Configurando um servidor de inicialização PXE no SUSE Linux Enterprise Server 16.0

O QUE É?

Configure um servidor de inicialização PXE com suporte para o Boot Seguro UEFI e o instalador Agama.

POR QUÊ?

Automatize e simplifique a instalação de vários sistemas SUSE Linux Enterprise Server 16.0 na rede.

DEDICAÇÃO

Para um administrador de sistema ou de rede, a leitura e a compreensão deste artigo costumam levar de 30 a 45 minutos.

META

Um servidor PXE funcional que pode inicializar várias arquiteturas no instalador Agama.

REQUISITOS

- Um sistema SUSE Linux Enterprise Server 16.0 com privilégios administrativos
- Conexão com a Internet para buscar as imagens ISO
- Configuração de IP estático para o servidor PXE

Data de Publicação: 11/12/2025

Conteúdo

1 Visão geral da inicialização PXE com o SUSE Linux Enterprise Server 16.0

A inicialização PXE permite que as máquinas sejam inicializadas por rede em um ambiente de instalação ou de runtime sem armazenamento local. Esta seção explica como funciona o PXE nas imagens do Agama e do instalador ativo do SUSE Linux Enterprise Server 16.0 com foco no GRUB 2.

1.1 O que é a inicialização PXE?

O Ambiente de Pré-execução (PXE, Preboot Execution Environment) é um método que permite que os sistemas recuperem carregadores de boot e instaladores de sistema operacional de um servidor de rede usando DHCP e TFTP ou HTTP. Ele é amplamente utilizado para provisionamento de máquinas sem mídia física ou de sistemas operacionais pré-instalados.

1.2 Benefícios da inicialização PXE

A inicialização PXE simplifica o provisionamento porque elimina a necessidade de mídia de instalação local ou configuração manual. Ela possibilita o seguinte:

- Instalação autônoma de muitos sistemas pela rede
- Gerenciamento centralizado das versões do instalador e das configurações de boot
- Suporte a várias arquiteturas e tipos de firmware, incluindo Boot Seguro UEFI
- Seleção dinâmica de instaladores ou parâmetros de instalação usando os menus do GRUB 2

1.3 Como funciona a inicialização PXE no SUSE Linux Enterprise Server 16.0

A inicialização PXE no SUSE Linux Enterprise Server 16.0 usa o GRUB 2 como carregador de boot e o instalador Agama como interface de instalação. Os carregadores de boot e os arquivos do instalador são fornecidos pela rede usando HTTP ou TFTP, e o GRUB 2 busca o kernel, o initrd e a imagem ativa. Os clientes PXE podem usar uma variedade de formatos de firmware (incluindo

os mais comuns, como BIOS ou UEFI), de executável de carregador de boot ou de imagem, conforme exigido pelas arquiteturas, como AMD64/Intel 64, AArch64, ppc64le e s390x. Além disso, eles devem funcionar em redes tanto IPv4 quanto IPv6.

O carregador de boot passa parâmetros do kernel, como `root=live:`, para carregar o sistema de arquivos raiz baseado em squashfs de uma imagem ISO ativa, iniciando a interface do Agama localmente ou como um serviço Web para uma interface de usuário Web remota.

1.3.1 Compatibilidade retroativa com o SLES 15.x

As informações neste artigo são voltadas principalmente ao SUSE Linux Enterprise Server 16.0 e versões mais recentes. O foco é nos fluxos de trabalho de inicialização PXE que se integram ao instalador Agama e dependem das imagens de instalação ativas. No contexto e no escopo deste artigo, o SLES 16.0, e versões mais recentes, é diferente do SLES 15.x das seguintes maneiras:

Instalador

Usa o `dracut` e o Agama em vez do `linuxrc` e do YaST.

Servidor DHCP

O uso do ISC DHCP foi descontinuado (EOL 2022). Como alternativa para um servidor DHCP, use Kea ou dnsmasq.

Parâmetros de boot

Use o parâmetro `root=live:` para carregar a imagem do instalador Agama e o `inst.install_url=` opcional para o repositório de instalação não padrão, em vez do parâmetro `install=`.

A escolha do carregador de boot (GRUB 2, pxelinux etc.) permanece flexível e não depende da versão.

1.3.2 Diferentes configurações e etapas possíveis

Este artigo consiste nas etapas de configuração obrigatórias e nas configurações opcionais ou alternativas. Siga apenas as seções relevantes à sua implantação e ignore todas as alternativas irrelevantes.

Obrigatória

As tarefas, como instalar componentes, preparar a imagem do instalador, configurar o GRUB 2 e validar o servidor, devem ser realizadas em todas as configurações.

Método de entrega de arquivo

Um servidor HTTP (recomendado com o Agama), como `nginx`, e/ou um servidor TFTP, como `tftp` ou `dnsmasq`.

Servidor DHCP

Escolha entre Kea ou dnsmasq.

Nota: Limitações e recursos do método de sua escolha

- Use o **Kea**, o novo servidor DHCP da ISC, como o substituto moderno do ISC DHCP. Para obter mais informações sobre o Kea, consulte https://www.isc.org/kea/. Para conferir o aviso sobre o fim do serviço do ISC DHCP, acesse https://www.isc.org/dhcp/. Kea é um servidor DHCP que requer um software de servidor TFTP separado. O servidor DHCP Kea suporta as opções de inicialização TFTP/PXE por IPv4 e IPv6, além da inicialização HTTP por IPv4. Para a inicialização HTTP por IPv6, o servidor DHCPv6 deve ser capaz de enviar a `Vendor Class Option` (consulte `RFC3315, Section 22.16`), supostamente para uso "por um cliente para identificar o fornecedor," de volta ao cliente, e não há suporte a isso no momento.

- **dnsmasq** como uma combinação dos servidores DNS, DHCP e TFTP. Você pode usá-lo para transmitir o carregador de boot, o kernel, o initrd (e outros arquivos) por TFTP. Para obter mais informações sobre o dnsmasq, consulte https://thekelleys.org.uk/dnsmasq/doc.html. O servidor DHCP dnsmasq suporta as opções de inicialização TFTP/PXE por IPv4 e IPv6, além da inicialização HTTP por IPv4. Para a inicialização HTTP por IPv6, o servidor DHCPv6 deve ser capaz de enviar a `Vendor Class Option` (consulte `RFC3315, Section 22.16`), supostamente para uso "por um cliente para identificar o fornecedor," de volta ao cliente, e não há suporte a isso no momento.

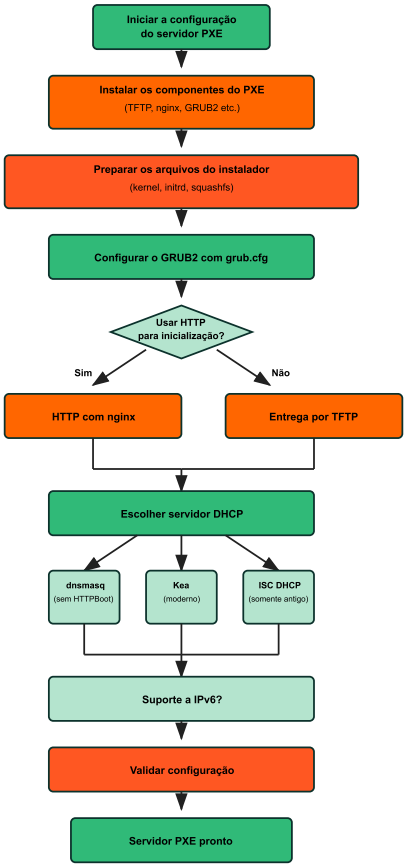

FIGURA 1: FLUXO DE TRABALHO PARA CONFIGURAÇÃO DO SERVIDOR PXE DE AMOSTRA

2 Preparando a rede para os serviços de inicialização PXE

Este módulo descreve os requisitos de infraestrutura de rede para implantar os serviços de inicialização PXE no SUSE Linux Enterprise Server 16.0.

2.1 Introdução

O servidor PXE consiste em três servidores: um servidor DHCP que fornece o endereço e o local do arquivo de inicialização (carregador de boot) e um servidor TFTP e/ou HTTP para recuperar os arquivos. Além disso, pode haver um servidor DNS, um servidor NTP e um roteador com suporte a IPv6. Geralmente, eles são separados do servidor PXE em uma rede de produção. Um servidor PXE que executa o SUSE Linux Enterprise Server 16.0 também pode precisar de uma configuração de interface de rede específica, determinadas regras persistentes adicionadas ao firewall e algumas permissões no `SELinux`. Esta seção ilustra uma rede de amostra com intervalos de IPs adequados e as regras necessárias para o firewall e o SELinux.

2.2 Suposições e configuração de rede de amostra

Neste artigo, consideramos o seguinte:

- O servidor PXE está em execução na interface de rede `eno1` com a seguinte configuração de rede:

TABELA 1: CONFIGURAÇÃO DE REDE PXE DE AMOSTRA

	IPv4	IPv6	Nome DNS
Rede 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	

- Por padrão, o roteador e os servidores NTP e DNS são externos e executados em outra máquina. Este artigo apresenta algumas dicas, mas não aborda a configuração completa.

2.3 Configurar interface de rede, firewall e SELinux para serviços PXE

Configure a interface de rede e o firewall para permitir os serviços de rede exigidos pelo servidor PXE. Ajuste as configurações do `SELinux` para permitir testes de instalação e definir políticas locais persistentes.

1. Verifique e atribua a interface de rede do PXE à zona do firewalld apropriada.
    a. Verifique as zonas que estão ativas e as respectivas interfaces atribuídas:

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

    b. Se `eno1` não foi atribuído à zona `public`, faça isso:

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

    c. Torne a atribuição da interface persistente a reinicializações:

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

2. Configure o firewall para acesso ao serviço DNS.
    a. Permita o serviço DNS na sessão atual:

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

    b. Torne a mudança persistente:

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

3. Configure o firewall para acesso ao serviço NTP.
    a. Permita o serviço NTP na sessão atual:

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

    b. Torne a mudança persistente:

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

4. Configure o firewall para acesso ao serviço DHCP (IPv4).

a. Permita o serviço DHCP na sessão atual:

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

b. Torne a mudança persistente:

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

5. Configure o firewall para acesso ao serviço DHCPv6.

a. Permita o serviço DHCPv6 na sessão atual:

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

b. Torne a mudança persistente:

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

6. Configure o firewall para acesso ao serviço TFTP.

a. Permita o serviço TFTP na sessão atual:

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

b. Torne a mudança persistente:

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

7. Configure o firewall para acesso ao serviço HTTP.

a. Permita o serviço HTTP na sessão atual:

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

b. Torne a mudança persistente:

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

8. Configure o firewall para acesso ao serviço HTTPS.

a. Permita o serviço HTTPS na sessão atual:

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

b. Torne a mudança persistente:

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

9. Desabilite temporariamente o SELinux para os testes de configuração.

   a. Defina o SELinux para o modo permissivo:

   ```
   > sudo setenforce 0
   ```

   b. Verifique o status do SELinux:

   ```
   > sudo sestatus
   ```

10. Gere e instale os módulos de políticas locais do SELinux para os serviços relacionados ao PXE.

    a. Crie e instale um 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. Crie e instale um 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. Crie e instale um 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. Habilite novamente o modo de imposição no `SELinux`.

    a. Defina o `SELinux` para o modo de imposição:

    ```
    > sudo setenforce 1
    ```

    b. Verifique o status do `SELinux`:

    ```
    > sudo sestatus
    ```

2.4 Resumo

Este procedimento garantiu a configuração correta da interface de rede do servidor PXE, do firewall e da política do `SELinux` para uma operação segura e funcional.

- Verificou e atribuiu a interface de uso do PXE (`eno1`, neste exemplo) à zona `public` do firewalld.
- Abriu os serviços de firewall necessários à operação do PXE, incluindo `dns`, `ntp`, `dhcp`, `dhcpv6`, `tftp`, `http` e `https`.
- Definiu temporariamente o `SELinux` para o modo `permissive` para facilitar os testes de serviço e registrar negações do AVC.
- Usou **`ausearch`** e **`audit2allow`** para gerar e instalar módulos de políticas do SELinux personalizados para serviços como `nginx`, `dnsmasq` e `in.tftpd`.
- Restaurou o `SELinux` ao modo `enforcing` para proteger o sistema para uso em produção.

Com essas etapas concluídas, o servidor PXE foi configurado de forma segura e está pronto para atender às máquinas clientes pela rede usando IPv4 ou IPv6.

3 Instalando os componentes necessários do servidor PXE

Esta seção explica como instalar os pacotes necessários para suportar a inicialização PXE no SUSE Linux Enterprise Server 16.0, incluindo os componentes GRUB 2, DHCP, TFTP e/ou HTTP.

3.1 Introdução

Para configurar um servidor de inicialização PXE no SUSE Linux Enterprise Server 16.0, você precisa instalar vários serviços e ferramentas. Dependendo da sua configuração, você pode precisar dos seguintes itens:

- O pacote `dnsmasq` fornece uma combinação dos servidores DNS, TFTP e DHCP (DHCPv4 e DHCPv6) com suporte limitado a anúncio do roteador (RA, Router Advertising) IPv6. Ele oferece o seguinte:
  - Servidor DHCP dnsmasq: Suporta entrega condicional de opções DHCP dependendo da solicitação e da arquitetura do cliente para:
    - Solicitações de inicialização PXE por DHCPv4 e DHCPv6
    - Solicitações de inicialização HTTP por DHCPv4

    

    ### Nota: Limitações do dnsmasq para inicialização HTTP por DHCPv6

    Atualmente, o dnsmasq não suporta o envio da opção necessária `vendor-class` do DHCPv6.

  - Servidor TFTP dnsmasq: Entrega arquivos de carregador de boot, kernel e initrd por TFTP durante a inicialização PXE.

    - Servidor DNS dnsmasq: Fornece uma resolução recursiva de nomes de domínio e endereços IP para o firmware do cliente e o `/etc/resolv.conf` no instalador/sistema operacional.
    - RA IPv6 dnsmasq: Suporta o envio de RA IPv6 quando o servidor PXE também atua como roteador (capacidade de configuração limitada a um “padrão de RA comum”).
- O pacote `kea` inclui um servidor DHCP e um sucessor do servidor SC DHCP. Ele suporta entrega condicional de opções DHCP dependendo da solicitação e da arquitetura do cliente para:
    - Solicitações de inicialização PXE por DHCPv4 e DHCPv6
    - Solicitações de inicialização HTTP por DHCPv4

Nota: Limitações do KEA para inicialização HTTP por DHCPv6

Atualmente, o Kea não suporta o envio da opção necessária `vendor-class` do DHCPv6. Para obter mais informações, consulte https://kea.readthedocs.io/en/latest/arm/dhcp6-srv.html#id4.

- Um servidor TFTP entrega os arquivos de carregador de boot, o kernel e o initrd por TFTP, enquanto a inicialização PXE com o Kea é fornecida pelo pacote `tftp` e não é necessária para inicialização HTTP. Se você usa o `dnsmasq`, não precisa do pacote `tftp`.
- Um servidor Web, como o pacote `nginx`, para transmitir as imagens do instalador por HTTP.

Nota: Necessidade de servidores HTTP

Um servidor HTTP/HTTPS, como o nginx, é quase sempre necessário. Seu uso vai além de uma simples inicialização HTTP. Em particular, você pode precisar dele nos seguintes cenários:

- Ele é um requisito básico para a inicialização HTTP.
- É recomendado para fornecer o `squashfs.img`. Você pode usar `root=live:tftp://.../squashfs.img` na linha de comando de inicialização.
- Ele também é recomendado para fornecer RPMs ao Agama no parâmetro de linha de comando de inicialização `inst.install_url=http://.../install/` em um `SLES-16.0-Full-*.inline.iso`, junto com perfis de instalação e outros arquivos para instalação autônoma.

- Os pacotes do carregador de boot GRUB 2 fornecem inicialização de rede para arquiteturas e métodos suportados. Por exemplo, a arquitetura AMD64/Intel 64 oferece dois métodos para inicialização de rede: BIOS e UEFI. Além disso, a UEFI geralmente suporta inicialização PXE (TFTP) e HTTP. Outros carregadores de boot, como o pxelinux, não suportam UEFI e inicialização HTTP.
- Opcionalmente, um daemon de anúncio do roteador para IPv6, como o pacote `radvd`. Ele será necessário no SLES se também atuar como roteador para uma rede de instalador para realizar o seguinte:
  - Configurar o roteamento em uma rede para clientes de inicialização PXE ou HTTP.
  - Habilitar o uso de DHCPv6 em uma rede para clientes de inicialização PXE ou HTTP.

3.2 Requisitos

- Um sistema que executa o SUSE Linux Enterprise Server 16.0 com privilégios administrativos, registrado no SUSE Customer Center e configurado com acesso aos repositórios online apropriados usando SUSEConnect.
- Módulos do SLE habilitados: Módulo Server Applications, Módulo Legacy e Módulo Base System.
- Acesso aos repositórios de módulos do SLE para serviços de rede e carregadores de boot.
- Conexão com a Internet ativa para buscar os pacotes.

3.3 Instalando os pacotes

Siga as etapas abaixo para instalar os pacotes principais necessários para o servidor de inicialização PXE.

PROCEDIMENTO 1: INSTALANDO OS PACOTES NECESSÁRIOS PARA UM SERVIDOR DE INICIALIZAÇÃO PXE

1. Instale o carregador de boot GRUB 2 e o servidor HTTP nginx como requisitos comuns.

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

2. Execute qualquer um dos seguintes comandos para instalar os pacotes essenciais à sua abordagem:

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

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

   - `dnsmasq` como provedor comum para os servidores DHCP, DNS e TFTP

```
> sudo zypper install dnsmasq
```

Nota: Limitações de servidores DHCP fornecidos por Kea e dnsmasq

A inicialização HTTP por IPv6 *atualmente* não é suportada por servidores DHCP fornecidos pelos pacotes `kea` e `dnsmasq`. Ela não suporta o envio da opção `vendor-class` de volta ao cliente HTTP, conforme exigido pela especificação UEFI.

3. Se preferir, instale destinos adicionais do GRUB 2 específicos da arquitetura, se você planeja oferecer suporte a outras plataformas.

   - Para a arquitetura AMD64/Intel 64:

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

   - Para a arquitetura AArch64:

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

   - Para a arquitetura ppc64le:

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

   

   ### Nota: Como o servidor PXE entrega pacotes do GRUB 2 a clientes diferentes da arquitetura da máquina do servidor

   Os pacotes `noarch.rpm` específicos da arquitetura do GRUB 2 estão incluídos no subdiretório `noarch` da mídia/repositório de instalação, seja qual for a arquitetura da máquina em que o servidor PXE é configurado. Ou seja, você pode instalar os pacotes `grub2-arm64-efi` e `grub2-powerpc-ieee1275` em um servidor PXE executado em uma máquina AMD64/Intel 64, a fim de oferecer suporte a clientes com outras arquiteturas.

4. Você poderá instalar o pacote `shim` se precisar de Boot Seguro UEFI para AMD64/Intel 64 ou AArch64, mas não quiser usar os arquivos da mídia de instalação ISO.

   ```
   > sudo zypper install shim
   ```

5. Se preferir, instale o daemon de anúncio do roteador `radvd` para usar o servidor PXE como roteador (não recomendado para redes de produção).

   ```
   > sudo zypper install radvd
   ```

6. Instale o utilitário `rsync` para copiar ou sincronizar de maneira oportuna a ISO e a árvore de diretórios.

   ```
   > sudo zypper install rsync
   ```

7. Garanta que os serviços estejam instalados, mas ainda não tenham sido iniciados. A configuração será abordada em seções posteriores.

4 Criando diretórios NetBoot do GRUB 2 para servidor PXE

Esta seção explica como criar diretórios NetBoot do GRUB 2 para servidores PXE usando o comando **`grub2-mknetdir`**, que gera diretórios específicos da arquitetura para sistemas AMD64/Intel 64 (UEFI e BIOS), AArch64 e ppc64le. Para suporte a Boot Seguro UEFI, os administradores devem copiar os arquivos EFI assinados da mídia de instalação ou usar o pacote `shim` para substituir os arquivos de carregador de boot padrão não assinados.

4.1 Introdução

Esta seção descreve como configurar diretórios NetBoot do GRUB 2 para implantação do servidor PXE em várias arquiteturas. O comando **`grub2-mknetdir`** cria diretórios específicos da arquitetura em `/srv/tftpboot/boot/grub2/` para plataformas diferentes. Por exemplo, os sistemas AMD64/Intel 64 geram diretórios UEFI (`x86_64-efi`) e BIOS (`i386-pc`) antigos, enquanto os sistemas AArch64 e ppc64le criam seus respectivos diretórios UEFI (`arm64-efi` e `powerpc-ieee1275`).

Para suporte a Boot Seguro UEFI, que não é fornecido pelos arquivos `core.efi` padrão não assinados, os administradores podem copiar os arquivos EFI assinados da mídia de instalação ou instalar o pacote `shim` e copiar manualmente os arquivos de carregador de boot necessários (`shim.efi`, `grub.efi`, `MokManager.efi`) para os diretórios de arquitetura apropriados, garantindo uma resolução de link simbólico adequada para manter todos os arquivos no diretório raiz do TFTP.

4.2 Requisitos

- Garanta que você tenha instalado os seguintes pacotes: `grub2`, `tftp` e qualquer outro pacote do GRUB 2 específico da arquitetura, como `grub2-x86_64-efi` e `grub2-i386-pc`.
- Assegure que tenha a mídia de instalação (ISO) disponível para montagem ou o pacote `shim` instalado no sistema. Você pode baixar a mídia de instalação (ISO) para sua arquitetura de destino do SUSE Customer Center.

4.3 Preparando os diretórios NetBoot e o Boot Seguro UEFI

Este procedimento cria a estrutura de diretórios do GRUB 2 necessária para inicialização de rede PXE e, opcionalmente, configura o suporte a Boot Seguro UEFI em várias arquiteturas.

1. Crie uma estrutura de diretórios NetBoot do GRUB 2.

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

   Esse procedimento cria diretórios específicos da arquitetura:

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

   

   ### Atenção

   Não substitua manualmente o arquivo `grub.cfg` criado pelo **`grub2-mknetdir`**.

2. Copie outros diretórios independentes da arquitetura, como `fonts/` e `locale/`, que estão disponíveis no diretório `/srv/tftpboot/boot/grub2/` para o servidor TFTP.

3. Você também pode usar o arquivo `/srv/tftpboot/boot/grub2/ARCH-efi/core.efi` instalado pelo comando **`grub2-mknetdir`** para arquiteturas AMD64/Intel 64 ou AArch64 para PXE UEFI. No entanto, ele *não é assinado* e não suporta Boot Seguro UEFI. Opcionalmente, para habilitar o Boot Seguro UEFI para as arquiteturas AMD64/Intel 64 e AArch64 suportadas, siga qualquer uma destas etapas:

   - Copie os arquivos necessários da mídia de instalação ISO:

     a. Monte a imagem ISO:

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

     b. Copie os arquivos EFI.

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

     (1) Substitua *ARCH*`-efi` por `x86_64-efi` ou `arm64-efi`, as arquiteturas suportadas para Boot Seguro UEFI.

     c. Desmonte a mídia de instalação ISO.

     ```
     > sudo umount /mnt
     ```

   - Use o pacote `shim` se você não quiser usar os arquivos da mídia de instalação ISO:

     a. Se ainda não foi instalado, instale o pacote `shim`.

     ```
     > sudo zypper install shim
     ```

     b. Copie os arquivos de carregador de boot assinados para a arquitetura necessária:

        i. Copie o arquivo `shim.efi`.

        - Para a arquitetura 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 a arquitetura AArch64:

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

ii. Copie o arquivo `grub.efi`.

- Para a arquitetura AMD64/Intel 64:

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

- Para a arquitetura AArch64:

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

iii. Copie o arquivo `MokManager.efi`.

- Para a arquitetura AMD64/Intel 64:

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

- Para a arquitetura AArch64:

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

Nota

O flag `-L` resolve links simbólicos para garantir que os arquivos permaneçam na raiz do TFTP.

5 Preparando o conteúdo da imagem do instalador

Esta seção descreve como extrair e organizar arquivos do instalador da mídia de instalação do SUSE Linux Enterprise Server 16.0 para ambientes de inicialização PXE. Ela aborda as imagens `.install.iso` e os pacotes RPM, com instruções específicas para diversas arquiteturas e tipos de instalação.

5.1 Introdução

O SUSE Linux Enterprise Server 16.0 inclui arquivos do instalador em vários formatos para suportar diferentes cenários de inicialização PXE. O instalador Agama requer três arquivos essenciais: a imagem do kernel (`linux`), o disco RAM inicial (`initrd`) e o sistema de arquivos raiz compactado (`squashfs.img`). Esses arquivos devem ser extraídos da mídia de instalação e organizados em uma estrutura de diretórios acessível por TFTP e HTTP.

Esta seção apresenta os métodos de preparação para as imagens `.install.iso` e os pacotes RPM, garantindo a compatibilidade com várias arquiteturas e tipos de instalação suportados pelo SUSE Linux Enterprise Server 16.0.

5.2 Requisitos

- Mídia de instalação do SUSE Linux Enterprise Server 16.0, conforme disponível no SUSE Customer Center. Escolha:
  - ISO online: Somente instalador para instalações de rede (`SLES-16.0-Online-`*`ARCH-BUILD`*`.install.iso`)
  - ISO completa: Instalador com repositório de instalação (`SLES-16.0-Full-`*`ARCH-BUILD`*`.install.iso`)
  - Pacotes RPM: `tftpboot-agama-installer-SUSE_SLE_16_PXE-`*`ARCH`*
- Um ponto de montagem temporário, como `/mnt`.
- Espaço em disco suficiente em `/srv/tftpboot` e `/srv/install` para o método de instalação escolhido.
- Privilégios administrativos para criar diretórios e copiar arquivos.

5.3 Preparando arquivos do instalador com base em imagens ISO

As imagens ISO oferecem um método simples para extrair arquivos do instalador. Os procedimentos a seguir abordam os tipos de ISO online e completa para diferentes arquiteturas.

5.3.1 Usando imagens ISO online

As imagens ISO online contêm apenas os componentes do instalador, exigindo acesso da rede aos repositórios de instalação durante a instalação do sistema. Isso corresponde à entrada do menu de inicialização do `SLES-16.0 Online Installation` no GRUB.

PROCEDIMENTO 2: EXTRAINDO ARQUIVOS DA ISO ONLINE (X86_64 E AARCH64)

1. Crie a estrutura de diretórios para os arquivos do instalador:

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

2. Monte a imagem ISO online:

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

3. Copie o kernel e os arquivos 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 o sistema de arquivos raiz compactado:

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

5. Desmonte a imagem ISO:

```
> sudo umount /mnt
```

PROCEDIMENTO 3: EXTRAINDO ARQUIVOS DA ISO ONLINE (PPC64LE)

1. Crie a estrutura do diretório:

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

2. Monte a imagem ISO:

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

3. Copie o kernel e os arquivos initrd (observe a estrutura de caminho diferente 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 o sistema de arquivos raiz compactado:

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

5. Desmonte a imagem ISO:

```
> sudo umount /mnt
```

5.3.2 Usando as imagens ISO completas

As imagens ISO completas incluem tanto o instalador quanto os repositórios de instalação, permitindo instalações locais sem dependências da rede externa. Isso corresponde à entrada do menu de inicialização do `SLES-16.0 Local Installation` no GRUB com o parâmetro `inst.install_url=http://pxe.example.net/install/SLES-16.0/${arch}` adicional.

PROCEDIMENTO 4: EXTRAINDO ARQUIVOS DA ISO COMPLETA

1. Crie diretórios para os arquivos do instalador e o repositório de instalação:

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

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

2. Monte a imagem ISO completa:

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

3. Copie o kernel e os arquivos initrd (ajuste os caminhos para ppc64le conforme mostrado nos procedimentos 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 o sistema de arquivos raiz compactado:

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

5. Copie o repositório de instalação para acesso ao servidor HTTP local:

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

6. Desmonte a imagem ISO:

```
> sudo umount /mnt
```

5.4 Preparando arquivos do instalador com base em pacotes RPM

Os pacotes RPM oferecem um método alternativo para obter os arquivos do instalador online.

PROCEDIMENTO 5: INSTALANDO E USANDO OS PACOTES RPM TFTPBOOT

1. Instale os pacotes obrigatórios:

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

2. Copie o linux,initrd,squashfs.img para 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 Estrutura de diretórios recomendada

Organize os arquivos extraídos de acordo com o layout de diretório abaixo para garantir consistência e facilidade de manutenção. Esta estrutura suporta várias arquiteturas e tipos de instalação.

EXEMPLO 1: LAYOUT COMPLETO DE DIRETÓRIO DO 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 (1)
│           │   ├── initrd (2)
│           │   └── squashfs.img (3)
│           ├── aarch64/
│           └── ppc64le/
/srv/install/
└── SLES-16.0/
    ├── x86_64/ (4)
    ├── aarch64/
    └── ppc64le/
```

1. Imagem do kernel extraída da mídia de instalação
2. Imagem de disco RAM inicial
3. Sistema de arquivos raiz compactado para instalador Agama
4. Repositório de instalação do diretório `install` com base na ISO completa (opcional)

5.6 Verificando a instalação

Depois de extrair e organizar os arquivos do instalador, verifique se todos os componentes necessários estão presentes e acessíveis.

PROCEDIMENTO 6: ETAPAS DE VERIFICAÇÃO

1. Verifique se os arquivos essenciais estão presentes:

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

2. Garanta as permissões de arquivo apropriadas:

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

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

Importante: Acessibilidade dos arquivos

Garanta que todos os arquivos extraídos possam ser lidos pelos serviços TFTP e HTTP. Os arquivos serão acessados pelos clientes PXE durante o processo de inicialização, portanto, as permissões e a configuração do serviço apropriadas são essenciais para o sucesso das implantações.

5.7 Próximas etapas

Com os arquivos do instalador devidamente preparados e organizados, você pode prosseguir para:

- Configurar o GRUB 2 para inicialização PXE com entradas de menu que mencionam esses arquivos
- Configurar os serviços HTTP e TFTP para transmitir o conteúdo extraído
- Configurar o DHCP para direcionar os clientes PXE aos carregadores de boot apropriados

Os arquivos extraídos serão mencionados na configuração do GRUB 2 usando caminhos como `root=live:http://pxe.example.net/boot/images/SLES-16.0/ARCH/squashfs.img`.

6 Configurando o GRUB 2 para inicialização PXE

Esta seção descreve como configurar o carregador de boot GRUB 2 para inicialização baseada em PXE no SUSE Linux Enterprise Server 16.0. Ela aborda a criação da estrutura de diretórios de inicialização de rede, a configuração de carregadores de boot específicos da arquitetura e a implementação de um sistema de configuração flexível com suporte a várias arquiteturas e cenários de instalação.

6.1 Introdução

O GRUB 2 atua como carregador de boot de rede para clientes PXE, carregando o kernel e os arquivos initrd para iniciar o instalador Agama. Esta seção demonstra como criar uma configuração sofisticada do GRUB 2 que detecta automaticamente a arquitetura do cliente, gerencia a seleção da interface de rede e oferece um menu de inicialização unificado que suporta vários tipos de instalação e arquiteturas de destino.

A abordagem de configuração usa um design modular com arquivos separados para detecção de arquitetura, definições de variáveis e entradas do menu de inicialização. Isso permite o suporte a configurações específicas da máquina e perfis de instalação automatizados, mantendo a consistência entre plataformas de hardware diferentes.

6.2 Requisitos

- Garanta que a estrutura de diretórios de inicialização de rede do GRUB 2 já esteja pronta, conforme descrito nas seções anteriores.
- Certifique-se de que os arquivos do instalador estejam devidamente organizados, conforme descrito nas seções anteriores.
- Os pacotes GRUB 2 para todas as arquiteturas de destino devem ser instalados: `grub2-x86_64-efi`, `grub2-i386-pc`, `grub2-aarch64-efi` e `grub2-ppc64le-ieee1275`
- O pacote `shim` para suporte a Boot Seguro UEFI (opcional).
- Acesso administrativo ao `/srv/tftpboot` ou à raiz do PXE equivalente.

6.3 Criando a configuração do GRUB 2

O arquivo de configuração do GRUB 2 processa três tarefas principais: detectar a arquitetura do cliente, gerenciar as interfaces de rede e carregar outros arquivos de configuração. Esta abordagem modular oferece flexibilidade para diversos cenários de implantação.

PROCEDIMENTO 7: CONFIGURANDO O ARQUIVO `grub.cfg` PRINCIPAL

- Crie o arquivo de configuração principal do GRUB 2 em `/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
```

PRINCIPAIS ELEMENTOS DA CONFIGURAÇÃO

Detecção de arquitetura

Mapeia os tipos de CPU do GRUB 2 para as arquiteturas de distribuição, permitindo entradas de menu unificadas que funcionam em plataformas de hardware diferentes

Gerenciamento de interface de rede

Define uma variável `${ipcfg}` usando a variável grub2 `${net_default_mac}` para ativar o DHCP apenas na interface de inicialização PXE chamada `pxe0`, o que evita problemas de sondagem de rede em sistemas com várias interfaces.

Definições de utilitários

Define uma variável `${sconsole}` típica com parâmetros de console serial.

Configuração específica da máquina

Carrega os arquivos de configuração opcionais por máquina com base no endereço MAC, permitindo parâmetros de inicialização personalizados por máquina e perfis de instalação automatizados

6.4 Criando o menu de inicialização unificado

O menu de inicialização usa variáveis da configuração principal para fornecer entradas de menu independentes da arquitetura, que se adaptam automaticamente a diferentes plataformas de hardware e tipos de instalação.

PROCEDIMENTO 8: CONFIGURANDO O ARQUIVO MENU.CFG

- Crie o menu de inicialização unificado em `/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: Flexibilidade de entrada de menu

As entradas de menu usam variáveis que são automaticamente preenchidas com base na arquitetura e na configuração do cliente. A variável `${arch}` garante que os arquivos corretos sejam carregados.

A variável `${ipcfg}` opcional faz com que apenas a interface de rede selecionada pelo PXE seja configurada.

A variável `${sconsole}` opcional habilita um console serial no sistema do instalador.

6.5 Configurações específicas da máquina

Em implantações avançadas, você pode criar arquivos de configuração específicos da máquina para substituir as configurações padrão ou fornecer parâmetros de instalação automatizados.

PROCEDIMENTO 9: CRIANDO UMA CONFIGURAÇÃO ESPECÍFICA DA MÁQUINA

1. Crie um diretório para configurações específicas da máquina:

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

2. Para uma máquina com o endereço MAC `aa:bb:cc:dd:ee:ff`, crie uma configuração específica:

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

3. Crie o `grub.cfg` específico da máquina:

```
> 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=eno1: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
```

Se preferir, forneça uma entrada de menu própria no `grub.cfg` específico do host (por exemplo, gerada para uma tentativa de inicialização específica):

```
> 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=eno1:dhcp
  initrd /boot/images/SLES-16.0/${arch}/initrd
}
EOF
```

EXEMPLO 2: PARÂMETROS COMUNS ESPECÍFICOS DA MÁQUINA

`default`
: Especifica qual entrada de menu deve ser inicializada automaticamente

`timeout`
: Define o tempo de espera de inicialização em segundos

`ipcfg`
: Substitui a configuração da interface de rede para um hardware específico

`autoinstall`
: Fornece URLs dos perfis de instalação automatizada específicos da máquina

6.6 Verificando a configuração do GRUB 2

Depois de criar os arquivos de configuração, verifique se a configuração está correta e se todos os arquivos necessários estão disponíveis.

PROCEDIMENTO 10: ETAPAS DE VERIFICAÇÃO

1. Verifique a estrutura de diretórios do GRUB 2:

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

2. Verifique a sintaxe do arquivo de configuração fazendo um teste com as ferramentas do GRUB 2:

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

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

3. Garanta as permissões de arquivo apropriadas:

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

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

Importante: Teste da configuração

Teste a configuração do GRUB 2 com clientes PXE reais para garantir a detecção da arquitetura e a funcionalidade de menu apropriadas. A variável `${net_default_mac}` está disponível apenas durante cenários de inicialização de rede reais.

6.7 Solucionando problemas da configuração do GRUB 2

Problemas comuns e suas soluções ao trabalhar com configurações PXE do GRUB 2. Cada problema inclui as etapas de diagnóstico e os comandos específicos para resolvê-lo.

6.7.1 Falha na detecção de arquitetura

Quando o GRUB 2 não consegue detectar a arquitetura correta, os clientes podem ser inicializados com binários incorretos ou nem ser carregados.

PROCEDIMENTO 11: DEPURANDO A DETECÇÃO DE ARQUITETURA

1. Adicione a saída da depuração à configuração do GRUB 2 para ver os 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. Teste a sintaxe da configuração:

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

3. Se o mapeamento da arquitetura estiver incompleto, estenda a lógica de detecção:

```
> 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 se os diretórios específicos da arquitetura existem:

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

6.7.2 Interface de rede não encontrada

Algumas implementações de firmware podem não definir a variável `${net_default_mac}` corretamente, causando falhas na configuração de rede.

PROCEDIMENTO 12: DIAGNOSTICANDO PROBLEMAS NA INTERFACE DE REDE

1. Adicione a saída da depuração para verificar as variáveis de rede:

```
> 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. Crie uma configuração de rede de fallback:

```
> 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. Teste a configuração de rede com uma interface específica:

```
> sudo echo 'set ipcfg="ip=eno1:dhcp"' > /srv/tftpboot/boot/config/test-network.cfg
```

4. Verifique os nomes das interfaces de rede no sistema de destino:

```
> ip link show
```

6.7.3 Caminhos de arquivo não encontrados

Caminhos de arquivos incorretos impedem o GRUB 2 de carregar o kernel e os arquivos initrd, causando falhas na inicialização.

PROCEDIMENTO 13: VERIFICANDO A ACESSIBILIDADE DOS CAMINHOS DE ARQUIVOS

1. Verifique se os arquivos do instalador existem nos locais esperados:

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

2. Verifique o acesso por TFTP aos arquivos de inicialização:

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

3. Teste o acesso por HTTP aos arquivos do instalador:

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

4. Verifique as permissões e a propriedade dos arquivos:

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

5. Corrija as permissões, se necessário:

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

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

6. Verifique se os links simbólicos não estão corrompidos:

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

6.7.4 Falhas na inicialização EFI

Os problemas com EFI e Boot Seguro podem impedir a inicialização adequada do carregador de boot ou causar falhas na autenticação.

PROCEDIMENTO 14: DIAGNOSTICANDO PROBLEMAS NA INICIALIZAÇÃO EFI

1. Verifique se os arquivos do Boot Seguro estão presentes:

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

2. Verifique se os arquivos shim (bootx64.efi ou shim.efi), grub.efi e MokManager.efi foram copiados de maneira apropriada:

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

3. Verifique a integridade do arquivo EFI:

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

4. Teste se os arquivos são acessíveis por TFTP:

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

5. Para sistemas aarch64, verifique os arquivos EFI ARM64:

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

6. Verifique se a configuração do DHCP fornece os caminhos corretos do carregador de boot:

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

7. Se os arquivos estiverem ausentes, copie-os novamente da ISO montada em /mnt ou dos arquivos do pacote shim:

```
> sudo cp -v /mnt/EFI/BOOT/*.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 Entradas de menu não carregadas

Quando o GRUB 2 faz o carregamento, mas as entradas de menu apresentam falham ou erros, o problema costuma estar relacionado à expansão de variáveis ou às referências de arquivos.

PROCEDIMENTO 15: DEPURANDO PROBLEMAS DE ENTRADAS DE MENU

1. Teste a sintaxe da configuração do menu:

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

2. Adicione a saída da depuração às entradas de menu:

```
> 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 se a expansão da variável funciona corretamente:

```
> 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. Faça o teste uma entrada de menu 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. Carregue o menu de teste temporariamente:

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

6. Restaure o menu original após o teste:

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

6.7.6 Habilitando o registro detalhado

Para problemas persistentes, habilite o registro completo para capturar informações detalhadas sobre o processo de inicialização.

PROCEDIMENTO 16: CONFIGURANDO O REGISTRO DE DEPURAÇÃO DO GRUB 2

1. Crie uma versão de depuração da configuração principal:

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

2. Adicione a saída de depuração 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. Inclua a configuração de depuração no arquivo principal:

```
> sudo sed -i '1i\source "${prefix}/debug.cfg"' /srv/tftpboot/boot/grub2/grub.cfg
```

4. Monitore os registros do TFTP durante as tentativas de inicialização:

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

5. Monitore os registros do DHCP para solicitações de PXE:

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

6. Desabilite o modo de depuração após a solução de problemas:

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

6.8 Próximas etapas

Com o GRUB 2 devidamente configurado, você pode prosseguir para:

- Configurar os serviços HTTP e TFTP para transmitir os arquivos de inicialização e o conteúdo do instalador
- Configurar os serviços DHCP para direcionar os clientes PXE aos carregadores de boot apropriados
- Testar o processo de inicialização PXE completo no hardware de destino

O sistema de configuração do GRUB 2 flexível oferece uma base para cenários sofisticados de implantação PXE, para suportar várias arquiteturas e tipos de instalação em uma interface unificada.

7 Configurando o TFTP para inicialização PXE

Esta seção explica como configurar os serviços TFTP para transmitir os carregadores de boot GRUB 2 e o conteúdo de inicialização PXE para instalações do SUSE Linux Enterprise Server 16.0. Ela aborda o servidor `in.tftpd` tradicional e a funcionalidade TFTP integrada fornecida por `dnsmasq`.

7.1 Introdução

O TFTP transmite os arquivos do carregador de boot para os clientes PXE durante o processo de inicialização de rede. O SUSE Linux Enterprise Server 16.0 suporta duas implementações de servidor TFTP: o servidor `in.tftpd` tradicional do pacote `tftp`, e a funcionalidade TFTP integrada em `dnsmasq`.

7.2 Requisitos

- O pacote `tftp` ou `dnsmasq` instalado
- Arquivos de inicialização PXE organizados em `/srv/tftpboot`
- Privilégios administrativos para configurar os serviços

7.3 Configurando o servidor in.tftpd

O servidor `in.tftpd` usa o arquivo de configuração `/etc/sysconfig/tftp` para definir o diretório raiz do TFTP e as opções de servidor.

PROCEDIMENTO 17: CONFIGURANDO O SERVIDOR TFTP IN.TFTPD

1. Opcionalmente, habilite o registro detalhado definindo as opções de TFTP:

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

   A opção `-v` habilita o registro detalhado para ver os nomes de arquivo buscados por TFTP.

2. Habilite e inicie o serviço TFTP:

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

7.4 Configurando o servidor TFTP dnsmasq

O `dnsmasq` oferece um servidor TFTP incorporado que pode ser habilitado e configurado para usar o diretório `/srv/tftpboot`.

PROCEDIMENTO 18: CONFIGURANDO A FUNCIONALIDADE DO TFTP DNSMASQ

1. Crie o arquivo de configuração do TFTP:

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

2. Habilite e inicie o serviço dnsmasq:

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

7.5 Verificando a configuração do TFTP

Teste a funcionalidade do servidor TFTP para garantir que ele possa transmitir arquivos aos clientes PXE.

PROCEDIMENTO 19: TESTANDO A FUNCIONALIDADE DO SERVIDOR TFTP

1. Crie um arquivo de teste:

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

2. Recupere o arquivo de teste por TFTP:

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

3. Verifique se o arquivo foi recuperado com êxito:

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

4. Limpe os arquivos de teste:

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

7.6 Solucionando problemas da configuração do TFTP

Problemas comuns ao configurar serviços TFTP para ambientes de inicialização PXE.

7.6.1 Conflitos de serviços na porta 69

Tanto o `in.tftpd` quanto o `dnsmasq` usam a porta UDP 69 para serviços TFTP e não podem ser executados simultaneamente.

PROCEDIMENTO 20: RESOLVENDO CONFLITOS DE SERVIÇOS TFTP

1. Verifique quais serviços estão em execução:

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

2. Verifique que serviço está usando a porta 69:

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

3. Pare o serviço em conflito (exemplo para dnsmasq):

```
> sudo systemctl stop dnsmasq
```

4. Inicie o serviço TFTP de sua preferência:

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

7.6.2 Problemas do diretório TFTP

Problemas ao acessar o sistema de arquivos raiz do TFTP que podem impedir a transmissão de arquivos.

PROCEDIMENTO 21: VERIFICANDO A CONFIGURAÇÃO DO DIRETÓRIO TFTP

1. Verifique a configuração do diretório TFTP para in.tftpd:

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

2. Verifique a configuração do diretório TFTP para dnsmasq:

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

3. Verifique se o diretório existe:

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

4. Crie o diretório se ainda não existir:

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

7.6.3 Habilitando o registro do TFTP

O registro detalhado ajuda a identificar problemas de acesso a arquivos com transferências por TFTP.

PROCEDIMENTO 22: HABILITANDO O REGISTRO DETALHADO DO TFTP

1. Verifique as opções atuais do TFTP:

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

2. Habilite o registro detalhado:

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

3. Reinicie o serviço TFTP:

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

4. Monitores os registros do TFTP:

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

7.7 Próximas etapas

Com o TFTP configurado, você pode prosseguir para a configuração dos serviços HTTP, para transmitir arquivos do instalador, e dos serviços DHCP, para direcionar os clientes PXE aos carregadores de boot apropriados.

8 Configurando o nginx para entrega por HTTP

Esta seção explica como configurar o nginx para fornecer o conteúdo da inicialização PXE por HTTP, permitindo que os clientes carreguem os arquivos do instalador, como kernel, initrd e imagens squashfs, de um local central. A entrega por HTTP oferece um desempenho melhor do que o TFTP para arquivos grandes e é necessária para as instalações do SUSE Linux Enterprise Server 16.0 pelo Agama.

8.1 Introdução

O nginx atua como servidor HTTP para ambientes de inicialização PXE, fornecendo acesso aos arquivos do instalador por meio de entrega baseada na Web. O servidor HTTP expõe o diretório de inicialização e os repositórios de instalação do TFTP, permitindo que os clientes PXE baixem as imagens do kernel, os arquivos initrd e os componentes do instalador Agama por HTTP, em vez do protocolo TFTP mais lento.

8.2 Requisitos

- O pacote `nginx` instalado
- Arquivos de inicialização PXE organizados em `/srv/tftpboot/boot`
- Repositórios de instalação disponíveis em `/srv/install`
- Privilégios administrativos para modificar a configuração do nginx

8.3 Configurando o nginx para inicialização PXE

A configuração do nginx define aliases de local que expõem o diretório de boot TFTP e os repositórios de instalação por meio de URLs HTTP.

PROCEDIMENTO 23: CONFIGURANDO O SERVIDOR HTTP NGINX

1. Edite o arquivo de configuração do nginx:

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

2. Configure o bloco do servidor HTTP na seção `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. Teste a sintaxe da configuração do nginx:

```
> sudo nginx -t
```

4. Habilite e inicie o serviço nginx:

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

8.4 Verificando a configuração do nginx

Teste a funcionalidade do servidor HTTP para garantir que ele possa transmitir os arquivos de inicialização PXE e o conteúdo de instalação aos clientes.

PROCEDIMENTO 24: TESTANDO O SERVIDOR HTTP NGINX

1. Teste o acesso por HTTP aos arquivos de inicialização:

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

2. Teste o acesso ao diretório de instalação:

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

3. Verifique se um arquivo do instalador específico está acessível:

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

8.5 Solucionando problemas da configuração do nginx

Problemas comuns ao configurar o nginx para entrega por HTTP com inicialização PXE.

8.5.1 Erros na sintaxe da configuração

A sintaxe incorreta da configuração do nginx impede que o serviço seja iniciado ou recarregado de maneira apropriada.

PROCEDIMENTO 25: RESOLVENDO PROBLEMAS DA CONFIGURAÇÃO DO NGINX

1. Teste a sintaxe da configuração:

```
> sudo nginx -t
```

2. Verifique o status do serviço nginx se a inicialização falhar:

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

3. Veja os registros detalhados de erros:

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

4. Consulte o arquivo de registro de erros do nginx:

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

8.5.2 Problemas de acesso e permissão de arquivos

O nginx pode falhar ao transmitir arquivos devido a permissões incorretas ou diretórios ausentes.

PROCEDIMENTO 26: RESOLVENDO PROBLEMAS DE ACESSO A ARQUIVOS

1. Verifique se o diretório de inicialização existe e está acessível:

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

2. Verifique se o diretório de instalação existe:

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

3. Verifique se o nginx pode ler os diretórios:

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

4. Crie os diretórios ausentes, se necessário:

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

5. Defina as permissões apropriadas:

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

8.5.3 Conflitos de vinculação de porta

Pode haver falha para iniciar o nginx se outro serviço está usando a porta 80.

PROCEDIMENTO 27: RESOLVENDO CONFLITOS DE PORTA

1. Verifique que serviço está usando a porta 80:

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

2. Pare os serviços em conflito, se necessário:

```
> sudo systemctl stop apache2
```

3. Inicie o serviço nginx:

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

4. Verifique se o nginx escuta na porta 80:

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

8.6 Próximas etapas

Com o nginx configurado para entrega por HTTP, você pode prosseguir para a configuração dos serviços DHCP, para direcionar os clientes PXE aos carregadores de boot e recursos HTTP apropriados.

9 Configurando um servidor DNS usando dnsmasq

Esta seção explica como configurar os serviços DNS usando o dnsmasq para fornecer resolução de nomes de host aos clientes PXE que acessam os recursos de instalação do SUSE Linux Enterprise Server 16.0. A configuração de DNS permite que os clientes usem nomes de host em vez de endereços IP nos URLs de inicialização e nas configurações de DHCP.

9.1 Introdução

Os serviços DNS permitem que os clientes PXE resolvam os nomes de host nos URLs de inicialização e nas fontes de instalação. A configuração completa do servidor DNS está fora do escopo deste documento, mas esta seção apresenta uma configuração de DNS básica usando o dnsmasq, que permite que os clientes resolvam o nome de host do servidor PXE (*PXE.EXAMPLE.NET*) para os respectivos endereços IP.

Sem a configuração de DNS, os URLs de inicialização devem usar diretamente os endereços IP, como `http://192.168.1.200/` ou `http://[2001:db8:0:1::200]/`. Algumas implementações de firmware BIOS/UEFI não suportam nomes de host em URLs DHCP/TFTP e exigem endereços IP como `tftp://[2001:db8:0:1::200]/`.

9.2 Requisitos

- O pacote `dnsmasq` instalado
- Configuração de endereços IP estáticos para o servidor PXE
- Privilégios administrativos para configurar os serviços DNS

9.3 Configurando serviços DNS do dnsmasq

A configuração de DNS do dnsmasq fornece uma resolução de nome de host local e usa servidores de nomes upstream para consultas externas.

PROCEDIMENTO 28: CONFIGURANDO O SERVIDOR DNS DO DNSMASQ:

1. Crie o arquivo de configuração de DNS para o 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. Adicione entradas de nome de host ao arquivo de hosts do sistema:

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

3. Teste a configuração do dnsmasq:

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

4. Habilite e inicie o serviço dnsmasq:

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

Nota: Comportamento do encaminhamento de DNS

Por padrão, o dnsmasq usa os servidores de nomes em `/etc/resolv.conf` como encaminhadores e fornece registros de `/etc/hosts`. Isso permite que o servidor PXE resolva nomes de host externos enquanto fornece uma resolução local para serviços relacionados ao PXE.

9.4 Verificando a configuração de DNS

Teste a funcionalidade do servidor DNS para garantir que a resolução de nomes de host funcione para os clientes PXE.

PROCEDIMENTO 29: TESTANDO A FUNCIONALIDADE DO SERVIDOR DNS

1. Teste a resolução de nome de host IPv4:

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

2. Teste a resolução de nome de host IPv6:

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

3. Teste a pesquisa DNS reversa para IPv4:

```
> nslookup 192.168.1.200 localhost
```

4. Verifique se o encaminhamento de DNS externo ainda funciona:

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

9.5 Solucionando problemas da configuração de DNS

Problemas comuns ao configurar o dnsmasq para serviços DNS em ambientes PXE.

9.5.1 Problemas de configuração e serviço

Pode haver falha para iniciar o dnsmasq devido a erros de configuração ou conflitos de porta.

PROCEDIMENTO 30: RESOLVENDO PROBLEMAS DA CONFIGURAÇÃO DE DNS

1. Teste a sintaxe de configuração do dnsmasq:

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

2. Verifique o status do serviço dnsmasq:

```
> systemctl status dnsmasq
```

3. Verifique que serviço está usando a porta DNS 53:

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

4. Veja os registros de erros do dnsmasq:

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

5. Pare os serviços DNS em conflito, se necessário:

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

9.5.2 Falhas na resolução de nome de host

As consultas DNS podem falhar devido à configuração incorreta ou a entradas de nome de host ausentes.

PROCEDIMENTO 31: DIAGNOSTICANDO PROBLEMAS DA RESOLUÇÃO DE DNS

1. Verifique se as entradas de nome de host existem no arquivo hosts:

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

2. Verifique a configuração do domínio no dnsmasq:

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

3. Teste a consulta DNS com uma saída detalhada:

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

4. Monitore os registros da consulta dnsmasq:

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

5. Reinicie o dnsmasq para recarregar a configuração:

```
> sudo systemctl restart dnsmasq
```

9.5.3 Problemas de encaminhamento de DNS

As consultas DNS externas poderão falhar se a configuração do servidor de nomes upstream estiver incorreta.

PROCEDIMENTO 32: SOLUCIONANDO PROBLEMAS DE ENCAMINHAMENTO DE DNS

1. Verifique a configuração do servidor de nomes upstream:

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

2. Teste a consulta direta no servidor de nomes upstream:

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

3. Verifique a configuração do encaminhamento de dnsmasq:

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

4. Adicione um servidor de nomes upstream específico, se necessário:

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

5. Reinicie o serviço dnsmasq:

```
> sudo systemctl restart dnsmasq
```

9.6 Próximas etapas

Com os serviços DNS configurados, os clientes PXE agora podem resolver os nomes de host nos URLs de inicialização e nas fontes de instalação. Você pode prosseguir para configurar os serviços DHCP que fazem referência ao servidor DNS para configuração do cliente.

10 Configurando um servidor NTP com o chrony

Esta seção explica como configurar os serviços NTP usando o `chrony` para fornecer sincronização de horário precisa aos clientes PXE durante as instalações do SUSE Linux Enterprise Server 16.0. A sincronização de horário apropriada é essencial para validação de certificados e registro do sistema durante as instalações baseadas em rede.

10.1 Introdução

Os serviços NTP garantem a sincronização de horário precisa em toda a infraestrutura de rede. Para ambientes de inicialização PXE, o horário sincronizado é crucial para validação de certificados durante conexões HTTPS, marcações de horário apropriadas dos registros e operações coordenadas do sistema. Esta seção apresenta a configuração básica do servidor NTP usando o `chrony`.

10.2 Requisitos

- O pacote `chrony` instalado

```
> sudo zypper install chrony
```

- Conectividade de rede com os servidores NTP upstream
- Privilégios administrativos para configurar os serviços NTP

10.3 Configurando o serviço NTP chrony

O serviço de `chrony` oferece a funcionalidade NTP com sincronização automática de horário para servidores upstream e recursos de exibição de horário local para clientes de rede.

PROCEDIMENTO 33: CONFIGURANDO O SERVIDOR NTP DO `chrony`

- Habilite e inicie o serviço `chrony`:

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

10.4 Verificando a configuração do NTP

Teste a funcionalidade do serviço NTP para garantir que a sincronização de horário funcione corretamente.

PROCEDIMENTO 34: TESTANDO A FUNCIONALIDADE DO SERVIDOR NTP

1. Verifique o status do serviço `chrony`:

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

2. Veja o status da sincronização de horário atual:

```
> chronyc tracking
```

3. Liste as fontes de NTP configuradas:

```
> chronyc sources
```

4. Verifique as estatísticas do servidor NTP:

```
> chronyc sourcestats
```

10.5 Solucionando problemas da configuração do NTP

Problemas comuns ao configurar o `chrony` para serviços NTP em ambientes PXE.

10.5.1 Problemas de inicialização do serviço

Pode haver falha para iniciar o serviço `chrony` devido a erros de configuração ou problemas de conectividade de rede.

PROCEDIMENTO 35: RESOLVENDO PROBLEMAS DO SERVIÇO NTP

1. Verifique o status e os registros do serviço `chrony`:

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

2. Veja os registros detalhados do serviço:

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

3. Teste a configuração do `chrony`:

```
> sudo chronyd -Q
```

4. Reinicie os serviços, se necessário:

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

10.5.2 Falhas de sincronização de horário

Pode haver falha na sincronização de horário devido a problemas de rede ou à configuração incorreta do servidor.

PROCEDIMENTO 36: DIAGNOSTICANDO PROBLEMAS DE SINCRONIZAÇÃO DE HORÁRIO

1. Verifique o status da sincronização atual:

```
> chronyc tracking
```

2. Veja a conectividade da fonte de NTP:

```
> chronyc sources -v
```

3. Force a sincronização imediata:

```
> sudo chronyc makestep
```

4. Compare o horário do sistema com o relógio do hardware:

```
> timedatectl status
```

5. Verifique a conectividade de rede com os servidores NTP:

```
> chronyc activity
```

10.5.3 Problemas de firewall e rede

As regras de firewall podem bloquear o tráfego NTP, impedindo a sincronização de horário.

PROCEDIMENTO 37: RESOLVENDO A CONECTIVIDADE DE REDE NTP

1. Verifique se a porta NTP está aberta no firewall:

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

2. Adicione o serviço NTP ao firewall, se necessário:

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

3. Recarregue a configuração do firewall:

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

4. Teste a conectividade NTP manualmente:

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

5. Verifique o uso da porta do `chrony`:

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

10.6 Próximas etapas

Com os serviços NTP configurados, o servidor PXE e os clientes mantêm a sincronização de horário precisa. Isso garante a validação apropriada de certificados e operações coordenadas do sistema durante instalações baseadas em rede.

11 Configurando o anúncio do roteador IPv6

Esta seção descreve como configurar a funcionalidade de anúncio do roteador IPv6 para fornecer anúncios do roteador adequados aos clientes PXE. O RA IPv6 habilita a configuração do roteamento IPv6 e a configuração automática de endereço DHCPv6 com informações de estado para as instalações do SUSE Linux Enterprise Server 16.0.

11.1 Introdução

O anúncio do roteador (RA, Router Advertisement) IPv6 fornece informações essenciais da configuração de rede aos clientes PXE, incluindo roteamento IPv6 e definições automática de configuração de endereço DHCPv6. Esta seção considera que um roteador IPv6 está configurado para fornecer anúncios do roteador adequados para configurar o roteamento IPv6 para a rede e a rota padrão e para habilitar a configuração automática de endereço DHCPv6 com informações de estado usando `AdvManagedFlag on`.

11.2 Requisitos

- O pacote `radvd` instalado
- Configuração de rede IPv6 na interface do servidor
- Privilégios administrativos para configurar os serviços de anúncio do roteador

11.3 Configurando o `radvd` para anúncio do roteador IPv6

O serviço `radvd` oferece a funcionalidade de anúncio do roteador IPv6 com base na configuração definida em `/etc/radvd.conf`.

PROCEDIMENTO 38: CONFIGURANDO O ANÚNCIO DO ROTEADOR IPV6 DE `radvd`

1. Configure o serviço `radvd`:

```
> sudo cat > /etc/radvd.conf << 'EOF'
interface eno1
{
    # 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 o serviço `radvd`:

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

11.4 Verificando o anúncio do roteador IPv6

Teste a funcionalidade RA do IPv6 RA para garantir configuração e operação apropriadas.

PROCEDIMENTO 39: TESTANDO O ANÚNCIO DO ROTEADOR IPV6

1. Verifique o status do serviço `radvd`:

```
> systemctl status radvd
```

2. Revise e verifique as configurações de RA do IPv6 usando o **`ravdump`**:

```
> radvdump
```

   O utilitário **`radvdump`** exibe as configurações de RA do IPv6 enviadas pelo roteador IPv6 a cada poucos minutos.

11.5 Configurando o encaminhamento de IP para a funcionalidade do roteador

Se o servidor PXE também atua como roteador, o encaminhamento de IP deve ser habilitado para permitir que o sistema funcione na função de roteador.

PROCEDIMENTO 40: HABILITANDO O ENCAMINHAMENTO DE IP NO SERVIDOR PXE

1. Crie o arquivo de configuração de rede:

```
> 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 as configurações de rede:

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

Nota: Considerações sobre a configuração do roteador

Por padrão, um roteador não processa RAs do IPv6 para configuração automática de host. Para aceitar RA do IPv6 em uma interface uplink do roteador, é necessária a configuração do sysctl `accept_ra = 2`. Consulte a seção Configuração de rede na Guia de Administração para obter mais detalhes sobre a configuração do roteador, incluindo ajustes de firewall e outras etapas necessárias.

11.6 Solucionando problemas de anúncio do roteador IPv6

Problemas comuns ao configurar o anúncio do roteador IPv6 para ambientes PXE.

11.6.1 Problemas do serviço `radvd`

Pode haver falha para iniciar o serviço `radvd` devido a erros de configuração ou problemas de interface.

PROCEDIMENTO 41: RESOLVENDO PROBLEMAS DO SERVIÇO `radvd`

1. Verifique o status e os registros do serviço `radvd`:

```
> systemctl status radvd
```

2. Veja os registros detalhados do serviço:

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

3. Teste a sintaxe de configuração do `radvd`:

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

4. Verifique se a interface especificada existe:

```
> ip link show eno1
```

5. Reinicie o serviço depois de corrigir a configuração:

```
> sudo systemctl restart radvd
```

11.6.2 Problemas de configuração do encaminhamento de IP

Configurações de encaminhamento de IP incorretas podem impedir a funcionalidade adequada do roteador.

PROCEDIMENTO 42: DIAGNOSTICANDO PROBLEMAS DE ENCAMINHAMENTO DE IP

1. Verifique o status atual do encaminhamento de IP:

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

2. Verifique o status do encaminhamento de IPv6:

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

3. Verifique o arquivo de configuração do sysctl:

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

4. Aplique a configuração se os valores estiverem incorretos:

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

5. Verifique a configuração de accept_ra na interface uplink:

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

11.6.3 Problemas de recebimento de anúncios do roteador

Os clientes podem não receber ou processar corretamente os anúncios do roteador IPv6.

PROCEDIMENTO 43: SOLUCIONANDO PROBLEMAS DE RECEBIMENTO DE RA

1. Monitore os anúncios do roteador usando o **ravdump**:

```
> radvdump -d
```

2. Verifique a configuração da interface IPv6 nos clientes:

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

3. Verifique a tabela de roteamento de IPv6 nos clientes:

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

4. Teste a conectividade do IPv6 com o roteador:

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

5. Verifique as regras de firewall para ICMPv6:

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

11.7 Próximas etapas

Com o anúncio do roteador IPv6 configurado, os clientes PXE pode receber uma configuração de rede IPv6 adequada. Isso habilita a funcionalidade DHCPv6 e a conectividade IPv6 nas instalações baseadas em rede.

12 Configurando um servidor DHCP com o dnsmasq

Esta seção explica como configurar os serviços DHCP com o dnsmasq para fornecer informações de configuração de rede e inicialização PXE às instalações do SUSE Linux Enterprise Server 16.0. O servidor DHCP dnsmasq usa uma configuração baseada em tags para suportar clientes PXE tanto IPv4 quanto IPv6 com recursos de inicialização UEFI e BIOS.

12.1 Introdução

O servidor DHCP dnsmasq fornece as informações de configuração de rede e de arquivo de inicialização aos clientes PXE usando um sistema baseado em tags para corresponder os tipos de cliente e fornecer os carregadores de boot apropriados. Essa configuração suporta ambas as correspondências de PXEClient e HTTPClient que funcionam para DHCPv4 e DHCPv6, o que permite a inicialização por sistemas UEFI e BIOS em várias arquiteturas.

Importante: Limitações do HTTPClient no dnsmasq

O dnsmasq versão 2.90 e anterior não suporta o envio da opção de classe de fornecedor 6:16 de volta aos clientes DHCPv6 para configurações de HTTPClient. Para suporte completo do HTTPClient, considere usar os servidores DHCP Kea ou ISC.

12.2 Requisitos

- O pacote `dnsmasq` instalado
- Arquivos de inicialização PXE devidamente organizados em `/srv/tftpboot`
- Interface de rede configurada para o serviço DHCP
- Privilégios administrativos para configurar os serviços DHCP

12.3 Configurando serviços DHCP do dnsmasq

A configuração do DHCP dnsmasq inclui a correspondência de tipos de cliente, os intervalos de rede e as atribuições de arquivos de inicialização para ambas as redes IPv4 e IPv6.

PROCEDIMENTO 44: CONFIGURANDO O SERVIDOR DHCP DO DNSMASQ

1. Crie o arquivo de configuração de DHCP para o 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 o intervalo e as opções de DHCP 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 as opções de inicialização 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 o intervalo e as opções de DHCP 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 as opções de inicialização 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. Teste a configuração do dnsmasq:

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

7. Habilite e inicie o serviço dnsmasq:

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

12.4 Verificando a configuração da DHCP

Teste a funcionalidade do servidor DHCP para garantir a configuração de rede e a entrega de arquivos de inicialização apropriadas para os clientes PXE.

PROCEDIMENTO 45: TESTANDO O SERVIDOR DHCP DNSMASQ

1. Verifique o status do serviço dnsmasq:

```
> systemctl status dnsmasq
```

2. Verifique a vinculação da porta DHCP:

```
> ss -ulnp | grep :67
```

3. Monitore as atribuições de concessão DHCP:

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

4. Verifique as concessões DHCP ativas:

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

12.5 Solucionando problemas da configuração do DHCP dnsmasq

Problemas comuns ao configurar o dnsmasq para serviços DHCP em ambientes PXE.

12.5.1 Problemas de inicialização e configuração de serviço

O dnsmasq pode falhar ao ser iniciado devido a erros de configuração ou conflitos de porta com outros serviços DHCP.

PROCEDIMENTO 46: RESOLVENDO PROBLEMAS DO SERVIÇO DHCP DNSMASQ

1. Teste a sintaxe de configuração do dnsmasq:

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

2. Verifique se há conflitos de porta DHCP:

```
> ss -ulnp | grep :67
```

3. Pare os serviços DHCP em conflito:

```
> sudo systemctl stop dhcpd
```

4. Veja os registros detalhados do serviço:

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

5. Reinicie o dnsmasq depois de resolver os conflitos:

```
> sudo systemctl restart dnsmasq
```

12.5.2 Problemas de atribuição de concessão DHCP

Os clientes podem não receber endereços IP devido a problemas de configuração de intervalos ou conectividade de rede.

PROCEDIMENTO 47: DIAGNOSTICANDO PROBLEMAS DE CONCESSÃO DHCP

1. Verifique a configuração de intervalos do DHCP:

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

2. Monitore as solicitações DHCP em tempo real:

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

3. Verifique o status da interface de rede:

```
> ip addr show
```

4. Verifique a configuração de autorização do DHCP:

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

5. Teste a resposta do DHCP com dhcping:

```
> dhcping -s 192.168.1.200
```

12.5.3 Problemas na entrega de arquivos de inicialização PXE

Os clientes PXE podem receber endereços IP, mas não podem ser inicializados devido à configuração incorreta do arquivo de inicialização ou a problemas de correspondência de tipo de cliente.

PROCEDIMENTO 48: SOLUCIONANDO PROBLEMAS DE CONFIGURAÇÃO DA INICIALIZAÇÃO PXE

1. Verifique a correspondência de classe do fornecedor do cliente:

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

2. Verifique os caminhos dos arquivos de inicialização:

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

3. Teste o acesso por TFTP aos arquivos de inicialização:

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

4. Monitore os registros do DHCP específicos do PXE:

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

5. Verifique a atribuição de tags nos registros:

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

12.5.4 Problemas na configuração do DHCP IPv6

Os clientes DHCP IPv6 exigem a configuração apropriada do anúncio do roteador e podem ter requisitos de endereçamento diferentes do IPv4.

PROCEDIMENTO 49: RESOLVENDO PROBLEMAS DO DHCP IPV6

1. Verifique a configuração de intervalos do DHCP IPv6:

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

2. Verifique o status do anúncio do roteador IPv6:

```
> systemctl status radvd
```

3. Monitore as solicitações DHCPv6:

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

4. Teste a conectividade do IPv6:

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

5. Verifique a configuração da opção IPv6:

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

12.6 Próximas etapas

Com os serviços DHCP dnsmasq configurados, os clientes PXE podem receber informações de configuração de rede e de arquivos de inicialização para os ambientes tanto IPv4 quanto IPv6. O sistema baseado em tags oferece atribuição flexível de arquivos de inicialização com base na arquitetura do cliente e nos requisitos do método de inicialização.

13 Configurando um servidor DHCP com o Kea

Esta seção explica como configurar os serviços DHCP com o Kea para fornecer informações de configuração de rede e inicialização PXE às instalações do SUSE Linux Enterprise Server 16.0. Kea é um servidor DHCP moderno que suporta IPv4 e IPv6 com correspondência de classe do cliente para cenários de inicialização PXE e HTTP.

13.1 Introdução

Kea é o servidor DHCP moderno desenvolvido pela ISC como sucessor do servidor ISC DHCP antigo. Ele oferece suporte avançado para DHCPv4 e DHCPv6 com recursos de classificação de cliente que permitem a entrega apropriada de arquivos de inicialização com base na arquitetura do cliente e no método de inicialização. O Kea usa os arquivos de configuração baseados em JSON e suporta recursos avançados, como identificação de classe de fornecedor para inicialização HTTP.

13.2 Requisitos

- Pacotes Kea DHCP instalados: `kea-dhcp4` e `kea-dhcp6`
- Arquivos de inicialização PXE devidamente organizados em `/srv/tftpboot`
- Interface de rede configurada para o serviço DHCP
- Privilégios administrativos para configurar os serviços DHCP

13.3 Configurando o servidor Kea DHCPv4

A configuração do Kea DHCPv4 usa as classes de cliente para corresponder os tipos de cliente PXE e HTTP e fornecer os arquivos de inicialização apropriados para diferentes arquiteturas.

PROCEDIMENTO 50: CONFIGURANDO O SERVIDOR KEA DHCPV4

1. Configure o servidor Kea DHCPv4:

```
> sudo cat > /etc/kea/kea-dhcp4.conf << 'EOF'
{
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [
        "eno1"
      ]
    },
    "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. Crie o diretório de registro do Kea:

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

3. Teste a configuração do Kea DHCPv4:

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

4. Habilite e inicie o serviço Kea DHCPv4:

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

13.4 Configurando o servidor Kea DHCPv6

A configuração do Kea DHCPv6 fornece atribuição de endereços IPv6 e informações de arquivos de inicialização usando a correspondência de classe de fornecedor para diferentes arquiteturas de cliente.

PROCEDIMENTO 51: CONFIGURANDO O SERVIDOR KEA DHCPV6

1. Configure o servidor Kea DHCPv6:

```
> sudo cat > /etc/kea/kea-dhcp6.conf << 'EOF'
{
  "Dhcp6": {
    "interfaces-config": {
      "interfaces": [
        "eno1"
      ]
    },
```

```
    "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": "sntp-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. Teste a configuração do Kea DHCPv6:

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

3. Habilite e inicie o serviço Kea DHCPv6:

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

13.5 Verificando a configuração do Kea DHCP

Teste a funcionalidade do servidor Kea DHCP para garantir a configuração de rede e a entrega de arquivos de inicialização apropriadas para os clientes PXE.

PROCEDIMENTO 52: TESTANDO OS SERVIDORES KEA DHCP

1. Verifique o status do serviço Kea DHCPv4:

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

2. Verifique o status do serviço Kea DHCPv6:

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

3. Verifique a vinculação da porta DHCP:

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

4. Monitore os registros do DHCPv4:

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

5. Monitore os registros do DHCPv6:

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

6. Verifique as concessões DHCP ativas:

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

13.6 Solucionando problemas da configuração do Kea DHCP

Problemas comuns ao configurar serviços Kea DHCP para ambientes de inicialização PXE.

13.6.1 Problemas de configuração e serviço

Pode haver falha para iniciar os serviços Kea devido a erros de configuração do JSON ou problemas de interface de rede.

PROCEDIMENTO 53: RESOLVENDO PROBLEMAS DA CONFIGURAÇÃO DO KEA

1. Teste a sintaxe de configuração do DHCPv4:

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

2. Teste a sintaxe de configuração do DHCPv6:

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

3. Verifique se há erros de sintaxe do JSON:

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

4. Verifique a configuração da interface de rede:

```
> ip addr show eno1
```

5. Verifique os registros do serviço Kea:

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

13.6.2 Problemas de atribuição de concessão DHCP

Os clientes podem não receber endereços IP devido a problemas de configuração de sub-rede ou esgotamento de pool.

PROCEDIMENTO 54: DIAGNOSTICANDO PROBLEMAS DE CONCESSÃO DO KEA

1. Verifique a configuração da sub-rede e do pool:

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

2. Monitore as atribuições de concessão em tempo real:

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

3. Verifique se há conflitos no banco de dados de concessão:

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

4. Verifique a vinculação da interface:

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

5. Limpe o banco de dados de concessão, se necessário:

```
> 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 correspondência de classe de cliente PXE

Os clientes PXE podem receber endereços IP, mas não obtêm os arquivos de inicialização corretos devido a problemas de configuração da classe do cliente.

PROCEDIMENTO 55: SOLUCIONANDO PROBLEMAS DE CLASSIFICAÇÃO DO CLIENTE KEA

1. Verifique as definições de classe de cliente:

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

2. Monitore a correspondência de classe de cliente nos registros:

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

3. Verifique os padrões do identificador de classe de cliente:

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

4. Teste a acessibilidade do arquivo de inicialização:

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

5. Habilite o registro de depuração para análise detalhada do cliente:

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

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

13.6.4 Problemas específicos do DHCPv6

Os clientes DHCP IPv6 exigem a configuração apropriada do anúncio do roteador e têm um gerenciamento de opções de classe de fornecedor diferente do IPv4.

PROCEDIMENTO 56: RESOLVENDO PROBLEMAS DE DHCPV6 DO KEA

1. Verifique a configuração da sub-rede DHCPv6:

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

2. Verifique o status do anúncio do roteador IPv6:

```
> systemctl status radvd
```

3. Monitore a correspondência de classe de fornecedor do DHCPv6:

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

4. Verifique o formato da opção bootfile-url IPv6:

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

5. Teste a conectividade do IPv6 com o servidor de inicialização:

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

13.7 Próximas etapas

Com os serviços DHCP Kea configurados, os clientes PXE podem receber informações abrangentes de configuração de rede e de arquivos de inicialização para os ambientes tanto IPv4 quanto IPv6. O sistema de classificação de cliente fornece atribuição precisa de arquivos de inicialização com base na arquitetura do cliente e suporta os métodos de inicialização PXE tradicionais e HTTP modernos.

14 Configurando um servidor DHCP com o ISC DHCP

Esta seção explica como configurar o servidor ISC DHCP para fornecer informações de configuração de rede e inicialização PXE às instalações do SUSE Linux Enterprise Server 15. O pacote dhcp-server da ISC não está mais disponível no SUSE Linux Enterprise Server 16.0. O ISC DHCP usa a correspondência de classe e subclasse para suportar cenários de inicialização PXE e HTTP em diferentes arquiteturas de cliente.

14.1 Introdução

O ISC DHCP é o servidor DHCP tradicional que fornece informações de configuração de rede e arquivo de inicialização para clientes PXE usando um sistema de classe e subclasse. A ISC anunciou o fim do serviço desse servidor a partir de 2022, mas ele ainda é amplamente utilizado nas implantações existentes e oferece suporte robusto a cenários de inicialização PXE e HTTP com identificação de classe de fornecedor.

Importante: Status de fim do serviço do ISC DHCP

O fim do serviço do ISC DHCP foi anunciado pela ISC em 2022. Para novas implantações, considere usar o Kea ou dnsmasq em vez dele. Esta configuração é fornecida para compatibilidade com as instalações existentes do ISC DHCP.

14.2 Requisitos

- Pacotes ISC DHCP instalados: `dhcp-server`
- Arquivos de inicialização PXE devidamente organizados em `/srv/tftpboot`
- Interface de rede configurada para o serviço DHCP
- Privilégios administrativos para configurar os serviços DHCP

14.3 Configurando o servidor ISC DHCPv4

A configuração do ISC DHCPv4 usa as declarações de classe e subclasse para corresponder os tipos de cliente PXE e HTTP e fornecer os arquivos de inicialização apropriados para diferentes arquiteturas.

PROCEDIMENTO 57: CONFIGURANDO O SERVIDOR ISC DHCPV4

1. Configure o 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 a interface DHCP no sysconfig:

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

3. Teste a configuração do DHCPv4:

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

4. Habilite e inicie o serviço ISC DHCPv4:

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

14.4 Configurando o servidor ISC DHCPv6

A configuração do ISC DHCPv6 fornece atribuição de endereços IPv6 e informações de arquivos de inicialização usando a correspondência de classe de fornecedor para o gerenciamento adequado da opção DHCPv6.

PROCEDIMENTO 58: CONFIGURANDO O SERVIDOR ISC DHCPV6

1. Configure o 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 a interface DHCPv6 no sysconfig:

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

3. Teste a configuração do DHCPv6:

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

4. Habilite e inicie o serviço ISC DHCPv6:

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

14.5 Verificando a configuração do ISC DHCP

Teste a funcionalidade do servidor ISC DHCP para garantir a configuração de rede e a entrega de arquivos de inicialização apropriadas para os clientes PXE.

PROCEDIMENTO 59: TESTANDO OS SERVIDORES ISC DHCP

1. Verifique o status do serviço ISC DHCPv4:

```
> systemctl status dhcpd
```

2. Verifique o status do serviço ISC DHCPv6:

```
> systemctl status dhcpd6
```

3. Verifique a vinculação da porta DHCP:

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

4. Monitore os registros do DHCP:

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

5. Verifique as concessões DHCP ativas:

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

6. Monitore as atividades do DHCPv6:

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

14.6 Solucionando problemas da configuração do ISC DHCP

Problemas comuns ao configurar os servidores ISC DHCP para ambientes de inicialização PXE.

14.6.1 Problemas de configuração e serviço

Pode haver falha para iniciar os serviços ISC DHCP devido a erros na sintaxe de configuração ou problemas de vinculação de interface.

PROCEDIMENTO 60: RESOLVENDO PROBLEMAS DA CONFIGURAÇÃO DO ISC DHCP

1. Teste a sintaxe de configuração do DHCPv4:

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

2. Teste a sintaxe de configuração do DHCPv6:

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

3. Verifique a configuração da interface:

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

4. Verifique o status da interface de rede:

```
> ip addr show eno1
```

5. Verifique se há conflitos de porta:

```
> ss -ulnp | grep :67
```

6. Veja os registros detalhados do serviço:

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

14.6.2 Problemas de atribuição de concessão DHCP

Os clientes podem não receber endereços IP devido a problemas de configuração de sub-rede ou autorização.

PROCEDIMENTO 61: DIAGNOSTICANDO PROBLEMAS DE CONCESSÃO ISC DHCP

1. Verifique a configuração da sub-rede e do intervalo:

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

2. Verifique a configuração de autorização:

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

3. Monitore as atribuições de concessão em tempo real:

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

4. Verifique se há erros no banco de dados de concessão:

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

5. Teste a resposta do DHCP manualmente:

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

14.6.3 Problemas de correspondência de classe e subclasse

Os clientes PXE podem receber endereços IP, mas não obtêm os arquivos de inicialização corretos devido a problemas de configuração de correspondência de classe.

PROCEDIMENTO 62: SOLUCIONANDO PROBLEMAS DA CORRESPONDÊNCIA DE CLASSE DO ISC DHCP

1. Verifique as definições de classe:

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

2. Verifique as entradas de subclasse:

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

3. Monitore a identificação de classe de fornecedor:

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

4. Teste a acessibilidade do arquivo de inicialização:

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

5. Habilite o registro detalhado:

```
> sudo sed -i '1i\log-facility local7;' /etc/dhcpd.conf
```

```
> sudo systemctl restart dhcpd
```

14.6.4 Problemas de opção de classe de fornecedor DHCPv6

Os clientes DHCP IPv6 têm um gerenciamento de opções de classe de fornecedor complexo que pode exigir uma configuração específica para oferecer o suporte adequado à inicialização PXE.

PROCEDIMENTO 63: RESOLVENDO PROBLEMAS DO ISC DHCPV6

1. Verifique as definições de opção do DHCPv6:

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

2. Verifique a análise de string de classe de fornecedor:

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

3. Monitore a correspondência de classe de fornecedor do DHCPv6:

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

4. Verifique o formato do bootfile-url IPv6:

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

5. Verifique a dependência de anúncio do roteador:

```
> systemctl status radvd
```

6. Teste a conectividade do IPv6:

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

14.7 Próximas etapas

Com os serviços ISC DHCP configurados, os clientes PXE podem receber informações de configuração de rede e arquivo de inicialização usando o sistema de classe e subclasse tradicional. O ISC DHCP chegou ao fim do serviço, mas esta configuração fornece compatibilidade com as implantações existentes que exigem a funcionalidade de inicialização PXE e HTTP em várias arquiteturas de cliente.

15 Validando a configuração do servidor PXE

Esta seção descreve como validar e testar a configuração completa do servidor PXE para garantir que todos os componentes estejam funcionando corretamente para as instalações de rede do SUSE Linux Enterprise Server 16.0. Ela aborda a verificação de serviço, o teste de conectividade de rede e a validação completa da inicialização PXE.

15.1 Introdução

Depois de configurar todos os componentes do servidor PXE, incluindo os serviços de carregador de boot TFTP, HTTP, DNS, DHCP e GRUB 2, é essencial validar o devido funcionamento de todo o sistema. Essa validação garante que os clientes PXE possam ser inicializados com êxito no instalador Agama e executar instalações baseadas em rede do SUSE Linux Enterprise Server 16.0.

15.2 Requisitos

- Todos os componentes do servidor PXE configurados e em execução
- Sistemas de cliente de teste com capacidade para inicialização PXE
- Conectividade de rede entre o servidor PXE e os clientes
- Acesso administrativo para monitorar os serviços do servidor

15.3 Validando os serviços do servidor PXE

Verifique se todos os serviços essenciais do servidor PXE estão em execução e devidamente configurados antes de fazer o teste com os clientes PXE.

PROCEDIMENTO 64: VERIFICANDO O STATUS DO SERVIÇO DO SERVIDOR PXE

1. Verifique o status do serviço TFTP:

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

   Resultado esperado: O serviço deve estar ativo e escutar na porta 69.

2. Verifique o serviço HTTP nginx:

```
> systemctl status nginx
```

   Resultado esperado: O serviço deve estar ativo e escutar na porta 80.

3. Verifique o serviço DNS (se usar o dnsmasq):

```
> systemctl status dnsmasq
```

   Resultado esperado: O serviço deve estar ativo e escutar na porta 53.

4. Verifique o status do serviço DHCP (escolha o serviço apropriado):

```
> systemctl status dhcpd
```

   Para DHCP dnsmasq:

```
> systemctl status dnsmasq
```

   Para DHCP Kea:

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

   Resultado esperado: O serviço DHCP deve estar ativo e escutar nas portas apropriadas.

5. Verifique o anúncio do roteador IPv6 (se configurado):

```
> systemctl status radvd
```

   Resultado esperado: O serviço deve estar ativo para os ambientes IPv6.

6. Verifique o serviço NTP:

```
> systemctl status chronyd
```

   Resultado esperado: O serviço deve estar ativo e sincronizado.

15.4 Testando a conectividade de rede e o acesso a arquivos

Valide que os clientes PXE podem acessar os arquivos de inicialização e o conteúdo da instalação pela rede usando ambos os protocolos TFTP e HTTP.

PROCEDIMENTO 65: TESTANDO O ACESSO AOS ARQUIVOS DE REDE

1. Teste o acesso por TFTP aos arquivos do carregador de boot:

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

   Verifique se o arquivo foi recuperado:

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

   Limpe o arquivo de teste:

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

2. Teste o acesso HTTP à configuração do GRUB 2:

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

   Resultado esperado: Resposta HTTP 200 OK.

3. Verifique o acesso por HTTP aos arquivos do instalador:

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

   Resultado esperado: Resposta HTTP 200 OK com tamanho do conteúdo apropriado.

4. Teste a resolução de DNS (se o DNS local estiver configurado):

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

   Resultado esperado: Resolução de registro adequada A e AAAA.

5. Verifique a navegação de diretórios para os locais de autoindex:

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

   Resultado esperado: Listagem de diretórios mostrando os arquivos de inicialização.

15.5 Validando a funcionalidade do DHCP

Teste as respostas do servidor DHCP e verifique se as informações de inicialização adequadas são fornecidas a diferentes tipos de cliente.

PROCEDIMENTO 66: TESTANDO AS RESPOSTAS DO SERVIDOR DHCP

1. Verifique a vinculação da porta DHCP:

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

   Resultado esperado: Serviços DHCP que escutam nas portas 67 (IPv4) e 547 (IPv6).

2. Monitore as solicitações DHCP em tempo real:

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

   Ou para dnsmasq:

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

   Deixe-o em execução para observar a atividade do DHCP durante o teste.

3. Teste a resposta do DHCP usando dhcping (se disponível):

   ```
   > dhcping -s 192.168.1.200
   ```

   Resultado esperado: Resposta do DHCP bem-sucedida do servidor.

4. Verifique as concessões DHCP ativas:

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

   Ou para Kea:

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

   Resultado esperado: Entradas de concessão para clientes de teste.

15.6 Teste da inicialização PXE completo

Faça testes completos da inicialização PXE com os sistemas de clientes reais para validar todo o processo de inicialização, do DHCP à inicialização do instalador Agama.

PROCEDIMENTO 67: TESTANDO O PROCESSO DE INICIALIZAÇÃO PXE COMPLETO

1. Prepare um sistema de cliente de teste:
    - Configurar BIOS/UEFI para habilitar inicialização de rede
    - Definir a inicialização de rede como prioridade de primeira inicialização
    - Conectar o cliente à mesma rede que o servidor PXE
2. Monitore os registros do servidor PXE durante a inicialização do cliente:

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

3. Inicialize o cliente de teste e observe a seguinte sequência:
    1. O cliente deve receber o endereço IP por DHCP
    2. O cliente deve baixar o carregador de boot por TFTP
    3. O menu do GRUB 2 deve aparecer com as opções de instalação
    4. O kernel e o initrd devem ser carregados por HTTP
    5. O instalador Agama deve ser iniciado com êxito
4. Verifique a detecção de arquitetura de cliente testando diferentes tipos de cliente:
    - Sistemas BIOS x86_64 antigos (deve obter core.0)
    - Sistemas UEFI x86_64 (deve obter bootx64.efi)
    - Sistemas UEFI aarch64 (deve obter boota64.efi)
5. Teste a inicialização PXE do IPv6 (se o IPv6 estiver configurado):
    - Habilitar a configuração de rede somente IPv6 no cliente de teste
    - Verificar a atribuição de endereços DHCPv6
    - Confirmar a entrega do bootfile-url IPv6

15.7 Validando a funcionalidade do instalador Agama

Verifique se o instalador Agama é iniciado corretamente e pode acessar as fontes de instalação para realizar as instalações do SUSE Linux Enterprise Server 16.0.

PROCEDIMENTO 68: TESTANDO A INICIALIZAÇÃO DO INSTALADOR AGAMA

1. Verifique a acessibilidade da interface da Web do Agama:
   Durante a inicialização do cliente, observe o endereço IP atribuído e o acesso:

   ```
   http://CLIENT_IP_ADDRESS
   ```

   Resultado esperado: A interface da Web do Agama deve ser carregada com êxito.

2. Verifique os registros do instalador Agama no cliente:
   Alterne para o console (Alt + F2) e execute:

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

   Resultado esperado: Nenhum erro crítico na inicialização do Agama.

3. Verifique a acessibilidade da fonte de instalação:
   Para instalações com ISO completa, verifique o acesso ao repositório:

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

   Resultado esperado: Resposta HTTP 200 OK com a listagem de diretórios.

4. Teste a capacidade de instalação do pacote:
   Na interface do Agama, verifique se:

   - O sistema pode detectar os discos disponíveis
   - A configuração da rede está preservada
   - O repositório de pacotes está acessível
   - A instalação pode prosseguir até a conclusão

15.8 Solução de problemas de falhas de validação

Problemas comuns durante a validação do servidor PXE e as respectivas etapas de resolução.

15.8.1 Falhas de atribuição de DHCP

Os clientes não recebem endereços IP durante a inicialização PXE.

PROCEDIMENTO 69: RESOLVENDO PROBLEMAS DE VALIDAÇÃO DE DHCP

1. Verifique os conflitos do serviço DHCP:

```
> ss -ulnp | grep :67
```

2. Verifique se a interface de rede está em funcionamento:

```
> ip addr show eno1
```

3. Verifique a disponibilidade do intervalo DHCP:

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

4. Monitore possíveis erros nos registros do DHCP:

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

15.8.2 Falhas na entrega dos arquivos de inicialização

Os clientes recebem os endereços IP, mas não conseguem baixar os arquivos de inicialização.

PROCEDIMENTO 70: RESOLVENDO PROBLEMAS DE ARQUIVOS DE INICIALIZAÇÃO

1. Verifique a acessibilidade do serviço TFTP:

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

2. Verifique as permissões de arquivo:

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

3. Monitore os registros de acesso por TFTP:

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

4. Verifique a detecção de arquitetura de cliente:

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

15.8.3 Falhas na inicialização do instalador Agama

Os arquivos de inicialização são carregados com êxito, mas o instalador Agama não é iniciado.

PROCEDIMENTO 71: RESOLVENDO PROBLEMAS DE INICIALIZAÇÃO DO AGAMA

1. Verifique o acesso por HTTP aos arquivos do instalador:

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

2. Verifique a sintaxe do parâmetro do kernel na configuração do GRUB 2:

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

3. Monitore o processo de inicialização do cliente:

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

4. Verifique a persistência da configuração de rede:

```
# ip addr show
```

15.9 Lista de verificação de validação do servidor PXE

Use essa lista de verificação para conferir sistematicamente todos os aspectos da configuração do servidor PXE.

TABELA 2: LISTA DE VERIFICAÇÃO DE VALIDAÇÃO DO SERVIDOR PXE

Componente	Etapa de validação	Status
Serviço TFTP	Serviço ativo, porta de escuta 69, arquivos acessíveis	☐
Serviço HTTP	nginx ativo, porta de escuta 80, arquivos do instalador acessíveis	☐
Serviço DNS	Resolução de nomes de host funcionando, porta de escuta 53	☐
Serviço DHCP	Atribuição de IP funcionando, opções de inicialização entregues	☐
Configuração do GRUB 2	Menu carregado, detecção de arquitetura funcionando	☐

Componente	Etapa de validação	Status
Suporte ao IPv6	Anúncio do roteador ativo, DHCPv6 funcionando	☐
Inicialização PXE	Cliente inicializado com êxito, recebe o carregador de boot correto	☐
Instalador Agama	Instalador iniciado, interface da Web acessível	☐
Fonte de instalação	Repositório acessível, pacotes instaláveis	☐
Persistência da rede	Configuração de rede mantida durante a instalação	☐

15.10 Conclusão da validação

Um servidor PXE devidamente validado deve demonstrar a funcionalidade completa e bem-sucedida da inicialização de rede do cliente por meio da inicialização do instalador Agama. Todos os serviços devem funcionar sem erros, e os clientes podem concluir as instalações do SUSE Linux Enterprise Server 16.0 pela rede. Os testes de validação regulares garantem a confiabilidade contínua da infraestrutura do PXE para implantações automatizadas.

16 Informações legais

Todas as informações deste manual foram compiladas com a maior atenção possível aos detalhes. Entretanto, isso não garante uma precisão absoluta. A SUSE LLC, suas afiliadas, os autores ou tradutores não serão responsáveis por possíveis erros nem pelas consequências resultantes de tais erros.

A GNU Free Documentation License

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. Secondarily, 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.