SERVIDOR PXE

Componente	Paso de validación	Estado
Servicio TFTP	Servicio activo, puerto 69 a la escucha, archivos accesibles	<input type="checkbox"/>
Servicio HTTP	nginx activo, puerto 80 a la escucha, archivos de instalador accesibles	<input type="checkbox"/>
Servicio DNS	La resolución de nombres de host funciona, puerto 53 a la escucha	<input type="checkbox"/>
Servicio DHCP	La asignación de IP funciona, las opciones de arranque se entregan	<input type="checkbox"/>
Configuración de GRUB 2	El menú se carga, la detección de arquitectura funciona	<input type="checkbox"/>
Compatibilidad con IPv6	Anuncios de router activos, DHCPv6 funciona	<input type="checkbox"/>
Arranque PXE	El cliente arranca correctamente, recibe el cargador de arranque correcto	<input type="checkbox"/>
Instalador Agama	El instalador se inicia, interfaz web accesible	<input type="checkbox"/>
Origen de la instalación	Repositorio accesible, paquetes instalables	<input type="checkbox"/>
Persistencia de la red	La configuración de red se mantiene durante la instalación	<input type="checkbox"/>

15.10 Conclusión de la validación

Un servidor PXE debidamente validado debe demostrar una funcionalidad completa y correcta desde el arranque de la red del cliente hasta el inicio del instalador Agama. Todos los servicios deben funcionar sin errores y los clientes deben poder completar las instalaciones de SUSE Linux Enterprise Server 16.0 a través de la red. Las pruebas de validación periódicas garantizan la fiabilidad continua de la infraestructura PXE para implementaciones automatizadas.

16 Información legal

Copyright© 2006–2025 SUSE LLC y colaboradores. Reservados todos los derechos.

Está permitido copiar, distribuir y modificar este documento según los términos de la licencia de documentación gratuita GNU, versión 1.2 o (según su criterio) versión 1.3. Esta información de copyright y licencia deberán permanecer inalterados. En la sección titulada “GNU Free Documentation License” (Licencia de documentación gratuita GNU) se incluye una copia de la versión 1.2 de la licencia.

Para obtener información sobre las marcas comerciales de SUSE, consulte <https://www.suse.com/company/legal/>. Todas las marcas comerciales de otros fabricantes son propiedad de sus respectivas empresas. Los símbolos de marcas comerciales (®, ™, etc.) indican marcas comerciales de SUSE y sus filiales. Los asteriscos (*) indican marcas comerciales de otros fabricantes. Toda la información recogida en esta publicación se ha compilado prestando toda la atención posible al más mínimo detalle. Sin embargo, esto no garantiza una precisión total. Ni SUSE LLC, ni sus filiales, ni los autores o traductores serán responsables de los posibles errores o las consecuencias que de ellos pudieran derivarse.

A GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent

copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through

arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <https://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the GNU Free Documentation License, Version 1.2  
or any later version published by the Free Software Foundation;  
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.  
A copy of the license is included in the section entitled "GNU  
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the  
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.