SUSE Linux Enterprise Server 16.0でのPXEブートサーバの設定

概要

UEFIセキュアブートとAgama インストーラをサポートするPXEブートサーバを設定します。

目的

ネットワーク経由で複数の SUSE Linux Enterprise Server 16.0システムのインストールを自動化し、効率化します。

所要時間

システム管理者やネットワーク管理者の場合、この記事の理解に通常30〜45分ほどを要します。

目標

複数のアーキテクチャをAgamaインストーラで起動できる、機能するPXEサーバの構築。

要件

- 管理者特権を持つSUSE Linux Enterprise Server 16.0システム
- ISOイメージを取得するためのインターネット接続
- PXEサーバの静的IP設定

発行日: 01/10/2026

目次

1 SUSE Linux Enterprise Server 16.0におけるPXEブートの概要 4
2 PXEブートサービス用のネットワークの準備 7
3 必要なPXEサーバコンポーネントのインストール 12
4 PXEサーバ用のGRUB 2 NetBootディレクトリの作成 17
5 インストーライメージコンテンツの準備 20
6 PXEブート用のGRUB 2の設定 26
7 PXEブート用TFTPの設定 37
8 HTTP配信用のnginxの設定 41
9 dnsmasqを使用したDNSサーバの設定 45
10 chronyを使用したNTPサーバの設定 50
11 IPv6ルータ広告の設定 53
12 dnsmasqを使用したDHCPサーバの設定 58
13 Keaを使用したDHCPサーバの設定 64
14 ISC DHCPを使用したDHCPサーバの設定 74

15 PXEサーバのセットアップの検証 83
16 法的事項 91
A GNU Free Documentation License 92

1 SUSE Linux Enterprise Server 16.0におけるPXEブートの概要

PXEブートにより、ローカルストレージなしで、マシンをネットワーク経由でインストールまたはランタイム環境にブートできます。このセクションでは SUSE Linux Enterprise Server 16.0 AgamaとライブインストーライメージにおけるPXEの仕組みについて、GRUB 2に焦点を当てて説明します。

1.1 PXEブートとは

PXE (Preboot Execution Environment)は、DHCPおよびTFTPまたはHTTPを使用して、システムがネットワークサーバからブートローダとOSインストーラを取得できるようにする方法です。物理メディアやプリインストールされたオペレーティングシステムがないマシンのプロビジョニングに広く使用されています。

1.2 PXEブートの利点

PXEブートは、ローカルインストールメディアや手動セットアップの必要性をなくし、プロビジョニングを簡素化します。PXEブートにより、以下が可能になります。

- ネットワークを介した多数のシステムの無人インストール
- インストーラのバージョンとブート設定の集中管理
- UEFIセキュアブートを含む、多様なアーキテクチャとファームウェアタイプのサポート
- GRUB 2メニューを使用したインストーラまたはインストールパラメータの動的選択

1.3 SUSE Linux Enterprise Server 16.0におけるPXEブートの仕組み

SUSE Linux Enterprise Server 16.0のPXEブートは、ブートローダとしてGRUB 2を使用し、インストールインタフェースとしてAgamaインストーラを使用します。ブートローダとインストーラファイルは、HTTPまたはTFTPを使用してネットワーク経由で提供され、GRUB 2がカーネル、initrd、ライブイメージを取得します。PXEクライアント

は、AMD64/Intel64、AArch64、ppc64le、s390xなどのアーキテクチャに応じて、さまざまなファームウェア(BIOSやUEFIなどの最も一般的なものを含む)、ブートローダ実行ファイル、またはイメージ形式を使用できます。さらに、IPv4とIPv6の両方のネットワークで動作する必要があります。

ブートローダは、`root=live:`などのカーネルパラメータを渡し、ライブISOイメージからsquashfsベースのルートファイルシステムをロードし、Agamaインタフェースをローカルでまたはリモート Web UI用のWeb サービスとして起動します。

1.3.1 SLES 15.xとの後方互換性

この記事の情報は、主に SUSE Linux Enterprise Server 16.0以降に適用されます。Agamaインストーラと統合し、ライブインストールイメージに依存するPXEブートワークフローに焦点を当てています。この記事の文脈と範囲において、 SLES 16.0以降のバージョンはSLES 15.xとは以下の点で異なります。

インストーラ
: `linuxrc`とYaSTの代わりに`dracut`とAgamaを使用します。

DHCPサーバ
: ISC DHCPの使用は廃止されました(EOL 2022)。DHCPサーバには、代わりにKeaまたはdnsmasqを使用します。

ブートパラメータ
: `root=live:`パラメータを使用してagamaインストーライメージをロードし、`install=`パラメータの代わりに、オプションの`inst.install_url=`を使用してデフォルト以外のインストールリポジトリを指定します。

ブートローダの選択(GRUB 2、pxelinuxなど)は柔軟性を保ち、バージョンに依存しません。

1.3.2 さまざまなセットアップと手順

この記事は、必須のセットアップ手順と、オプションまたは代替の設定で構成されています。自身の展開に関連するセクションにのみ従い、展開に該当しない代替セクションはスキップしてください。

必須
: コンポーネントのインストール、インストーライメージの準備、GRUB 2の設定、サーバの検証などのタスクは、すべてのセットアップで完了する必要があります。

ファイル配信方法

`nginx`などのHTTPサーバ(Agamaで推奨)、および/または`tftp` や`dnsmasq`などのTFTPサーバ。

DHCPサーバ

Keaまたはdnsmasqのいずれかを選択します。

注記: 選択した方法の制限事項と機能

- ISC DHCPの最新の代替として、ISCの新しいDHCPサーバである**Kea**を使用します。Keaの詳細については、https://www.isc.org/kea/を参照してください。ISC DHCP EOL通知については、https://www.isc.org/dhcp/を参照してください。KeaはDHCPサーバであり、別途TFTPサーバソフトウェアが必要です。Kea DHCPサーバは、IPv4およびIPv6経由のTFTP/PXEブートと、IPv4経由のHTTPブートのオプションをサポートしています。IPv6経由のHTTPブートでは、DHCPv6サーバが、「クライアントがベンダを識別するために」使用すると想定される`Vendor Class Option` (`RFC3315, Section 22.16`を参照)をクライアントに返送できることが必要ですが、これは現在サポートされていません。

- DNSサーバ、DHCPサーバ、TFTPサーバの組み合わせである**dnsmasq**を使用します。dnsmasqは、ブートローダ、カーネル、initrd (およびその他のファイル)をTFTP経由で提供するために使用できます。dnsmasqの詳細については、https://thekelleys.org.uk/dnsmasq/doc.htmlを参照してください。dnsmasq DHCPサーバは、IPv4およびIPv6経由のTFTP/PXEブートと、IPv4経由のHTTPブートのオプションをサポートしています。IPv6経由のHTTPブートでは、DHCPv6サーバが、「クライアントがベンダを識別するために」使用すると想定される`Vendor Class Option`(`RFC3315, Section 22.16`を参照)をクライアントに返送できることが必要ですが、これは現在サポートされていません。

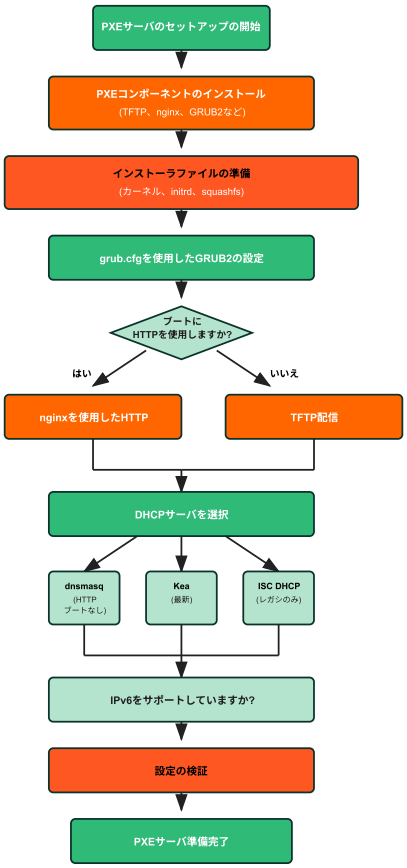

図 1: PXEサーバセットアップワークフローの例

2 PXEブートサービス用のネットワークの準備

このモジュールでは、PXEブートサービスをSUSE Linux Enterprise Server 16.0上で展開するためのネットワークインフラストラクチャ要件について説明します。

2.1 概要

PXEサーバは、アドレスとブートファイル(ブートローダ)の場所を提供するDHCPサーバと、ファイルを取得するためのTFTPサーバおよび/またはHTTPサーバの3つのサーバで構成されています。さらに、DNSサーバ、NTPサーバ、IPv6をサポートするルータが存在する場合も

あります。通常、運用ネットワークではこれらはPXEサーバとは別個に存在します。SUSE Linux Enterprise Server 16.0を実行するPXEサーバでは、特定のネットワークインタフェースの設定、ファイアウォールへの特定の永続ルールの追加、およびSELinuxでのいくつかの権限が必要になる場合もあります。このセクションでは、適切なIP範囲と、ファイアウォールとSELinuxに必要なルールを持つサンプルネットワークを示します。

2.2 前提条件とサンプルネットワーク設定

この記事では以下のように仮定しています。

- PXEサーバは、以下のネットワーク設定で、eno1ネットワークインタフェース上で実行されています。

  表 1: サンプルPXEネットワーク設定

	IPv4	IPv6	DNS名
PXEネットワーク	192.168.1.0/24	2001:db8:0:1::/64	example.net
PXEサーバ	192.168.1.200	2001:db8:0:1::200	pxe.example.net
PXEゲートウェイ	192.168.1.1	2001:db8:0:1::1	
DNSサーバ	192.168.1.200	2001:db8:0:1::200	
NTPサーバ	192.168.1.1	2001:db8:0:1::1	

- デフォルトでは、ルータ、NTP、DNSサーバは外部にあり、別のマシンで実行されています。この記事では、いくつかのヒントを提供しますが、完全な設定をカバーするものではありません。

2.3 PXEサービス用のネットワークインタフェース、ファイアウォール、SELinuxの設定

PXEサーバが必要とするネットワークサービスを許可するように、ネットワークインタフェースとファイアウォールを設定します。SELinux設定を調整して、インストールテストを有効にし、永続的なローカルポリシーを定義します。

1. PXEネットワークインタフェースを確認し、適切なfirewalldゾーンに割り当てます。

   a. 現在アクティブなゾーンと割り当てられたインタフェースを確認します。

```
> sudofirewall-cmd --get-active-zones
```

b. publicゾーンにeno1が割り当てられていない場合は、割り当てます。

```
> sudofirewall-cmd --zone=public --change-interface=eno1
```

c. インタフェースの割り当てを、再起動しても永続化するようにします。

```
> sudofirewall-cmd --permanent --zone=public --add-interface=eno1
```

2. DNSサービスへのアクセス用にファイアウォールを設定します。

a. 現在のセッションでDNSサービスを許可します。

```
> sudofirewall-cmd --zone=public --add-service=dns
```

b. 変更を永続化します。

```
> sudofirewall-cmd --permanent --zone=public --add-service=dns
```

3. NTPサービスへのアクセス用にファイアウォールを設定します。

a. 現在のセッションでNTPサービスを許可します。

```
> sudofirewall-cmd --zone=public --add-service=ntp
```

b. 変更を永続化します。

```
> sudofirewall-cmd --permanent --zone=public --add-service=ntp
```

4. DHCP (IPv4)サービスへのアクセス用にファイアウォールを設定します。

a. 現在のセッションでDHCPサービスを許可します。

```
> sudofirewall-cmd --zone=public --add-service=dhcp
```

b. 変更を永続化します。

```
> sudofirewall-cmd --permanent --zone=public --add-service=dhcp
```

5. DHCPv6サービスへのアクセス用にファイアウォールを設定します。

a. 現在のセッションでDHCPv6サービスを許可します。

```
> sudofirewall-cmd --zone=public --add-service=dhcpv6
```

b. 変更を永続化します。

```
> sudofirewall-cmd --permanent --zone=public --add-service=dhcpv6
```

6. TFTPサービスへのアクセス用にファイアウォールを設定します。

a. 現在のセッションでTFTPサービスを許可します。

```
> sudofirewall-cmd --zone=public --add-service=tftp
```

b. 変更を永続化します。

```
> sudofirewall-cmd --permanent --zone=public --add-service=tftp
```

7. HTTPサービスへのアクセス用にファイアウォールを設定します。

a. 現在のセッションでHTTPサービスを許可します。

```
> sudofirewall-cmd --zone=public --add-service=http
```

b. 変更を永続化します。

```
> sudofirewall-cmd --permanent --zone=public --add-service=http
```

8. HTTPSサービスへのアクセス用にファイアウォールを設定します。

a. 現在のセッションでHTTPSサービスを許可します。

```
> sudofirewall-cmd --zone=public --add-service=https
```

b. 変更を永続化します。

```
> sudofirewall-cmd --permanent --zone=public --add-service=https
```

9. セットアップテストのため、SELinuxを一時的に無効にします。

a. SELinuxを許容モードに設定します。

```
> sudosetenforce 0
```

b. SELinuxステータスをチェックします。

```
> sudosestatus
```

10. PXE関連サービス用のローカルSELinuxポリシーモジュールを生成し、インストールします。

a. nginx用のモジュールを作成し、インストールします。

```
> sudoif 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
```

```
> sudofi
```

b. dnsmasq用のモジュールを作成し、インストールします。

```
> sudoif 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
```

```
> sudofi
```

c. in.tftpd用のモジュールを作成し、インストールします。

```
> sudoif 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
```

```
> sudofi
```

11. SELinux強制モードを再度有効化します。

a. SELinuxを強制モードに設定します。

```
> sudosetenforce 1
```

b. SELinuxのステータスを確認します。

```
> sudosestatus
```

2.4 まとめ

この手順により、PXEサーバのネットワークインタフェース、ファイアウォール、およびSELinuxポリシーが、安全かつ機能的に動作するように正しく設定されていることが確認されました。

- PXEサービングインタフェース(この例ではeno1)を確認し、public firewalldゾーンに割り当てました。
- dns、ntp、dhcp、dhcpv6、tftp、http、httpsを含む、PXE操作に必要なファイアウォールサービスを開きました。
- サービステストを容易にし、AVC拒否のログを記録するため、SELinuxを一時的にpermissiveモードに設定しました。
- **ausearch**と**audit2allow**を使用して、nginx、dnsmasq、in.tftpdなどのサービス用のカスタムSELinuxポリシーモジュールを生成し、インストールしました。
- SELinuxをenforcingモードに復元し、運用システムの安全を確保しました。

これらの手順が完了すると、PXEサーバは安全に設定され、IPv4またはIPv6を使用してネットワーク経由でクライアントマシンにサービスを提供する準備が整います。

3 必要なPXEサーバコンポーネントのインストール

このセクションでは、SUSE Linux Enterprise Server 16.0で、PXEブートをサポートするために必要なパッケージ(GRUB 2、DHCP、TFTP、および/またはHTTPコンポーネントを含む)をインストールする方法について説明します。

3.1 概要

SUSE Linux Enterprise Server 16.0でPXEブートサーバを設定するには、いくつかのサービスとツールをインストールする必要があります。セットアップによっては、以下のものが必要になる場合があります。

- dnsmasqパッケージは、DNSサーバ、TFTPサーバ、DHCPサーバ(DHCPv4およびDHCPv6)の組み合わせを提供し、IPv6ルータ広告(RA)を限定的にサポートします。以下のものを提供します。

- dnsmasq DHCPサーバ:以下の要求とクライアントのアーキテクチャに応じて、DHCPオプションの条件付き配信をサポートします。
  - DHCPv4およびDHCPv6を使用したPXEブート要求
  - DHCPv4を使用したHTTPブート要求

  ### 注記: DHCPv6経由のHTTPブートにおけるdnsmasqの制限事項

  現在、dnsmasqは必要な`vendor-class` DHCPv6オプションの送信をサポートしていません。

- dnsmasq TFTPサーバ:PXEブート中にTFTP経由でブートローダファイル、カーネル、initrdを配信します。
- dnsmasq DNSサーバ:インストーラ/OS内のクライアントファームウェアと`/etc/resolv.conf`のドメイン名とIPアドレスの再帰的解決を提供します。
- dnsmasq IPv6 RA:PXEサーバがルータとしても動作している場合、IPv6 RAの送信をサポートします(設定可能なのは「一般的なRAパターン」に制限されます)。

- `kea`パッケージはDHCPサーバで、ISC DHCPサーバの後継です。以下の要求とクライアントのアーキテクチャに応じて、DHCPオプションの条件付き配信をサポートします。
  - DHCPv4およびDHCPv6を使用したPXEブート要求
  - DHCPv4を使用したHTTPブート要求

  ### 注記: DHCPv6経由のHTTPブートにおけるKeaの制限事項

  現在、Keaは必要な`vendor-class` DHCPv6オプションの送信をサポートしていません。詳細については、https://kea.readthedocs.io/en/latest/arm/dhcp6-srv.html#id4 を参照してください。

- TFTPサーバは、ブートローダファイル、カーネル、およびinitrdをTFTP経由で配信します。一方、keaによるPXEブートは`tftp`パッケージで提供され、HTTPブートには必要ありません。`dnsmasq` を使用している場合、`tftp`パッケージは必要ありません。

- HTTP経由でインストーライメージを提供するための`nginx`パッケージのような Webサーバ。

注記: HTTPサーバの必要性

nginxのようなHTTP/HTTPSサーバはほぼ常に必要です。その用途はHTTPブートだけにとどまりません。特に、以下のようなシナリオで必要になることがあります。

- HTTPブートの基本要件です。
- `squashfs.img`を提供するために推奨されます。ブートコマンドラインで`root=live:tftp://.../squashfs.img`を使用できます。
- また、`SLES-16.0-Full-*.inline.iso`の`inst.install_url=http://.../install/`ブートコマンドラインパラメータで、無人インストール用のインストールプロファイルやその他のファイルとともにRPMを Agamaに提供する場合にも推奨されます。

- GRUB 2ブートローダパッケージは、サポートされているアーキテクチャと方法でネットワークブートを提供します。たとえば、AMD64/Intel 64アーキテクチャは、ネットワークブートに2つの方法を提供しています。BIOSとUEFI。さらに、UEFIは通常、PXE(TFTP)とHTTPブートをサポートしています。pxelinuxのような他のブートローダはUEFIとHTTPブートをサポートしていません。
- オプションで、IPv6用のルータ広告デーモン(`radvd`パッケージなど)。これは、 SLESがインストーラネットワークのルータとしても動作する場合に、以下を実行する場合に必要です。
  - PXEまたはHTTPブートクライアントのネットワーク上でルーティングを設定する。
  - PXEまたはHTTPブートクライアントのネットワーク上でDHCPv6の使用を有効にする。

3.2 要件

- SUSE Linux Enterprise Server 16.0を管理者特権で実行し、SUSEカスタマーセンターに登録され、SUSEConnectを使用して適切なオンラインリポジトリにアクセスできるように設定されているシステム。
- 有効なSLEモジュール:Server Applications Module、レガシモジュール、およびBase System Module。
- ネットワークサービスおよびブートローダ用SLEモジュールリポジトリへのアクセス。
- パッケージを取得するための機能しているインターネット接続。

3.3 パッケージのインストール

以下の手順で、PXEブートサーバに必要なコアパッケージをインストールします。

手順 1: PXEブートサーバに必要なパッケージのインストール

1. 共通の要件として、GRUB 2ブートローダとnginx HTTPサーバをインストールします。

```
> sudozypper install grub2 nginx
```

2. 以下のいずれかのコマンドを実行して、ご使用のアプローチに不可欠なパッケージをインストールします。
   - DHCPサーバの場合は `kea`、TFTPサーバの場合は`tftp`

```
> sudozypper install kea tftp
```

   - DHCP、DNS、およびTFTPサーバの共通プロバイダとして`dnsmasq`

```
> sudozypper install dnsmasq
```

注記: KeaとdnsmasqがDHCPサーバの制限事項

IPv6経由のHTTPブートは、`kea`と`dnsmasq`パッケージが提供するDHCPサーバでは**現在**サポートされていません。UEFI仕様で要求されているように、HTTPクライアントに`vendor-class`オプションを返送することもサポートされていません。

3. オプションで、他のプラットフォームをサポートする予定であれば、追加のアーキテクチャ固有のGRUB 2ターゲットをインストールします。

- AMD64/Intel 64アーキテクチャの場合:

```
> sudozypper install grub2-x86_64-efi grub2-i386-pc
```

- AArch64アーキテクチャの場合:

```
> sudozypper install grub2-aarch64-efi
```

- ppc64leアーキテクチャの場合:

```
> sudozypper install grub2-ppc64le-ieee1275
```

注記: PXEサーバがサーバマシンのアーキテクチャとは異なるクライアントにGRUB 2パッケージを配信する方法

GRUB 2のアーキテクチャ固有の`noarch.rpm`パッケージは、PXEサーバが設定されているマシンのアーキテクチャに関係なく、インストールメディア/リポジトリの`noarch`サブディレクトリに含まれています。つまり、他のアーキテクチャのクライアントをサポートするために、AMD64/Intel64マシンで動作するPXEサーバに`grub2-arm64-efi` パッケージと`grub2-powerpc-ieee1275`パッケージをインストールすることができます。

4. AMD64/Intel 64またはAArch64用のUEFIセキュアブートが必要で、インストールメディアISOのファイルを使用しない場合は、オプションで`shim`パッケージをインストールできます。

```
> sudozypper install shim
```

5. オプションで、PXEサーバをルータとして使用する場合は、ルータ広告デーモン`radvd`をインストールします(運用ネットワークでは推奨されません)。

```
> sudozypper install radvd
```

6. ISOとディレクトリツリーを簡単にコピーまたは同期できるように、`rsync`ユーティリティをインストールします。

```
> sudozypper install rsync
```

7. サービスがインストールされているが、まだ開始されていないことを確認します。設定については以降のセクションで説明します。

4 PXEサーバ用のGRUB 2 NetBootディレクトリの作成

このセクションでは、**grub2-mknetdir**を使用して、PXEサーバ用のGRUB 2 NetBootディレクトリを作成する方法について説明します。このコマンドは、AMD64/Intel 64 (UEFIとBIOS)、 AArch64、およびppc64leシステム用のアーキテクチャ固有のディレクトリを生成します。UEFIセキュアブートをサポートするには、管理者はインストールメディアから署名付きEFIファイルをコピーするか、shimパッケージを使用してデフォルトの署名なしブートローダファイルを置き換える必要があります。

4.1 概要

このセクションでは、複数のアーキテクチャでPXEサーバを展開するためにGRUB 2 NetBootディレクトリを設定する方法について説明します。**grub2-mknetdir**コマンドは、プラットフォームごとに/srv/tftpboot/boot/grub2/の下に、アーキテクチャ固有のディレクトリを作成します。たとえば、AMD64/Intel 64システムは、UEFI (x86_64-efi)とレガシBIOS (i386-pc)の両方のディレクトリを生成し、AArch64とppc64leシステムはそれぞれのUEFIディレクトリ (arm64-efiとpowerpc-ieee1275)を作成します。

デフォルトの署名なしのcore.efiファイルでは提供されないUEFIセキュアブートをサポートするには、管理者は、インストールメディアから署名付きEFIファイルをコピーするか、shimパッケージをインストールして、必要なブートローダファイル(shim.efi、grub.efi、MokManager.efi)を適切なアーキテクチャディレクトリに手動でコピーします。これにより、適切なシンボリックリンク解決が確保され、すべてのファイルをTFTPルートディレクトリ内に保持することができます。

4.2 要件

- 次のパッケージ(grub2、tftp)、および他のアーキテクチャ固有のGRUB 2 パッケージ(grub2-x86_64-efiやgrub2-i386-pcなど)がインストールされていることを確認します。
- インストールメディア(ISO)がマウント可能であるか、shimパッケージがシステムにインストールされていることを確認します。ターゲットアーキテクチャ用のインストールメディア(ISO)は、SUSEカスタマーセンターからダウンロードできます。

4.3 NetBootディレクトリとUEFIセキュアブートの準備

この手順では、PXEネットワークブートに必要なGRUB 2ディレクトリ構造を作成し、オプションで複数のアーキテクチャにわたる UEFIセキュアブートのサポートを設定します。

1. GRUB 2 NetBootディレクトリ構造を作成します。

```
> sudogrub2-mknetdir --net-directory=/srv/tftpboot
--subdir=/boot/grub2
```

これにより、アーキテクチャ固有のディレクトリが作成されます。

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

警告

`grub2-mknetdir`によって作成された`grub.cfg`ファイルを手動で上書きしないでください。

2. `/srv/tftpboot/boot/grub2/`ディレクトリの下にある`fonts/`や`locale/`など、その他のアーキテクチャに依存しないディレクトリをTFTPサーバにコピーします。
3. AMD64/Intel 64またはAArch64アーキテクチャでは、**`grub2-mknetdir`**コマンドでインストールされた`/srv/tftpboot/boot/grub2/ARCH-efi/core.efi`ファイルをUEFI PXEにも使用できます。ただし、これらは**署名されておらず**、UEFIセキュアブートをサポートしていません。サポートされているAMD64/Intel 64およびAArch64アーキテクチャで、UEFIセキュアブートをオプションで有効にするには、以下の手順のいずれかを実行します。
   - インストールメディアISOから必要なファイルをコピーします。
     a. ISOイメージをマウントします。

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

     b. EFIファイルをコピーします。

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

❶ ARCH-efiをx86_64-efiまたはarm64-efi(UEFIセキュアブートでサポートされているアーキテクチャ)に置き換えます。

c. インストールメディアISOをアンマウントします。

```
> sudoumount /mnt
```

- インストールメディアISOのファイルを使用しない場合は、shimパッケージを使用します。

a. まだインストールしていない場合は、shimパッケージをインストールします。

```
> sudozypper install shim
```

b. 必要なアーキテクチャの署名済みブートローダファイルをコピーします。

i. shim.efiファイルをコピーします。

- AMD64/Intel 64アーキテクチャの場合:

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

- AArch64アーキテクチャの場合:

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

ii. grub.efiファイルをコピーします。

- AMD64/Intel 64アーキテクチャの場合:

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

- AArch64アーキテクチャの場合:

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

iii. MokManager.efiファイルをコピーします。

- AMD64/Intel 64アーキテクチャの場合:

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

- AArch64アーキテクチャの場合:

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

注記

`-L`フラグは、シンボリックリンクを解決して、ファイルがTFTPルート内に留まるようにします。

5 インストーライメージコンテンツの準備

このセクションでは、PXEブート環境用にSUSE Linux Enterprise Server 16.0インストールメディアからインストーラファイルを抽出して整理する方法を説明します。このセクションは、`.install.iso`イメージとRPMパッケージの両方をカバーし、異なるアーキテクチャやインストールタイプに関する具体的な手順を示します。

5.1 概要

SUSE Linux Enterprise Server 16.0は、さまざまなPXEブートシナリオをサポートする複数の形式のインストーラファイルを提供します。Agamaインストーラは、カーネルイメージ(`linux`)、初期RAMディスク(`initrd`)、圧縮されたルートファイルシステム(`squashfs.img`)の3つの必須ファイルを必要とします。これらのファイルは、インストールメディアから抽出し、TFTPやHTTP経由でアクセス可能なディレクトリ構造に整理する必要があります。

このセクションでは、`.install.iso`イメージとRPMパッケージの両方の準備方法について説明し、SUSE Linux Enterprise Server 16.0でサポートされるさまざまなアーキテクチャとインストールタイプとの互換性を確保します。

5.2 要件

- SUSEカスタマーセンターで入手可能なSUSE Linux Enterprise Server 16.0インストールメディア。以下の項目を選択することができます。
  - オンラインISO:ネットワークインストール用のインストーラのみ(`SLES-16.0-Online-ARCH-BUILD.install.iso`)
  - フルISO:インストールリポジトリ付きのインストーラ(`SLES-16.0-Full-ARCH-BUILD.install.iso`)
  - RPMパッケージ: `tftpboot-agama-installer-SUSE_SLE_16_PXE-ARCH`
- 一時的なマウントポイント(`/mnt`など)
- 選択したインストール方法に応じて、`/srv/tftpboot`および`/srv/install`の下の十分なディスク容量
- ディレクトリの作成やファイルのコピーのための管理者特権。

5.3 ISOイメージからのインストーラファイルの準備

ISOイメージは、インストーラファイルを抽出するための簡単な方法を提供します。以下の手順は、異なるアーキテクチャのオンラインとフルISOタイプの両方をカバーします。

5.3.1 オンラインISOイメージの使用

オンラインISOイメージにはインストーラコンポーネントのみが含まれており、システムインストール時にインストールリポジトリへのネットワークアクセスが必要です。これはGRUBの`SLES-16.0 Online Installation`ブートメニューエントリに対応しています。

手順 2: オンライン ISO (X86_64とAARCH64)からのファイルの抽出

1. インストールファイルのディレクトリ構造を作成します。

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

2. オンラインISOイメージをマウントします。

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

3. カーネルファイルとInitrdファイルをコピーします。

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

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

4. 圧縮されたルートファイルシステムをコピーします。

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

5. ISOイメージをアンマウントします。

```
> sudoumount /mnt
```

手順 3: オンライン ISO (PPC64LE)からのファイルの抽出

1. 次のディレクトリ構造を作成します。

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

2. ISOイメージをマウントします。

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

3. カーネルファイルとinitrdファイルをコピーします(ppc64leの場合、パス構造が異なることに注意してください)。

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

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

4. 圧縮されたルートファイルシステムをコピーします。

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

5. ISOイメージをアンマウントします。

```
> sudoumount /mnt
```

5.3.2 フルISOイメージの使用

フルISOイメージには、インストーラとインストールリポジトリの両方が含まれており、外部ネットワークに依存することなくローカルにインストー ルすることができます。これは、`inst.install_url=http://pxe.example.net/install/SLES-16.0/${arch}`パラメータが追加されたgrubの`SLES-16.0 Local Installation`ブートメニューエントリに対応します。

手順 4: フルISOからのファイルの抽出

1. インストーラファイルとインストールリポジトリの両方のディレクトリを作成します。

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

```
> sudomkdir -p /srv/install/SLES-16.0
```

2. フルISOイメージをマウントします。

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

3. カーネルファイルとinitrdファイルをコピーします(前の手順で示したようにppc64le用にパスを調整してください)。

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

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

4. 圧縮されたルートファイルシステムをコピーします。

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

5. ローカルHTTPサーバアクセス用のインストールリポジトリをコピーします。

```
> sudorsync -avP /mnt/install/ /srv/install/SLES-16.0/ARCH/
```

6. ISOイメージをアンマウントします。

```
> sudoumount /mnt
```

5.4 RPMパッケージからのインストーラファイルの準備

RPMパッケージは、オンラインインストーラファイルを入手するための代替方法を提供します。

手順 5: TFTPBOOT RPMパッケージのインストールと使用

1. 必要なパッケージをインストールします。

```
> sudozypper in tftpboot-agama-installer-SUSE_SLE_16-ARCH
```

2. linux、initrd、squashfs.imgを tftpbootにコピーします。

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

```
> sudocd
/srv/tftpboot/boot/images/SLES-16.0/ARCH
```

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

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

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

5.5 推奨ディレクトリ構造

抽出したファイルは、一貫性と保守の容易さを確保するために、以下のディレクトリレイアウトに従って整理します。この構造は、複数のアーキテクチャとインストールタイプをサポートします。

例 1: 完全なPXEサーバのディレクトリレイアウト

```
/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 インストールメディアから抽出したカーネルイメージ

❷ 初期RAMディスクイメージ

❸ Agamaインストーラ用の圧縮されたルートファイルシステム

❹ フルISOの`install`ディレクトリからのインストールリポジトリ(オプション)

5.6 インストールの検証

インストーラファイルを抽出して整理した後、必要なコンポーネントがすべて存在し、アクセス可能であることを検証します。

手順 6: 検証手順

1. 必要なファイルがあるか確認します。

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

2. 適切なファイルアクセス権があることを確認します。

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

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

重要: ファイルアクセシビリティ

抽出されたすべてのファイルが、TFTPおよびHTTPサービスで読み取り可能であることを確認します。ファイルは、ブートプロセス中にPXEクライアントによってアクセスされるため、適切な権限とサービス設定が、展開を成功させるために不可欠です。

5.7 次のステップ

インストーラファイルが適切に準備され、整理されていれば、以下の手順に進むことができます。

- これらのファイルを参照するメニューエントリを使用したPXEブート用GRUB 2の設定
- 抽出したコンテンツを提供するためのHTTPとTFTPサービスの設定
- PXEクライアントを適切なブートローダに誘導するためのDHCPの設定

抽出されたファイルは、`root=live:http://pxe.example.net/boot/images/SLES-16.0/ARCH/squashfs.img`のようなパスを使用してGRUB 2設定で参照されます。

6 PXEブート用のGRUB 2の設定

このセクションでは、SUSE Linux Enterprise Server 16.0でPXEベースのブート用にGRUB 2ブートローダを設定する方法について説明します。ネットワークブートディレクトリ構造の作成、アーキテクチャ固有のブートローダの設定、複数のアーキテクチャとインストールシナリオをサポートする柔軟な設定システムの実装について説明します。

6.1 概要

GRUB 2はPXEクライアントのネットワークブートローダとして機能し、カーネルファイルとinitrdファイルをロードしてAgamaインストーラを起動します。このセクションでは、クライアントアーキテクチャを自動的に検出し、ネットワークインタフェースの選択を管理し、複数のインストールタイプとターゲットアーキテクチャをサポートする統合ブートメニューを提供する、洗練されたGRUB 2設定を作成する方法を示します。

設定アプローチは、アーキテクチャの検出、変数定義、ブートメニューエントリのための個別のファイルを持つモジュラー設計を使用しています。これにより、異なるハードウェアプラットフォーム間で一貫性を維持しながら、マシン固有の設定や自動インストールプロファイルのサポートが可能になります。

6.2 要件

- 前のセクションで説明したように、GRUB 2のネットワークブートディレクトリ構造が整っていることを確認します。
- 前のセクションで説明したように、インストーラファイルが適切に整理されていることを確認します。
- すべてのターゲットアーキテクチャ用のGRUB 2パッケージ(`grub2-x86_64-efi`、`grub2-i386-pc`、`grub2-aarch64-efi`、および `grub2-ppc64le-ieee1275`)をインストールする必要があります。
- UEFIセキュアブートサポート用の`shim`パッケージ(オプション)。
- `/srv/tftpboot`または同等のPXEルートへの管理アクセス。

6.3 GRUB 2設定の作成

GRUB 2設定ファイルは、クライアントのアーキテクチャの検出、ネットワークインタフェースの管理、他の設定ファイルのロードという3つの主要なタスクを処理します。このモジュラー方式は、さまざまな展開シナリオに柔軟に対応できます。

手順 7: 主な`grub.cfg`ファイルの設定

- メインのGRUB 2設定ファイルを`/srv/tftpboot/boot/grub2/grub.cfg`に作成します。

```
> sudocat > /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
```

主な設定要素

アーキテクチャの検出

GRUB 2のCPUタイプをディストリビューションアーキテクチャにマッピングし、異なるハードウェアプラットフォームで動作する統合メニューエントリを可能にします。

ネットワークインタフェース管理

`pxe0`というPXEブートインタフェース上でのみdhcpを有効にするために、 grub2変数`${net_default_mac}`を使用して`${ipcfg}` 変数を定義し、 マルチインタフェースシステムでのネットワークプロービングの問題を回避します。

ユーティリティ定義

シリアルコンソールパラメータを指定して、一般的な`${sconsole}`変数を定義します。

マシン固有の設定

MACアドレスに基づいてオプションのマシンごとの設定ファイルをロードし、カスタマイズされたマシンごとのブートパラメータと自動インストールプロファイルを可能にします。

6.4 統合ブートメニューの作成

ブートメニューは、異なるハードウェアプラットフォームやインストールタイプに自動的に適応する、アーキテクチャに依存しないメニューエントリを提供するために、メイン設定からの変数を使用します。

手順 8: MENU.CFGファイルの設定

- `/srv/tftpboot/boot/grub2/menu.cfg`に統合ブートメニューを作成します。

```
> sudocat > /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
```

注記: メニューエントリの柔軟性

メニューエントリは、クライアントのアーキテクチャと設定に基づいて自動的に入力される変数を使用します。`${arch}`変数は、正しいファイルがロードされることを保証します。

オプションの`${ipcfg}`変数を指定すると、PXEで選択されたネットワークインタフェースのみが設定されます。

オプションの`${sconsole}`変数は、インストーラシステムでシリアルコンソールを有効にします。

6.5 マシン固有の設定

高度な展開では、デフォルト設定を上書きしたり、自動化されたインストールパラメータを提供するマシン固有の設定ファイルを作成できます。

手順 9: マシン固有の設定の作成

1. マシン固有の設定用のディレクトリを作成します。

```
> sudomkdir -p /srv/tftpboot/boot/config
```

2. MACアドレスがaa:bb:cc:dd:ee:ffのマシンの場合、固有の設定を作成します。

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

3. マシン固有のgrub.cfgを作成します。

```
> sudocat > /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
```

または、ホスト固有のgrub.cfgに独自のメニューエントリを提供します(例: 特定のブート試行用に生成)。

```
> sudocat > /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
```

例 2: マシン固有の共通パラメータ

`default`
: 自動的にブートするメニューエントリを指定します

`timeout`
: ブートタイムアウトを秒単位で設定します

`ipcfg`
: 特定のハードウェアのネットワークインタフェース設定を上書きします

`autoinstall`
: マシン固有の自動インストールプロファイルのURLを提供します。

6.6 GRUB 2設定の検証

設定ファイルを作成したら、セットアップが正しく、必要なファイルがすべて揃っていることを検証します。

手順 10: 検証手順

1. GRUB 2のディレクトリ構造を確認します。

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

2. GRUB 2ツールでテストして、設定ファイルの構文を確認します。

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

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

3. 適切なファイルアクセス権があることを確認します。

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

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

重要: 設定テスト

実際のPXEクライアントでGRUB 2設定をテストし、適切なアーキテクチャ検出とメニュー機能を確認します。`${net_default_mac}`変数は、実際のネットワークブートシナリオでのみ使用可能です。

6.7 GRUB 2設定のトラブルシューティング

GRUB 2 PXE設定で発生するよくある問題とその解決策。それぞれの問題には、問題を解決するための診断手順と具体的なコマンドが記載されています。

6.7.1 アーキテクチャの検出の失敗

GRUB 2が正しいアーキテクチャを検出できない場合、クライアントは正しくないバイナリで起動したり、完全にロードに失敗したりすることがあります。

手順 11: アーキテクチャ検出のデバッグ

1. GRUB 2設定にデバッグ出力を追加して、検出された値を確認します。

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

2. 設定構文をテストします。

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

3. アーキテクチャのマッピングが不完全な場合は、検出ロジックを拡張します。

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

4. アーキテクチャ固有のディレクトリが存在することを確認します。

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

6.7.2 ネットワークインタフェースが見つからない

ファームウェアの実装によっては、`${net_default_mac}`変数が正しく設定されず、ネットワーク設定に失敗することがあります。

手順 12: ネットワークインタフェースの問題の診断

1. ネットワーク変数をチェックするためのデバッグ出力を追加します。

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

2. フォールバックネットワーク設定を作成します。

```
> sudocat >> /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. 特定のインタフェースでネットワーク設定をテストします。

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

4. ターゲットシステムのネットワークインタフェース名を確認します。

```
> ip link show
```

6.7.3 ファイルパスが見つからない

ファイルパスが正しくないと、GRUB 2がカーネルファイルとinitrdファイルをロードできず、ブートに失敗します。

手順 13: ファイルパスのアクセシビリティの確認

1. インストーラファイルが想定される場所に存在するかどうかを確認します。

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

2. ブートファイルへのTFTPアクセスを確認します。

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

3. インストーラファイルへのHTTPアクセスをテストします。

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

4. ファイルアクセス権と所有権を確認します。

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

5. 必要に応じて権限を修正します。

```
> sudochmod -R 644 /srv/tftpboot/boot/images/
```

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

6. シンボリックリンクが壊れていないことを確認します。

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

6.7.4 EFIブートの失敗

EFIおよびセキュアブートの問題により、ブートローダが正しく初期化されなかったり、認証に失敗したりすることがあります。

手順 14: EFIブートの問題の診断

1. セキュアブートファイルが存在することを確認します。

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

2. shim (bootx64.efiまたはshim.efi)、grub.efi、MokManager.efiファイルが正しくコピーされていることを確認します。

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

3. EFIファイルの整合性を確認します。

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

4. ファイルがTFTP経由でアクセス可能かどうかをテストします。

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

5. aarch64システムの場合、ARM64 EFIファイルを確認します。

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

6. DHCP設定で正しいブートローダのパスが提供されていることを確認します。

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

7. ファイルがない場合は、/mntにマウントされたISOまたはshimパッケージファイルから再度コピーします。

```
> sudocp -v /mnt/EFI/BOOT/*.efi /srv/tftpboot/boot/grub2/x86_64-efi/
```

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

6.7.5 メニューエントリがロードされない

GRUB 2がロードされたが、メニューエントリが失敗したり、エラーが表示されたりする場合、問題は変数展開やファイル参照に関連していることが多いです。

手順 15: メニューエントリに関する問題のデバッグ

1. メニュー設定構文をテストします。

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

2. メニューエントリにデバッグ出力を追加します。

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

3. 変数展開が正しく機能していることを確認します。

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

4. 簡略化したメニューエントリでテストします。

```
> sudocat > /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. テストメニューを一時的にロードします。

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

6. テスト後、元のメニューを復元します。

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

6.7.6 詳細ログの有効化

永続的な問題については、包括的なログを有効にして、ブートプロセスに関する詳細な情報を取得します。

手順 16: GRUB 2のデバッグログの設定

1. メイン設定のデバッグバージョンを作成します。

```
> sudocp /srv/tftpboot/boot/grub2/grub.cfg /srv/tftpboot/boot/grub2/grub.cfg.backup
```

2. 包括的なデバッグ出力を追加します。

```
> sudocat > /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. デバッグ設定をメインファイルに含めます。

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

4. ブート試行中のTFTPログを監視します。

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

5. DHCPログでPXE要求を監視します。

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

6. トラブルシューティングの後、デバッグモードを無効にします。

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

6.8 次のステップ

GRUB 2を適切に設定したら、以下の手順に進むことができます。

- ブートファイルとインストーラコンテンツを提供するためのHTTPとTFTPサービスの設定
- PXEクライアントを適切なブートローダに誘導するためのDHCPサービスの設定
- ターゲットハードウェア上での完全なPXEブートプロセスのテスト

柔軟なGRUB 2設定システムは、洗練されたPXE展開シナリオの基盤を提供し、統一されたインタフェースを通じて複数のアーキテクチャとインストールタイプをサポートします。

7 PXEブート用TFTPの設定

このセクションでは、SUSE Linux Enterprise Server 16.0インストール向けにGRUB 2ブートローダとPXEブートコンテンツを提供するようにTFTPサービスを設定する方法を説明します。従来の`in.tftpd`サーバと、`dnsmasq`が提供する統合TFTP機能について説明します。

7.1 概要

TFTPは、ネットワークブートプロセス中にPXEクライアントにブートローダファイルを提供します。SUSE Linux Enterprise Server 16.0は、`tftp`パッケージに含まれる従来の`in.tftpd`サーバと、`dnsmasq`に統合されたTFTP機能の2つのTFTPサーバ実装をサポートしています。

7.2 要件

- インストール済みの`tftp`パッケージまたは`dnsmasq`パッケージのいずれか
- `/srv/tftpboot`下に整理されたPXEブートファイル
- サービスを設定するための管理者特権

7.3 in.tftpdサーバの設定

`in.tftpd`サーバは、設定ファイル`/etc/sysconfig/tftp`を使用して、TFTPルートディレクトリおよびサーバオプションを定義します。

手順 17: IN.TFTPD TFTPサーバの設定

1. オプションで、TFTPオプションを設定して詳細ログを有効にします。

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

   `-v`オプションを使用すると、TFTP経由で取得されたファイル名を確認するための詳細ログが有効になります。

2. TFTPサービスを有効にして開始します。

   ```
   > sudosystemctl enable --now tftp.service
   ```

7.4 dnsmasq TFTPサーバの設定

`dnsmasq`は、`/srv/tftpboot`ディレクトリを使用するように有効化および設定できる、組み込みのTFTPサーバを提供します。

手順 18: DNSMASQ TFTP機能の設定

1. TFTP設定ファイルを作成します。

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

2. dnsmasqサービスを有効にして開始します。

   ```
   > sudosystemctl enable --now dnsmasq
   ```

7.5 TFTP設定の検証

TFTPサーバの機能をテストし、PXEクライアントにファイルを提供できることを確認します。

手順 19: TFTPサーバ機能のテスト

1. テストファイルを作成します。

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

2. TFTP経由でテストファイルを取得します。

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

3. ファイルが正常に取得されたことを確認します。

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

4. テストファイルをクリーンアップします。

```
> sudorm /srv/tftpboot/test.txt /tmp/tftp-test.txt
```

7.6 TFTP設定のトラブルシューティング

PXEブート環境でTFTPサービスを設定する際によくある問題。

7.6.1 ポート69でのサービスの競合

`in.tftpd`と`dnsmasq`の両方がTFTPサービスにUDPポート69を使用するため、同時に実行できません。

手順 20: TFTPサービスの競合の解決

1. 実行中のサービスを確認します。

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

2. ポート69を使用しているサービスを確認します。

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

3. 競合するサービスを停止します(dnsmasqの例)。

```
> sudosystemctl stop dnsmasq
```

4. 優先するTFTPサービスを開始します。

```
> sudosystemctl start tftp.service
```

7.6.2 TFTPディレクトリの問題

TFTPルートディレクトリへのアクセスに問題があると、ファイル提供が妨げられることがあります。

手順 21: TFTPディレクトリ設定の確認

1. in.tftpdのTFTPディレクトリ設定を確認します。

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

2. dnsmasqのTFTPディレクトリ設定を確認します。

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

3. ディレクトリが存在するかどうかを確認します。

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

4. ディレクトリが存在しない場合は、ディレクトリを作成します。

```
> sudomkdir -p /srv/tftpboot
```

7.6.3 TFTPログの有効化

詳細ログは、TFTP転送でのファイルアクセスの問題を特定するのに役立ちます。

手順 22: TFTP詳細ログの有効化

1. 現在のTFTPオプションを確認します。

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

2. 詳細ログを有効にします。

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

3. TFTPサービスを再起動します。

```
> sudosystemctl restart tftp.service
```

4. TFTPログを監視します。

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

7.7 次のステップ

TFTPを設定したら、インストーラファイルを提供するHTTPサービスと、PXEクライアントを適切なブートローダに誘導するためのDHCPサービスの設定に進むことができます。

8 HTTP配信用のnginxの設定

このセクションでは、PXEブートコンテンツをHTTP経由で提供するようにnginxを設定して、クライアントがカーネル、initrd、squashfsイメージなどのインストーラファイルを中央の場所からロードできるようにする方法を説明します。HTTP配信は、大きなファイルの場合に、TFTPよりも優れたパフォーマンスを提供し、SUSE Linux Enterprise Server 16.0 Agamaのインストールに必要です。

8.1 概要

nginxはPXEブート環境のHTTPサーバとして機能し、Webベースの配信を通じてインストーラファイルへのアクセスを提供します。HTTPサーバはTFTPブートディレクトリとインストールリポジトリを公開し、PXEクライアントがカーネルイメージ、initrdファイル、Agamaインストーラコンポーネントを低速のTFTPプロトコルではなくHTTP経由でダウンロードできるようにします。

8.2 要件

- インストール済みの`nginx`パッケージ
- `/srv/tftpboot/boot`下に整理されたPXEブートファイル
- `/srv/install`で利用可能なインストールリポジトリ
- nginxの設定を変更するための管理者特権

8.3 PXEブート用のnginxの設定

nginx設定は、HTTP URL経由で TFTPブートディレクトリとインストールリポジトリを公開するロケーションエイリアスを定義します。

手順 23: NGINX HTTPサーバの設定

1. nginx設定ファイルを編集します。

```
> sudovim /etc/nginx/nginx.conf
```

2. httpセクションで、HTTPサーバブロックを設定します。

```
> sudocat > /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. nginx設定構文をテストします。

```
> sudonginx -t
```

4. nginxサービスを有効にして開始します。

```
> sudosystemctl enable --now nginx.service
```

8.4 nginxx設定の検証

HTTPサーバの機能をテストし、PXEブートファイルとインストールコンテンツをクライアントに提供できることを確認します。

手順 24: NGINX HTTPサーバのテスト

1. ブートファイルへのHTTPアクセスをテストします。

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

2. インストールディレクトリへのアクセスをテストします。

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

3. 特定のインストーラファイルにアクセスできることを確認します。

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

8.5 nginx設定のトラブルシューティング

PXEブートHTTP配信用にnginxを設定する際によくある問題。

8.5.1 設定構文エラー

nginxの設定構文が正しくないため、サービスが正しく開始または再ロードされません。

手順 25: NGINX設定問題の解決

1. 設定構文をテストします。

```
> sudonginx -t
```

2. 起動に失敗した場合は、nginxサービスのステータスを確認します。

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

3. 詳細なエラーログを表示します。

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

4. nginxのエラーログファイルを確認します。

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

8.5.2 ファイルアクセスと権限の問題

nginxは権限が正しくないか、ディレクトリが見つからないためにファイルの提供に失敗することがあります。

手順 26: ファイルアクセスの問題の解決

1. ブートディレクトリが存在し、アクセス可能かどうかを確認します。

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

2. インストールディレクトリが存在するかどうかを確認します。

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

3. nginxがディレクトリを読み込めることを確認します。

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

4. 必要であれば、不足しているディレクトリを作成します。

```
> sudomkdir -p /srv/install
```

5. 適切な権限を設定します。

```
> sudochmod -R 755 /srv/tftpboot/boot /srv/install
```

8.5.3 ポートバインディングの競合

他のサービスがポート80を使用している場合、nginxの起動に失敗することがあります。

手順 27: ポートの競合の解決

1. ポート80を使用しているサービスを確認します。

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

2. 必要であれば、競合するサービスを停止します。

```
> sudosystemctl stop apache2
```

3. nginxサービスを開始します。

```
> sudosystemctl start nginx.service
```

4. nginxがポート80でリスンしていることを確認します。

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

8.6 次のステップ

nginxをHTTP配信用に設定したら、PXEクライアントを適切なブートローダとHTTPリソースに誘導するためのDHCP サービスの設定に進むことができます。

9 dnsmasqを使用したDNSサーバの設定

このセクションでは、SUSE Linux Enterprise Server 16.0インストールリソースにアクセスするPXEクライアントにホスト名解決を提供するために、dnsmasqを使用してDNSサービスを設定する方法を説明します。DNS設定により、クライアントはブートURLやDHCP設定でIPアドレスの代わりにホスト名を使用できるようになります。

9.1 概要

DNSサービスにより、PXEクライアントはブートURLやインストールソース内のホスト名を解決できます。DNSサーバの完全な設定はこのドキュメントの範囲外ですが、このセクションでは、クライアントがPXEサーバのホスト名(`PXE.EXAMPLE.NET`)をIPアドレスに解決できるようにする、dnsmasqを使用した基本的なDNS設定について説明します。

DNS設定がない場合、ブートURLは`http://192.168.1.200/`や`http://[2001:db8:0:1::200]/`のようなIPアドレスを直接使用する必要があります。BIOS/UEFIファームウェアの実装によっては、DHCP TFTP URLのホスト名をサポートしておらず、`tftp://[2001:db8:0:1::200]/`のようなIPアドレスを必要とするものもあります。

9.2 要件

- インストール済みの`dnsmasq`パッケージ
- PXEサーバ用に設定された静的IPアドレス
- DNSサービスを設定するための管理者特権

9.3 dnsmasq DNSサービスの設定

dnsmasq DNS設定はローカルホストの名前解決を提供し、外部クエリにはアップストリームネームサーバを使用します。

手順 28: DNSMASQ DNSサーバの設定

1. dnsmasq用のDNS設定ファイルを作成します。

```
> sudocat > /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. システムのhostsファイルにホスト名のエントリを追加します。

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

3. dnsmasqの設定をテストします。

```
> sudodnsmasq --test
```

4. dnsmasqサービスを有効にして開始します。

```
> sudosystemctl enable --now dnsmasq
```

注記: DNS転送の動作

デフォルトでは、dnsmasqは`/etc/resolv.conf`のネームサーバをフォワーダとして使用し、`/etc/hosts`からレコードを提供します。これにより、PXEサーバは、外部ホスト名を解決しながら、PXE関連サービスにローカル解決を提供できます。

9.4 DNS設定の検証

DNSサーバの機能をテストし、PXEクライアントのホスト名解決が機能することを確認します。

手順 29: DNSサーバ機能のテスト

1. IPv4ホスト名解決をテストします。

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

2. IPv6ホスト名解決をテストします。

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

3. IPv4のDNS逆引きをテストします。

```
> nslookup 192.168.1.200 localhost
```

4. 外部DNS転送がまだ機能していることを確認します。

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

9.5 DNS設定のトラブルシューティング

PXE環境でDNSサービス用にdnsmasqを設定する際によくある問題。

9.5.1 設定とサービスの問題

dnsmasqは、設定エラーやポートの競合が原因で起動に失敗することがあります。

手順 30: DNS設定の問題の解決

1. dnsmasq設定構文をテストします。

```
> sudodnsmasq --test
```

2. dnsmasqサービスの状態を確認します。

```
> systemctl status dnsmasq
```

3. DNSポート53を使用しているサービスを確認します。

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

4. dnsmasqのログでエラーを確認します。

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

5. 必要であれば、競合するDNSサービスを停止します。

```
> sudosystemctl stop systemd-resolved
```

9.5.2 ホスト名解決の失敗

DNSクエリは、誤った設定やホスト名エントリの欠落が原因で失敗することがあります。

手順 31: DNS解決の問題の診断

1. hostsファイルにホスト名のエントリが存在するかどうかを確認します。

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

2. dnsmasqでドメイン設定を確認します。

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

3. 詳細出力でDNSクエリをテストします。

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

4. dnsmasqのクエリログを監視します。

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

5. dnsmasqを再起動して設定を再ロードします。

```
> sudosystemctl restart dnsmasq
```

9.5.3 DNS転送の問題

アップストリームネームサーバの設定が正しくない場合、外部DNSクエリが失敗することがあります。

手順 32: DNS転送に関する問題のトラブルシューティング

1. アップストリームネームサーバの設定を確認します。

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

2. アップストリームネームサーバへの直接クエリをテストします。

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

3. dnsmasqの転送設定を確認します。

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

4. 必要に応じて、特定のアップストリームネームサーバを追加します。

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

5. dnsmasqサービスを再起動します。

```
> sudosystemctl restart dnsmasq
```

9.6 次のステップ

DNSサービスが設定されたので、PXEクライアントはブートURLやインストールソース内のホスト名を解決できるようになりました。クライアント設定のためにDNSサーバを参照するDHCPサービスの設定に進むことができます。

10 chronyを使用したNTPサーバの設定

このセクションでは、 SUSE Linux Enterprise Server 16.0のインストール中にPXEクライアントに正確な時刻同期を提供するために、chronyを使用してNTPサービスを設定する方法を説明します。適切な時刻同期は、ネットワークベースのインストール時の証明書の検証とシステムログに不可欠です。

10.1 概要

NTPサービスは、ネットワークインフラストラクチャ全体の正確な時刻同期を保証します。PXEブート環境では、HTTPS接続時の証明書の検証、適切なログのタイムスタンプ、および調整されたシステム操作のために、時刻の同期は極めて重要です。このセクションでは、chronyを使用した基本的なNTPサーバの設定について説明します。

10.2 要件

- インストール済みのchronyパッケージ

```
> sudozypper install chrony
```

- アップストリームNTPサーバへのネットワーク接続
- NTPサービスを設定するための管理者特権

10.3 chrony NTPサービスの設定

chronyサービスは、アップストリームサーバへの自動時刻同期と、ネットワーククライアントへのローカル時刻提供機能を備えたNTP機能を提供します。

手順 33: chrony NTPサーバの設定

- chronyサービスを有効にして開始します。

```
> sudosystemctl enable --now chronyd.service
```

10.4 NTP設定の検証

NTPサービスの機能をテストし、時刻同期が正しく機能することを確認します。

手順 34: NTPサーバ機能のテスト

1. chronyサービスの状態を確認します。

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

2. 現在の時刻同期ステータスを表示します。

```
> chronyc tracking
```

3. 設定されたNTPソースを一覧表示します。

```
> chronyc sources
```

4. NTPサーバ統計情報を確認します。

```
> chronyc sourcestats
```

10.5 NTP設定のトラブルシューティング

PXE環境でNTPサービス用にchronyを設定する際によくある問題。

10.5.1 サービスの起動の問題

chronyサービスが設定エラーやネットワーク接続の問題により起動できないことがあります。

手順 35: NTPサービスの問題の解決

1. chronyサービスの状態とログを確認します。

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

2. 詳細なサービスログを表示します。

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

3. chrony設定をテストします。

```
> sudochronyd -Q
```

4. 必要に応じてサービスを再起動します。

```
> sudosystemctl restart chronyd.service
```

10.5.2 時刻同期の失敗

ネットワークの問題やサーバの設定が正しくないために、時刻同期に失敗することがあります。

手順 36: 時刻同期の問題の診断

1. 現在の時刻同期ステータスを確認します。

```
> chronyc tracking
```

2. NTPソースの接続性を表示します。

```
> chronyc sources -v
```

3. 即時同期を強制実行します。

```
> sudochronyc makestep
```

4. システムの時刻をハードウェアクロックと照合します。

```
> timedatectl status
```

5. NTPサーバへのネットワーク接続を確認します。

```
> chronyc activity
```

10.5.3 ファイアウォールとネットワークの問題

NTPトラフィックがファイアウォールルールによってブロックされ、時刻同期が妨げられることがあります。

手順 37: NTPネットワーク接続の解決

1. ファイアウォールでNTPポートが開いているか確認します。

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

2. 必要に応じてNTPサービスをファイアウォールに追加します。

```
> sudofirewall-cmd --permanent --add-service=ntp
```

3. ファイアウォール設定を再ロードします。

```
> sudofirewall-cmd --reload
```

4. NTP接続を手動でテストします。

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

5. chronyポートの使用状況を確認します。

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

10.6 次のステップ

NTPサービスが設定されたら、PXEサーバとクライアントは正確な時刻同期を維持します。これにより、ネットワークベースのインストール時に、適切な証明書の検証および調整されたシステム運用が確保されます。

11 IPv6ルータ広告の設定

このセクションでは、PXEクライアントに適切なルータ広告を提供するために、IPv6ルータ広告機能を設定する方法について説明します。IPv6 RAは、SUSE Linux Enterprise Server 16.0インストールにおいて、IPv6ルーティング設定とステートフルDHCPv6アドレスの自動設定を可能にします。

11.1 概要

IPv6ルータ広告(RA)は、IPv6ルーティングやDHCPv6アドレス自動設定など、PXEクライアントに不可欠なネットワーク設定情報を提供します。このセクションでは、IPv6ルータが、ネットワークとデフォルトルートへのIPv6ルーティングを設定するための適切なルータ広告を提供し、`AdvManagedFlag on`を使用してステートフルDHCPv6アドレス自動設定を有効にするように設定されていることを前提としています。

11.2 要件

- インストール済みの`radvd`パッケージ
- サーバインタフェースのIPv6ネットワーク設定
- ルータ広告サービスを設定するための管理者特権

11.3 IPv6ルータ広告のためのradvdの設定

radvdサービスは、/etc/radvd.confで定義された設定を使用してIPv6ルータ広告機能を提供します。

手順 38: radvd IPV6ルータ広告の設定

1. radvdサービスを設定します。

```
> sudocat > /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. radvdサービスを有効にして開始します。

```
> sudosystemctl enable --now radvd
```

11.4 IPv6ルータ広告の確認

IPv6 RAの機能をテストし、適切な設定と動作を確認します。

手順 39: IPV6ルータ広告のテスト

1. radvdサービスの状態を確認します。

```
> systemctl status radvd
```

2. **ravdump**を使用してIPv6 RA設定を確認します。

```
> radvdump
```

radvdumpユーティリティは、数分ごとにIPv6ルータから送信されるIPv6 RA設定を表示します。

11.5 ルータ機能のためのIP転送の設定

PXEサーバがルータとしても機能する場合は、システムがルータの役割で機能できるように、IP転送を有効にする必要があります。

手順 40: PXEサーバでIP転送を有効にする

1. ネットワーク設定ファイルを作成します。

```
> sudocat > /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. ネットワーク設定を適用します。

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

注記: ルータ設定に関する考慮事項

ルータはデフォルトで、ホスト自動設定のためのIPv6 RAを処理しません。ルータのアップリンクインタフェースでIPv6 RAを受け入れるには、`accept_ra = 2` sysctl設定が必要です。ファイアウォールの調整やその他の必要な手順など、ルータ設定の詳細については、『管理ガイド』の「ネットワーク設定」セクションを参照してください。

11.6 IPv6ルータ広告のトラブルシューティング

PXE環境でIPv6ルータ広告を設定する際によくある問題。

11.6.1 radvdサービスの問題

設定エラーやインタフェースの問題により、radvdサービスが開始できないことがあります。

手順 41: radvdサービスの問題の解決

1. radvdサービスの状態とログを確認します。

```
> systemctl status radvd
```

2. 詳細なサービスログを表示します。

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

3. radvd設定の構文をテストします。

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

4. 指定されたインタフェースが存在するかどうかを確認します。

```
> ip link show eno1
```

5. 設定を修正した後、サービスを再起動します。

```
> sudosystemctl restart radvd
```

11.6.2 IP転送設定の問題

IP転送設定が正しくないと、ルータが正しく機能しなくなることがあります。

手順 42: IP転送の問題の診断

1. 現在のIP転送ステータスを確認します。

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

2. IPv6の転送ステータスを確認します。

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

3. sysctl設定ファイルを確認します。

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

4. 値が正しくない場合は設定を適用します。

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

5. アップリンクインタフェースのaccept_ra設定を確認します。

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

11.6.3 ルータ広告の受信に関する問題

クライアントがIPv6ルータ広告を正しく受信または処理できない場合があります。

手順 43: RA受信に関する問題のトラブルシューティング

1. **ravdump**を使用してルータ広告を監視します。

```
> radvdump -d
```

2. クライアントのIPv6インタフェースの設定を確認します。

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

3. クライアントのIPv6ルーティングテーブルを確認します。

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

4. ルータへのIPv6接続をテストします。

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

5. ICMPv6のファイアウォールルールを確認します。

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

11.7 次のステップ

IPv6ルータ広告が設定されると、PXEクライアントは適切なIPv6ネットワーク設定を受け取ることができます。これにより、ネットワークベースのインストールでDHCPv6機能とIPv6接続が有効になります。

12 dnsmasqを使用したDHCPサーバの設定

このセクションでは、SUSE Linux Enterprise Server 16.0インストールにネットワーク設定とPXEブート情報を提供するために、dnsmasqを使用してDHCPサービスを設定する方法を説明します。dnsmasq DHCPサーバは、タグベースの設定を使用して、UEFIとBIOSブート機能を持つIPv4とIPv6の両方のPXEクライアントをサポートします。

12.1 概要

dnsmasq DHCPサーバは、タグベースのシステムを使用してPXEクライアントにネットワーク設定とブートファイル情報を提供し、クライアントのタイプを照合し、適切なブートローダを提供します。この設定は、DHCPv4とDHCPv6で動作するPXEClientとHTTPClientの両方の一致をサポートし、複数のアーキテクチャにわたるUEFIとBIOSシステム経由でのブートを可能にします。

重要: dnsmasqにおけるHTTPClientの制限事項

dnsmasqバージョン2.90以前では、HTTPClient設定のDHCPv6クライアントへのvendor-class option6:16の返送をサポートしていません。HTTPClientを完全にサポートするには、KeaまたはISC DHCPサーバの使用を検討してください。

12.2 要件

- インストール済みの`dnsmasq`パッケージ
- `/srv/tftpboot`下に適切に整理されたPXEブートファイル
- DHCPサービス用に設定されたネットワークインタフェース
- DHCPサービスを設定するための管理者特権

12.3 dnsmasq DHCPサービスの設定

dnsmasq DHCP設定には、IPv4とIPv6の両方のネットワークに対するクライアントタイプの一致、ネットワーク範囲、ブートファイルの割り当てが含まれます。

手順 44: DNSMASQ DHCPサーバの設定

1. dnsmasq用のDHCP設定ファイルを作成します。

```
> sudocat > /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. IPv4 DHCPの範囲とオプションを設定します。

```
> sudocat >> /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. IPv4 PXEブートオプションを設定します。

```
> sudocat >> /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. IPv6 DHCPの範囲とオプションを設定します。

```
> sudocat >> /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. IPv6 PXEブートオプションを設定します。

```
> sudocat >> /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. dnsmasqの設定をテストします。

```
> sudodnsmasq --test
```

7. dnsmasqサービスを有効にして開始します。

```
> sudosystemctl enable --now dnsmasq
```

12.4 DHCP設定の検証

DHCPサーバの機能をテストし、適切なネットワーク設定とPXEクライアントへのブートファイル配信を確認します。

手順 45: DNSMASQ DHCPサーバのテスト

1. dnsmasqサービスの状態を確認します。

```
> systemctl status dnsmasq
```

2. DHCPポートバインディングを確認します。

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

3. DHCPリースの割り当てを監視します。

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

4. アクティブなDHCPリースを確認します。

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

12.5 dnsmasq DHCP設定のトラブルシューティング

PXE環境でDHCPサービス用にdnsmasqを設定する際によくある問題。

12.5.1 サービスの起動と設定に関する問題

dnsmasqは、設定エラーや他のDHCPサービスとのポートの競合が原因で起動に失敗することがあります。

手順 46: DNSMASQ DHCPサービスの問題の解決

1. dnsmasq設定構文をテストします。

```
> sudodnsmasq --test
```

2. DHCPポートの競合を確認します。

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

3. 競合するDHCPサービスを停止します。

```
> sudosystemctl stop dhcpd
```

4. 詳細なサービスログを表示します。

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

5. 競合の解決後にdnsmasqを再起動します。

```
> sudosystemctl restart dnsmasq
```

12.5.2 DHCPリース割り当ての問題

クライアントは、範囲設定やネットワーク接続の問題により、IPアドレスを受信できないことがあります。

手順 47: DHCPリースの問題の診断

1. DHCP範囲設定を確認します。

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

2. DHCP要求をリアルタイムで監視します。

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

3. ネットワークインタフェースのステータスを確認します。

```
> ip addr show
```

4. DHCP権限設定を確認します。

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

5. dhcpingでDHCP応答をテストします。

```
> dhcping -s 192.168.1.200
```

12.5.3 PXEブートファイルの配信に関する問題

PXEクライアントは、ブートファイルの設定が正しくないか、クライアントタイプの一致に問題があるため、IPアドレスを受信できてもブートに失敗することがあります。

手順 48: PXEブート設定のトラブルシューティング

1. クライアントのベンダクラスの一致を確認します。

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

2. ブートファイルのパスを確認します。

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

3. ブートファイルへのTFTPアクセスをテストします。

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

4. PXE固有のDHCPログを監視します。

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

5. ログでタグの割り当てを確認します。

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

12.5.4 IPv6 DHCP設定の問題

IPv6 DHCPクライアントは適切なルータ広告設定を必要とし、IPv4とは異なるアドレス指定要件がある場合があります。

手順 49: IPV6 DHCPの問題の解決

1. IPv6 DHCP範囲設定を確認します。

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

2. IPv6ルータ広告ステータスを確認します。

```
> systemctl status radvd
```

3. DHCPv6要求を監視します。

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

4. IPv6接続をテストします。

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

5. IPv6オプションの設定を確認します。

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

12.6 次のステップ

dnsmasq DHCPサービスを設定すると、PXEクライアントはIPv4とIPv6の両方の環境のネットワーク設定とブートファイル情報を受信できます。タグベースのシステムは、クライアントのアーキテクチャとブート方法の要件に基づき、柔軟なブートファイル割り当てを提供します。

13 Keaを使用したDHCPサーバの設定

このセクションでは、SUSE Linux Enterprise Server 16.0インストールにネットワーク設定とPXEブート情報を提供するために、Keaを使用してDHCPサービスを設定する方法を説明します。Keaは、PXEおよびHTTPブートシナリオにおいて、クライアントクラス一致機能を備え、IPv4とIPv6の両方をサポートする最新のDHCPサーバです。

13.1 概要

Keaは、レガシISC DHCPサーバの後継としてISCが開発した最新のDHCPサーバです。クライアントのアーキテクチャとブート方法に基づいて適切なブートファイルの配信を可能にするクライアント分類機能を備え、DHCPv4とDHCPv6の両方を堅牢にサポートします。KeaはJSONベースの設定ファイルを使用し、HTTPブートのベンダクラス識別のような高度な機能をサポートしています。

13.2 要件

- インストールされたKea DHCPパッケージ(`kea-dhcp4`と `kea-dhcp6`)
- `/srv/tftpboot`下に適切に整理されたPXEブートファイル
- DHCPサービス用に設定されたネットワークインタフェース
- DHCPサービスを設定するための管理者特権

13.3 Kea DHCPv4サーバの設定

Kea DHCPv4設定は、クライアントクラスを使用してPXEとHTTPクライアントのタイプを照合し、さまざまなアーキテクチャに適したブートファイルを提供します。

手順 50: KEA DHCPV4サーバの設定

1. Kea DHCPv4サーバを設定します。

```
> sudocat > /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. Keaログディレクトリを作成します。

```
> sudomkdir -p /var/log/kea
```

3. Kea DHCPv4設定をテストします。

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

4. Kea DHCPv4サービスを有効にして開始します。

```
> sudosystemctl enable --now kea-dhcp4
```

13.4 Kea DHCPv6サーバの設定

Kea DHCPv6設定は、異なるクライアントアーキテクチャのベンダクラスの一致を使用して、IPv6アドレス割り当てと、ブートファイル情報を提供します。

手順 51: KEA DHCPV6サーバの設定

1. Kea DHCPv6サーバを設定します。

```
> sudocat > /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. Kea DHCPv6設定をテストします。

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

3. Kea DHCPv6サービスを有効にして開始します。

```
> sudosystemctl enable --now kea-dhcp6
```

13.5 Kea DHCP設定の検証

Kea DHCPサーバの機能をテストし、適切なネットワーク設定とPXEクライアントへのブートファイル配信を確認します。

手順 52: KEA DHCPサーバのテスト

1. Kea DHCPv4サービスの状態を確認します。

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

2. Kea DHCPv6サービスの状態を確認します。

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

3. DHCPポートバインディングを確認します。

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

4. DHCPv4のログを監視します。

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

5. DHCPv6のログを監視します。

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

6. アクティブなDHCPリースを確認します。

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

13.6 Kea DHCP設定のトラブルシューティング

PXEブート環境でKea DHCPサーバを設定する際によくある問題。

13.6.1 設定とサービスの問題

JSON設定エラーやネットワークインタフェースの問題により、Keaサービスが開始できないことがあります。

手順 53: KEA設定問題の解決

1. DHCPv4設定構文をテストします。

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

2. DHCPv6設定構文をテストします。

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

3. JSONの構文エラーを確認します。

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

4. ネットワークインタフェースの設定を確認します。

```
> ip addr show eno1
```

5. Keaサービスログを確認します。

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

13.6.2 DHCPリース割り当ての問題

クライアントは、サブネット設定やプール枯渇の問題により、IPアドレスを受信できないことがあります。

手順 54: KEAリースの問題の診断

1. サブネットとプールの設定を確認します。

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

2. リースの割り当てをリアルタイムで監視します。

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

3. リースデータベースの競合を確認します。

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

4. インタフェースバインディングを確認します。

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

5. 必要に応じてリースデータベースをクリアします。

```
> sudosystemctl stop kea-dhcp4
```

```
> sudomv /var/lib/kea/dhcp4.leases /var/lib/kea/dhcp4.leases.backup
```

```
> sudosystemctl start kea-dhcp4
```

13.6.3 PXEクライアントクラスの一致の問題

PXEクライアントは、クライアントクラスの設定の問題により、IPアドレスを受信できても正しいブートファイルを取得できないことがあります。

手順 55: KEAクライアント分類のトラブルシューティング

1. クライアントクラスの定義を確認します。

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

2. クライアントクラスの一致をログで監視します。

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

3. ベンダクラス識別子のパターンを確認します。

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

4. ブートファイルのアクセシビリティをテストします。

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

5. 詳細なクライアント分析のためにデバッグログを有効にします。

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

```
> sudosystemctl restart kea-dhcp4
```

13.6.4 DHCPv6固有の問題

IPv6 DHCPクライアントは適切なルータ広告設定を必要とし、IPv4とは異なるベンダクラスオプション処理を行います。

手順 56: KEA DHCPV6の問題の解決

1. DHCPv6サブネット設定を確認します。

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

2. IPv6ルータ広告ステータスを確認します。

```
> systemctl status radvd
```

3. DHCPv6ベンダクラスの一致を監視します。

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

4. IPv6 bootfile-urlオプションの形式を確認します。

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

5. ブートサーバへのIPv6接続をテストします。

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

13.7 次のステップ

Kea DHCPサービスを設定すると、PXEクライアントはIPv4とIPv6の両方の環境の包括的なネットワーク設定とブートファイル情報を受信できます。クライアント分類システムは、クライアントアーキテクチャに基づいた正確なブートファイル割り当てを提供し、従来のPXEブート方法と最新のHTTPブート方法の両方をサポートします。

14 ISC DHCPを使用したDHCPサーバの設定

このセクションでは、SUSE Linux Enterprise Server 15インストールにネットワーク設定とPXEブート情報を提供するために、ISC DHCPサーバを設定する方法を説明します。ISC dhcp-serverパッケージは、SUSE Linux Enterprise Server 16.0では利用できなくなりました。ISC DHCPはクラスとサブクラスの一致を使用して、異なるクライアントアーキテクチャのPXEとHTTPブートシナリオをサポートします。

14.1 概要

ISC DHCPは、従来のDHCPサーバで、クラスとサブクラスのシステムを使用して、PXEクライアントにネットワーク設定とブートファイル情報を提供します。ISCは2022年時点でこのサーバのサービス終了を宣言していますが、既存の展開では依然として広く使用されており、ベンダクラス識別によるPXEおよびHTTPブートシナリオに対する堅牢なサポートを提供しています。

重要: ISC DHCPサービス終了ステータス

ISC DHCPは、ISCによって2022年にサービス終了が宣言されています。新規展開の場合は、代わりにKeaまたはdnsmasqの使用を検討してください。この設定は、既存のISC DHCPインストール環境との互換性のために提供されています。

14.2 要件

- インストールされたISC DHCPパッケージ(`dhcp-server`)
- `/srv/tftpboot`下に適切に整理されたPXEブートファイル
- DHCPサービス用に設定されたネットワークインタフェース
- DHCPサービスを設定するための管理者特権

14.3 ISC DHCPv4サーバの設定

ISC DHCPv4設定は、クラスとサブクラス宣言を使用してPXEとHTTPクライアントのタイプを照合し、さまざまなアーキテクチャに適したブートファイルを提供します。

手順 57: ISC DHCPV4サーバの設定

1. ISC DHCPv4サーバを設定します。

```
> sudocat > /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. sysconfigでDHCPインタフェースを設定します。

```
> sudoecho 'DHCPD_INTERFACE="eno1"' > /etc/sysconfig/dhcpd
```

3. DHCPv4設定をテストします。

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

4. ISC DHCPv4サービスを有効にして開始します。

```
> sudosystemctl enable --now dhcpd
```

14.4 ISC DHCPv6サーバの設定

ISC DHCPv6設定は、ベンダクラスの一致と適切なDHCPv6オプション処理を使用して、IPv6アドレス割り当てと、ブートファイル情報を提供します。

手順 58: ISC DHCPV6サーバの設定

1. ISC DHCPv6サーバを設定します。

```
> sudocat > /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. sysconfigでDHCPv6インタフェースを設定します。

```
> sudoecho 'DHCPD6_INTERFACE="eno1"' >> /etc/sysconfig/dhcpd
```

3. DHCPv6設定をテストします。

```
> sudodhcpd -6 -t -cf /etc/dhcpd6.conf
```

4. ISC DHCPv6サービスを有効にして開始します。

```
> sudosystemctl enable --now dhcpd6
```

14.5 ISC DHCP設定の検証

ISC DHCPサーバの機能をテストし、適切なネットワーク設定とPXEクライアントへのブートファイル配信を確認します。

手順 59: ISC DHCPサーバのテスト

1. ISC DHCPv4サービスの状態を確認します。

```
> systemctl status dhcpd
```

2. ISC DHCPv6サービスの状態を確認します。

```
> systemctl status dhcpd6
```

3. DHCPポートバインディングを確認します。

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

4. DHCPログを監視します。

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

5. アクティブなDHCPリースを確認します。

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

6. DHCPv6アクティビティを監視します。

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

14.6 ISC DHCP設定のトラブルシューティング

PXEブート環境でISC DHCPサーバを設定する際によくある問題。

14.6.1 設定とサービスの問題

設定構文エラーやインタフェースバインディングの問題により、ISC DHCPサービスが開始できないことがあります。

手順 60: ISC DHCP設定問題の解決

1. DHCPv4設定構文をテストします。

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

2. DHCPv6設定構文をテストします。

```
> sudodhcpd -6 -t -cf /etc/dhcpd6.conf
```

3. インタフェースの設定を確認します。

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

4. ネットワークインタフェースのステータスを確認します。

```
> ip addr show eno1
```

5. ポートの競合を確認します。

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

6. 詳細なサービスログを表示します。

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

14.6.2 DHCPリース割り当ての問題

クライアントは、サブネット設定や認証の問題により、IPアドレスを受信できないことがあります。

手順 61: ISC DHCPリースの問題の診断

1. サブネットと範囲の設定を確認します。

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

2. 権限設定を確認します。

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

3. リースの割り当てをリアルタイムで監視します。

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

4. リースデータベースにエラーがないか確認します。

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

5. DHCP応答を手動でテストします。

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

14.6.3 クラスとサブクラスの一致に関する問題

PXEクライアントは、クラス一致設定の問題により、IPアドレスを受信できても正しいブートファイルを取得できないことがあります。

手順 62: ISC DHCPクラスの一致に関するトラブルシューティング

1. クラス定義を確認します。

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

2. サブクラスのエントリを確認します。

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

3. ベンダのクラス識別を監視します。

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

4. ブートファイルのアクセシビリティをテストします。

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

5. 詳細ログを有効にします。

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

```
> sudosystemctl restart dhcpd
```

14.6.4 DHCPv6ベンダクラスオプションの問題

IPv6 DHCPクライアントには複雑なベンダクラスオプションの処理があり、適切なPXEブートサポートのために特別な設定が必要になる場合があります。

手順 63: ISC DHCPV6の問題の解決

1. DHCPv6オプション定義を確認します。

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

2. ベンダクラスの文字列解析を確認します。

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

3. DHCPv6ベンダクラスの一致を監視します。

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

4. IPv6 bootfile-url形式を確認します。

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

5. ルータ広告の依存関係を確認します。

```
> systemctl status radvd
```

6. IPv6接続をテストします。

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

14.7 次のステップ

ISC DHCPサービスを設定すると、PXEクライアントは、従来のクラスとサブクラスシステムを使用して、ネットワーク設定とブートファイル情報を受信できます。ISC DHCPはサポート終了となりましたが、この設定は、複数のクライアントアーキテクチャにわたってPXEおよびHTTPブート機能を必要とする既存の展開環境との互換性を提供します。

15 PXEサーバのセットアップの検証

このセクションでは、SUSE Linux Enterprise Server 16.0ネットワークインストールで、すべてのコンポーネントが正しく動作していることを確認するために、PXEサーバセットアップ全体を検証し、テストする方法を説明します。サービス検証、ネットワーク接続性テスト、エンドツーエンドのPXEブート検証をカバーしています。

15.1 概要

TFTP、HTTP、DNS、DHCP、GRUB 2ブートローダサービスなど、すべてのPXEサーバコンポーネントを設定した後、システム全体が正しく機能することを検証することが重要です。この検証により、PXEクライアントがAgamaインストーラで正常に起動し、 SUSE Linux Enterprise Server 16.0のネットワークベースのインストールを実行できることが保証されます。

15.2 要件

- すべてのPXEサーバコンポーネントが設定され、実行されていること
- PXEブート可能なテストクライアントシステム
- PXEサーバとクライアント間のネットワーク接続
- サーバサービスを監視するための管理アクセス権

15.3 PXEサーバサービスの検証

PXEクライアントでテストする前に、すべての必須PXEサーバサービスが実行され、適切に設定されていることを確認します。

手順 64: PXEサーバのサービス状態の確認

1. TFTPサービスの状態を確認します。

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

   予想される結果:サービスはアクティブで、ポート69でリスンしている必要があります。

2. nginx HTTPサービスを確認します。

   ```
   > systemctl status nginx
   ```

   予想される結果:サービスはアクティブで、ポート80でリスンしている必要があります。

3. DNSサービスを確認します(dnsmasqを使用している場合)。

   ```
   > systemctl status dnsmasq
   ```

   予想される結果:サービスはアクティブで、ポート53でリスンしている必要があります。

4. DHCPサービスの状態を確認します(適切なサービスを選択してください)。

   ```
   > systemctl status dhcpd
   ```

   dnsmasq DHCPの場合:

   ```
   > systemctl status dnsmasq
   ```

   Kea DHCPの場合:

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

   予想される結果:DHCPサービスはアクティブで、適切なポートでリスンしている必要があります。

5. IPv6ルータ広告を確認します(設定されている場合)。

   ```
   > systemctl status radvd
   ```

   予想される結果:IPv6環境でサービスがアクティブである必要があります。

6. NTPサービスを確認します。

```
> systemctl status chronyd
```

予想される結果:サービスはアクティブで、同期されている必要があります。

15.4 ネットワーク接続およびファイルアクセスのテスト

PXEクライアントが、TFTPとHTTPの両方のプロトコルを使用して、ネットワーク経由でブートファイルとインストールコンテンツにアクセスできることを検証します。

手順 65: ネットワークファイルアクセスのテスト

1. ブートローダファイルへのTFTPアクセスをテストします。

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

   ファイルが取得されたことを確認します。

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

   テストファイルをクリーンアップします。

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

2. GRUB 2設定へのHTTPアクセスをテストします。

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

   予想される結果:HTTP 200 OK応答。

3. インストーラファイルへのHTTPアクセスを確認します。

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

   予想される結果:適切なコンテンツ長を持つHTTP 200 OK応答。

4. DNS解決をテストします(ローカルDNSが設定されている場合)。

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

   予想される結果:適切なAレコードとAAAAレコードの解決。

5. 自動インデックスの場所のディレクトリ参照を確認します。

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

   予想される結果:ブートファイルを表示するディレクトリー覧。

15.5 DHCP機能の検証

DHCPサーバの応答をテストし、さまざまなクライアントタイプに適したブート情報が提供されていることを確認します。

手順 66: DHCPサーバ応答のテスト

1. DHCPポートバインディングを確認します。

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

   予想される結果:DHCPサービスがポート67 (IPv4)および547 (IPv6)でリスンしています。

2. DHCP要求をリアルタイムで監視します。

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

   またはdnsmasqの場合:

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

   テスト中にDHCPアクティビティを監視するために、このコマンドを実行したままにしておきます。

3. dhcpingを使用してDHCP応答をテストします(利用可能な場合)。

   ```
   > dhcping -s 192.168.1.200
   ```

   予想される結果:サーバからのDHCP応答に成功します。

4. アクティブなDHCPリースを確認します。

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

   または、Keaの場合:

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

   予想される結果:テストクライアントのリースエントリ。

15.6 エンドツーエンドのPXEブートテスト

実際のクライアントシステムで完全なPXEブートテストを行い、DHCPからAgamaインストーラ起動までのブートプロセス全体を検証します。

手順 67: PXEブートプロセス全体のテスト

1. テストクライアントシステムを準備します。
    - BIOS/UEFIを設定してネットワークブートを有効にする
    - ネットワークブートを最初のブート優先度として設定する
    - クライアントをPXEサーバと同じネットワークに接続する
2. クライアントのブート中にPXEサーバのログを監視します。

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

3. テストクライアントを起動し、以下のシーケンスを確認します。
    1. クライアントはDHCP経由でIPアドレスを受信する
    2. クライアントはTFTP経由でブートローダをダウンロードする
    3. GRUB 2のメニューが表示され、インストールオプションが表示される
    4. カーネルとinitrdがHTTP経由でロードされる
    5. Agamaインストーラが正常に起動する
4. さまざまなクライアントタイプをテストして、クライアントアーキテクチャの検出を確認します。
    - レガシBIOS x86_64システム(core.0を取得する必要があります)
    - UEFI x86_64システム(bootx64.efiを取得する必要があります)
    - UEFI aarch64システム(bootaa64.efiを取得する必要があります)
5. IPv6 PXEブートをテストします(IPv6が設定されている場合)。
    - テストクライアントでIPv6のみのネットワーク設定を有効にする
    - DHCPv6アドレス割り当てを確認する
    - IPv6 bootfile-urlの配信を確認する

15.7 Agamaインストーラの機能の検証

Agamaインストーラが正しく起動し、 SUSE Linux Enterprise Server 16.0のインストールを完了するためにインストールソースにアクセスできることを確認します。

手順 68: AGAMAインストーラの起動テスト

1. Agama Webインタフェースのアクセシビリティを確認します。
   クライアントのブート中に、割り当てられたIPアドレスをメモして、アクセスします。

   ```
   http://CLIENT_IP_ADDRESS
   ```

   予想される結果:Agama Webインタフェースが正常にロードされるはずです。

2. クライアントのAgamaインストーラのログを確認します。
   コンソールに切り替え(Alt+F2)、次のコマンドを実行します。

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

   予想される結果:Agamaの起動時に致命的なエラーはありません。

3. インストールソースへのアクセシビリティを確認します。
   フルISOインストールの場合は、リポジトリへのアクセスを確認します。

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

   予想される結果:ディレクトリ一覧を含むHTTP 200 OK応答。

4. パッケージインストール機能をテストします。
   Agamaインタフェースで次のことを確認します。

   - システムが利用可能なディスクを検出できること
   - ネットワーク設定が保持されていること
   - パッケージリポジトリにアクセスできること
   - インストールを完了まで進められること

15.8 検証失敗のトラブルシューティング

PXEサーバの検証中によくある問題とその解決手順。

15.8.1 DHCP割り当ての失敗

PXEブート中にクライアントがIPアドレスを受信できません。

手順 69: DHCP検証問題の解決

1. DHCPサービスの競合を確認します。

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

2. ネットワークインタフェースが起動していることを確認します。

```
> ip addr show eno1
```

3. DHCP範囲の可用性を確認します。

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

4. DHCPログでエラーを監視します。

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

15.8.2 ブートファイルの配信失敗

クライアントはIPアドレスを受信するが、ブートファイルのダウンロードに失敗します。

手順 70: ブートファイルの問題の解決

1. TFTPサービスへのアクセシビリティを確認します。

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

2. ファイルアクセス権を確認します。

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

3. TFTPアクセスログを監視します。

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

4. クライアントアーキテクチャの検出を確認します。

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

15.8.3 Agamaインストーラの起動失敗

ブートファイルは正常にロードされますが、Agamaインストーラが起動に失敗します。

手順 71: AGAMAの起動に関する問題の解決

1. インストーラファイルへのHTTPアクセスを確認します。

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

2. GRUB 2設定のカーネルパラメータ構文を確認します。

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

3. クライアントのブートプロセスを監視します。

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

4. ネットワーク設定の永続性を確認します。

```
# ip addr show
```

15.9 PXEサーバ検証チェックリスト

このチェックリストを使用して、PXEサーバ設定のあらゆる側面を体系的に検証してください。

表 2: PXEサーバ検証チェックリスト

コンポーネント	検証手順	Status
TFTP Service	サービスがアクティブ、ポート69がリスン中、ファイルにアクセス可能	☐
HTTPサービス	nginxがアクティブ、ポート80がリスン中、インストーラファイルにアクセス可能	☐
DNSサービス	ホスト名解決が機能している、ポート53がリスン中	☐
DHCPサービス	IP割り当てが機能している、ブートオプションが配信されている	☐
GRUB 2設定	メニューがロードされている、アーキテクチャ検出が機能している	☐
IPv6のサポート	ルータ広告がアクティブ、DHCPv6が機能している	☐
PXEブート	クライアントが正常に起動し、正しいブートローダを受信	☐

コンポーネント	検証手順	Status
Agamaインストーラ	インストーラが起動、Webインタフェースにアクセスできる	☐
インストールソース	リポジトリにアクセスできる、パッケージがインストール可能	☐
ネットワークの永続性	インストール時にネットワーク設定が維持される	☐

15.10 検証の結論

適切に検証されたPXEサーバは、クライアントのネットワークブートからAgamaインストーラの起動まで、エンドツーエンドで正常に機能することを実証する必要があります。すべてのサービスがエラーなく動作し、クライアントがネットワーク経由でSUSE Linux Enterprise Server 16.0のインストールを完了できる必要があります。定期的な検証テストにより、自動展開用のPXEインフラストラクチャの継続的な信頼性が確保されます。

16 法的事項

Copyright© 2006–2026 SUSE LLC and contributors. All rights reserved.

この文書は、GNU Free Documentation Licenseのバージョン1.2または(オプションとして)バージョン1.3の条項に従って、複製、頒布、および/または改変が許可されています。ただし、この著作権表示およびライセンスは変更せずに記載すること。ライセンスバージョン1.2のコピーは、「GNU Free Documentation License」セクションに含まれています。

SUSEの商標については、https://www.suse.com/company/legal/を参照してください。その他の第三者のすべての商標は、各社の所有に帰属します。商標記号(®、™など)は、SUSEおよび関連会社の商標を示します。アスタリスク(*)は、第三者の商標を示します。

本書のすべての情報は、細心の注意を払って編集されています。しかし、このことは正確性を完全に保証するものではありません。SUSE LLC、その関係者、著者、翻訳者のいずれも誤りまたはその結果に対して一切責任を負いかねます。

A GNU Free Documentation License

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

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. 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.