Einrichten eines PXE-Startservers unter SUSE Linux Enterprise Server 16.0

WAS?

Richten Sie einen PXE-Startserver mit Unterstützung für UEFI Secure Boot und das Agama-Installationsprogramm ein.

WARUM?

Automatisieren und optimieren Sie die Installation mehrerer SUSE Linux Enterprise Server 16.0-Systeme über das Netzwerk.

AUFWAND

Ein System- oder Netzwerkadministrator benötigt in der Regel 30 bis 45 Minuten, um diesen Artikel zu lesen und zu verstehen.

ZIEL

Ein funktionierender PXE-Server, der mehrere Architekturen im Agama-Installationsprogramm starten kann.

ANFORDERUNGEN

- Ein SUSE Linux Enterprise Server 16.0-System mit Administratorrechten
- Internetverbindung zum Abrufen von ISO-Images
- Konfiguration statischer IP-Adressen für den PXE-Server

Veröffentlicht: 11.12.2025

Inhalt

1 Übersicht über den PXE-Start mit SUSE Linux Enterprise Server 16.0

Der PXE-Start ermöglicht es Rechnern, über das Netzwerk in einer Installations- oder Laufzeitumgebung ohne lokalen Speicher zu starten. In diesem Abschnitt wird erklärt, wie PXE in SUSE Linux Enterprise Server 16.0 Agama und Live-Installationsprogramm-Images funktioniert, wobei der Fokus auf GRUB 2 liegt.

1.1 Was ist der PXE-Start?

PXE (Preboot Execution Environment) ist eine Methode, mit der Systeme Bootloader und Betriebssystem-Installationsprogramme mithilfe von DHCP und TFTP oder HTTP auf einem Netzwerkserver abrufen können. Es wird häufig für die Bereitstellung von Rechnern ohne physische Medien oder vorinstallierte Betriebssysteme verwendet.

1.2 Vorteile des PXE-Starts

Der PXE-Start vereinfacht die Bereitstellung, da kein lokales Installationsmedium oder keine manuelle Einrichtung erforderlich sind. Er ermöglicht Folgendes:

- Unbeaufsichtigte Installation vieler Systeme über das Netzwerk
- Zentralisierte Verwaltung von Installationsprogrammversionen und Startkonfigurationen
- Unterstützung für verschiedene Architekturen und Firmware-Typen, einschließlich UEFI Secure Boot
- Dynamische Auswahl von Installationsprogrammen oder Installationsparametern mithilfe der GRUB 2-Menüs

1.3 Funktionsweise des PXE-Starts in SUSE Linux Enterprise Server 16.0

Beim PXE-Start in SUSE Linux Enterprise Server 16.0 wird GRUB 2 als Bootloader und das Agama-Installationsprogramm als Installationsoberfläche verwendet. Bootloader und Installationsdateien werden über das Netzwerk mithilfe von HTTP oder TFTP bereitgestellt, wobei GRUB

2 den Kernel, Initrd und das Live-Image abruft. PXE-Clients können eine Vielzahl an Firmware (einschließlich der gängigsten wie BIOS oder UEFI), ausführbaren Bootloader-Dateien oder Image-Formaten verwenden, je nach den Anforderungen ihrer Architekturen wie AMD64/Intel 64, AArch64, ppc64le und s390x. Darüber hinaus müssen sie sowohl in IPv4- als auch in IPv6-Netzwerken funktionieren.

Der Bootloader übergibt Kernel-Parameter wie `root=live:`, um das squashfs-basierte Root-Dateisystem aus einem Live-ISO-Image zu laden, wodurch die Agama-Oberfläche entweder lokal oder als Webservice für eine Remote-Web-Benutzeroberfläche gestartet wird.

1.3.1 Abwärtskompatibilität mit SLES 15.x

Die Informationen in diesem Artikel beziehen sich hauptsächlich auf SUSE Linux Enterprise Server 16.0 und höher. Er konzentriert sich auf PXE-Start-Workflows, die in das Agama-Installationsprogramm integriert werden und auf Live-Installations-Images basieren. Im Kontext und Umfang dieses Artikels unterscheiden sich SLES 16.0 und höhere Versionen in den folgenden Punkten von SLES 15.x:

Installationsprogramm
: Verwendet `dracut` und Agama anstelle von `linuxrc` und YaST.

DHCP-Server
: Die Verwendung von ISC-DHCP wird eingestellt (Ende der Lebensdauer 2022). Verwenden Sie für einen DHCP-Server stattdessen entweder Kea oder dnsmasq.

Boot-Parameter
: Verwendet den Parameter `root=live:`, um das Agama-Installationsprogramm-Image und den optionalen Parameter `inst.install_url=` für das nicht standardmäßige Installations-Repository anstelle des Parameters `install=` zu laden.

Die Bootloader-Auswahl (GRUB 2, pxelinux usw.) bleibt flexibel und ist nicht versionsabhängig.

1.3.2 Verschiedene mögliche Einrichtungen und Schritte

Dieser Artikel enthält obligatorische Einrichtungsschritte und optionale oder alternative Konfigurationen. Befolgen Sie nur die Abschnitten, die für Ihre Bereitstellung relevant sind, und überspringen Sie alle Alternativen, die nicht für Ihre Bereitstellung gelten.

Obligatorisch

Aufgaben wie das Installieren von Komponenten, das Vorbereiten des Installationsprogramm-Images, das Konfigurieren von GRUB 2 und das Validieren des Servers müssen bei allen Einrichtungen abgeschlossen werden.

Dateizustellungsmethode

Ein HTTP-Server (mit Agama empfohlen) wie `nginx` und/oder ein TFTP-Server wie `tftp` oder `dnsmasq`.

DHCP-Server

Wählen Sie entweder Kea oder dnsmasq aus.

Anmerkung: Einschränkungen und Funktionen der von Ihnen ausgewählten Methode

- Verwenden Sie **Kea** – den neuen DHCP-Server von ISC – als modernen Ersatz für ISC DHCP. Weitere Informationen zu Kea finden Sie unter https://www.isc.org/kea/. Den Hinweis zum Ende der Lebensdauer von ISC-DHCP finden Sie unter https://www.isc.org/dhcp/. Kea ist ein DHCP-Server und benötigt eine separate TFTP-Serversoftware. Der Kea-DHCP-Server unterstützt Optionen für TFTP bzw. den PXE-Start über IPv4 und IPv6 sowie für den HTTP-Start über IPv4. Der HTTP-Start über IPv6 setzt voraus, dass der DHCPv6-Server die `Vendor Class Option` (siehe `RFC3315, Section 22.16`), bei der angenommen wird, dass sie „von einem Client zur Identifizierung des Herstellers“ verwendet wird, wieder an den Client senden kann und wird derzeit nicht unterstützt.
- **dnsmasq** als Kombination aus einem DNS-Server, einem DHCP-Server und einem TFTP-Server. Sie können es verwenden, um den Bootloader, den Kernel, initrd (und andere Dateien) per TFTP bereitzustellen. Weitere Informationen zu dnsmasq finden Sie unter https://thekelleys.org.uk/dnsmasq/doc.html. Der dnsmasq-DHCP-Server unterstützt Optionen für TFTP bzw. den PXE-Start über IPv4 und IPv6 sowie für den HTTP-Start über IPv4. Der HTTP-Start über IPv6 setzt voraus, dass der DHCPv6-Server die `Vendor Class Option` (siehe `RFC3315, Section 22.16`), bei der angenommen wird, dass sie „von einem Client zur Identifizierung des Herstellers“ verwendet wird, wieder an den Client senden kann und wird derzeit nicht unterstützt.

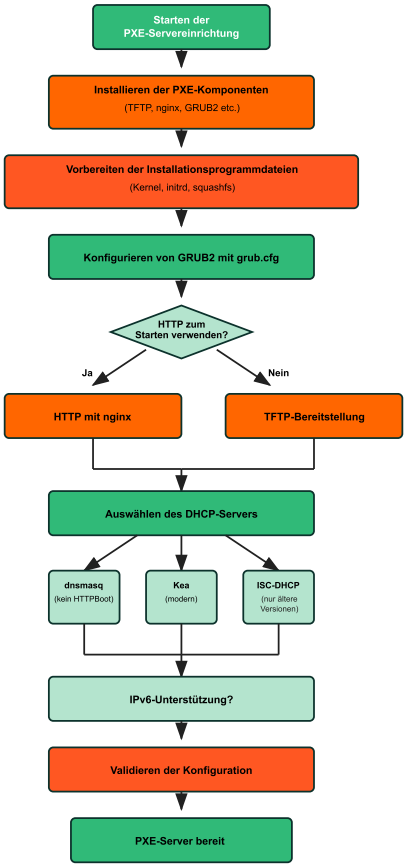

ABBILDUNG 1: BEISPIEL FÜR EINEN WORKFLOW ZUR EINRICHTUNG EINES PXE-SERVERS

2 Vorbereiten des Netzwerks für PXE-Startdienste

Dieses Modul beschreibt die Anforderungen an die Netzwerkinfrastruktur für die Bereitstellung von PXE-Startdiensten unter SUSE Linux Enterprise Server 16.0.

2.1 Einführung

Ein PXE-Server besteht aus drei Servern: einem DHCP-Server, der die Adresse und den Speicherort der Startdatei (Bootloader) bereitstellt, und einem TFTP- und/oder HTTP-Server zum Abrufen der Dateien. Darüber hinaus kann es einen DNS-Server, einen NTP-Server und einen Rou-

ter mit IPv6-Unterstützung geben. Diese sind in der Regel in einem Produktionsnetzwerk vom PXE-Server getrennt. Ein PXE-Server, auf dem SUSE Linux Enterprise Server 16.0 ausgeführt wird, benötigt möglicherweise auch eine spezielle Netzwerkschnittstellen-Einrichtung, bestimmte dauerhafte Regeln, die der Firewall hinzugefügt wurden, und einige Berechtigungen in `SELinux`. Dieser Abschnitt zeigt ein Beispielnetzwerk mit geeigneten IP-Bereichen und den notwendigen Regeln für die Firewall und SELinux.

2.2 Annahmen und Beispielkonfiguration eines Netzwerks

In diesem Artikel wird von Folgendem ausgegangen:

- Der PXE-Server wird auf der `eno1`-Netzwerkschnittstelle mit der folgenden Netzwerkkonfiguration ausgeführt:

  TABELLE 1: BEISPIELKONFIGURATION EINES PXE-NETZWERKS

	IPv4	IPv6	DNS-Name
PXE-Netzwerk	192.168.1.0/24	2001:db8:0:1::/64	example.net
PXE-Server	192.168.1.200	2001:db8:0:1::200	pxe.example.net
PXE-Gateway	192.168.1.1	2001:db8:0:1::1	
DNS-Server	192.168.1.200	2001:db8:0:1::200	
NTP-Server	192.168.1.1	2001:db8:0:1::1	

- Standardmäßig sind Router, NTP- und DNS-Server extern und werden auf einem anderen Computer ausgeführt. Dieser Artikel enthält einige Hinweise, behandelt jedoch nicht deren vollständige Konfiguration.

2.3 Konfigurieren der Netzwerkschnittstelle, der Firewall und von SELinux für PXE-Dienste

Konfigurieren Sie die Netzwerkschnittstelle und die Firewall so, dass die vom PXE-Server benötigten Netzwerkdienste zugelassen werden. Passen Sie die `SELinux`-Einstellungen an, um Installationstests zu ermöglichen und dauerhafte lokale Richtlinien zu definieren.

1. Überprüfen Sie die PXE-Netzwerkschnittstelle und weisen Sie sie der entsprechenden firewalld-Zone zu.

    a. Überprüfen Sie die aktuell aktiven Zonen und die ihnen zugewiesenen Schnittstellen:

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

    b. Wenn `eno1` der Zone `public` nicht zugewiesen ist, weisen Sie es zu:

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

    c. Stellen Sie sicher, dass die Schnittstellenzuweisung auch bei Neustarts beibehalten wird:

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

2. Konfigurieren Sie die Firewall für den DNS-Dienstzugriff.

    a. Lassen Sie den DNS-Dienst für die aktuelle Sitzung zu:

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

    b. Stellen Sie sicher, dass die Änderung dauerhaft ist:

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

3. Konfigurieren Sie die Firewall für den NTP-Dienstzugriff.

    a. Lassen Sie den NTP-Dienst für die aktuelle Sitzung zu:

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

    b. Stellen Sie sicher, dass die Änderung dauerhaft ist:

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

4. Konfigurieren Sie die Firewall für den DHCP-Dienstzugriff (IPv4).

    a. Lassen Sie den DHCP-Dienst für die aktuelle Sitzung zu:

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

b. Stellen Sie sicher, dass die Änderung dauerhaft ist:

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

5. Konfigurieren Sie die Firewall für den DHCPv6-Dienstzugriff.

   a. Lassen Sie den DHCPv6-Dienst für die aktuelle Sitzung zu:

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

   b. Stellen Sie sicher, dass die Änderung dauerhaft ist:

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

6. Konfigurieren Sie die Firewall für den TFTP-Dienstzugriff.

   a. Lassen Sie den TFTP-Dienst für die aktuelle Sitzung zu:

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

   b. Stellen Sie sicher, dass die Änderung dauerhaft ist:

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

7. Konfigurieren Sie die Firewall für den HTTP-Dienstzugriff.

   a. Lassen Sie den HTTP-Dienst für die aktuelle Sitzung zu:

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

   b. Stellen Sie sicher, dass die Änderung dauerhaft ist:

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

8. Konfigurieren Sie die Firewall für den HTTPS-Dienstzugriff.

   a. Lassen Sie den HTTPS-Dienst für die aktuelle Sitzung zu:

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

   b. Stellen Sie sicher, dass die Änderung dauerhaft ist:

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

9. Deaktivieren Sie `SELinux` vorübergehend für Einrichtungstests.

    a. Legen Sie für `SELinux` den permissiven Modus fest:

    ```
    > sudo setenforce 0
    ```

    b. Überprüfen Sie den `SELinux`-Status:

    ```
    > sudo sestatus
    ```

10. Generieren und installieren Sie lokale `SELinux`-Richtlinienmodule für PXE-bezogene Dienste.

    a. Erstellen und installieren Sie ein Modul für `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. Erstellen und installieren Sie ein Modul für `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. Erstellen und installieren Sie ein Modul für `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. Aktivieren Sie den SELinux-Durchsetzungsmodus erneut.

    a. Legen Sie für SELinux den Durchsetzungsmodus fest:

    ```
    > sudo setenforce 1
    ```

    b. Überprüfen Sie den SELinux-Status:

    ```
    > sudo sestatus
    ```

2.4 Zusammenfassung

Dieses Verfahren stellte sicher, dass die Netzwerkschnittstelle, die Firewall und die SELinux-Richtlinie des PXE-Servers für einen sicheren und funktionsfähigen Betrieb ordnungsgemäß konfiguriert wurden.

- Die PXE-Bereitstellungsschnittstelle (in diesem Beispiel `eno1`) wurde überprüft und der firewalld-Zone `public` zugewiesen.
- Die erforderlichen Firewall-Dienste für den PXE-Betrieb, einschließlich `dns`, `ntp`, einschließlich `dhcp`, `dhcpv6`, `tftp`, `http` und `https`, wurden geöffnet.
- Legen Sie `SELinux` vorübergehend auf den Modus `permissive` fest, um das Testen von Diensten zu erleichtern und AVC-Verweigerungen zu protokollieren.
- Mit **`ausearch`** und **`audit2allow`** wurden benutzerdefinierte SELinux-Richtlinienmodule für Dienste wie `nginx`, `dnsmasq` und `in.tftpd` generiert und installiert.
- `SELinux` wurde wieder auf den Modus `enforcing` festgelegt, um das System für die Produktion zu schützen.

Nach Abschluss dieser Schritte ist der PXE-Server sicher konfiguriert und bereit, Client-Computer über das Netzwerk mit IPv4 oder IPv6 bereitzustellen.

3 Installieren der erforderlichen PXE-Serverkomponenten

In diesem Abschnitt wird erklärt, wie Sie die erforderlichen Pakete installieren, um den PXE-Start unter SUSE Linux Enterprise Server 16.0 zu unterstützen, einschließlich GRUB 2-, DHCP-, TFTP- und/oder HTTP-Komponenten.

3.1 Einführung

Um einen PXE-Startserver unter SUSE Linux Enterprise Server 16.0 zu konfigurieren, müssen Sie mehrere Dienste und Werkzeuge installieren. In Abhängigkeit von Ihrer Einrichtung benötigen Sie möglicherweise Folgendes:

- Das `dnsmasq`-Paket bietet eine Kombination aus einem DNS-Server, einem TFTP-Server und einem DHCP-Server (DHCPv4 und DHCPv6) mit eingeschränkter Unterstützung für IPv6-Router Advertisement (RA). Es bietet Folgendes:
  - dnsmasq-DHCP-Server: Unterstützt die bedingte Bereitstellung von DHCP-Optionen je nach Anfrage und Client-Architektur für:
    - PXE-Startanforderungen mit DHCPv4 und DHCPv6
    - HTTP-Startanforderungen mit DHCPv4

    

    ### Anmerkung: Beschränkungen von dnsmasq für den HTTP-Start über DHCPv6

    Derzeit unterstützt dnsmasq das Senden der erforderlichen DHCPv6-Option `vendor-class` nicht.

  - dnsmasq-TFTP-Server: Stellt Bootloader-Dateien, Kernel und initrd per TFTP beim PXE-Start bereit.

- dnsmasq-DNS-Server: Ermöglicht die rekursive Auflösung von Domainnamen und IP-Adressen für die Client-Firmware und `/etc/resolv.conf` im Installalationsprogramm/Betriebssystem.
- dnsmasq-IPv6-RA: Unterstützt das Senden von IPv6-RA, wenn der PXE-Server auch als Router fungiert (die Konfigurierbarkeit ist auf ein „häufiges RA-Muster“ beschränkt).

- Das `kea`-Paket ist ein DHCP-Server und ein Nachfolger des ISC-DHCP-Servers. Es unterstützt die bedingte Bereitstellung von DHCP-Optionen je nach Anfrage und Client-Architektur für:
  - PXE-Startanforderungen mit DHCPv4 und DHCPv6
  - HTTP-Startanforderungen mit DHCPv4

  

  ### Anmerkung: Beschränkungen von Kea für den HTTP-Start über DHCPv6

  Derzeit unterstützt Kea das Senden der erforderlichen DHCPv6-Option `vendor-class` nicht. Weitere Informationen finden Sie unter https://kea.readthedocs.io/en/latest/arm/dhcp6-srv.html#id4.

- Ein TFTP-Server bietet die Bootloader-Dateien, den Kernel und initrd per TFTP, während der PXE-Start mit Kea vom `tftp`-Paket bereitgestellt wird und für den HTTP-Start nicht erforderlich ist. Wenn Sie `dnsmasq` verwenden, benötigen Sie das `tftp`-Paket nicht.
- Ein Webserver wie das `nginx`-Paket, um Installationsprogramm-Images per HTTP bereitzustellen.

Anmerkung: Notwendigkeit für HTTP-Server

Ein HTTP/HTTPS-Server wie nginx ist fast immer erforderlich. Seine Verwendung geht über den reinen HTTP-Start hinaus. Sie benötigen ihn möglicherweise insbesondere bei den folgenden Szenarien:

- Er ist eine Grundvoraussetzung für den HTTP-Start.
- Er wird für die Bereitstellung von `squashfs.img` empfohlen. Sie können `root=live:tftp://.../squashfs.img` in der Startbefehlszeile verwenden.
- Es wird auch für die Bereitstellung von RPMs für Agama im Startbefehlszeilen-Parameter `inst.install_url=http://.../install/` in einer Datei `SLES-16.0-Full-*.inline.iso` zusammen mit Installationsprofilen und anderen Dateien für die unbeaufsichtigte Installation empfohlen.

- Die GRUB 2-Bootloader-Pakete bieten einen Netzwerkstart für unterstützte Architekturen und Methoden. Die AMD64/Intel 64-Architektur bietet beispielsweise zwei Methoden für den Netzwerkstart: BIOS und UEFI. Zusätzlich unterstützt UEFI im Allgemeinen den PXE-Start (TFTP) und den HTTP-Start. Andere Bootloader wie pxelinux unterstützen UEFI und den HTTP-Start nicht.
- Optional ein RA-Daemon für IPv6, z. B. das `radvd`-Paket. Es ist unter SLES erforderlich, wenn es auch als Router für ein Installationsprogramm-Netzwerk fungiert, um Folgendes auszuführen:
  - Konfigurieren von Routing in einem Netzwerk für PXE- oder HTTP-Start-Clients
  - Ermöglichen der Verwendung von DHCPv6 in einem Netzwerk für PXE- oder HTTP-Start-Clients

3.2 Anforderungen

- Ein System, auf dem SUSE Linux Enterprise Server 16.0 mit Administratorrechten ausgeführt wird, das beim SUSE Customer Center registriert und mit SUSEConnect für den Zugriff auf die entsprechenden Online-Repositorys konfiguriert wurde.
- Aktivierte SLE-Module: Serveranwendungsmodul, Legacy-Modul und Basissystemmodul.

- Zugriff auf die SLE-Modul-Repositorys für Netzwerkdienste und Bootloader.
- Eine funktionierende Internetverbindung zum Abrufen von Paketen

3.3 Installieren der Pakete

Führen Sie die folgenden Schritte aus, um die für den PXE-Startserver erforderlichen Kernpakete zu installieren.

VORGEHEN 1: INSTALLIEREN DER ERFORDERLICHEN PAKETE FÜR EINEN PXE-STARTSERVER

1. Installieren Sie den GRUB 2-Bootloader und den nginx-HTTP-Server als allgemeine Anforderungen.

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

2. Führen Sie einen der folgenden Befehle aus, um die für Ihren Ansatz unerlässlichen Pakete zu installieren:

   - `kea` für den DHCP-Server, `tftp` für den TFTP-Server

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

   - `dnsmasq` als allgemeiner Anbieter für DHCP-, DNS- und TFTP-Server

```
> sudo zypper install dnsmasq
```

Anmerkung: Beschränkungen für die von Kea und dnsmasq bereitgestellten DHCP-Server

Der HTTP-Start per IPv6 wird *derzeit* von DHCP-Servern, die von den Paketen `kea` und `dnsmasq` bereitgestellt werden, nicht unterstützt. Das Zurücksenden einer `vendor-class`-Option an den HTTP-Client, wie es die UEFI-Spezifikation vorschreibt, wird dadurch nicht unterstützt.

3. Installieren Sie optional zusätzliche architekturspezifische GRUB 2-Ziele, wenn Sie andere Plattformen unterstützen möchten.

   - Für die AMD64/Intel 64-Architektur:

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

- Für die AArch64-Architektur:

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

- Für die ppc64le-Architektur:

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

Anmerkung: Art und Weise der Bereitstellung von GRUB 2-Paketen durch den PXE-Server an Clients, die sich von der Architektur des Servercomputers unterscheiden

Die für die architekturspezifischen `noarch.rpm`-Pakete von GRUB 2 sind unabhängig von der Architektur des Computers, auf dem der PXE-Server eingerichtet ist, im Unterverzeichnis `noarch` des Installationsmediums/Repositorys enthalten. Das heißt, Sie können auf einem PXE-Server, der auf einem AMD64/Intel 64-Computer ausgeführt wird, die Pakete `grub2-arm64-efi` und `grub2-powerpc-ieee1275` installieren, um Clients mit anderen Architekturen zu unterstützen.

4. Optional können Sie das `shim`-Paket installieren, wenn Sie UEFI Secure Boot für AMD64/Intel 64 oder AArch64 benötigen, aber die Dateien aus dem ISO-Image des Installationsmediums nicht verwenden möchten.

```
> sudo zypper install shim
```

5. Installieren Sie optional den Router Advertisement-Daemon `radvd`, wenn Sie den PXE-Server als Router verwenden möchten (für Produktionsnetzwerke nicht empfohlen).

```
> sudo zypper install radvd
```

6. Installieren Sie das Dienstprogramm `rsync`, um das ISO-Image und den Verzeichnisbaum bequem zu kopieren oder zu synchronisieren.

```
> sudo zypper install rsync
```

7. Stellen Sie sicher, dass die Dienste installiert, aber noch nicht gestartet wurden. Die Konfiguration wird in späteren Abschnitten behandelt.

4 Erstellen von GRUB 2-NetBoot-Verzeichnissen für den PXE-Server

In diesem Abschnitt wird das Erstellen von GRUB 2-NetBoot-Verzeichnissen für PXE-Server mit **`grub2-mknetdir`** erklärt, womit für die Architektur spezifische Verzeichnisse für AMD64/Intel 64- (UEFI und BIOS), AArch64- und ppc64le-Systeme generiert werden. Für die Unterstützung von UEFI Secure Boot müssen Administratoren signierte EFI-Dateien vom Installationsmedium kopieren oder das `shim`-Paket verwenden, um die standardmäßigen nicht signierten Bootloader-Dateien zu ersetzen.

4.1 Einführung

In diesem Abschnitt wird die Einrichtung von GRUB 2-NetBoot-Verzeichnissen für die PXE-Serverbereitstellung auf mehreren Architekturen beschrieben. Der Befehl **`grub2-mknetdir`** erstellt architekturspezifische Verzeichnisse unter `/srv/tftpboot/boot/grub2/` für verschiedene Plattformen. AMD64/Intel 64-Systeme generieren beispielsweise sowohl UEFI-Verzeichnisse (`x86_64-efi`) als auch Legacy-BIOS-Verzeichnisse (`i386-pc`), während AArch64- und ppc64le-Systeme ihre jeweiligen UEFI-Verzeichnisse (`arm64-efi` und `powerpc-ieee1275`) erstellen.

Zur Unterstützung von UEFI Secure Boot, das von den standardmäßigen nicht signierten `core.efi`-Dateien nicht bereitgestellt wird, können Administratoren entweder signierte EFI-Dateien vom Installationsmedium kopieren oder das `shim`-Paket installieren und die erforderlichen Bootloader-Dateien (`shim.efi`, `grub.efi`, `MokManager.efi`) manuell in die entsprechenden Architekturverzeichnisse kopieren, um eine ordnungsgemäße Auflösung symbolischer Links sicherzustellen, damit alle Dateien im TFTP-Stammverzeichnis verbleiben.

4.2 Anforderungen

- Stellen Sie sicher, dass Sie die folgenden Pakete installiert haben: `grub2`, `tftp` und alle anderen architekturspezifischen GRUB 2-Paket wie `grub2-x86_64-efi` und `grub2-i386-pc`.
- Stellen Sie sicher, dass entweder das Installationsmedium (ISO) zum Einbinden verfügbar ist oder dass das `shim`-Paket auf dem System installiert ist. Sie können das Installationsmedium (ISO) für Ihre Zielarchitektur aus dem SUSE Customer Center herunterladen.

4.3 Vorbereiten der NetBoot-Verzeichnisse und von UEFI Secure Boot

Dieses Verfahren erstellt die erforderliche GRUB 2-Verzeichnisstruktur für den PXE-Netzwerkstart und konfiguriert optional die Unterstützung von UEFI Secure Boot für mehrere Architekturen.

1. Erstellen Sie eine GRUB 2-NetBoot-Verzeichnisstruktur.

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

   Hiermit werden architekturspezifische Verzeichnisse erstellt:

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

   Warnung

   Überschreiben Sie die von **`grub2-mknetdir`** erstellte `grub.cfg`-Datei nicht manuell.

2. Kopieren Sie andere von der Architektur unabhängige Verzeichnisse wie `fonts/` und `locale/`, die unter dem Verzeichnis `/srv/tftpboot/boot/grub2/` verfügbar sind, auf den TFTP-Server.

3. Sie können die mit dem Befehl **`grub2-mknetdir`** installierte Datei `/srv/tftpboot/boot/grub2/ARCH-efi/core.efi` auch für AMD64/Intel 64- oder AArch64-Architekturen für UEFI-PXE verwenden. Sie sind jedoch *nicht signiert* und unterstützen UEFI Secure Boot nicht. Um UEFI Secure Boot optional für die unterstützten AMD64/Intel 64- und AArch64-Architekturen zu aktivieren, führen Sie einen der folgenden Schritte aus:

   - Kopieren Sie die erforderlichen Dateien aus dem ISO-Image des Installationsmediums:

     a. Binden Sie das ISO-Image ein.

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

     b. Kopieren Sie die EFI-Dateien.

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

     (1) Ersetzen Sie *ARCH*`-efi` durch `x86_64-efi` oder `arm64-efi` - die unterstützten Architekturen für UEFI Secure Boot.

     c. Heben Sie die Einbindung des ISO-Images auf.

     ```
     > sudo umount /mnt
     ```

   - Verwenden Sie das `shim`-Paket, wenn Sie die Dateien aus dem ISO-Image des Installationsmediums nicht verwenden möchten:

     a. Installieren Sie das `shim`-Paket, falls es nicht bereits installiert ist.

     ```
     > sudo zypper install shim
     ```

     b. Kopieren Sie die signierten Bootloader-Dateien für die erforderliche Architektur:

        i. Kopieren Sie die Datei `shim.efi`.

        - Für die AMD64/Intel 64-Architektur:

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

- Für die AArch64-Architektur:

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

ii. Kopieren Sie die Datei `grub.efi`.

- Für die AMD64/Intel 64-Architektur:

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

- Für die AArch64-Architektur:

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

iii. Kopieren Sie die Datei `MokManager.efi`.

- Für die AMD64/Intel 64-Architektur:

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

- Für die AArch64-Architektur:

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

Anmerkung

Das Flag `-L` löst symbolische Links auf, um sicherzustellen, dass die Dateien im TFTP-Stammverzeichnis verbleiben.

5 Vorbereiten des Installationsprogramm-Image-Inhalts

In diesem Abschnitt wird beschrieben, wie Sie Installationsprogrammdateien von SUSE Linux Enterprise Server 16.0-Installationsmedien für PXE-Startumgebungen extrahieren und organisieren. Er deckt sowohl `.install.iso`-Images als auch RPM-Pakete ab und enthält spezifische Anweisungen für verschiedene Architekturen und Installationstypen.

5.1 Einführung

SUSE Linux Enterprise Server 16.0 bietet Installationsprogrammdateien in mehreren Formaten, damit verschiedene PXE-Startszenarien unterstützt werden. Das Agama-Installationsprogramm benötigt drei wichtige Dateien: das Kernel-Image (`linux`), das ursprüngliche RAM-Laufwerk (`initrd`) und das komprimierte Root-Dateisystem (`squashfs.img`). Diese Dateien müssen vom Installationsmedium extrahiert und in einer Verzeichnisstruktur organisiert werden, auf die über TFTP und HTTP zugegriffen werden kann.

In diesem Abschnitt werden Vorbereitungsmethoden für `.install.iso`-Images und RPM-Pakete behandelt, um die Kompatibilität mit den verschiedenen Architekturen und Installationstypen sicherzustellen, die von SUSE Linux Enterprise Server 16.0 unterstützt werden.

5.2 Anforderungen

- SUSE Linux Enterprise Server 16.0-Installationsmedien, wie im SUSE Customer Center erhältlich. Folgende Möglichkeiten stehen zur Auswahl:
  - Online-ISO-Image: Reines Installationsprogramm für Netzwerkinstallationen (`SLES-16.0-Online-`*`ARCH-BUILD`*`.install.iso`)
  - Vollständiges ISO-Image: Installationsprogramm mit Installations-Repository (`SLES-16.0-Full-`*`ARCH-BUILD`*`.install.iso`)
  - RPM-Pakete: `tftpboot-agama-installer-SUSE_SLE_16_PXE-`*`ARCH`*
- Ein vorübergehender Einhängepunkt wie `/mnt`.

- Genügend Speicherplatz unter `/srv/tftpboot` und `/srv/install` für die von Ihnen gewählte Installationsmethode.
- Administratorrechte zum Erstellen von Verzeichnissen und Kopieren von Dateien.

5.3 Vorbereiten von Installationsprogrammdateien aus ISO-Images

ISO-Images bieten eine einfache Methode zum Extrahieren von Installationsprogrammdateien. Die folgenden Verfahren decken die Typen "Online-ISO-Image" und "Vollständiges ISO-Image" für verschiedene Architekturen ab.

5.3.1 Verwenden von Online-ISO-Images

Online-ISO-Images enthalten nur die Installationsprogrammkomponenten und erfordern während der Systeminstallation Netzwerkzugriff auf die Installations-Repositorys. Dies entspricht dem Startmenüeintrag der `SLES-16.0 Online Installation` in GRUB.

VORGEHEN 2: EXTRAHIEREN VON DATEIEN AUS DEM ONLINE-ISO-IMAGE (X86_64 UND AARCH64)

1. Erstellen Sie die Verzeichnisstruktur für Installationsprogrammdateien:

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

2. Binden Sie das Online-ISO-Image ein:

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

3. Kopieren Sie die Kernel- und initrd-Dateien:

```
> 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. Kopieren Sie das komprimierte Root-Dateisystem:

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

5. Heben Sie das Einbinden des ISO-Images auf:

```
> sudo umount /mnt
```

VORGEHEN 3: EXTRAHIEREN VON DATEIEN AUS DEM ONLINE-ISO-IMAGE (PPC64LE)

1. Erstellen Sie folgende Verzeichnisstruktur:

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

2. Hängen Sie das ISO-Image ein:

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

3. Kopieren Sie die Kernel- und Initrd-Dateien (beachten Sie die andere Pfadstruktur für 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. Kopieren Sie das komprimierte Root-Dateisystem:

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

5. Heben Sie das Einbinden des ISO-Images auf:

```
> sudo umount /mnt
```

5.3.2 Verwenden vollständiger ISO-Images

Vollständige ISO-Images enthalten sowohl das Installationsprogramm als auch die Installations-Repositorys und ermöglichen so lokale Installationen ohne Abhängigkeiten von externen Netzwerken. Dies entspricht dem Startmenüeintrag der `SLES-16.0 Local Installation` in GRUB mit dem zusätzlichen Parameter `inst.install_url=http://pxe.example.net/install/SLES-16.0/${arch}`.

VORGEHEN 4: EXTRAHIEREN VON DATEIEN AUS DEM VOLLSTÄNDIGEN ISO-IMAGE

1. Erstellen Sie Verzeichnisse für die Installationsprogrammdateien und das Installations-Repository:

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

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

2. Binden Sie das vollständige ISO-Image ein:

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

3. Kopieren Sie die Kernel- und Initrd-Dateien (passen Sie die Pfade für ppc64le wie in den vorherigen Verfahren gezeigt an):

```
> 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. Kopieren Sie das komprimierte Root-Dateisystem:

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

5. Kopieren Sie das Installations-Repository für den lokalen HTTP-Serverzugriff:

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

6. Heben Sie das Einbinden des ISO-Images auf:

```
> sudo umount /mnt
```

5.4 Vorbereiten von Installationsprogrammdateien aus RPM-Paketen

RPM-Pakete bieten eine alternative Methode zum Abrufen von Online-Installationsprogrammdateien.

VORGEHEN 5: INSTALLIEREN UND VERWENDEN VON RPM-PAKETEN

1. Installieren Sie die erforderlichen Pakete:

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

2. Kopieren Sie Linux, initrd, squashfs.img nach 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 Empfohlene Verzeichnisstruktur

Organisieren Sie die extrahierten Dateien gemäß dem folgenden Verzeichnislayout, um Konsistenz und eine einfache Wartung sicherzustellen. Diese Struktur unterstützt mehrere Architekturen und Installationstypen.

BEISPIEL 1: VOLLSTÄNDIGES PXE-SERVERVERZEICHNISLAYOUT

```
/srv/tftpboot/
├── boot/
│   ├── grub2/
│   │   ├── x86_64-efi/
│   │   │   ├── bootx64.efi
│   │   │   └── grub.cfg
│   │   ├── i386-pc/
│   │   │   └── core.0
│   │   ├── arm64-efi/
│   │   │   └── bootaa64.efi
│   │   └── powerpc-ieee1275/
│   │       └── core.elf
│   └── images/
│       └── SLES-16.0/
│           ├── x86_64/
│           │   ├── linux ❶
│           │   ├── initrd ❷
│           │   └── squashfs.img ❸
│           ├── aarch64/
│           └── ppc64le/
/srv/install/
└── SLES-16.0/
    ├── x86_64/ ❹
    ├── aarch64/
    └── ppc64le/
```

❶ Vom Installationsmedium extrahiertes Kernel-Image

2. Image des ursprünglichen RAM-Laufwerks
3. Komprimiertes Root-Dateisystem für das Agama-Installationsprogramm
4. Installations-Repository aus dem Verzeichnis `install` des vollständigen ISO-Images (optional)

5.6 Überprüfen der Installation

Stellen Sie nach dem Extrahieren und Organisieren der Installationsprogrammdateien sicher, dass alle erforderlichen Komponenten vorhanden und aufrufbar sind.

VORGEHEN 6: ÜBERPRÜFUNGSSCHRITTE

1. Überprüfen Sie, ob wichtige Dateien vorhanden sind:

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

2. Stellen Sie sicher, dass die Dateiberechtigungen richtig sind:

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

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

Wichtig: Aufrufbarkeit von Dateien

Stellen Sie sicher, dass alle extrahierten Dateien für die TFTP- und HTTP-Dienste lesbar sind. PXE-Clients greifen während des Startvorgangs auf die Dateien zu. Daher sind die richtigen Berechtigungen und die Dienstkonfiguration für erfolgreiche Bereitstellungen unerlässlich.

5.7 Nächste Schritte

Wenn die Installationsdateien ordnungsgemäß vorbereitet und organisiert wurden, können Sie mit folgenden Aktionen fortfahren:

- Konfigurieren von GRUB 2 für den PXE-Start mit Menüeinträgen, die auf diese Dateien verweisen
- Einrichten von HTTP- und TFTP-Diensten, um den extrahierten Inhalt bereitzustellen
- Konfigurieren von DHCP, sodass PXE-Clients zu den entsprechenden Bootloadern weitergeleitet werden

Auf die extrahierten Dateien wird in der GRUB 2-Konfiguration mit Pfaden wie `root=live:http://pxe.example.net/boot/images/SLES-16.0/ARCH/squashfs.img` verwiesen.

6 Konfigurieren von GRUB 2 für den PXE-Start

In diesem Abschnitt wird beschrieben, wie Sie den GRUB 2-Bootloader für PXE-basiertes Starten unter SUSE Linux Enterprise Server 16.0 konfigurieren. Es umfasst die Erstellung der Netzwerk-Startverzeichnisstruktur, die Einrichtung architekturspezifischer Bootloader und die Implementierung eines flexiblen Konfigurationssystems, das mehrere Architekturen und Installationsszenarien unterstützt.

6.1 Einführung

GRUB 2 dient als Netzwerk-Bootloader für PXE-Clients und lädt Kernel- und initrd-Dateien, um das Agama-Installationsprogramm zu starten. In diesem Abschnitt wird gezeigt, wie Sie eine komplexe GRUB 2-Konfiguration erstellen, die die Client-Architektur automatisch erkennt, die Auswahl der Netzwerkschnittstelle verwaltet und ein einheitliches Startmenü bietet, das mehrere Installationstypen und Zielarchitekturen unterstützt.

Der Konfigurationsansatz verwendet ein modulares Design mit separaten Dateien für die Architekturerkennung, Variablendefinitionen und Startmenüeinträge. Dies ermöglicht die Unterstützung computerspezifischer Konfigurationen und automatisierter Installationsprofile und stellt gleichzeitig die Konsistenz auf verschiedenen Hardwareplattformen sicher.

6.2 Anforderungen

- Stellen Sie sicher, dass die GRUB 2-Netzwerk-Startverzeichnisstruktur vorhanden ist, wie in den vorherigen Abschnitten beschrieben ist.
- Stellen Sie sicher, dass die Installationsprogrammdateien ordnungsgemäß organisiert wurden, wie in den vorherigen Abschnitten beschrieben ist.
- GRUB 2-Pakete für alle Zielarchitekturen müssen installiert sein: `grub2-x86_64-efi`, `grub2-i386-pc`, `grub2-aarch64-efi` und `grub2-ppc64le-ieee1275`
- Das `shim`-Paket zur Unterstützung von UEFI Secure Boot (optional).
- Administratorzugriff auf `/srv/tftpboot` oder einen gleichwertigen PXE-Root.

6.3 Erstellen der GRUB 2-Konfiguration

Die GRUB 2-Konfigurationsdatei übernimmt drei Hauptaufgaben: die Erkennung der Architektur des Clients, die Verwaltung der Netzwerkschnittstellen und das Laden anderer Konfigurationsdateien. Dieser modulare Ansatz bietet Flexibilität für verschiedene Einsatzszenarien.

VORGEHEN 7: EINRICHTEN DER HAUPTDATEI `grub.cfg`

- Erstellen Sie die GRUB 2-Hauptkonfigurationsdatei unter `/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
```

WICHTIGE KONFIGURATIONSELEMENTE

Architekturerkennung

Ordnet GRUB 2-CPU-Typen Distributionsarchitekturen zu und ermöglicht so einheitliche Menüeinträge, die auf verschiedenen Hardwareplattformen verwendet werden können

Netzwerkschnittstellenverwaltung

Definiert eine Variable `${ipcfg}`, die die grub2-Variable `${net_default_mac}` verwendet, um DHCP nur für die angegebenen PXE-Startschnittstelle mit dem Namen `pxe0` zu aktivieren, wodurch Netzwerkprüfungsprobleme auf Systemen mit mehreren Schnittstellen vermieden werden.

Dienstprogrammdefinitionen

Definiert eine typische Variable `${sconsole}` mit seriellen Konsolenparametern.

Computerspezifische Konfiguration

Lädt optionale Konfigurationsdateien pro Computer anhand der MAC-Adresse und ermöglicht so angepasste Startparameter pro Computer und automatische Installationsprofile

6.4 Erstellen des einheitlichen Startmenüs

Das Startmenü verwendet Variablen aus der Hauptkonfiguration, um architekturunabhängige Menüeinträge bereitzustellen, die sich automatisch an verschiedene Hardwareplattformen und Installationstypen anpassen.

VORGEHEN 8: EINRICHTEN DER DATEI „MENU.CFG“

- Erstellen Sie ein einheitliches Startmenü unter `/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
```

Anmerkung: Flexibilität bei Menüeinträgen

Die Menüeinträge verwenden Variablen, die basierend auf der Client-Architektur und -Konfiguration automatisch ausgefüllt werden. Die Variable `${arch}` stellt sicher, dass die richtigen Dateien geladen werden.

Die optionale Variable `${ipcfg}` bewirkt, dass nur die von PXE ausgewählte Netzwerkschnittstelle eingerichtet wird.

Die optionale Variable `${sconsole}` aktiviert eine serielle Konsole im Installationsprogrammsystem.

6.5 Computerspezifische Konfigurationen

Für erweiterte Bereitstellungen können Sie computerspezifische Konfigurationsdateien erstellen, die Standardeinstellungen überschreiben oder automatische Installationsparameter bereitstellen.

VORGEHEN 9: ERSTELLEN DER COMPUTERSPEZIFISCHEN KONFIGURATION

1. Erstellen Sie ein Verzeichnis für computerspezifische Konfigurationen:

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

2. Erstellen Sie für einen Computer mit einer MAC-Adresse `aa:bb:cc:dd:ee:ff` eine bestimmte Konfiguration:

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

3. Erstellen Sie die computerspezifische Datei `grub.cfg`:

```
> 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
```

   Geben Sie alternativ einen eigenen Menüeintrag in der Host-spezifischen Datei `grub.cfg` an (z. B. für einen bestimmten Startversuch generiert):

```
> 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
```

BEISPIEL 2: ALLGEMEINE COMPUTERSPEZIFISCHE PARAMETER

`default`
: Gibt an, welcher Menüeintrag automatisch gestartet werden soll

`timeout`
: Legt die Startzeitüberschreitung in Sekunden fest

`ipcfg`
: Überschreibt die Netzwerkschnittstellenkonfiguration für bestimmte Hardware

`autoinstall`
: Stellt computerspezifische URLs für automatische Installationsprofile bereit

6.6 Überprüfen der GRUB 2-Konfiguration

Überprüfen Sie nach dem Erstellen der Konfigurationsdateien sicher, ob die Einrichtung richtig ist und alle erforderlichen Dateien vorhanden sind.

VORGEHEN 10: ÜBERPRÜFUNGSSCHRITTE

1. Überprüfen Sie die GRUB 2-Verzeichnisstruktur:

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

2. Überprüfen Sie die Syntax der Konfigurationsdatei, indem Sie sie mit GRUB 2-Werkzeugen testen:

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

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

3. Stellen Sie sicher, dass die Dateiberechtigungen richtig sind:

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

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

Wichtig: Konfigurationstests

Testen Sie die GRUB 2-Konfiguration mit tatsächlichen PXE-Clients, um eine ordnungsgemäße Architekturerkennung und Menüfunktionalität sicherzustellen. Die Variable `${net_default_mac}` ist nur in tatsächlichen Netzwerk-Startszenarien verfügbar.

6.7 Beheben von Fehlern bei der GRUB 2-Konfiguration

Häufige Probleme und ihre Lösungen beim Verwenden von GRUB 2-PXE-Konfigurationen. Jedes Problem umfasst Diagnoseschritte und spezifische Befehle zum Beheben des Problems.

6.7.1 Fehler bei der Architekturerkennung

Wenn GRUB 2 nicht die richtige Architektur erkennt, starten Clients möglicherweise mit falschen Binärdateien oder können überhaupt nicht geladen werden.

VORGEHEN 11: DEBUGGING DER ARCHITEKTURERKENNUNG

1. Fügen Sie der GRUB 2-Konfiguration eine Debug-Ausgabe hinzu, um die erkannten Werte anzuzeigen:

```
> 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. Testen Sie die Konfigurationssyntax:

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

3. Wenn die Architekturzuordnung unvollständig ist, erweitern Sie die Erkennungslogik:

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

4. Überprüfen Sie, ob die architekturspezifischen Verzeichnisse vorhanden sind:

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

6.7.2 Netzwerkschnittstelle nicht gefunden

Bei einigen Firmware-Implementierungen wird die Variable `${net_default_mac}` möglicherweise nicht richtig festgelegt, was zu Fehlern bei der Netzwerkkonfiguration führt.

VORGEHEN 12: DIAGNOSE VON PROBLEMEN MIT DER NETZWERKSCHNITTSTELLE

1. Fügen Sie eine Debug-Ausgabe hinzu, um Netzwerkvariablen zu überprüfen:

```
> 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. Erstellen Sie eine Fallback-Netzwerkkonfiguration:

```
> 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. Testen Sie die Netzwerkkonfiguration mit einer bestimmten Schnittstelle:

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

4. Überprüfen Sie die Namen der Netzwerkschnittstellen auf dem Zielsystem:

```
> ip link show
```

6.7.3 Dateipfade nicht gefunden

Falsche Dateipfade verhindern, dass GRUB 2 Kernel- und initrd-Dateien lädt, was zu Fehlern beim Starten führt.

VORGEHEN 13: ÜBERPRÜFEN DER AUFRUFBARKEIT VON DATEIPFADEN

1. Überprüfen Sie, ob die Installationsprogrammdateien an den erwarteten Speicherorten vorhanden sind:

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

2. Überprüfen Sie den TFTP-Zugriff auf Startdateien:

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

3. Testen Sie den HTTP-Zugriff auf die Installationsprogrammdateien:

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

4. Überprüfen Sie die Dateiberechtigungen und die Eigentümerschaft:

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

5. Korrigieren Sie Berechtigungen bei Bedarf:

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

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

6. Überprüfen Sie, dass die symbolischen Links nicht beschädigt sind:

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

6.7.4 Fehler beim EFI-Start

EFI- und Secure Boot-Probleme können eine ordnungsgemäße Initialisierung des Bootloaders verhindern oder zu Authentifizierungsfehlern führen.

VORGEHEN 14: DIAGNOSE VON PROBLEMEN BEIM EFI-START

1. Überprüfen Sie, ob die Secure Boot-Dateien vorhanden sind:

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

2. Überprüfen Sie, ob die Dateien „shim“ („bootx64.efi“ oder „shim.efi“), „grub.efi“ und „MokManager.efi“ ordnungsgemäß kopiert wurden:

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

3. Überprüfen Sie die Integrität der EFI-Dateien:

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

4. Testen Sie, ob Dateien über TFTP aufgerufen werden können:

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

5. Überprüfen Sie bei aarch64-Systemen die ARM64-EFI-Dateien:

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

6. Überprüfen Sie, ob die DHCP-Konfiguration die richtigen Bootloader-Pfade bereitstellt:

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

7. Wenn Dateien fehlen, kopieren Sie sie erneut aus dem unter /mnt eingebundenen ISO-Image oder aus den shim-Paketdateien:

```
> 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 Menüeinträge werden nicht geladen

Wenn GRUB 2 geladen wird, Menüeinträge aber fehlschlagen oder Fehler angezeigt werden, ist das Problem häufig mit Variablenerweiterungen oder Dateiverweisen verbunden.

VORGEHEN 15: DEBUGGEN VON PROBLEMEN BEI MENÜEINTRÄGEN

1. Testen Sie die Syntax der Menükonfiguration:

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

2. Fügen Sie die Debug-Ausgabe den Menüeinträgen hinzu:

```
> 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. Überprüfen Sie, ob die Variablenerweiterung ordnungsgemäß funktioniert:

```
> 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. Testen Sie dies mit einem vereinfachten Menüeintrag:

```
> 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. Laden Sie das Testmenü vorübergehend:

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

6. Stellen Sie das ursprüngliche Menü nach dem Testen wieder her:

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

6.7.6 Aktivieren der detaillierten Protokollierung

Wenn die Probleme weiterhin bestehen, aktivieren Sie die umfassende Protokollierung, um detaillierte Informationen zum Startvorgang zu erfassen.

VORGEHEN 16: EINRICHTEN DER GRUB 2-DEBUG-PROTOKOLLIERUNG

1. Erstellen Sie eine Debug-Version der Hauptkonfiguration:

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

2. Fügen Sie eine umfassende Debug-Ausgabe hinzu:

```
> 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. Fügen Sie die Debug-Konfiguration in die Hauptdatei ein:

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

4. Überwachen Sie die TFTP-Protokolle bei Startversuchen:

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

5. Überwachen Sie die DHCP-Protokolle auf PXE-Anforderungen:

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

6. Deaktivieren Sie den Debug-Modus nach der Fehlerbehebung:

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

6.8 Nächste Schritte

Wenn GRUB 2 ordnungsgemäß konfiguriert wurde, können Sie mit folgenden Aktionen fortfahren:

- Konfigurieren von HTTP- und TFTP-Diensten, um die Startdateien und den Inhalt des Installationsprogramms bereitzustellen
- Einrichten von DHCP-Diensten, sodass PXE-Clients zu den entsprechenden Bootloadern weitergeleitet werden
- Testen des kompletten PXE-Startvorgangs auf der Zielhardware

Das flexible GRUB 2-Konfigurationssystem bietet eine Grundlage für komplexe PXE-Bereitstellungsszenarien und unterstützt mehrere Architekturen und Installationstypen über eine einheitliche Oberfläche.

7 Konfigurieren von TFTP für den PXE-Start

In diesem Abschnitt wird erklärt, wie TFTP-Dienste so konfiguriert werden, dass GRUB 2-Bootloader und PXE-Startinhalt für SUSE Linux Enterprise Server 16.0-Installationen bereitgestellt werden. Es deckt den traditionellen `in.tftpd`-Server und die integrierte TFTP-Funktionalität ab, die von `dnsmasq` bereitgestellt wird.

7.1 Einführung

TFTP stellt PXE-Clients während des Netzwerk-Startvorgangs Bootloader-Dateien bereit. SUSE Linux Enterprise Server 16.0 unterstützt zwei TFTP-Serverimplementierungen: den traditionellen `in.tftpd`-Server aus dem `tftp`-Paket und die in `dnsmasq` integrierte TFTP-Funktionalität.

7.2 Anforderungen

- Entweder ist das `tftp`-Paket oder das `dnsmasq`-Paket installiert
- Unter `/srv/tftpboot` organisierte PXE-Startdateien
- Administratorrechte zum Konfigurieren von Diensten

7.3 Konfigurieren des in.tftpd-Servers

Der `in.tftpd`-Server verwendet die Konfigurationsdatei `/etc/sysconfig/tftp`, um das TFTP-Stammverzeichnis und die Serveroptionen zu definieren.

VORGEHEN 17: EINRICHTEN DES IN.TFTPD TFTP-SERVERS

1. Aktivieren Sie optional die ausführliche Protokollierung, indem Sie die TFTP-Optionen festlegen:

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

   Die Option `-v` ermöglicht eine ausführliche Protokollierung, um die über TFTP abgerufenen Dateinamen anzuzeigen.

2. Aktivieren und starten Sie den TFTP-Dienst:

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

7.4 Konfigurieren des dnsmasq-TFTP-Servers

`dnsmasq` bietet einen integrierten TFTP-Server, der für die Verwendung des Verzeichnisses `/srv/tftpboot` aktiviert und konfiguriert werden kann.

VORGEHEN 18: EINRICHTEN DER DNSMASQ-TFTP-FUNKTIONALITÄT

1. Erstellen Sie die TFTP-Konfigurationsdatei:

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

2. Aktivieren und starten Sie den dnsmasq-Dienst:

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

7.5 Überprüfen der TFTP-Konfiguration

Testen Sie die Funktionalität des TFTP-Servers, um sicherzustellen, dass er Dateien für PXE-Clients bereitstellen kann.

VORGEHEN 19: TESTEN DER FUNKTIONALITÄT DES TFTP-SERVERS

1. Erstellen Sie eine Testdatei:

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

2. Rufen Sie die Testdatei per TFTP ab:

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

3. Überprüfen Sie, ob die Datei erfolgreich abgerufen wurde:

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

4. Bereinigen Sie die Testdateien:

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

7.6 Beheben von Fehlern bei der TFTP-Konfiguration

Häufige Probleme beim Konfigurieren von TFTP-Diensten für PXE-Startumgebungen.

7.6.1 Dienstkonflikte bei Port 69

Sowohl `dnsmasq` als auch `in.tftpd` verwenden den UDP-Port 69 für TFTP-Dienste und können nicht gleichzeitig ausgeführt werden.

VORGEHEN 20: LÖSEN VON KONFLIKTEN BEIM TFTP-DIENST

1. Überprüfen Sie, welche Dienste ausgeführt werden:

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

2. Überprüfen Sie, wovon Port 69 verwendet wird:

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

3. Halten Sie den in Konflikt stehenden Dienst (beispielsweise dnsmasq) an:

```
> sudo systemctl stop dnsmasq
```

4. Starten Sie Ihren bevorzugten TFTP-Dienst:

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

7.6.2 Probleme mit dem TFTP-Verzeichnis

Probleme beim Zugriff auf das TFTP-Stammverzeichnis können die Dateibereitstellung verhindern.

VORGEHEN 21: ÜBERPRÜFEN DER KONFIGURATION DES TFTP-VERZEICHNISSES

1. Überprüfen Sie die TFTP-Verzeichniseinstellung für in.tftpd:

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

2. Überprüfen Sie die TFTP-Verzeichniseinstellung für dnsmasq:

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

3. Überprüfen Sie, ob das Verzeichnis vorhanden ist:

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

4. Erstellen Sie das Verzeichnis, wenn es fehlt:

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

7.6.3 Aktivieren der TFTP-Protokollierung

Die ausführliche Protokollierung hilft beim Identifizieren von Dateizugriffsproblemen bei TFTP-Übertragungen.

VORGEHEN 22: AKTIVIEREN DER AUSFÜHRLICHEN TFTP-PROTOKOLLIERUNG

1. Überprüfen Sie die aktuellen TFTP-Optionen:

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

2. Aktivieren Sie die ausführliche Protokollierung:

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

3. Starten Sie den TFTP-Service neu:

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

4. Überwachen Sie TFTP-Protokolle:

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

7.7 Nächste Schritte

Wenn TFTP konfiguriert ist, können Sie mit der Konfiguration von HTTP-Diensten für die Bereitstellung von Installationsdateien und von DHCP-Diensten zur Weiterleitung von PXE-Clients an die entsprechenden Bootloader fortfahren.

8 Konfigurieren von nginx für die HTTP-Bereitstellung

In diesem Abschnitt wird erklärt, wie nginx so konfiguriert wird, dass PXE-Startinhalte per HTTP bereitgestellt werden, sodass Clients Installationsprogrammdateien wie Kernel-, initrd- und squashfs-Images von einem zentralen Ort aus laden können. Die HTTP-Bereitstellung bietet bei großen Dateien eine bessere Leistung als TFTP und ist für SUSE Linux Enterprise Server 16.0-Agama-Installationen erforderlich.

8.1 Einführung

nginx fungiert als HTTP-Server für PXE-Startumgebungen und bietet über eine webbasierte Bereitstellung Zugriff auf Installationsprogrammdateien. Der HTTP-Server macht das TFTP-Startverzeichnis und die Installations-Repositorys verfügbar, sodass PXE-Clients Kernel-Images, initrd-Dateien und die Komponenten des Agama-Installationsprogramms über HTTP herunterladen können anstatt über das langsamere TFTP-Protokoll.

8.2 Anforderungen

- Das installierte `nginx`-Paket
- Unter `/srv/tftpboot/boot` organisierte PXE-Startdateien
- Unter `/srv/install` verfügbare Installations-Repositorys
- Administratorrechte zum Ändern der nginx-Konfiguration

8.3 Konfigurieren von nginx für den PXE-Start

Die nginx-Konfiguration definiert Standortaliase, die das TFTP-Startverzeichnis und die Installations-Repositorys über HTTP-URLs verfügbar machen.

VORGEHEN 23: EINRICHTEN DES NGINX-HTTP-SERVERS

1. Bearbeiten Sie die Konfigurationsdatei:

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

2. Konfigurieren Sie den HTTP-Serverblock in Abschnitt `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. Testen Sie die Syntax der nginx-Konfiguration:

```
> sudo nginx -t
```

4. Aktivieren und starten Sie den nginx-Dienst:

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

8.4 Überprüfen der nginx-Konfiguration

Testen Sie die Funktionalität des HTTP-Servers, um sicherzustellen, dass er PXE-Startdateien und Installationsinhalte für Clients bereitstellen kann.

VORGEHEN 24: TESTEN DES NGINX-HTTP-SERVERS

1. Testen Sie den HTTP-Zugriff auf Startdateien:

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

2. Testen Sie den Zugriff auf das Installationsverzeichnis:

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

3. Überprüfen Sie, ob auf eine bestimmte Installationsprogrammdatei zugegriffen werden kann:

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

8.5 Beheben von Fehlern bei der nginx-Konfiguration

Häufige Probleme beim Konfigurieren von nginx für die HTTP-Bereitstellung beim PXE-Start.

8.5.1 Fehler bei der Konfigurationssyntax

Eine falsche nginx-Konfigurationssyntax verhindert, dass der Dienst ordnungsgemäß gestartet oder neu geladen wird.

VORGEHEN 25: BEHEBEN VON PROBLEMEN BEI DER NGINX-KONFIGURATION

1. Testen Sie die Konfigurationssyntax:

```
> sudo nginx -t
```

2. Überprüfen Sie den nginx-Dienststatus, ob beim Start ein Fehler auftritt:

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

3. Zeigen Sie detaillierte Fehlerprotokolle an:

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

4. Überprüfen Sie die nginx-Fehlerprotokolldatei:

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

8.5.2 Probleme beim Dateizugriff und bei Berechtigungen

nginx kann aufgrund falscher Berechtigungen oder fehlender Verzeichnisse möglicherweise keine Dateien bereitstellen.

VORGEHEN 26: BEHEBEN VON PROBLEMEN BEIM DATEIZUGRIFF

1. Überprüfen Sie, ob das Startverzeichnis vorhanden und aufrufbar ist:

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

2. Überprüfen Sie, ob das Installationsverzeichnis vorhanden ist:

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

3. Überprüfen Sie, ob nginx die Verzeichnisse lesen kann:

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

4. Erstellen Sie bei Bedarf fehlende Verzeichnisse:

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

5. Legen Sie entsprechenden Berechtigungen fest:

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

8.5.3 Konflikte bei der Portbindung

nginx kann möglicherweise nicht gestartet werden, wenn ein anderer Dienst Port 80 verwendet.

VORGEHEN 27: LÖSEN VON ANSCHLUSSKONFLIKTEN

1. Überprüfen Sie, wovon Port 80 verwendet wird:

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

2. Halten Sie in Konflikt stehende Dienste bei Bedarf an:

```
> sudo systemctl stop apache2
```

3. Starten Sie den nginx-Dienst:

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

4. Überprüfen Sie, ob nginx Port 80 überwacht:

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

8.6 Nächste Schritte

Wenn nginx für die HTTP-Bereitstellung konfiguriert ist, können Sie mit der Konfiguration von DHCP-Diensten zur Weiterleitung von PXE-Clients an die entsprechenden Bootloader und HTTP-Ressourcen fortfahren.

9 Konfigurieren eines DNS-Servers mit dnsmasq

In diesem Abschnitt wird erklärt, wie DNS-Dienste mithilfe von dnsmasq konfiguriert werden, um die Hostnamenauflösung für PXE-Clients bereitzustellen, die auf SUSE Linux Enterprise Server 16.0-Installationsressourcen zugreifen. Die DNS-Konfiguration ermöglicht es Clients, Hostnamen anstelle von IP-Adressen in Start-URLs und DHCP-Konfigurationen zu verwenden.

9.1 Einführung

DNS-Dienste ermöglichen es PXE-Clients, Hostnamen in Start-URLs und Installationsquellen aufzulösen. Da die vollständige DNS-Serverkonfiguration den Rahmen dieses Dokuments sprengen würde, bietet dieser Abschnitt eine grundlegende DNS-Konfiguration mit dnsmasq, mit der Clients den Hostnamen des PXE-Servers (*PXE.EXAMPLE.NET*) in seine IP-Adressen auflösen können.

Ohne DNS-Konfiguration müssen Start-URLs direkt IP-Adressen verwenden, z. B. `http://192.168.1.200/` oder `http://[2001:db8:0:1::200]/`. Einige BIOS/UEFI-Firmware-Implementierungen unterstützen keine Hostnamen in DHCP-TFTP-URLs und erfordern IP-Adressen wie `tftp://[2001:db8:0:1::200]/`.

9.2 Anforderungen

- Das installierte `dnsmasq`-Paket
- Statische IP-Adressen, die für den PXE-Server konfiguriert sind
- Administratorrechte zum Konfigurieren von DNS-Diensten

9.3 Konfiguration der dnsmasq-DNS-Dienste

Die dnsmasq-DNS-Konfiguration bietet eine lokale Hostnamenauflösung und verwendet Upstream-Namenserver für externe Abfragen.

VORGEHEN 28: EINRICHTEN DES DNSMASQ-DNS-SERVERS

1. Erstellen Sie die DNS-Konfigurationsdatei für 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. Fügen Sie der Datei mit den System-Hosts Hostnameneinträge hinzu:

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

3. Testen Sie die dnsmasq-Konfiguration:

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

4. Aktivieren und starten Sie den dnsmasq-Dienst:

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

Anmerkung: Verhalten bei DNS-Weiterleitungen

Standardmäßig verwendet dnsmasq die Namenserver in `/etc/resolv.conf` als Forwarder und stellt Datensätze aus `/etc/hosts` bereit. Dadurch kann der PXE-Server externe Hostnamen auflösen und gleichzeitig eine lokale Auflösung für PXE-bezogene Dienste bereitstellen.

9.4 Überprüfen der DNS-Konfiguration

Testen Sie die Funktionalität des DNS-Servers, um sicherzustellen, dass die Hostnamenauflösung für PXE-Clients funktioniert.

VORGEHEN 29: TESTEN DER FUNKTIONALITÄT DES DNS-SERVERS

1. Testen Sie die IPv4-Hostnamenauflösung:

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

2. Testen Sie die IPv6-Hostnamenauflösung:

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

3. Testen Sie die DNS-Rückwärtssuche für IPv4:

```
> nslookup 192.168.1.200 localhost
```

4. Stellen Sie sicher, dass die externe DNS-Weiterleitung weiterhin funktioniert:

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

9.5 Beheben von Fehlern bei der DNS-Konfiguration

Häufige Probleme bei der Konfiguration von dnsmasq für DNS-Dienste in PXE-Umgebungen.

9.5.1 Probleme bei der Konfiguration und den Diensten

dnsmasq kann aufgrund von Konfigurationsfehlern oder Portkonflikten nicht gestartet werden.

VORGEHEN 30: BEHEBEN VON PROBLEMEN BEI DER DNS-KONFIGURATION

1. Testen Sie die Syntax der dnsmasq-Konfiguration:

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

2. Überprüfen Sie den dnsmasq-Dienststatus:

```
> systemctl status dnsmasq
```

3. Überprüfen Sie, wovon der DNS-Port 53 verwendet wird:

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

4. Suchen Sie in den dnsmasq-Protokollen nach Fehlern:

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

5. Halten Sie in Konflikt stehende DNS-Dienste bei Bedarf an:

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

9.5.2 Fehler bei der Hostnamenauflösung

Bei DNS-Abfragen können aufgrund einer falschen Konfiguration oder fehlender Hostnameneinträge Fehler auftreten.

VORGEHEN 31: DIAGNOSE VON PROBLEMEN BEI DER DNS-AUFLÖSUNG

1. Überprüfen Sie, ob Hostnameneinträge in der Datei mit den Hosts vorhanden sind:

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

2. Überprüfen Sie die Domänenkonfiguration in dnsmasq:

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

3. Testen Sie die DNS-Abfrage mit ausführlicher Ausgabe:

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

4. Überwachen Sie die dnsmasq-Abfrageprotokolle:

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

5. Starten Sie dnsmasq neu, um die Konfiguration neu zu laden:

```
> sudo systemctl restart dnsmasq
```

9.5.3 Probleme bei DNS-Weiterleitungen

Bei externen DNS-Abfragen können Fehler auftreten, wenn die Konfiguration des Upstream-Namenservers falsch ist.

VORGEHEN 32: BEHEBUNG VON PROBLEMEN BEI DNS-WEITERLEITUNGEN

1. Überprüfen Sie die Konfiguration des Upstream-Namenservers:

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

2. Testen Sie die direkte Anfrage an den Upstream-Namenserver:

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

3. Überprüfen Sie die Konfiguration der dnsmasq-Weiterleitung:

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

4. Fügen Sie bei Bedarf einen bestimmten Upstream-Namenserver hinzu:

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

5. Starten Sie den dnsmasq-Dienst neu:

```
> sudo systemctl restart dnsmasq
```

9.6 Nächste Schritte

Wenn DNS-Dienste konfiguriert wurden, können PXE-Clients nun Hostnamen in Start-URLs und Installationsquellen auflösen. Sie können mit der Konfiguration von DHCP-Diensten fortfahren, die für die Client-Konfiguration auf den DNS-Server verweisen.

10 Konfigurieren eines NTP-Servers mit chrony

In diesem Abschnitt wird erklärt, wie NTP-Dienste mithilfe von `chrony` konfiguriert werden, um bei SUSE Linux Enterprise Server 16.0-Installationen eine genaue Zeitsynchronisierung für PXE-Clients bereitzustellen. Eine ordnungsgemäße Zeitsynchronisierung ist bei netzwerkbasierten Installationen für die Zertifikatvalidierung und Systemprotokollierung unerlässlich.

10.1 Einführung

NTP-Dienste stellen eine genaue Zeitsynchronisierung in der gesamten Netzwerkinfrastruktur sicher. In PXE-Startumgebungen ist die synchronisierte Zeit entscheidend für die Zertifikatvalidierung bei HTTPS-Verbindungen, ordnungsgemäßen Protokollzeitstempeln und koordinierten Systemvorgängen. In diesem Abschnitt wird die grundlegende Konfiguration des NTP-Servers mithilfe von `chrony` beschrieben.

10.2 Anforderungen

- Das installierte `chrony`-Paket

```
> sudo zypper install chrony
```

- Netzwerkkonnektivität mit Upstream-NTP-Servern
- Administratorrechte zum Konfigurieren von NTP-Diensten

10.3 Konfigurieren des chrony-NTP-Diensts

Der chrony-Dienst bietet NTP-Funktionen mit automatischer Zeitsynchronisierung mit Upstream-Servern und Funktionen zur lokalen Zeitbereitstellung für Netzwerk-Clients.

VORGEHEN 33: EINRICHTEN EINES chrony-TFTP-SERVERS

- Aktivieren und starten Sie den chrony-Dienst:

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

10.4 Überprüfen der NTP-Konfiguration

Testen Sie die Funktionalität des NTP-Diensts, um sicherzustellen, dass die Zeitsynchronisierung ordnungsgemäß funktioniert.

VORGEHEN 34: TESTEN DER FUNKTIONALITÄT DES NTP-SERVERS

1. Überprüfen Sie den chrony-Dienststatus:

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

2. Zeigen Sie den aktuellen Status der Zeitsynchronisierung an:

```
> chronyc tracking
```

3. Listen Sie die konfigurierten NTP-Quellen auf:

```
> chronyc sources
```

4. Überprüfen Sie die NTP-Serverstatistiken:

```
> chronyc sourcestats
```

10.5 Beheben von Fehlern bei der NTP-Konfiguration

Häufige Probleme bei der Konfiguration von `chrony` für NTP-Dienste in PXE-Umgebungen.

10.5.1 Probleme beim Starten des Diensts:

Der `chrony`-Dienst kann aufgrund von Konfigurationsfehlern oder Problemen mit der Netzwerkkonnektivität möglicherweise nicht gestartet werden.

VORGEHEN 35: BEHEBEN VON PROBLEMEN BEIM NTP-DIENST

1. Überprüfen Sie den Status und die Protokolle des `chrony`-Diensts:

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

2. Sehen Sie sich detaillierte Dienstprotokolle an:

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

3. Testen Sie die `chrony`-Konfiguration.

```
> sudo chronyd -Q
```

4. Starten Sie den Dienst bei Bedarf neu:

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

10.5.2 Fehler bei der Zeitsynchronisierung

Bei der Zeitsynchronisierung können aufgrund von Netzwerkproblemen oder einer falschen Serverkonfiguration Fehler auftreten.

VORGEHEN 36: DIAGNOSE VON PROBLEMEN BEI DER ZEITSYNCHRONISIERUNG

1. Überprüfen Sie den aktuellen Status der Synchronisierung:

```
> chronyc tracking
```

2. Zeigen Sie die NTP-Quellkonnektivität an:

```
> chronyc sources -v
```

3. Erzwingen Sie die sofortige Synchronisierung:

```
> sudo chronyc makestep
```

4. Überprüfen Sie die Systemzeit im Vergleich zur Hardware-Uhr:

```
> timedatectl status
```

5. Überprüfen Sie die Netzwerkkonnektivität mit NTP-Servern:

```
> chronyc activity
```

10.5.3 Firewall- und Netzwerkprobleme

Der NTP-Datenverkehr kann durch Firewall-Regeln blockiert werden, wodurch die Zeitsynchronisierung verhindert wird.

VORGEHEN 37: AUFLÖSEN DER NTP-NETZWERKKONNEKTIVITÄT

1. Überprüfen Sie, ob der NTP-Port in der Firewall offen ist:

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

2. Fügen Sie bei Bedarf den NTP-Dienst der Firewall hinzu:

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

3. Laden Sie die Firewall-Konfiguration neu:

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

4. Testen Sie die NTP-Konnektivität manuell:

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

5. Überprüfen Sie die `chrony`-Portnutzung:

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

10.6 Nächste Schritte

Wenn die NTP-Dienste konfiguriert sind, sorgen der PXE-Server und die Clients für eine genaue Zeitsynchronisierung. Dies stellt bei netzwerkbasierten Installationen eine ordnungsgemäße Zertifikatvalidierung und koordinierte Systemvorgänge sicher.

11 Konfigurieren des IPv6-Router Advertisement

In diesem Abschnitt wird beschrieben, wie die Funktionalität des IPv6-Router Advertisement konfiguriert wird, um angemessene Router Advertisements für PXE-Clients bereitzustellen. IPv6-RA ermöglicht die IPv6-Routing-Konfiguration und die statusbehaftete automatische DHCPv6-Adresskonfiguration für SUSE Linux Enterprise Server 16.0-Installationen.

11.1 Einführung

IPv6-Router-Advertisement (RA) bietet wichtige Informationen zur Netzwerkkonfiguration für PXE-Clients, einschließlich IPv6-Routing und Einstellungen der automatischen DHCPv6-Adresskonfiguration. In diesem Abschnitt wird davon ausgegangen, dass ein IPv6-Router so konfiguriert ist, dass er angemessene Router Advertisements bereitstellt, um das IPv6-Routing zum Netzwerk und zur Standardroute zu konfigurieren und die automatische Konfiguration von statusbehafteten DHCPv6-Adressen mithilfe von `AdvManagedFlag on` zu ermöglichen.

11.2 Anforderungen

- Das installierte `radvd`-Paket
- IPv6-Netzwerkkonfiguration auf der Serverschnittstelle
- Administratorrechte zum Konfigurieren von Router Advertisement-Diensten

11.3 Konfigurieren von `radvd` für das IPv6-Router Advertisement

Der `radvd`-Dienst bietet die Funktionalität des IPv6-Router Advertisement mithilfe der in `/etc/radvd.conf` definierten Konfiguration.

VORGEHEN 38: EINRICHTEN DES radvd-IPV6-ROUTER ADVERTISEMENT

1. Konfigurieren Sie den radvd-Dienst:

```
> 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. Aktivieren und starten Sie den radvd-Dienst:

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

11.4 Überprüfen des IPv6-Router Advertisement

Testen Sie die IPv6-RA-Funktionalität, um die ordnungsgemäße Konfiguration und den ordnungsgemäßen Betrieb sicherzustellen.

VORGEHEN 39: TESTEN DES IPV6-ROUTER ADVERTISEMENT

1. Überprüfen Sie den `radvd`-Dienststatus:

```
> systemctl status radvd
```

2. Überprüfen und verifizieren Sie die IPv6-RA-Einstellungen mit **`ravdump`**

```
> radvdump
```

Das Dienstprogramm **`radvdump`** zeigt IPv6-RA-Einstellungen an, die alle paar Minuten vom IPv6-Router gesendet werden.

11.5 Konfigurieren der IP-Weiterleitung für die Routerfunktionalität

Wenn der PXE-Server auch als Router fungiert, muss die IP-Weiterleitung aktiviert sein, damit das System in einer Routerrolle funktionieren kann.

VORGEHEN 40: AKTIVIEREN DER IP-WEITERLEITUNG AUF DEM PXE-SERVER

1. Erstellen Sie die Netzwerkkonfigurationsdatei:

```
> 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. Wenden Sie die Einstellungen der Netzwerkkonfiguration an:

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

Anmerkung: Überlegungen zur Routerkonfiguration

Ein Router verarbeitet IPv6-RAs für die automatische Hostkonfiguration nicht standardmäßig. Um IPv6-RA auf einer Router-Uplink-Schnittstelle zu akzeptieren, ist die sysctl-Einstellung `accept_ra = 2` erforderlich. Weitere Informationen zur Routerkonfiguration, einschließlich Firewall-Anpassungen und anderer erforderlicher Schritte, finden Sie in Abschnitt „Netzwerkkonfiguration“ im Verwaltungshandbuch.

11.6 Beheben von Fehlern beim IPv6-Router Advertisement

Häufige Probleme bei der Konfiguration von IPv6-Router-Advertisement für PXE-Umgebungen.

11.6.1 Probleme beim `radvd`-Dienst

Der `radvd`-Dienst kann aufgrund von Konfigurationsfehlern oder Schnittstellenproblemen möglicherweise nicht gestartet werden.

VORGEHEN 41: BEHEBEN VON PROBLEMEN BEIM `radvd`-DIENST

1. Überprüfen Sie den Status und die Protokolle des `radvd`-Diensts:

```
> systemctl status radvd
```

2. Sehen Sie sich detaillierte Dienstprotokolle an:

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

3. Testen Sie die `radvd`-Konfigurationssyntax:

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

4. Überprüfen Sie, ob die angegebene Schnittstelle vorhanden ist:

```
> ip link show eno1
```

5. Starten Sie den Dienst neu, nachdem Sie die Konfiguration korrigiert haben:

```
> sudo systemctl restart radvd
```

11.6.2 Probleme bei der Konfiguration der IP-Weiterleitung

Falsche Einstellungen der IP-Weiterleitung können die ordnungsgemäße Routerfunktionalität verhindern.

VORGEHEN 42: DIAGNOSE VON PROBLEMEN BEI DER IP-WEITERLEITUNG

1. Überprüfen Sie den aktuellen Status der IP-Weiterleitung:

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

2. Überprüfen Sie den Status der IPv6-Weiterleitung:

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

3. Überprüfen Sie die sysctl-Konfigurationsdatei:

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

4. Wenden Sie die Konfiguration an, wenn die Werte falsch sind:

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

5. Überprüfen Sie die accept_ra-Einstellung auf der Uplink-Schnittstelle:

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

11.6.3 Probleme beim Empfang des Router Advertisement

Clients empfangen oder verarbeiten IPv6-Router Advertisements möglicherweise nicht ordnungsgemäß.

VORGEHEN 43: BEHEBEN VON PROBLEMEN BEIM RA-EMPFANG

1. Überwachen Sie das Router Advertisement mit **ravdump**:

```
> radvdump -d
```

2. Überprüfen Sie die IPv6-Schnittstellenkonfiguration auf den Clients:

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

3. Überprüfen Sie die IPv6-Routingtabelle auf den Clients:

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

4. Testen Sie die IPv6-Konnektivität mit dem Router:

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

5. Überprüfen Sie die Firewall-Regeln für ICMPv6:

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

11.7 Nächste Schritte

Wenn das IPv6-Router Advertisement konfiguriert ist, können PXE-Clients eine ordnungsgemäße IPv6-Netzwerkkonfiguration erhalten. Dies ermöglicht die DHCPv6-Funktionalität und IPv6-Konnektivität für netzwerkbasierte Installationen.

12 Konfigurieren eines DHCP-Servers mit dnsmasq

In diesem Abschnitt wird erklärt, wie DHCP-Dienste mithilfe von dnsmasq konfiguriert werden, um die Netzwerkkonfigurations- und PXE-Startinformationen für SUSE Linux Enterprise Server 16.0-Installationen bereitzustellen. Der dnsmasq-DHCP-Server verwendet eine Tag-basierte Konfiguration, um sowohl IPv4- als auch IPv6-PXE-Clients mit UEFI- und BIOS-Startfunktionen zu unterstützen.

12.1 Einführung

Der dnsmasq-DHCP-Server stellt PXE-Clients Informationen zur Netzwerkkonfiguration und zu Startdateien bereit, wobei ein Tag-basiertes System verwendet wird, das den Client-Typen entspricht und die entsprechenden Bootloader bereitstellt. Diese Konfiguration unterstützt sowohl PXEClient- als auch HttpClient-Übereinstimmungen, die für DHCPv4 und DHCPv6 verwendet werden können und das Starten über UEFI- und BIOS-Systeme auf mehreren Architekturen ermöglichen.

Wichtig: Einschränkungen von HttpClient in dnsmasq

dnsmasq, Version 2.90 und früher, unterstützt das Zurücksenden der Vendor-Class-Option 6:16 an DHCPv6-Clients für HttpClient-Konfigurationen nicht. Für eine vollständige HttpClient-Unterstützung sollten Sie die Verwendung von Kea- oder ISC-DHCP-Servern in Betracht ziehen.

12.2 Anforderungen

- Das installierte `dnsmasq`-Paket
- Unter `/srv/tftpboot` ordnungsgemäß organisierte PXE-Startdateien
- Für den DHCP-Dienst konfigurierte Netzwerkschnittstelle
- Administratorrechte zum Konfigurieren von DHCP-Diensten

12.3 Konfiguration der dnsmasq-DHCP-Dienste

Die dnsmasq-DHCP-Konfiguration umfasst den Client-Typabgleich, Netzwerkbereiche und Startdateizuweisungen für IPv4- und IPv6-Netzwerke.

VORGEHEN 44: EINRICHTEN DES DNSMASQ-DHCP-SERVERS

1. Erstellen Sie die DHCP-Konfigurationsdatei für 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. Konfigurieren Sie den IPv4-DHCP-Bereich und die Optionen:

```
> 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. Konfigurieren Sie die IPv4-PXE-Startoptionen:

```
> 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. Konfigurieren Sie den IPv6-DHCP-Bereich und die Optionen:

```
> 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. Konfigurieren Sie die IPv6-PXE-Startoptionen:

```
> 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. Testen Sie die dnsmasq-Konfiguration:

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

7. Aktivieren und starten Sie den dnsmasq-Dienst:

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

12.4 Überprüfen der DHCP-Konfiguration

Testen Sie die Funktionalität des DHCP-Servers, um eine ordnungsgemäße Netzwerkkonfiguration und die Bereitstellung der Startdateien für die PXE-Clients sicherzustellen.

VORGEHEN 45: TESTEN DES DNSMASQ-DHCP-SERVERS

1. Überprüfen Sie den dnsmasq-Dienststatus:

```
> systemctl status dnsmasq
```

2. Überprüfen Sie die DHCP-Portbindung:

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

3. Überwachen Sie die DHCP-Lease-Zuweisungen:

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

4. Überprüfen Sie aktive DHCP-Leases:

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

12.5 Beheben von Fehlern bei der dnsmasq-DHCP-Konfiguration

Häufige Probleme bei der Konfiguration von dnsmasq für DHCP-Dienste in PXE-Umgebungen.

12.5.1 Probleme im Zusammenhang mit dem Dienststart und der Konfiguration

dnsmasq kann aufgrund von Konfigurationsfehlern oder Portkonflikten mit anderen DHCP-Diensten nicht gestartet werden.

VORGEHEN 46: BEHEBEN VON PROBLEMEN BEIM DNSMASQ-DHCP-DIENST

1. Testen Sie die Syntax der dnsmasq-Konfiguration:

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

2. Suchen Sie nach DHCP-Portkonflikten:

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

3. Halten Sie in Konflikt stehende DHCP-Dienste an:

```
> sudo systemctl stop dhcpd
```

4. Sehen Sie sich detaillierte Dienstprotokolle an:

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

5. Starten Sie dnsmasq neu, nachdem Sie Konflikte gelöst haben:

```
> sudo systemctl restart dnsmasq
```

12.5.2 Probleme bei DHCP-Lease-Zuweisungen

Clients erhalten möglicherweise aufgrund von Problemen mit der Bereichskonfiguration oder der Netzwerkkonnektivität keine IP-Adressen.

VORGEHEN 47: DIAGNOSE VON DHCP-LEASING-PROBLEMEN

1. Überprüfen Sie die DHCP-Bereichskonfiguration:

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

2. Überwachen Sie DHCP-Anforderungen in Echtzeit:

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

3. Überprüfen Sie den Status der Netzwerkschnittstelle:

```
> ip addr show
```

4. Überprüfen Sie die autorisierende DHCP-Einstellung:

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

5. Testen Sie die DHCP-Antwort mit dhcping:

```
> dhcping -s 192.168.1.200
```

12.5.3 Probleme bei der Bereitstellung von PXE-Startdateien

PXE-Clients erhalten möglicherweise IP-Adressen, können jedoch aufgrund einer falschen Startdateikonfiguration oder aufgrund von Problemen mit der Client-Typzuordnung nicht gestartet werden.

VORGEHEN 48: BEHEBEN VON FEHLERN BEI DER PXE-STARTKONFIGURATION

1. Überprüfen Sie den Klassenabgleich des Client-Herstellers:

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

2. Überprüfen Sie die Startdateipfade:

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

3. Testen Sie den TFTP-Zugriff auf Startdateien:

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

4. Überwachen Sie PXE-spezifische DHCP-Protokolle:

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

5. Überprüfen Sie die Tag-Zuweisung in Protokollen:

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

12.5.4 Probleme bei der IPv6-DHCP-Konfiguration

IPv6-DHCP-Clients erfordern eine ordnungsgemäße Router Advertising-Konfiguration und haben möglicherweise andere Adressierungsanforderungen als IPv4.

VORGEHEN 49: BEHEBEN VON IPV6-DHCP-PROBLEMEN

1. Überprüfen Sie die IPv6-DHCP-Bereichskonfiguration:

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

2. Testen Sie den Status des IPv6-Router Advertisement:

```
> systemctl status radvd
```

3. Überwachen Sie DHCPv6-Anforderungen:

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

4. Testen Sie die IPv6-Konnektivität:

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

5. Überprüfen Sie die IPv6-Optionskonfiguration:

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

12.6 Nächste Schritte

Wenn die dnsmasq-DHCP-Dienste konfiguriert sind, können PXE-Clients Informationen zur Netzwerkkonfiguration und zu Startdateien sowohl für IPv4- als auch für IPv6-Umgebungen empfangen. Das Tag-basierte System bietet eine flexible Zuweisung von Startdateien anhand der Anforderungen der Client-Architektur und der Startmethode.

13 Konfigurieren eines DHCP-Servers mit Kea

In diesem Abschnitt wird erklärt, wie DHCP-Dienste mithilfe von Kea konfiguriert werden, um die Netzwerkkonfigurations- und PXE-Startinformationen für SUSE Linux Enterprise Server 16.0-Installationen bereitzustellen. Kea ist ein moderner DHCP-Server, der sowohl IPv4 als auch IPv6 mit Client-Klassenübereinstimmung für PXE- und HTTP-Startszenarien unterstützt.

13.1 Einführung

Kea ist der moderne DHCP-Server, der von ISC als Nachfolger des alten ISC-DHCP-Servers entwickelt wurde. Es bietet robuste Unterstützung für DHCPv4 und DHCPv6 mit Client-Klassifizierungsfunktionen, die eine ordnungsgemäße Bereitstellung der Startdateien anhand der Client-Architektur und der Startmethode ermöglichen. Kea verwendet JSON-basierte Konfigurationsdateien und unterstützt erweiterte Funktionen wie die Identifizierung von Herstellerklassen für den HTTP-Start.

13.2 Anforderungen

- Installierte Kea-DHCP-Pakete: `kea-dhcp4` und `kea-dhcp6`
- Unter `/srv/tftpboot` ordnungsgemäß organisierte PXE-Startdateien
- Für den DHCP-Dienst konfigurierte Netzwerkschnittstelle
- Administratorrechte zum Konfigurieren von DHCP-Diensten

13.3 Konfigurieren des Kea-DHCPv4-Servers

Die Kea-DHCPv4-Konfiguration verwendet Client-Klassen, um PXE- und HTTP-Client-Typen abzugleichen und geeignete Startdateien für verschiedene Architekturen bereitzustellen.

VORGEHEN 50: EINRICHTEN DES KEA-DHCPV4-SERVERS

1. Konfigurieren Sie den Kea-DHCPv4-Server:

```
> 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. Erstellen Sie das Kea-Protokollverzeichnis:

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

3. Testen Sie die Kea-DHCPv4-Konfiguration:

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

4. Aktivieren und starten Sie den Kea-DHCPv4-Dienst:

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

13.4 Konfigurieren des Kea-DHCPv6-Servers

Die Kea-DHCPv6-Konfiguration bietet die IPv6-Adresszuweisung und Informationen zu Startdateien mithilfe des Klassenabgleichs des Herstellers für verschiedene Client-Architekturen.

VORGEHEN 51: EINRICHTEN DES KEA-DHCPV6-SERVERS

1. Konfigurieren Sie den Kea-DHCPv6-Server:

```
> 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. Testen Sie die Kea-DHCPv6-Konfiguration:

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

3. Aktivieren und starten Sie den Kea-DHCPv6-Dienst:

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

13.5 Überprüfen der Kea-DHCP-Konfiguration

Testen Sie die Funktionalität des Kea-DHCP-Servers, um eine ordnungsgemäße Netzwerkkonfiguration und die Bereitstellung der Startdateien für die PXE-Clients sicherzustellen.

VORGEHEN 52: TESTEN DER KEA-DHCP-SERVER

1. Überprüfen Sie den Kea-DHCPv4-Dienststatus:

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

2. Überprüfen Sie den Kea-DHCPv6-Dienststatus:

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

3. Überprüfen Sie die DHCP-Portbindung:

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

4. Überwachen Sie DHCPv4-Protokolle:

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

5. Überwachen Sie DHCPv6-Protokolle:

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

6. Überprüfen Sie aktive DHCP-Leases:

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

13.6 Beheben von Fehlern bei der Kea-DHCP-Konfiguration

Häufige Probleme beim Konfigurieren von Kea-DHCP-Servern für PXE-Startumgebungen.

13.6.1 Probleme bei der Konfiguration und den Diensten

Der Kea-Dienst kann aufgrund von JSON-Konfigurationsfehlern oder Problemen bei der Netzwerkschnittstelle möglicherweise nicht gestartet werden.

VORGEHEN 53: BEHEBEN VON PROBLEMEN BEI DER KEA-KONFIGURATION

1. Testen Sie die Syntax der DHCPv4-Konfiguration:

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

2. Testen Sie die Syntax der DHCPv6-Konfiguration:

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

3. Suchen Sie nach JSON-Syntaxfehlern:

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

4. Überprüfen Sie die Konfiguration der Netzwerkschnittstelle:

```
> ip addr show eno1
```

5. Überprüfen Sie die Kea-Dienstprotokolle:

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

13.6.2 Probleme bei DHCP-Lease-Zuweisungen

Clients erhalten möglicherweise aufgrund von Problemen mit der Subnetzkonfiguration oder der Pool-Auslastung keine IP-Adressen.

VORGEHEN 54: DIAGNOSE VON KEA-LEASING-PROBLEMEN

1. Überprüfen Sie die Subnetz- und Pool-Konfiguration:

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

2. Überwachen Sie Lease-Zuweisungen in Echtzeit:

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

3. Überprüfen Sie die Lease-Datenbank auf Konflikte:

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

4. Überprüfen Sie die Schnittstellenbindung:

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

5. Löschen Sie die Lease-Datenbank bei Bedarf:

```
> 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 Probleme beim PXE-Client-Klassenabgleich

PXE-Clients erhalten möglicherweise IP-Adressen, jedoch aufgrund von Problemen bei der Client-Klassenkonfiguration nicht die richtigen Startdateien.

VORGEHEN 55: BEHEBEN VON FEHLERN BEI DER KEA-CLIENT-KLASSIFIZIERUNG

1. Überprüfen Sie Client-Klassendefinitionen:

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

2. Überwachen Sie den Client-Klassenabgleich in Protokollen:

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

3. Überprüfen Sie die Muster des Herstellerklassenbezeichners:

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

4. Testen Sie die Aufrufbarkeit von Startdateien:

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

5. Aktivieren Sie die Debug-Protokollierung für eine detaillierte Client-Analyse:

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

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

13.6.4 DHCPv6-spezifische Probleme

IPv6-DHCP-Clients erfordern eine ordnungsgemäße Router Advertising-Konfiguration und verarbeiten Herstellerklassenoptionen anders als IPv4.

VORGEHEN 56: BEHEBEN VON KEA-DHCPV6-PROBLEMEN

1. Überprüfen Sie die DHCPv6-Subnetzkonfiguration:

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

2. Überprüfen Sie den Status des IPv6-Router Advertisement:

```
> systemctl status radvd
```

3. Überwachen Sie den DHCPv6-Klassenabgleich des Herstellers:

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

4. Überprüfen Sie das Format der IPv6-Startdatei-URL-Option:

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

5. Testen Sie die IPv6-Konnektivität mit dem Startserver:

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

13.7 Nächste Schritte

Wenn die Kea-DHCP-Dienste konfiguriert sind, können PXE-Clients umfassende Informationen zur Netzwerkkonfiguration und zu Startdateien sowohl für IPv4- als auch für IPv6-Umgebungen empfangen. Das Client-Klassifizierungssystem ermöglicht eine präzise Zuweisung der Startdateien anhand der Client-Architektur und unterstützt sowohl traditionelle PXE- als auch moderne HTTP-Startmethoden.

14 Konfigurieren eines DHCP-Servers mit ISC-DHCP

In diesem Abschnitt wird erklärt, wie der ISC-DHCP-Server konfiguriert wird, um die Netzwerkkonfigurations- und PXE-Startinformationen für SUSE Linux Enterprise Server 15-Installationen bereitzustellen. Das dhcp-server-Paket von ISC ist in SUSE Linux Enterprise Server 16.0 nicht mehr verfügbar. ISC-DHCP verwendet den Klassen- und Unterklassenabgleich, um PXE- und HTTP-Bootszenarien auf verschiedenen Client-Architekturen zu unterstützen.

14.1 Einführung

ISC-DHCP ist der traditionelle DHCP-Server, der PXE-Clients mithilfe eines Klassen- und Unterklassensystems Informationen zur Netzwerkkonfiguration und zu Startdateien bietet. ISC hat zwar das Ende der Lebensdauer dieses Servers für 2022 erklärt, er wird jedoch in vorhandenen Bereitstellungen weiterhin häufig verwendet und bietet robuste Unterstützung für PXE- und HTTP-Startszenarien mit Herstellerklassenbezeichner.

Wichtig: Status am Ende der Lebensdauer von ISC-DHCP

ISC hat das Ende der Lebensdauer von ISC-DHCP für 2022 erklärt. Für neue Bereitstellungen sollten Sie stattdessen Kea oder dnsmasq verwenden. Diese Konfiguration wird für die Kompatibilität mit vorhandenen ISC-DHCP-Installationen bereitgestellt.

14.2 Anforderungen

- Installierte ISC-DHCP-Pakete: `dhcp-server`
- Unter `/srv/tftpboot` ordnungsgemäß organisierte PXE-Startdateien
- Für den DHCP-Dienst konfigurierte Netzwerkschnittstelle
- Administratorrechte zum Konfigurieren von DHCP-Diensten

14.3 Konfigurieren des ISC-DHCPv4-Servers

Die ISC-DHCPv4-Konfiguration verwendet Klassen- und Unterklassendeklarationen, um PXE- und HTTP-Client-Typen abzugleichen und geeignete Startdateien für verschiedene Architekturen bereitzustellen.

VORGEHEN 57: EINRICHTEN DES ISC-DHCPV4-SERVERS

1. Konfigurieren Sie den ISC-DHCPv4-Server:

```
> 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. Konfigurieren Sie die DHCP-Schnittstelle in sysconfig:

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

3. Testen Sie die DHCPv4-Konfiguration:

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

4. Aktivieren und starten Sie den ISC-DHCPv4-Dienst:

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

14.4 Konfigurieren des ISC-DHCPv6-Servers

Die ISC-DHCPv6-Konfiguration bietet die IPv6-Adresszuweisung und Informationen zu Startdateien mithilfe des Klassenabgleichs des Herstellers mit ordnungsgemäßer Verarbeitung der DHCPV6-Option.

VORGEHEN 58: EINRICHTEN DES ISC-DHCPV6-SERVERS

1. Konfigurieren Sie den ISC-DHCPv6-Server:

```
> 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. Konfigurieren Sie die DHCPv6-Schnittstelle in sysconfig:

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

3. Testen Sie die DHCPv6-Konfiguration:

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

4. Aktivieren und starten Sie den ISC-DHCPv6-Dienst:

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

14.5 Überprüfen der ISC-DHCP-Konfiguration

Testen Sie die Funktionalität des ISC-DHCP-Servers, um eine ordnungsgemäße Netzwerkkonfiguration und die Bereitstellung der Startdateien für die PXE-Clients sicherzustellen.

VORGEHEN 59: TESTEN DER ISC-DHCP-SERVER

1. Überprüfen Sie den ISC-DHCPv4-Dienststatus:

```
> systemctl status dhcpd
```

2. Überprüfen Sie den ISC-DHCPv6-Dienststatus:

```
> systemctl status dhcpd6
```

3. Überprüfen Sie die DHCP-Portbindung:

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

4. Überwachen Sie DHCP-Protokolle:

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

5. Überprüfen Sie aktive DHCP-Leases:

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

6. Überwachen Sie die DHCPv6-Aktivität:

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

14.6 Beheben von Fehlern bei der ISC-DHCP-Konfiguration

Häufige Probleme beim Konfigurieren von ISC-DHCP-Servern für PXE-Startumgebungen.

14.6.1 Probleme bei der Konfiguration und den Diensten

Der ISC-DHCP-Dienst kann aufgrund von Konfigurationssyntaxfehlern oder Problemen bei der Schnittstellenbindung möglicherweise nicht gestartet werden.

VORGEHEN 60: BEHEBEN VON PROBLEMEN BEI DER ISC-DHCP-KONFIGURATION

1. Testen Sie die Syntax der DHCPv4-Konfiguration:

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

2. Testen Sie die Syntax der DHCPv6-Konfiguration:

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

3. Überprüfen Sie die Schnittstellenkonfiguration:

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

4. Überprüfen Sie den Status der Netzwerkschnittstelle:

```
> ip addr show eno1
```

5. Suchen Sie nach Portkonflikten:

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

6. Sehen Sie sich detaillierte Dienstprotokolle an:

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

14.6.2 Probleme bei DHCP-Lease-Zuweisungen

Clients erhalten möglicherweise aufgrund von Problemen mit der Subnetzkonfiguration oder der Autorisierung keine IP-Adressen.

VORGEHEN 61: DIAGNOSE VON ISC-DHCP-LEASING-PROBLEMEN

1. Überprüfen Sie die Subnetz- und Bereichskonfiguration:

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

2. Überprüfen Sie die autorisierende Einstellung:

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

3. Überwachen Sie Lease-Zuweisungen in Echtzeit:

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

4. Überprüfen Sie die Lease-Datenbank auf Fehler:

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

5. Testen Sie die DHCP-Antwort manuell:

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

14.6.3 Probleme beim Klassen- und Unterklassenabgleich

PXE-Clients erhalten möglicherweise IP-Adressen, jedoch aufgrund von Problemen bei der Klassenabgleichskonfiguration nicht die richtigen Startdateien.

VORGEHEN 62: BEHEBEN VON FEHLERN BEIM ISC-DHCP-KLASSENABGLEICH

1. Überprüfen Sie die Klassendefinitionen:

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

2. Überprüfen Sie die Unterklasseneinträge:

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

3. Überwachen Sie den Herstellerklassenbezeichner:

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

4. Testen Sie die Aufrufbarkeit von Startdateien:

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

5. Aktivieren Sie die detaillierte Protokollierung:

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

```
> sudo systemctl restart dhcpd
```

14.6.4 Probleme bei DHCPv6-Herstellerklassenoptionen

IPv6-DHCP-Clients verfügen über eine komplexe Handhabung von Herstellerklassenoptionen, die möglicherweise eine spezielle Konfiguration für die Unterstützung des ordnungsgemäßen PXE-Starts erfordern.

VORGEHEN 63: BEHEBEN VON ISC-DHCPV6-PROBLEMEN

1. Überprüfen Sie die DHCPv6-Optionsdefinitionen:

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

2. Überprüfen Sie die Zeichenfolgenanalyse der Herstellerklasse:

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

3. Überwachen Sie den DHCPv6-Klassenabgleich des Herstellers:

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

4. Überprüfen Sie das Format der IPv6-Startdatei-URL:

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

5. Überprüfen Sie die Abhängigkeit von Router-Advertisement:

```
> systemctl status radvd
```

6. Testen Sie die IPv6-Konnektivität:

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

14.7 Nächste Schritte

Wenn die ISC-DHCP-Dienste konfiguriert sind, können PXE-Clients mithilfe des traditionellen Klassen- und Unterklassensystems Informationen zur Netzwerkkonfiguration und zu Startdateien erhalten. Auch wenn ISC-DHCP das Ende der Lebensdauer erreicht hat, bietet diese Konfiguration Kompatibilität für vorhandene Bereitstellungen, die PXE- und HTTP-Startfunktionen für mehrere Client-Architekturen erfordern.

15 Validieren der PXE-Servereinrichtung

In diesem Abschnitt wird beschrieben, wie die komplette PXE-Servereinrichtung validiert und getestet wird, um sicherzustellen, dass alle Komponenten für SUSE Linux Enterprise Server 16.0-Netzwerkinstallationen ordnungsgemäß funktionieren. Er behandelt die Dienstverifizierung, das Testen der Netzwerkkonnektivität und die durchgängige PXE-Startvalidierung.

15.1 Einführung

Nach der Konfiguration aller PXE-Serverkomponenten, einschließlich der TFTP-, HTTP-, DNS-, DHCP- und GRUB 2-Bootloader-Dienste, muss unbedingt überprüft werden, ob das gesamte System ordnungsgemäß funktioniert. Diese Überprüfung stellt sicher, dass PXE-Clients im Agama-Installationsprogramm erfolgreich gestartet werden und netzwerkbasierte Installationen von SUSE Linux Enterprise Server 16.0 vornehmen können.

15.2 Anforderungen

- Alle PXE-Serverkomponenten wurden konfiguriert und werden ausgeführt
- Testen, dass Client-Systeme, den PXE-Start vornehmen können
- Netzwerkkonnektivität zwischen dem PXE-Server und den Clients
- Administratorzugriff zum Überwachen der Serverdienste

15.3 Validieren der PXE-Serverdienste

Überprüfen Sie, ob alle wichtigen PXE-Serverdienste ausgeführt werden und ordnungsgemäß konfiguriert sind, bevor Sie Tests mit PXE-Clients vornehmen.

VORGEHEN 64: ÜBERPRÜFEN DES PXE-SERVERDIENSTSTATUS

1. Überprüfen Sie den TFTP-Dienststatus:

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

   Erwartetes Ergebnis: Der Dienst sollte aktiv sein und Port 69 überwachen.

2. Überprüfen Sie den nginx-HTTP-Dienst:

   ```
   > systemctl status nginx
   ```

   Erwartetes Ergebnis: Der Dienst sollte aktiv sein und Port 80 überwachen.

3. Überprüfen Sie den DNS-Dienst (wenn Sie dnsmasq verwenden):

   ```
   > systemctl status dnsmasq
   ```

Erwartetes Ergebnis: Der Dienst sollte aktiv sein und Port 53 überwachen.

4. Überprüfen Sie den DHCP-Dienststatus (wählen Sie den entsprechenden Dienst aus):

```
> systemctl status dhcpd
```

Für dnsmasq-DHCP:

```
> systemctl status dnsmasq
```

Für Kea-DHCP:

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

Erwartetes Ergebnis: Der DHCP-Dienst sollte aktiv sein und die entsprechenden Ports überwachen.

5. Überprüfen Sie den Status des IPv6-Router Advertisement (falls konfiguriert):

```
> systemctl status radvd
```

Erwartetes Ergebnis: Der Dienst sollte für IPv6-Umgebungen aktiv sein.

6. Überprüfen Sie den NTP-Dienst:

```
> systemctl status chronyd
```

Erwartetes Ergebnis: Der Dienst sollte aktiv und synchronisiert sein.

15.4 Testen der Netzwerkkonnektivität und des Dateizugriffs

Überprüfen Sie, ob PXE-Clients über das Netzwerk mithilfe von TFTP- und HTTP-Protokollen auf Startdateien und Installationsinhalte zugreifen können.

VORGEHEN 65: TESTEN DES NETZWERKDATEIZUGRIFFS

1. Testen Sie den TFTP-Zugriff auf Bootloader-Dateien:

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

Überprüfen Sie, ob die Datei abgerufen wurde:

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

Bereinigen Sie die Testdatei:

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

2. Testen Sie den HTTP-Zugriff auf die GRUB 2-Konfiguration:

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

Erwartetes Ergebnis: Antwort „HTTP 200 OK“.

3. Überprüfen Sie den HTTP-Zugriff auf die Installationsprogrammdateien:

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

Erwartetes Ergebnis: Antwort „HTTP 200 OK“ mit entsprechender Inhaltslänge.

4. Testen Sie die DNS-Auflösung (falls lokales DNS konfiguriert ist):

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

Erwartetes Ergebnis: Ordnungsgemäße A- und AAAA-Datensatzauflösung.

5. Überprüfen Sie Verzeichnis, indem Sie es nach Autoindex-Speicherorten durchsuchen:

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

Erwartetes Ergebnis: Verzeichnisauflistung mit Startdateien.

15.5 Validieren der DHCP-Funktionalität

Testen Sie die Antworten des DHCP-Servers und stellen Sie sicher, dass die richtigen Startinformationen für verschiedene Client-Typen bereitgestellt werden.

VORGEHEN 66: TESTEN DER ANTWORTEN DES DHCP-SERVERS

1. Überprüfen Sie die DHCP-Portbindung:

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

Erwartetes Ergebnis: DHCP-Dienste, die die Ports 67 (IPv4) und 547 (IPv6) überwachen.

2. Überwachen Sie DHCP-Anforderungen in Echtzeit:

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

Oder für dnsmasq:

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

Führen Sie dies weiterhin aus, um die DHCP-Aktivität während des Tests zu beobachten.

3. Testen Sie die DHCP-Antwort mit dhcping (falls verfügbar):

```
> dhcping -s 192.168.1.200
```

Erwartetes Ergebnis: Erfolgreiche DHCP-Antwort vom Server.

4. Überprüfen Sie aktive DHCP-Leases:

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

Oder für Kea:

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

Erwartetes Ergebnis: Lease-Einträge für Test-Clients.

15.6 Durchgängiger PXE-Starttest

Nehmen Sie vollständige PXE-Starttests mit tatsächlichen Client-Systemen vor, um den gesamten Startvorgang von DHCP bis zum Start des Agama-Installationsprogramms zu validieren.

VORGEHEN 67: TESTEN DES VOLLSTÄNDIGEN PXE-STARTVORGANGS

1. Bereiten Sie ein Test-Clientsystem vor:
   - Konfigurieren von BIOS/UEFI, um den Netzwerkstart zu aktivieren
   - Festlegen des Netzwerkstarts als erste Startpriorität
   - Verbinden des Clients mit demselben Netzwerk wie der PXE-Server
2. Überwachen Sie die PXE-Serverprotokolle während des Client-Starts:

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

3. Starten Sie den Test-Client und beobachten Sie Folgendes:
    1. Der Client sollte die IP-Adresse per DHCP erhalten.
    2. Der Client sollte den Bootloader per TFTP herunterladen.
    3. Das GRUB 2-Menü sollte mit den Installationsoptionen angezeigt werden.
    4. Kernel und initrd sollten per HTTP geladen werden.
    5. Das Agama-Installationsprogramm sollte erfolgreich gestartet werden.
4. Überprüfen Sie die Erkennung der Client-Architektur, indem Sie verschiedene Client-Typen testen:
    - Ältere BIOS-x86_64-Systeme (sollten core.0 erhalten)
    - UEFI-x86_64-Systeme (sollten bootx64.efi erhalten)
    - UEFI-aarch64-Systeme (sollten bootaa64.efi erhalten)
5. Testen Sie den IPv6-PXE-Start (falls IPv6 konfiguriert ist):
    - Ausschließliches Aktivieren der IPv6-Netzwerkkonfiguration auf dem Test-Client
    - Überprüfen der DHCPv6-Adresszuweisung
    - Bestätigen der Bereitstellung der IPv6-Startdatei-URL

15.7 Validierung der Funktionalität des Agama-Installationsprogramms

Überprüfen Sie, ob das Agama-Installationsprogramm ordnungsgemäß gestartet wird und auf die Installationsquellen zugreifen kann, um SUSE Linux Enterprise Server 16.0-Installationen abzuschließen.

VORGEHEN 68: TESTEN DES STARTS DES AGAMA-INSTALLATIONSPROGRAMMS

1. Überprüfen Sie die Aufrufbarkeit der Agama-Weboberfläche:
   Notieren Sie sich beim Starten des Clients die zugewiesene IP-Adresse und greifen Sie auf Folgendes zu:

   ```
   http://CLIENT_IP_ADDRESS
   ```

Erwartetes Ergebnis: Die Agama-Weboberfläche sollte erfolgreich geladen werden.

2. Überprüfen Sie die Protokolle des Agama-Installationsprogramms auf dem Client:
   Wechseln Sie zur Konsole (Alt + F2) und führen Sie Folgendes aus:

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

   Erwartetes Ergebnis: Keine kritischen Fehler beim Start von Agama.

3. Überprüfen Sie die Aufrufbarkeit der Installationsquelle:
   Überprüfen Sie für vollständige ISO-Installationen den Repository-Zugriff:

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

   Erwartetes Ergebnis: Antwort „HTTP 200 OK“ mit Verzeichnisliste.

4. Fähigkeit zur Installation von Testpaketen:
   Überprüfen Sie auf der Agama-Oberfläche Folgendes:

   - Das System kann verfügbare Festplatten erkennen.
   - Die Netzwerkkonfiguration wird beibehalten.
   - Auf das Paket-Repository kann zugegriffen werden.
   - Die Installation kann abgeschlossen werden.

15.8 Beheben von Fehlern bei der Validierung

Häufige Probleme bei der PXE-Servervalidierung und deren Lösungsschritte.

15.8.1 Fehler bei der DHCP-Zuweisung

Clients erhalten beim PXE-Start keine IP-Adressen.

VORGEHEN 69: BEHEBUNG VON PROBLEMEN BEI DER DHCP-VALIDIERUNG

1. Überprüfen Sie die DHCP-Dienstkonflikte:

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

2. Überprüfen Sie, ob die Netzwerkschnittstelle aktiv ist:

```
> ip addr show eno1
```

3. Überprüfen Sie die Verfügbarkeit des DHCP-Bereichs:

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

4. Überwachen Sie die DHCP-Protokolle auf Fehler:

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

15.8.2 Fehler bei der Bereitstellung von Startdateien

Clients erhalten IP-Adressen, können jedoch keine Startdateien herunterladen.

VORGEHEN 70: LÖSEN VON PROBLEME MIT STARTDATEIEN

1. Überprüfen Sie die Aufrufbarkeit des TFTP-Diensts:

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

2. Überprüfen Sie die Dateiberechtigungen:

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

3. Überwachen Sie die TFTP-Zugriffsprotokolle:

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

4. Überprüfen Sie die Architekturerkennung:

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

15.8.3 Fehler beim Start des Agama-Installationsprogramms

Die Startdateien werden erfolgreich geladen, aber das Agama-Installationsprogramm kann nicht gestartet werden.

VORGEHEN 71: LÖSEN VON PROBLEMEN BEIM START VON AGAMA

1. Überprüfen Sie den HTTP-Zugriff auf die Installationsprogrammdateien:

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

2. Überprüfen Sie die Syntax der Kernelparameter in der GRUB 2-Konfiguration:

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

3. Überwachen Sie den Client-Startvorgang:

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

4. Überprüfen Sie, ob die Netzwerkkonfiguration beibehalten wurde:

```
# ip addr show
```

15.9 Checkliste für die PXE-Servervalidierung

Verwenden Sie diese Checkliste, um systematisch alle Aspekte Ihrer PXE-Serverkonfiguration zu überprüfen.

TABELLE 2: CHECKLISTE FÜR DIE PXE-SERVERVALIDIERUNG

Komponente	Validierungsschritt	Status
TFTP-Dienst	Dienst aktiv, Port 69 überwacht, Dateien aufrufbar	☐
HTTP-Dienst	nginx aktiv, Port 80 überwacht, Installationsprogrammdateien aufrufbar	☐
DNS-Dienst	Hostnamenauflösung funktioniert, Port 53 überwacht	☐
DHCP-Dienst	IP-Zuweisung funktioniert, Startoptionen werden bereitgestellt	☐
GRUB 2-Konfiguration	Menü wird geladen, Architekturerkennung funktioniert	☐

Komponente	Validierungsschritt	Status
IPv6-Unterstützung	Router Advertisement aktiv, DHCPv6 funktioniert	☐
PXE-Boot	Client startet erfolgreich, erhält den richtigen Bootloader	☐
Agama-Installationsprogramm	Installationsprogramm wird gestartet; Weboberfläche aufrufbar	☐
Installationsquelle	Repository aufrufbar, Pakete installierbar	☐
Netzwerkbeibehaltung	Netzwerkkonfiguration wird während der Installation beibehalten	☐

15.10 Fazit der Validierung

Ein ordnungsgemäß validierter PXE-Server sollte vom Start des Client-Netzwerks bis zum Start des Agama-Installationsprogramms eine erfolgreiche und durchgängige Funktionalität aufweisen. Alle Dienste sollten fehlerfrei funktionieren und die Clients sollten in der Lage sein, SUSE Linux Enterprise Server 16.0-Installationen über Netzwerk abzuschließen. Regelmäßige Validierungstests stellen die kontinuierliche Zuverlässigkeit der PXE-Infrastruktur für automatisierte Bereitstellungen sicher.

16 Rechtliche Hinweise

Alle Informationen in diesem Buch wurden mit größter Sorgfalt zusammengestellt. Auch hierdurch kann jedoch keine hundertprozentige Richtigkeit gewährleistet werden. Weder SUSE LLC noch ihre Tochtergesellschaften noch die Autoren noch die Übersetzer können für mögliche Fehler und deren Folgen haftbar gemacht werden.

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.